International Journal of Society Reviews (INJOSER) e-ISSN: 3030-802X
Vol. 1 No. 8 2024, pages: 863~868

EXPLORING CYBER SECURITY THREATS: A SYSTEMATIC LITERATURE REVIEW

Ahmad Farhan Mahesa
Program Studi Informatika, Universitas Nasional, Indonesia

Arman Prasojo Sugiyarto
Program Studi Informatika, Universitas Nasional, Indonesia

Rima Tamara Aldisa *
Universitas Nasional
Correspondence author email: rimatamaraa@gmail.com

ABSTRACT

This research aims to determine the challenges faced including political provocation, mis information (hoax), issues related to ethnicity, religion and race (SARA), hate speech, radical ideology, terrorism, hacking, data breaches, online fraud, and various other cybercrime. Proactive anticipation, prevention and mitigation strategies are very important to ensure cyber security. This research uses a systematic literature review method of various articles discussing cybercrime and cybersecurity in a systematic literature review of modern challenges. The research results show that continuous education and training is needed to increase digital literacy and cyber security awareness for effective protection. Synergy between stakeholders in increasing digital literacy and cyber security awarenessis very important.

Keywords: Cybercrime, Cybersecurity, Literature Review.

INTRODUCTION

Cyber security is now the main focus of attention for all countries in the world, considering the role of information and communication technology which increasingly penetrates various aspects of life, involving aspects such as social, economic, legal, organizational, health, education, culture, government, security, and defense. The increase in the level of risk and threat of misuse of information and communication technology is in line with the increasing intensity of its use (Ginanjar, 2022). Although this rapid digital growth illustrates the progress of the digital economy, it should be noted that this increase is also accompanied by increasing threats to cyber security (Daeng et al., 2023).

Indonesia, which is known as the fourth largest contributor to the growth of internet users in the world, faces great opportunities and threats amidst the evolution of digital and internet technology in all social, political and economic dimensions. The challenges faced include political provocations, misinformation (hoaxes), issues related to ethnicity, religion and race (SARA), hate speech, radical ideology, terrorism, hacking, data breaches, online fraud and various other cybercrime. Proactive anticipation,

prevention and mitigation strategies are very important to ensure cyber security (Ginanjar, 2022). The transformation of society's behavior will have an impact on the behavior of the state or government. Responses from countries to these changes can vary, from implementing new regulations related to cyberspace to establishing special institutions responsible for handling these aspects, all of which reflect the country's adaptation efforts.

To address cybersecurity challenges, the Indonesian government has taken progressive measures to improve the country's digital security infrastructure. These actions include policy development, security technology improvements, and public awareness programs about cybersecurity dangers. One of the most significant actions was the passing of the Electronic Information and Transactions Law (UU ITE) (Najwa, 2024).

In terms of cyber security, the development of Indonesian law in the field of technology and information (IT) security can be traced since the enactment of Telecommunication Law no. 36 of 1999 and the Information and Electronic Transactions (ITE) Law no. 11 of 2008. These two laws are considered the embodiment of the Indonesian government's policy in dealing with security issues related to communications technology in general in Indonesia. Ratification by the President of the Republic of Indonesia Bacharuddin Jusuf Habibie and Minister of State Secretary Muladi, the Telecommunications Law became one of the initial milestones in the formation of special policies related to telecommunications activities in Indonesia (DPR RI, 1999). This law covers all forms of technology-based communication, such as television, radio, telephone and other media.

RESEARCH METHODS

This research adopts a qualitative descriptive approach to explore and analyze the readiness of all sectors to face challenges, both mitigation and threat, as a cyber security system. The main focus of the research is to review problems related to cyber security challenges and threats that arise in the era of the industrial revolution 4.0. In this case, in-depth research explores data relating to aspects of the cyber security system, the readiness of related sectors, as well as situations and conditions that influence responses to cyber security challenges in the industrial revolution 4.0 era. This research focuses on writings that have been submitted through publications in journals at both national and international levels. This research is also descriptive in nature, this study aims to describe and deepen understanding of cyber security threats, while presenting solutions that can be adopted by Indonesian society in responding to increasing cyber security threats. Thus, this research describes views regarding cyber security threats, as well as highlighting steps that can be taken by the nation to overcome and manage the challenges that arise as a result of high levels of cybercrime.

