Migration Letters

Volume: 21, No: 4, pp. 455-465

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)
www.migrationletters.com

The Role of Human Intelligence (Humint) in Deterring Cyber-Attacks and Digital Disruption

Editha Praditya[1], Syamsul Maarif[2], Yusuf Ali[3], Herlina Juni Risma Saragih[4], Rui Duarte[5]

Abstract

In the era of globalization and digitalization, cyber-attacks and digital disruption are becoming serious threats to information security. This research uses a qualitative approach to analyze cyberattacks, attack types, and their impact, focusing on the role of Human Intelligence (HUMINT) in addressing these threats. Cyberattacks, including malware, phishing, and DDoS, have devastating financial, reputational, and operational impacts. By engaging HUMINT, this research explored HUMINT's key role in understanding attacker motivation, social and psychological analysis, digital foot printing, and detailed information development. Collaboration between HUMINT and technical security teams is also emphasized to improve responsiveness to cyber threats. The results of this research provide a theoretical and practical foundation for the development of a holistic security strategy, emphasizing the important role of HUMINT in dealing with the evolving dynamics of cyberattacks.

Keywords: *Cyber Attack, Digital Disruption, Human Intelligence (HUMINT).*

Introduction

In the rapidly growing era of globalization and digitalization, information technology has become the backbone for various sectors of life, including business, government, and social interaction. While these advancements bring significant benefits, behind the sophistication are increasingly complex and serious threats to information security. Cyberattacks and digital disruptions have become major challenges that require deep understanding and effective responses.

In recent years, cyber-attacks have taken center stage in many walks of life. Organizations, both large and small, and individuals have all become potential targets for skilled and organized attackers. Cyberattacks not only include data hacking, but also involve the spread of malware, phishing, ransomware, and DDoS attacks that can undermine system integrity and harm operational sustainability.

The sustainability and success of businesses, as well as government functions, are increasingly dependent on information technology infrastructure. Therefore, a deep understanding of these threats and the implementation of effective security strategies is a necessity. This background highlights the importance of research to explore the impact of cyberattacks and digital disruptions and formulate a comprehensive approach to deal with them.

[1] Postgraduate Program of Republic of Indonesia Defense University
[2] Postgraduate Program of Republic of Indonesia Defense University
[3] Postgraduate Program of Republic of Indonesia Defense University
[4] Postgraduate Program of Republic of Indonesia Defense University
[5] Postgraduate Program of Republic of Indonesia Defense University

State administration in the digitalization era relies on good and secure information management, making intensive management and security in the cyber sector a critical aspect in supporting its achievement. Various government initiatives to adopt the use of information technology are increasingly widespread and evenly distributed in various fields, requiring readiness and careful preparation from various stakeholders. The issuance of the Presidential Regulation related to the establishment of the State Cyber and Crypto Agency (BSSN) has emphasized the urgency of structuring Cyber Security Human Resources to maintain the security of cyberspace for the management of national security conducive to economic growth. The Presidential Regulation also emphasizes that cyberspace is an integral part of the territory of the Unitary State of the Republic of Indonesia (NKRI) which is inseparable from other areas, namely land, sea and air.

In addition, Kominfo (2022) explains that the digitasl literacy index is divided into several community segments. First, the education segment consists of educators (lecturers and teachers), students and students. Second, the Government / Indonesian Army / Police segment consists of non-educator Civil Servant workers, Indonesian Army, and Police. Third, the general public segment consists of community groups outside the education sector and the Government/Indonesian Army/Police. The survey results show that the Government/Indonesian Army/Police segment has a high index score of 3.74. Meanwhile, workers and students in the education segment have an index score of 3.70 and the general public segment has an index score of 3.5. The use of computers and laptops has not yet become part of the work of most respondents. Those who work and use a computer/laptop are only 26.67%. As many as 73.33% of them do not use these devices.

