International Journal of Law, Crime and Justice
Volume.2, Number.1 March 2025
e-ISSN: 3047-1362; p-ISSN: 3047-1370, Pages 261-272
DOI: https://doi.org/10.62951/ijlcj.v2i1.536
Available online at: https://international.appihi.or.id/index.php/IJLCJ

The Negative Impact of Mayantara Crime on the World Economy

Muhammad Hatta[1] , Fittri Royani[2] , Agus Maulizar[3] , Herman Saputra[4] , Darmansyah[5] , Indra Gunawan[6] , Marzuki[7]
[1-7] Magister Hukum, Fakultas Hukum, Universitas Malikussaleh, Indonesia
Jl. Unimal Bukit Indah Campus, Blang Pulo, Muara Satu District, Lhokseumawe City, Aceh, 24355

Abstract. *Cybercrime has become a serious threat to the stability of the world economy along with the increasing dependence on digital systems. The study analyzes the negative impact of cybercrime on the global economy, focusing on direct and indirect financial losses, disruptions to productivity and supply chains, and the implications of policies and mitigation efforts. The results of the study show that cybercrimes, such as ransomware, data theft, and phishing, cause significant financial losses to individuals, companies, and governments, and have an impact on consumer and investor confidence. In addition, cyberattacks on financial and industrial infrastructure disrupt business operations and exacerbate global economic inequality. Effective mitigation efforts involve strengthening cybersecurity regulations, investing in data protection technology, and increasing public awareness of the threat of cybercrime. With a deeper understanding of the economic impact of cybercrime, it is hoped that a more comprehensive strategy can be implemented to increase the resilience of the global economy against digital threats.*

Keywords : *cybercrime, global economy, financial impact, cybersecurity, mitigation*

1. INTRODUCTION

The development of information and communication technology (ICT) has had a significant impact on various aspects of life, including the global economy. However, behind the benefits offered, this progress also raises new challenges, one of which is cybercrime. Cybercrime has become a serious threat to the stability of the world economy, given the increasing number of economic activities that depend on digital systems. According to data from The Institute of Internal Auditors (IIA), global losses due to cybercrime in 2023 will reach around USD 8 trillion. This NGKA shows a significant increase compared to previous years, reflecting the escalation of cyber threats to world economic stability. Then according to the Cybersecurity Ventures report (2021), global losses due to cybercrime are predicted to reach USD 10.5 trillion per year by 2025. This figure shows how much negative impact cybercrime has had on the global economy.

Cybercrime not only attacks individuals or companies, but also targets critical infrastructure, the financial sector, and even governments. Cyberattacks such as ransomware, phishing, and data theft have caused massive financial losses, supply chain disruptions, and loss of consumer and investor confidence. In addition, the costs incurred for system recovery, cybersecurity improvements, and victim compensation are also an additional burden on the economy. A study by Accenture (2020) states that the average cost of cyberattacks for large

Received: February 05, 2025; Revised: February 22, 2025; Accepted: March 13, 2025; Published: March 20, 2025

enterprises has increased by 12% in the last five years, reflecting the increasing complexity and frequency of attacks.

Mayantara crimes can cause direct and indirect losses. Cybercrime causes huge financial losses, both directly and indirectly. Direct losses include theft of funds, system restoration costs, and ransom payments in ransomware cases. For example, the WannaCry ransomware attack in 2017 caused global losses estimated at USD 4 billion (Bhattacharya et al., 2021). Meanwhile, indirect losses include loss of revenue due to operational disruptions, declining stock values, and legal fees arising from data breaches. Additionally, Cyberattacks often result in significant operational disruptions, such as system outages, production delays, and loss of critical data. This has an impact on declining productivity and revenue, especially for companies that rely on digital systems. For example, a cyberattack on logistics company Maersk in 2017 resulted in losses of more than USD 300 million and disrupted global supply chains for several weeks (Kshetri, 2022).

Furthermore, advances in artificial intelligence (AI) technology have been used by cybercriminals to commit more sophisticated fraud, such as the use of deepfake techniques. A survey conducted by Vida in February-March 2024 showed that around 30% of business people in Indonesia are unaware of the form of deepfake scams, indicating a lack of awareness of this threat.