RESULTS AND DISCUSSION

Cybercrime

Cybercrime is a crime that attacks computers, computer networks, or other devices connected to the internet. Cybercriminals are hackers or cybercriminals who commit crimes as individuals or members of organizations. This challenge affects business aspects in all sectors that need to be prepared to face global changes in the world.

Cybercrime is an activity that has a detrimental impact on internet users. Cybercrime can be defined as an attempt or act to gain access to another person's computing device with the intent to find, steal, damage, or hack personal information, which can result in privacy violations and damage to internet users' assets. Cybercrime not only harms individuals, but also has a significant influence on large organizations, internet users, digital system users, government business units, and various other targets that are targeted by cybercrime (Indah et al., 2022). The existence of cybercrime poses a major threat to human life, thereby questioning the ability of government institutions to face growing challenges in the field of computer technology. Cybercrime has a detrimental impact on the social aspects of society due to a lack of awareness of crimes in the internet environment and ineffective measures for the protection and security of personal data. Therefore, major steps are needed to overcome the problem of cybercrime by increasing public awareness of cyber dangers and improving cyber defense and personal information security.

Hackers or cybercriminals are involved in cybercrime with the aim of earning some money through their illegal actions. There are also political or personal motivations that underlie cybercrime activities, although these motives are rarely found because the majority of perpetrators tend to pursue profit alone. Various types of cybercrime that threaten the security of computer systems include identity fraud, phishing, cracking, spoofing, Denial-Of-Service (DDOS) attacks, carding, data falsification, SIM card swapping, cyberstalking, One-Time Password fraud (OTP), SQL injection, cyber espionage, and ransomware attacks. According to Salomon (2021), cybercrime can be interpreted in two meanings, namely first as computer related crime in general, often referred to as computer related crime, where the perpetrator illegally utilizes computer systems and networks. Second, in a more specific sense, cybercrime refers to computer crime, which involves illegal violations or attacks on computer security systems and data processed by other computers.

Cyber Attacks have several types that can be identified, including Cyber Warfare and Cyber Terrorism. The development of information and communication technology has brought various conveniences in carrying out government activities; however, its impact extends to a variety of new things that pose serious challenges to national integrity and security, known as cyber warfare. Cyber Warfare can be interpreted as war in cyberspace. The definition of cyber warfare includes conflict in Cyberspace, which is

substantially different from attacks in conventional war or other physical warfare. The main tools used in cyber warfare are computers and the internet. The targets in cyber warfare are not located in physical, territorial or geographic areas, but rather on objects located in cyberspace controlled by a country. Meanwhile, cyber terrorism is the action of a number of terrorist networks or groups that attempt to damage the social, political and economic security of a country through the use of internet technology. Examples involve attacks on official government websites, wiretapping of strategic communications networks in the political realm, hacking of electronic data in the banking sector, and similar forms of activity. The impact of this cyber activity is very serious because it can cause concern and panic on a wide scale (Ariyaningsih et al., 2023).

The involvement of law enforcement authorities, as regulated in Law Number 19 of 2016 concerning Amendments to the ITE Law, is very important in efforts to eradicate cybercrime. Their responsibilities include the detection, investigation and prosecution of individuals involved in cybercrime, as well as the implementation of prevention and response measures to cyberattacks. However, these organizations often face a variety of obstacles, including limited resources, lack of adequate skills and training, difficulties in collecting and storing digital evidence, threats to anonymity and mobility from cybercriminals, and complex jurisdictional issues. To combat cybercrime effectively, the capability and capacity of law enforcement agencies must be enhanced through collaboration, coordination at both national and international levels (Farhan et al., 2023).

Cyber Security

Cyber security is an effort to protect computer systems, networks, software and data from attack, unauthorized access, modification or destruction by unauthorized persons. Cybersecurity includes technologies, policies and practices designed to protect computers, networks and information systems from various types of cyber threats, such as malware attacks, phishing and denial of service (DoS) attacks (Soesanto et al., 2023).

Cybersecurity is a collection of tools, policies, protection principles, safety measures, guidelines, risk control strategies, efforts, training, high-level applications, warranties, and information that uses technology to protect digital environments and organizations online. The organizational and individual components of cybersecurity include computing functions, individuals, infrastructure, programs, services, telecommunications structures, and any records that enter and leave cyberspace. Cyber security can also be defined as the entire process of maintaining and reducing threats to privacy, integrity and availability of information, as well as steps to protect information systems from various types of physical and cyber attacks (Indah et al., 2022).