As for those who use laptops for work, less than 30% of the respondents were dissatisfied and very dissatisfied. It can be seen from the data below that almost half of the responses were satisfied and very satisfied. The highest satisfaction score in general was the ease of using the computer/laptop at work/school. While the lowest value is in the indicator of the amount of training to master the computer/laptop which is felt to be lacking. The use of the internet in education sector workers is mostly on extracting information through the internet, which is 36.5%. Other activities such as online learning and teaching processes and multimedia learning amounted to 27.6% and 17.1% respectively. Meanwhile, the use of virtual laboratories is still very low at 3.5%. However, the great satisfaction of workers using digital tools can still be perceived as a hindering factor. More than half of the respondents considered lack of budget (21.9%), lack of training (17.6%), and lack of supporting resources (16.3%) to be the dominant factors in hindering work using digital tools (Kominfo, 2022). Based on this explanation, it can be understood that the ability of human resources in operating the internet and its supporting devices in certain segments is still lacking, especially when faced with cyber-attacks that can cause huge losses in certain sectors.

The low level of digital literacy contributes to the impact of cyberattacks, which is not only limited to financial losses, but also includes loss of customer trust, loss of reputation, and potential disruption to public services. Therefore, understanding the dynamics of these attacks needs to continue to evolve, in line with the evolution of technology and attack methods used by irresponsible parties.

In this context, this research will contribute to further understanding of the impact of cyberattacks and digital disruption in an increasingly connected and technology-dependent environment. Additionally, it will explore the key role that HUMINT can play in responding to and addressing these threats. By delving into this background, it is hoped that this research can provide a theoretical and practical foundation for relevant parties, such as enterprises, government agencies, and security professionals, to develop effective strategies to protect their information assets and maintain operational stability in this digital age.

Research Method

This research utilizes a qualitative research methodology approach with a focus on analyzing writings that have been published in national and international journals. The characteristics of this research are descriptive in order to describe the meaning and substance of the role of HUMINT in deterring cyber-attacks and digital disruption. This research is conceptual in nature by explaining the strategic role of HUMINT in addressing the issue of cyber-attacks and digital disruption. The scope of the study involves an understanding of the role of HUMINT in overcoming cyber-attacks, meaning, forms of cyber-attacks and digital disruption. Hopefully, this research can interpret and implement the role of HUMINT in counteracting cyber-attacks on various aspects of the existing digital space.

Result and Discussion

Cyber-Attack and Digital Disruption

A cyberattack is a series of actions aimed at damaging, illegally accessing or stealing information from a computer system or network. These attacks can be carried out by individuals, groups, or even countries intending to achieve a variety of goals, including data theft, sabotage, or reconnaissance.

Cyberattacks are a form of offensive maneuver used by states, individuals, groups, or organizations to target computer information systems, infrastructure, computer networks, or personal computer devices through various malicious actions. Generally originating from anonymous sources, these attacks involve attempts to steal, alter, or destroy predetermined targets by hacking into vulnerable systems (Lin, 2016). These attacks can be classified as cyber campaigns, cyber warfare, or cyber terrorism depending on the context. Cyberattacks range widely, from the installation of surveillance devices on personal computers to attempts to destroy a country's entire infrastructure. The continued development of cyberattacks is reflected in their level of sophistication and danger, as seen in the recent Stuxnet worm (Karnouskos, 2011). To prevent such attacks, the analysis of user behavior and the use of Security Information Management Systems are critical. Digital intrusions can include a wide range of issues, such as hacking attacks, malware, signal interference, hardware or software failures, as well as many other types of digital security incidents. These can lead to data loss, information leakage, or even the unsustainable operation of a system.

Digital disruption refers to the transformative impact of digital technologies on various sectors and domains, including manufacturing, services, and education. This phenomenon involves the simultaneous emergence and coexistence of digital technological developments, the spread of digital devices and channels, and changes in customer behavior and expectations (Shrivastava, 2017). Digital disruption brings the potential to open up opportunities and present challenges. It can provide opportunities for organizations to deliver customized and seamless customer experiences, improve communication and project management, and enhance online education delivery (Thomas, 2018).

In addition, digital disruption can also refer to problems or disorders in the use of digital technologies or social media that can affect mental health, such as social media addiction or cyberbullying. In general, the definition of digital disruption can vary depending on the context, and can refer to different types of problems or disorders associated with the digital world.

Types of Cyber Attacks.

Malicious Software (Malware). Malware is software that is created with the purpose of damaging, corrupting, or stealing data from systems without authorization. They can

cause great harm by damaging system integrity or locking access to data. The emergence of malicious software has resulted in the birth of the discipline of malware analysis, which operates in a risky environment where attackers are constantly evolving their methods (Pierazzi & Srndic 2022). Some common types of malwares include Viruses, Worms, Trojans and Ransomware.