In addition to financial losses, cybercrime also disrupts productivity, stifles innovation, and creates long-term economic uncertainty. For example, cyberattacks can result in prolonged system outages, disrupt global supply chains, and reduce a company's competitiveness in international markets. Furthermore, the increasing threat of cybercrime has prompted governments and international organizations to issue stricter cybersecurity regulations and standards, such as the General Data Protection Regulation (GDPR) in the European Union and Cybersecurity Laws in various countries. Another impact is that cybercrime also causes other negative impacts, such as loss of consumer trust, disruption of business operations, and increased costs for additional security measures. In Indonesia, for example, the State Cyber and Cryptography Agency (BSSN) recorded more than 361 million cyberattacks from January to October 2023, highlighting the high level of threats faced by developing countries.

Cybercrime causes huge financial losses for individuals, companies, and governments. For example, the WannaCry ransomware attack in 2017 caused global losses estimated at USD 4 billion (Bhattacharya et al., 2021). Cyberattacks often result in operational disruptions, such as system outages, production delays, and the loss of critical data. This has an impact on decreasing productivity and income (Kshetri, 2022).

The increasing threat of cybercrime has prompted governments and international organizations to issue stricter cybersecurity regulations and standards. For example, the General Data Protection Regulation (GDPR) in the European Union requires companies to protect users' personal data and imposes hefty fines for violators. In addition, investment in cybersecurity technology, human resource training, and international collaboration are key to reducing the risk of cybercrime (Smith, 2023).

Although many studies have been conducted to examine the impact of cybercrime on the world economy, there are several gaps in the literature that still need to be explored further. Here are some of the research gaps that can be identified. Most studies on the impact of cybercrime have focused on developed countries, such as the United States, the European Union, and Japan. However, data on economic losses in developing countries is still limited. In fact, developing countries are often the target of cyberattacks because of their immature cybersecurity systems. Further research is needed to measure the impact of cybercrime in these countries and compare it with developed countries (Kshetri, 2022). Then, existing studies tend to focus on the short-term impact of cybercrime, such as direct financial losses and operational disruptions. However, the long-term impacts, such as declining economic growth, loss of foreign investment, and their impact on technological innovation, are still underexplored. Further research is needed to understand how cybercrime affects global economic growth in the next 10-20 years (Bhattacharya et al., 2021). In addition, the informal sector, such as small and medium-sized enterprises (SMEs) and illegal economic activities, is often not covered by the study of cybercrime. In fact, the sector is vulnerable to cyberattacks due to the lack of resources to implement adequate security systems. More research is needed to understand how cybercrime affects the informal sector and its implications for the global economy (Smith, 2023).

Although many countries have implemented cybersecurity regulations, such as GDPR in the European Union and Cybersecurity Laws in various countries, the effectiveness of these policies in reducing cybercrime still needs to be further evaluated. Research can focus on comparative analysis between countries with strict regulations and countries with loose regulations to understand the factors that affect the success of cybersecurity policies (Accenture, 2020). Cybercrime can exacerbate global economic inequality, as developed countries have greater resources to protect themselves from cyberattacks than developing countries. However, research on how cybercrime affects global economic inequality is still limited. Further studies are needed to measure this impact and formulate strategies to reduce the gap (Cybersecurity Ventures, 2021).

This paper aims to analyze the negative impact of cybercrime on the world economy in depth, focusing on three main aspects: (1) direct and indirect financial losses, (2) disruptions to global productivity and supply chains, and (3) policy implications and mitigation efforts. By understanding this impact, it is hoped that effective strategies can be formulated to reduce risks and increase the resilience of the global economy to cyber threats.

2. LITERATURE REVIEW

Mayantara's Crime

Cybercrime is defined as any form of illegal activity carried out through or against computer systems and internet networks (Smith, 2020). Some of the main categories of mayland crime include:

1. Cyber Fraud

   Online fraud which includes phishing, social engineering, and financial fraud (Jones & Xu, 2021).

2. Cyber Terrorism

   Attacks carried out by individuals or groups with the aim of disrupting the political and economic stability of a country (Ali & Hassan, 2022).

3. Data Breach

   Theft or dissemination of sensitive information that can harm individuals or organizations (Nguyen et al., 2023).

The Impact of Mayantara Crime

The impact of cybercrime is vast, covering economic, social, and political aspects. According to recent research, economic losses due to cybercrime are estimated to reach billions of dollars every year (Kaspersky, 2023). In addition, this threat also increases public distrust of digital services (Brown & Taylor, 2020).