Cybersecurity is a relatively new problem that occurs because many aspects of life, including economic, social, cultural, political, and military, become interconnected

through cyberspace (Samudra et al., 2023). Several recent events have placed Indonesia in the category of countries that have weak cyber security. This can be reinforced by a series of events, such as hacking of user or bank customer data, which recently occurred due to ransomware attacks. Ransomware is a criminal act that attacks software with the aim of limiting user access to files, locking the user's screen, or encrypting files before demanding a ransom (Darmawan, 2019).

CONCLUSION

A Systematic literature review on cybersecurity threats highlights the importance of a holistic approach in addressing these challenges, which includes the latest technologies, effective policies, and security awareness among users. The importance of cooperation across sectors and between countries is also frequently emphasized, given the cross-border nature of many cyber threats. Additionally, investment in cybersecurity education and training is needed to address skills shortages and increase resilience to cyberattacks. Technologies such as AI and ML can be used not only by attackers but also in defense strategies to detect and respond to threats automatically and efficiently.

Reference

1. Abdullah, M. S., & Ikasari, I. H. (2023, Juni). Perkembangan Terbaru Dalam Keamanan Siber, Ancaman Yang Diidentifikasi Dan Upaya Pencegahan, 1, 96-98.
2. Daeng, Y., Levin, J., & Prayudha, M. R. (2023). Analisis Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia. Innovative: Journal Of Social Science Research, 3(6), 1135–1145.
3. Farhan, M., Syaefunaldi, R., & Hidayat, P. R. D. (2023). Penerapan Hukum Dalam Menanggulangi Kejahatan Siber Penegakan Hukum Terhadap Tindak Pidana Siber. Jurnal Ilmu Hukum, Sosial, dan Humaniora, 1(6), 8–20.
4. Ginanjar, Y. (2022). Strategi Indonesia Membentuk *Cyber Security* Dalam Menghadapi Ancaman *Cyber Crime* Melalui Badan Siber Dan Sandi Negara. *Jurnal Dinamika Global* 7(2), 295–316.
5. Handayani, A. (2023, Oktober). Perlindungan Hukum atas Tindakan Pencurian Data Pribadi pada Layanan Fintech Lending Terhadap Ancaman Cyber Security di Indonesia, 6, 605-630.
6. Mahendra, Y. C., & Pinatih, N. K. D. S. A. (2023). STRATEGI PENANGANAN KEAMANAN SIBER (CYBER SECURITY) DI INDONESIA, 6, 1941-1948.
7. Najwa, F. R. (2024). Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus PenegakanHukum Siber di Indonesia. AL-BAHTS: Jurnal Ilmu Sosial, Politik, dan Hukum, 2(1), 8–16.
8. Rahmawati, C. (2019). Tantangan dan Ancaman Keamanan Siber Indonesia di Era Revolusi Industri 4.0. Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO AAU), 1(1), 299–306.
9. Salomon, A. M. (2021). Ancaman Perang Siber di Era Digital dan Solusi Keamanan Nasional Indonesia. Jurnal Oratio Directa, 3(2).

10. Septasari, D. (2023). Cyber Security and The Challenge of Society 5.0 Era in Indonesia. Aisyah Journal of Informatics and Electrical Engineering, 5(2), 227–233.
11. Soesanto, E., Kurniasih, F., Mutiara, P., & Afifi, S. T. (2023). Pengaruh Sistem Pengamanan Objek Vital, File Dan Cyber Terhadap Manajemen Sekuriti Pada Pt Freeport Indonesia. Journal Of Research And Publication Innovation, 1(2), 251-260.
12. Soesanto, E., Salsabilah, F., Abadi, I. C., & Rizky, M. (2023). Peran Manajemen Sekuriti di Bank BRI Dalam Pengamanan File Nasabah untuk Mencegah Ancaman Cyber Security dan Menjaga Objektivitas Nasional, 1, 497-502. https://journal.csspublishing/index.php/ijm
13. Solihin, K., & Kurniawan, F. A. (2022). Penguatan Manajemen Risiko Lembaga Keuangan Syariah Non-Bank dalam Menghadapi Ancaman Cyber Security. Journal of Indonesian Sharia Economics, 1(2), 1–20.