Phishing. Phishing is the fraudulent practice of attempting to collect sensitive information by posing as a trustworthy entity in electronic communications (Aphiya, et all, 2022). Phishing involves attempting to obtain sensitive information, such as passwords or financial details, by posing as a trusted entity through electronic communication. Phishing attacks often occur through fake emails, text messages, or websites designed to deceive users. Some forms of phishing include Email Phishing and Spear Phishing.

Ransomware. Ransomware, as explained earlier, is a type of malware that encrypts data on a system and demands a ransom to restore access to the data owner. Ransomware is a type of malicious software created with the aim of facilitating various malicious activities, such as blocking access to personal data unless a ransom payment is made (Khammas, 2020; Meland et al., 2020). These ransom payments are generally made using cryptocurrencies such as Bitcoin, making them difficult to trace in transactions and an ideal option for attackers to evade law enforcement (Kara and Aydos, 2020; Karapapas et al., 2020). These attacks can cause significant financial losses and put moral pressure on victims to pay to keep their data from being lost or disclosed.

Distributed Denial of Service (DDoS) attack. DDoS attacks aim to make a service or resource unavailable by flooding a system or network with massive amounts of traffic. DDoS attacks, which are distributed attacks, make them difficult to counter or track. Generally, perpetrators use manipulated IP addresses to disguise their true identity (Nisa & Ramadona, 2023). As a result, systems become unresponsive or disrupted, affecting service availability and harming the operations of organizations or individuals.

Social Engineering. This is an attack that uses humans as the main object of attack targets. This attack can be carried out by communicating with the target directly or indirectly. In general, the purpose of this attack is to obtain certain information from the target of the attack. However, it can also be used to influence the victim to carry out orders from the attacker. Social engineering actually focuses on human psychological manipulation with various media that aim to influence the victim's mind (Nurhidayat, T., 2022). Thus, in this case, of course, increasing the capacity of human resources in preventing various kinds of cyber-attacks is very crucial in order to avoid cyber-attacks that harm individuals, companies and the Government.

Impact of Cyber Attacks.

Cyberattacks can have a variety of detrimental impacts on individuals, companies, governments, and the general public. Cybersecurity attacks can have detrimental effects such as reputational damage, financial loss, and the risk of lawsuits that can involve claims of breach of contract or non-compliance with privacy policies or laws (McCarthy, 2023). Some of the impacts of cyberattacks include:

Financial Loss. Financial loss is a serious concern in many areas, including in the realm of cybercrime. There has been a significant increase in the frequency of attacks and expenditures related to cybercrime globally (Sharif & Mohammed, 2022). Cyberattacks can cause significant financial losses to organizations and individuals. Attackers often target financial information, such as credit card data or banking information, which can be used for theft of funds, and the cost of recovery after an attack, including the cost of securing and updating systems, can be a heavy financial burden.

Reputation. Cyberattacks often cause an organization or individual's reputation to suffer. Data security that is too easily breached can undermine the trust of customers and

business partners. Reputational damage can arise as a result of cyberattacks, affecting both public and private institutions. Cybersecurity breaches may result in significant reputational damage, causing a loss of trust on the part of customers and stakeholders (Litt et al., 2023). Organizations affected by cyberattacks need to respond with a strategic approach to manage and restore their affected image (Parera et al., 2022). Leaked information or data manipulation can also be detrimental to public image, causing a decrease in trust in the party affected by the attack.

Operational Disruption. The risks arising from cyberattacks involve operational and financial risks, as mentioned by Tosun (2021). Cyberattacks can cause serious operational disruptions. Infected or crippled computer systems due to DDoS attacks can halt normal business activities. Disrupted operational continuity can lead to decreased productivity, project delays, and even loss of customers or business opportunities.

Risk of Sensitive Data Loss. Intrusions into computer systems can result in the loss or theft of sensitive data. Valuable personal information, business secrets, or intellectual data can fall into the wrong hands, resulting in the risk of losing competitive advantage or serious privacy breaches. Organizations that store valuable data are prime targets for cybercrime. Various techniques, such as email phishing, man-in-the-middle attacks, and the use of malware, are used to gain access to sensitive information (Bhattacharjee et al., 2021).