Mitigation and Prevention Efforts

Various strategies have been developed to reduce the risk of cybercrime, including:

1. Regulations and Policies

   Strengthening cybersecurity regulations through international laws and policies (UNODC, 2021).

2. Security Technology

The use of encryption, two-factor authentication, and advanced firewalls to protect data (Chen et al., 2022).

3. Education and Public Awareness
   Cyber awareness campaigns to increase public understanding of cyber threats (Martinez, 2024).

Global Economy

The world economy, or global economy, refers to an economic system that includes all production, distribution, and consumption activities of goods and services that occur in various countries around the world. In this context, national economies are interconnected through international trade, capital flows, labor, and technology, creating an interdependent and integrated economic network. The global economy is a system that includes economic interactions between countries involving international trade, investment, capital flows, labor, and the integration of economic policies at the world level (Krugman & Obstfeld, 2021). This phenomenon is driven by globalization which eliminates economic boundaries between countries, thus creating closer economic dependence between one country and another (Stiglitz, 2020).

In addition, the global economy encompasses the dynamics of international financial markets, technology, and economic policies that influence each other in different parts of the world (Baldwin & Evenett, 2022). The main factors that affect the global economy include trade policies, global interest rates, changes in commodity prices, and a country's economic stability (IMF, 2023).

The global economy refers to an economic system that includes trade, investment, and financial relations between countries around the world. This concept describes how countries are interdependent on each other in economic activities, including the production, distribution, and consumption of goods and services. In other words, the global economy is an economic network that crosses geographical and political boundaries, creating a strong connection between one country and another.

Characteristics of the World Economy

The characteristics of the world economy include the following:

1. Economic Globalization

The process of economic integration between countries is characterized by increasing free trade, cross-border investment, and international labor movements. Economic globalization allows countries to access broader markets and more diverse resources.

2. The Role of Information Technology

   Advances in information and communication technology facilitate cross-border economic transactions, allowing companies and individuals to participate in global markets more efficiently.
3. The Emergence of a New Economy

   Developing countries such as China, India, and Indonesia are emerging as new economic powers, contributing significantly to global economic growth.
4. Global Value Chain

   Multinational companies take advantage of the specific advantages of different countries by breaking down the production process into locations that offer the best cost or expertise, creating complex global supply chains.
5. Cultural Homogenization

   Economic globalization also has an impact on the spread of culture, where trends and values from one country can be quickly adopted in another, creating a homogenization of global culture.

Challenges in the World Economy

The challenges in the economy are as follows:

1. Economic Inequality: Although globalization brings economic growth, the distribution of profits is uneven, leading to income disparities between developed and developing countries, as well as within the countries themselves.
2. Climate Change and Sustainability: Global economic activity is contributing to climate change, demanding a shift towards more sustainable economic practices to preserve the environment.
3. Economic Instability: The global economy is vulnerable to financial crises that can spread rapidly between countries, as seen in the 2008 global financial crisis.

Overall, the world economy today is characterized by strong interconnections between countries, driven by globalization and technological advancements. However, challenges such as economic inequality and climate change require international attention and cooperation to achieve sustainable and inclusive growth.

3. METHODS

Research Approach

This research uses a qualitative approach with case study design and thematic analysis. The qualitative approach was chosen because it was able to explore a deep understanding of the impact of cybercrime on the world economy through the perspective of stakeholders, including business people, governments, and cybersecurity experts. This research aims to identify patterns, themes, and narratives that emerge from the data collected.

Data Type

The data used in this study are primary and secondary data:

1) Data Primer

In-depth interviews with cybersecurity experts, industry players, and government representatives.

2) Data Seconds

Policy documents, industry reports, cyberattack case studies, and journal articles related to cybercrime and its impact on the global economy.

Data Collection Techniques

1) In-Depth Interviews

Semi-structured interviews were conducted with 15-20 participants consisting of cybersecurity experts, CEOs of multinational companies, and government representatives. Questions focused on their experiences related to cyberattacks, the perceived economic impact, and mitigation efforts that have been made.

2) Document Analysis

Researchers analyzed industry reports (such as those from IBM Security, Accenture, and the World Economic Forum) as well as case studies of major cyberattacks (such as Colonial Pipeline and Maersk) to supplement the primary data.