Definition of Human Intelligence (HUMINT).

HUMINT is a branch of intelligence that focuses on gathering information from human sources through direct interaction. This includes contact with informants, field agents, and other human sources. HUMINT expertise involves strong interpersonal skills, cultural sensitivity, and the ability to build relationships with various types of individuals, besides that HUMINT also needs to have the competence and expertise to carry out a series of risk management processes to identify, analyze and evaluate cybersecurity as a form of mitigation, including the adequacy of information security strategies, implementation of information security management, continuity and recovery management, and organizational achievements for the use of information technology.

In this digital era, HUMINT should be seen as an asset (Human Capital) rather than just a resource (Human Resource) so that it is necessary to build a conducive, directed, sustainable and measurable HUMINT human resource development ecosystem. HUMINT needs to understand the field of information security that uses the approach and analysis of the handling phase of cyber security incidents that include the phase before the cyber attack incident (Before Cyber Attack), the phase when the cyber attack incident (During Cyber Attack) and the phase after the cyber attack incident (After Cyber Attack).

The Role of Human Intelligence in Cyber Attack Deterrence.

Gunawan, B., Ratmono, B, & Abdullah, A. (2023) explains that the key competencies required for professionals in the field of cybersecurity and strategic management cover a wide range of skills and knowledge areas. Based on the information provided in the document, the following key competencies are essential for professionals in this field:

a. Technical Expertise: Proficiency in cybersecurity tools, technologies and best practices is essential to effectively identify, prevent and respond to cyber threats

b. Risk Management: Understand risk assessment methodologies, develop risk management strategies, and implement security controls to mitigate cybersecurity risks

c. Strategic Thinking: Ability to align cybersecurity initiatives with organizational goals and strategic objectives, integrating security into the overall business strategy

d. Regulatory Compliance: Knowledge of cybersecurity regulations, standards, and compliance requirements relevant to the organization's industry and geographic location

e. Incident Response: Proficiency in developing and implementing incident response plans to effectively address and mitigate the impact of cybersecurity incidents

f. Awareness and Training: Ability to develop and deliver cybersecurity awareness programs to educate employees and stakeholders on security best practices and threats

g. Communication Skills: Effective communication and collaboration with cross-functional teams, management, and external stakeholders to convey cybersecurity risks and strategies.

h. Economics and Management: Understanding the economic impact of cybersecurity, including cost-benefit analysis, market mechanisms, and strategic behaviors associated with cybersecurity investments.

i. Situational Awareness: The ability to gain deep insight into the current state of cybersecurity through Cyber Situational Awareness (CSA) and make informed decisions based on evolving cyber threats

j. Artificial Intelligence Decision Making: Familiarity in using artificial intelligence for decision-making in cybersecurity information processing

These competencies reflect the multidisciplinary nature of cybersecurity and strategic management, encompassing technical, strategic, regulatory, and communication skills critical to addressing the complex challenges of cybersecurity in today's organizations. HUMINT has a vital role in identifying and countering cyber-attacks and can provide several constructive contributions in the field of cyber security which include several things such as:

1. Understanding Motivation and Identifying Attackers.

HUMINT is required to have the ability to deeply understand the motivations behind cyber-attacks and have deep insight into what drives attackers to launch attacks so that they can respond to cyber threats more effectively. HUMINT can analyze and detail factors such as political, financial or ideological goals. which may have been the main impetus for the attack. It can be understood that every organization is the target of cyber-attacks, where every year this occurs, it shows that cyber-attacks are carried out against small organizations and large organizations and cover any sector, especially organizations that manage national critical infrastructure which is the backbone for the establishment of a country. This deep understanding allows HUMINT to recognize potential targets and develop more targeted strategies. For example, understanding political motivations can help in designing specific defenses against attacks that may originate from particular groups or countries. By leveraging a network of informants or field agents, HUMINT can play a key role in identifying cyber attackers. Human sources can provide detailed information about the attacker's identity, characteristics, and methods. This includes information such as digital footprints, previous attack patterns, and even possible affiliations with certain groups.

Attacker identification by HUMINT can provide valuable insights to security teams, allowing them to anticipate future attacks and provide faster, more targeted responses. This information can also help authorities initiate legal and diplomatic steps to deal with cyber-attacks. HUMINT's expertise in understanding attacker motivation and identification underscores the importance of integration with other intelligence, such as Signals Intelligence (SIGINT) and Technical Intelligence (TECHINT). Integration of data from multiple intelligence sources allows forming a completer and more accurate picture of cyber threats. Thus, HUMINT not only provides physical identification of the attacker, but also helps depict the broader context of the attack. This understanding opens up opportunities to develop holistic and effective response strategies in dealing with cyber-attacks.

2. Social and Psychological Analysis.

This section highlights the importance of HUMINT in conducting social and psychological analysis to address cyberattacks. Some relevant aspects such as:

a. Understanding the Psychological Characteristics of Attackers. Social and psychological analysis helps in understanding the psychological characteristics of cyber attackers. This includes motivations, dissatisfaction, or other factors that might prompt a person or group to launch an attack. By gaining these insights, HUMINT can analyze and detail these factors and identify behavioral patterns that can be used for attacker profiling.

b. Social Dynamics of Attackers. Understanding the social dynamics of the attack group was also a focus of the analysis. This includes interpersonal relationships, organizational structures, and ways of communication between them. By detailing these elements, HUMINT can formulate and construct a more complete picture of how a group or individual operates, enabling a better response. HUMINT enables active monitoring of groups or individuals involved in suspicious cyber activities. This can help authorities in taking preventive action or quick response to ongoing attacks.

c. Psychological Profile of Attackers. HUMINT can help in developing a psychological profile of cyberattack perpetrators. This analysis involves evaluating personality characteristics, motivations, and possible future behavior. These profiles can be used to predict possible attacks and provide a basis for identifying potential new attackers.

d. Anticipate Attacker's Psychological Changes. When a cyber attack occurs, HUMINT can collect evidence to support the investigation. This involves a deep understanding of attack methods, resources used by attackers, and digital footprints that can assist in law enforcement or security response. HUMINT conducted a more in-depth analysis of the motivation and objectives behind cyber attacks. This information can provide valuable insights for designing effective cybersecurity policies and better understanding the sources of threats. Through change analysis, HUMINT can help in detecting psychological changes in attackers. For example, a shift in motivation or a change in strategy can be revealed through a deeper understanding of psychological factors. This allows organizations to proactively adjust their security strategy.

e. Understanding the Digital and Social Lives of Attackers. HUMINT can also include an understanding of the attacker's digital and social life, every electronic system managed by every organization has vulnerabilities. This is caused by various factors that often occur, such as weaknesses in the software development phase (SDLC/Software Development Life Cycle) and ignorance and lack of awareness (Lack of Awareness) on the part of the programmer. What is even more important is that there are various vulnerabilities in the internet protocol itself for which no solution has yet been found. This includes online footprints, social media interactions, and connections in cyberspace. This analysis helps in establishing a comprehensive understanding of an attacker's digital identity, enabling organizations to follow developments and mitigate potential risks.

3. Digital Trace Tracking and Identifying Information Sources.

Tracking digital footprints and identifying information sources is a key aspect of HUMINT in dealing with cyber-attacks. In this context, HUMINT provides the ability to understand and analyze digital traces left by attackers. This process involves several detailed steps and focuses on gathering human information that can provide insight into the attacker's identity and goals. HUMINT works closely with cybersecurity specialists to combine understanding of online communities, attack methods and digital behavior. By gathering information directly from human sources involved in or knowledgeable about the attack group, HUMINT analysts can track and identify digital footprints that may be difficult to access through technical methods alone. HUMINT analysis also involves a deep understanding of the attack tactics and techniques used, which can assist in

identifying unique patterns associated with specific groups or individuals. By combining this information, security teams can detail and verify information sources that may be involved in a cyberattack.

The integration of digital tracking and human-sourced information allows organizations to take more targeted and effective steps in responding to cyber-attacks. In addition, this approach also provides broader strategic insight to mitigate risks and improve overall cyber defense.

4. Development of Detailed Information.

Development of Detailed Information through HUMINT expertise is a crucial element in fighting cyber-attacks. This process involves compiling in-depth and contextual information to provide a better understanding of the threat. Following are some key aspects of HUMINT's role in the development of detailed information.