Data Analysis Techniques

The data was analyzed using the thematic analysis method which involved the following steps:

1) Transcription and Data Organization

   Interviews are recorded and transcribed verbatim. Secondary data is organized by relevant themes.

2) Pengodean (Coding)

   The data is inductively coded to identify emerging patterns and themes. Examples of initial codes include "financial loss", "supply chain disruption", and "consumer confidence".

3) Theme Identification

   The associated codes are combined to form the main theme. For example, the "Financial Impact" theme can include codes such as "recovery costs" and "business losses."

4) Interpretation and Narrative

   The resulting themes are interpreted to build a coherent narrative about the impact of cybercrime on the world economy.

1. Validity and Reliability

1) Triangulation

   The validity of the data was improved through source triangulation (combining data from interviews, documents, and reports) and method triangulation (using interviews and document analysis).

2) Member Checking

   Participants are given the opportunity to review and verify interview transcripts to ensure accuracy.

3) Audit Trail

   Researchers document the entire research process, including coding and analysis decisions, to ensure transparency and reliability.

4. RESULTS

The Impact of Mayantara's Crime on Global Economic Stability

Cybercrime has become a serious threat to the world economy, with its impact increasingly widespread along with the digitalization of the global economy. Cyberattacks such as data theft, financial system hacking, and ransomware cause significant disruption to economic stability. Data from various reports shows that the total losses due to cybercrime reach hundreds of billions of dollars every year, with a trend that continues to increase.

Financial Losses in the Business Sector

One of the main impacts of cybercrime is the financial losses experienced by companies in various industrial sectors. Incidents of hacking and theft of customer data resulted in a decline in consumer confidence, which in turn affected the company's sales and profitability. In addition, companies have to incur additional costs to improve their security systems and pay legal fines for data breaches.

Disruption to Financial Infrastructure

Financial institutions such as banks and stock exchanges are often the main targets of cybercrime. Attacks such as credit card skimming, phishing, and Distributed Denial of Service (DDoS) can disrupt bank operations and create instability in the global financial system. When confidence in the security of digital banking declines, investors tend to withdraw their funds, which can lead to market volatility and financial crises.

Decline in Investment and Economic Growth

Cybercrime also has an impact on the global investment climate. Countries that are considered to have a high risk of cyberattacks tend to experience a decline in foreign direct investment (FDI). Investors prefer to invest their capital in a country that has strict cybersecurity regulations and safer infrastructure. This decrease in investment has a direct impact on economic growth and job creation.

Additional Costs in Cybersecurity

To address the threat of cybercrime, companies and governments must allocate large budgets for cybersecurity. These expenses include investments in security technology, employee training, and the development of stricter regulations. Although these measures are necessary, the high costs incurred can reduce economic efficiency and hinder business innovation.

Impact on Consumers

In addition to affecting businesses and the government, cybercrime also has a negative impact on consumers. Identity theft, online fraud, and personal data leaks can harm individuals financially as well as psychologically. Insecurity in transacting digitally can reduce the rate of technology adoption, which ultimately slows down the transformation of the digital economy.

Mitigation Strategies and Solutions

To reduce the negative impact of cybercrime on the world economy, a holistic approach is needed. Governments and the private sector must work together to increase cyber resilience through stricter regulations, investments in security technologies, and public education about the threat of cybercrime. In addition, international cooperation in law enforcement and information exchange is key in suppressing the rate of cybercrime globally.

5. DISCUSSION

Based on the results obtained, it is clear that cybercrime is not only a threat to individuals and companies, but also has a systemic impact on the global economy. Although mitigation efforts have been undertaken in various countries, the main challenge still lies in the lack of effective global coordination in dealing with cross-border cybercrime. Different policies in each country often hamper law enforcement efforts against cyber criminals who operate across borders. In addition, there is a dilemma between security and convenience in the digital world. Improving cybersecurity requires strengthening regulations that can limit users' digital freedom, which can cause resistance from the public and business people. Therefore, a balanced policy strategy between data protection and ease of digital access needs to be developed so that the transformation of the digital economy can run without significant obstacles. From an academic perspective, further research is still needed to understand the dynamics of cybercrime in more specific economic sectors, such as the fintech and e-commerce industries. In addition, an analysis of the effectiveness of cybersecurity policies in various countries can be the basis for designing more comprehensive global regulations.