HUMINT analysis involves an in-depth investigation of information gathered from human sources. HUMINT agents work in detail to understand the background, motivation and methods of cyberattack perpetrators. This includes interviews, observations, and behavioral analysis to detail information that may not be detected through technical approaches alone. HUMINT helps develop specific context around a cyberattack, providing additional information that may not be discoverable through technical data alone. For example, social, political, or economic factors that might motivate an attacker can be revealed through HUMINT skill analysis.

The development of detailed information through HUMINT allows organizations to gain a deep understanding of the identity, relationships, and history of the perpetrators of attacks. This can help in compiling a more complete profile, allowing organizations to anticipate the next move or identify threats that may emerge in the future, the digital transformation in the world of cyber crime thereby encouraging the industrialization of cyber attacks. This causes cyber attacks to increase in quality (sophisticated) and also become more complex. This phenomenon has caused the use of cyber attacks to become increasingly common, both by state actors and non-state actors. The process of acquiring cyber weapons is relatively easier and cheaper than conventional weapons. The use of cyber attacks also poses relatively minimal risks compared to carrying out physical attacks from the perspective of criminals.

Apart from that, Gunawan, B., Ratmono, B.M., & Setyoko, P.I. (2023) added that digital transformation has had a significant impact on public management functions in terms of information disclosure. The integration of technology into the public information ecosystem is very important to increase accessibility, transparency and efficiency in providing public information. This transformation enables easier and faster access to public information, so that citizens can be actively involved in decision-making processes and strengthen government accountability. In addition, digital tools and systems, such as online public information portals and integrated databases, have simplified and accelerated information disclosure, encouraging transparency and public participation. Information developed by HUMINT provides strategic insights to stakeholders. This not only helps in immediate response to ongoing cyberattacks, but also supports long-term planning for overall cybersecurity improvements. The development of detailed information through HUMINT provides a strong basis for effective decision making. A deeper understanding of threats and attackers allows organizations to design and execute more targeted security strategies.

5. Collaboration with the Technical Security Team.

Information obtained through HUMINT can be used to form more adaptive and responsive cybersecurity policies. Such policies can be more effective in dealing with growing threats in the cyber world. One key aspect of HUMINT's role in addressing cyber attacks is its collaboration with technical security teams. Integration of information

obtained through HUMINT with technical expertise can increase effectiveness and responsibility in fighting cyber threats. Some elements that highlight the importance of this collaboration are Collaboration between HUMINT and technical security teams enables real-time information exchange. Information obtained from human sources can be directly integrated with technical data obtained from computer security systems. This allows organizations to gain a more complete and rapid understanding of ongoing attacks or potential threats. Through collaboration, HUMINT analysts and technical security experts can combine their expertise to perform more in-depth analysis. Technical data can be given further context by human information, and vice versa. The result is a richer and more holistic understanding of cyber threats, allowing for the identification of attack methods, motivations and attacker goals. By combining human and technical information, security teams can make more accurate risk assessments. HUMINT can provide insight into the intent and sustainability of an attack, while technical teams can measure the effectiveness of security controls and identify potential vulnerabilities. This combination makes it possible to develop a more focused response strategy. Collaboration between HUMINT and technical security teams can enhance an organization's overall intelligence capabilities. Integration of data from multiple sources can create a more dynamic and responsive intelligence environment, enabling organizations to adapt quickly to changes in cyber threats.

Good collaboration between HUMINT and technical teams creates continuous monitoring capabilities of the cyber environment. By complementing each other, both teams can respond quickly to changes in attacker tactics and can identify potential threats before they escalate into more serious attacks and combining the power of HUMINT with the National Occupation strategy in the Cyber Security Function Area, a country can be more effective in protecting its interest’s nation from complex and ever-evolving cyber threats.

6. Increased Cybersecurity Security Awareness. In order to improve human resource capabilities, in this case for example to secure Electronic-Based Government Systems. This also includes developing HR competencies in application management and implementing an information security culture in the work environment and the organization as a whole.

Conclusion

The conclusions of this journal highlight the importance of a deep understanding of cyber-attacks and digital disruption in an era of growing globalization and digitalization. Cyber-attacks not only include data hacking, but also involve various forms of threats such as malware, phishing, ransomware and DDoS attacks. The impact of a cyber-attack includes financial loss, loss of customer trust, reputational harm, and potential disruption to public services. Understanding the type of attack, the attacker's motivation, and identification of information sources are critical in responding to this threat. Amid the complexity of cyber-attacks, this journal highlights the key role of HUMINT in overcoming these attacks. HUMINT's expertise in understanding attacker motivation and identification, social and psychological analysis, digital footprint tracking, detailed information development, and collaboration with technical security teams provides a strategic foundation for dealing with cyber threats holistically. Overall, this journal provides a theoretical and practical foundation for companies, government agencies, and security professionals to develop effective strategies for protecting information assets and maintaining operational stability in the digital era.

The use of technology for efficient public information disclosure has several benefits for society, including ease of access and transparency of public information which allows the public to monitor and evaluate government actions more effectively, increase accountability, and reduce the risk of corruption. In addition, technology enables faster and more precise disclosure of public information, speeding up the decision-making

process and creating more efficient public services. In addition, technology facilitates broader and more organized public participation, so that citizens can provide their input and opinions about public policies and government programs.

References

Alphiya, Yunoose., Aby, Rose, Varghese., Anagha, R., Abhirami, Prakash., Devika, Babu. (2022). Phishing. International journal of engineering technology and management sciences, doi: 10.46647/ijetms.2022.v06i05.092

Babys, S. A. M. (2021). ANCAMAN PERANG SIBER DI ERA DIGITAL DAN SOLUSI KEAMANAN NASIONAL INDONESIA Latar Belakang Era digital adalah satu kondisi dimana kehidupan manusia dilaksanakan dengan teknologi digital . sebagai perkemb. JURNAL ORATIO DIRECTA, 3(1), 425–442.

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. Computers and Security, 111. https://doi.org/10.1016/j.cose.2021.102490

Bhattacharjee, A., Badsha, S., Hossain, M. T., Konstantinou, C., & Liang, X. (2021). Vulnerability Characterization and Privacy Quantification for Cyber-Physical Systems. In Proceedings - IEEE Congress on Cybermatics: 2021 IEEE International Conferences on Internet of Things, iThings 2021, IEEE Green Computing and Communications, GreenCom 2021, IEEE Cyber, Physical and Social Computing, CPSCom 2021 and IEEE Smart Data, SmartData 2021 (pp. 217–223). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics53846.2021.00045

BSSN. (2023). Keamanan Siber dalam Sistem Pemerintah Berbasis Elektronik (SPBE). Dipaparkan pada Rapat Kerja Nasional Kejaksaan Republik Indonesia Tahun 2024, 9 Januari 2023.

Dermawan, I., Baidawi, A., Iksan, & Mellyana Dewi, S. (2023). Serangan Cyber dan Kesiapan Keamanan Cyber Terhadap Bank Indonesia. Jurnal Informasi Dan Teknologi, 5(3), 20–25. https://doi.org/10.60083/jidt.v5i3.364

Gunawan, B., Ratmono, B, & Abdullah, A. (2023). Cybersecurity and Strategic Management. Foresight and Sti Governance, 17 (3). Pp. 90-99.

Gunawan, B., Ratmono, B.M., & Setyoko, P.I. (2023). Digital Transformation in Public Management Functions for Public Information Disclosure. Journal of Governance, 8 (3). Pp. 348-366.

Herdiana, Y., Munawar, Z., & Indah Putri, N. (2021). Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19. Jurnal ICT : Information Communication & Technology, 20(1), 42–52. https://doi.org/10.36054/jict-ikmi.v20i1.305

Hinsa Siburian. “Peta Okupasi Nasional dalam Kerangka Kualifikasi Nasional Indonesia pada Area Fungsi Keamanan Siber,” 2019.

Indah, F., & Sidabutar, A. Q. (2022). Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka). Jurnal Bidang Penelitian Informatika, 1(1), 2. Retrieved from https://ejournal.kreatifcemerlang.id/index.php/jbpi/article/view/78%0Ahttps://ejournal.kreatifcemerlang.id/index.php/jbpi/article/download/78/8

Kara, I., & Aydos, M. (2020). Cyber Fraud: Detection and Analysis of the Crypto-Ransomware. In 2020 11th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2020 (pp. 0764–0769). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/UEMCON51285.2020.9298128

Karapapas, C., Pittaras, I., Fotiou, N., & Polyzos, G. C. (2020). Ransomware as a Service using Smart Contracts and IPFS. In IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2020. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICBC48266.2020.9169451

Karnouskos, S. (2011). Stuxnet worm impact on industrial cyber-physical system security. In IECON Proceedings (Industrial Electronics Conference) (pp. 4490–4494). https://doi.org/10.1109/IECON.2011.6120048

Khammas, B. M. (2020). Ransomware Detection using Random Forest Technique. ICT Express, 6(4), 325–331. https://doi.org/10.1016/j.icte.2020.11.001

Kominfo. (2022). Status Literasi Digital di Indonesia 2022. Jakarta: Kominfo.