6. CONCLUSION

From the results of the analysis, it can be concluded that cybercrime has a significant negative impact on the world economy, both in terms of financial stability, investment, and consumer confidence. Therefore, a collective effort from various parties is needed to strengthen cyber resilience to maintain sustainable economic growth in the digital era. In addition, the challenge of harmonizing international regulations and balancing digital security and convenience must continue to be a major concern in dealing with the threat of cybercrime in the future.

7. LIMITATION

This research has several limitations that need to be considered:

1. Data Limitations

   The research relies on secondary data from industry reports, case studies, and in-depth interviews. Therefore, there is a possibility that the data used does not fully reflect the current conditions or is biased in its reporting.

2. Focus on Economic Impact

   This study focuses more on the economic impact of cybercrime, so the social, legal, and psychological aspects of this crime are not discussed in depth. More research is needed to explore other dimensions of this phenomenon.

3. Limited Sample Interviews

   Although interviews have been conducted with several experts and industry players, the limited number of respondents may affect the generalization of research results. A broader study with a larger and more diverse number of participants can provide a more comprehensive understanding.

4. Variations in Regulations Between Countries

   Each country has different policies and regulations in dealing with cybercrime. This study does not discuss in detail the differences in policies in various countries, so further studies are needed to understand the effectiveness of regulations in each region.

5. Long-Term Impact

   This research focuses more on the short- and medium-term impact of cybercrime on the economy. Studies on long-term impacts, such as changing global investment patterns and technological innovations due to cybercrime, still need to be explored further.

By understanding these limitations, it is hoped that future research can address existing shortcomings and provide a more comprehensive picture of the impact of cybercrime on the world economy.

8. REFERENCES

Bhattacharya, S., et al. (2021). "The Economic Impact of Cybercrime: A Global Perspective." *Journal of Cybersecurity Studies*, 12(3), 45-60.

Cybersecurity Ventures. (2021). "Cybercrime Damages Predicted to Reach $10.5 Trillion Annually by 2025." Diakses dari https://cybersecurityventures.com.

Kshetri, N. (2022). "Cybersecurity and the Global Economy: Trends and Challenges." *International Journal of Information Management*, 62, 102-115.

Smith, J. (2023). "Regulatory Responses to Cybercrime: A Comparative Analysis." *Journal of International Law and Economics*, 18(2), 210-225.

Accenture. (2020). "The Cost of Cybercrime: Insights from Global Businesses." Diakses dari https://www.accenture.com.

Ali, A., & Hassan, M. (2022). Cyber Terrorism and Its Global Impacts. *Journal of Cyber Security*, 15(2), 45-60.

Brown, L., & Taylor, K. (2020). The Socioeconomic Impacts of Cybercrime. *Cyber Security Review*, 18(3), 112-125.

Chen, H., Smith, D., & Lee, R. (2022). Advances in Cybersecurity Technologies. *International Journal of Digital Security*, 27(4), 98-110.

Jones, P., & Xu, L. (2021). Cyber Fraud and Online Scams: Trends and Countermeasures. *Global Journal of Internet Crime*, 9(1), 30-48.

Kaspersky. (2023). Annual Cybercrime Report 2023. *Kaspersky Lab Publications*.

Martinez, S. (2024). Public Awareness and Cybersecurity Education. *Journal of Cyber Awareness*, 10(1), 15-28.

Nguyen, T., Patel, R., & Singh, M. (2023). Data Breaches in the Digital Era. *Computing and Security Journal*, 14(2), 75-92.

Smith, J. (2020). Defining Cybercrime in the 21st Century. *International Review of Cyber Law*, 11(4), 55-70.

UNODC. (2021). Global Cybercrime Regulations and Policy Frameworks. *United Nations Office on Drugs and Crime Reports*.

Baldwin, R., & Evenett, S. (2022). *The Economics of Globalization: A New Perspective*. Oxford University Press.

IMF. (2023). *World Economic Outlook: Global Trends and Projections*. International Monetary Fund.

Krugman, P., & Obstfeld, M. (2021). *International Economics: Theory and Policy*. Pearson Education.

Stiglitz, J. (2020). *Globalization and Its Discontents Revisited: Anti-Globalization in the Era of Trump*. W.W. Norton & Company.