Lin, T. C. W. (2016). Financial weapons of war. Minnesota Law Review, Vol. 100, p. 1377. https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2765010_code1573690.pdf?abstractid=2765010&mirid=1&type=2

Litt, B., Tanyi, P., & Watson, M. W. (2023). Cybersecurity Breach at a Big 4 Accounting Firm: Effects on Auditor Reputation. Journal of Information Systems, 37(2), 77–100. https://doi.org/10.2308/ISYS-2022-006

McCarthy, C. (2023). Protect Personal, Institutional Data from Cyberattacks. Women in Higher Education, 32(8), 9–15. https://doi.org/10.1002/whe.21308

Md Haris Uddin Sharif, & Mehmood Ali Mohammed. (2022). A literature review of financial losses statistics for cyber security and future trend. World Journal of Advanced Research and Reviews, 15(1), 138–156. https://doi.org/10.30574/wjarr.2022.15.1.0573

Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. (2020). The Ransomware-as-a-Service economy within the darknet. Computers and Security, 92. https://doi.org/10.1016/j.cose.2020.101762

Nisa, F., & Ramadona, S. (2023). Sistem Pencegahan Serangan Distributed Denial Of Service Pada Jaringan SDN. Jurnal Sistim Informasi dan Teknologi, 22-30.

Nurhidayat, T., et.al. (2022). Lanskap Keamanan Siber Indonesia. Jakarta: BSSN.

Parulian, S., Pratiwi, D. A., & Cahya Yustina, M. (2021). Ancaman dan Solusi Serangan Siber di Indonesia. Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT), 1(2), 85–92. Retrieved from http://ejournal.upi.edu/index.php/TELNECT/

Perera, S., Jin, X., Maurushat, A., & Opoku, D. G. J. (2022). Factors Affecting Reputational Damage to Organisations Due to Cyberattacks. Informatics, 9(1). https://doi.org/10.3390/informatics9010028

Pierazzi, F., & Srndic, N. (2022). WoRMA '22: 1st Workshop on Robust Malware Analysis. In ASIA CCS 2022 - Proceedings of the 2022 ACM Asia Conference on Computer and Communications Security (pp. 1271–1272). Association for Computing Machinery, Inc. https://doi.org/10.1145/3488932.3517205

Shrivastava, S. (2017). Digital Disruption is Redefining the Customer Experience: The Digital Transformation Approach of the Communications Service Providers. Telecom Business Review: SITM Journal, 10(1), 41–52. Retrieved from http://www.publishingindia.com

Shukla, A. S., Chavan, S. R., & R, S. (2023). Spear Watch: A Thorough Examination to Identify Spear Phishing Attacks. International Journal of Innovative Technology and Exploring Engineering, 12(8), 46–51. https://doi.org/10.35940/ijitee.h9680.0712823

Siagian, L., Budiarto, A., & Simatupang. (2018). Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional. Jurnal Prodi Perang Asimetris, 4(3), 1–18.

Thomas, D. R. (2016). Digital disruption: A transformation in graduate management online education. In Phantom Ex Machina: Digital Disruption's Role in Business Model Transformation (pp. 223–233). Springer International Publishing. https://doi.org/10.1007/978-3-319-44468-0_15

Tomicic, I. (2023). Social Engineering Aspects of Email Phishing: an Overview and Taxonomy. In 2023 46th ICT and Electronics Convention, MIPRO 2023 - Proceedings (pp. 1201–1207). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.23919/MIPRO57284.2023.10159691

Tosun, O. K. (2021). Cyber-attacks and stock market activity. International Review of Financial Analysis, 76. https://doi.org/10.1016/j.irfa.2021.101795