International Journal Publishing
INFLUENCE: International Journal of Science Review
Volume 5, No. 3, 2023
https://influence-journal.com/index.php/influence/index

Strategic Intelligence Analysis: Police Handling Efforts Against Security Threats in Electronic Commerce Transactions

Muhammad Agus Yulizar[1], Maria Puspitasari[2], Bondan Widiawan[3]
[1,2,3]*Universitas Indonesia, Depok, Indonesia*
Email: magusijal@gmail.com

Abstract. In the era of globalization and rapid development of information technology, electronic commerce transactions or E-commerce have become an integral part of business activities throughout the world. The growth of E-commerce in Indonesia began in 1999 and continues to grow rapidly along with increasing internet use. However, along with this development, cyber security threats have also emerged, such as online fraud, theft of personal data, and cyber-attacks. This research outlines the strategic intelligence steps taken by the Indonesian National Police (Polri) in dealing with security threats in electronic commerce transactions. Polri adopts a comprehensive approach involving planning, information gathering, data analysis, and policy making. They also collaborate with various related institutions and carry out educational campaigns to increase public understanding of the risks of cybercrime. This research then found that the National Police needed to strengthen cooperation with various parties, invest in advanced technology, monitor technological developments, and increase special investigation units. By taking these steps, the National Police can improve their ability to tackle cybercrime in electronic commerce transactions and create a more resilient digital security ecosystem.

Keywords: *Intelligence Analysis, E-commerce, Strategy, Law Enforcement.*

A. INTRODUCTION

In the era of globalization and rapid development of information technology, electronic commerce transactions or E-commerce have become an integral part of business activities throughout the world. According to Turban, electronic commerce or E-commerce is the activity or process of trading goods via the internet or as an exchange of products, services, and information via information networks, including the internet (Xiao et al., 2022). According to Mustajibah, the journey of e-commerce in Indonesia began in 1999, which was the beginning of the birth of e-commerce in Indonesia. The KASKUS forum became the forerunner of online shops in Indonesia which was founded by Andrew Darwis, followed by Bhinneka.com which is also a place for online buying and selling in Indonesia. The rapid development of e-commerce is the impact of people starting to become more widely aware of the internet (Schwob et al., 2023).

Mechant Machine, in its research results, also stated that the number of internet users in Indonesia, which is more than 100 million users, is one of the forces driving the growth of e-commerce. The average amount of money Indonesian people spend on online shopping sites reaches US$ 228 per person or around Rp. 3.19 million per person. With the continued growth in the number of internet users in Indonesia, many individuals and companies have turned to E-commerce as their primary method of doing business and shopping. However, along with the surge in E-commerce use, there is also an increase in the potential for cybercrime. Threats such as online fraud, theft of personal data, and cyber attacks are increasingly becoming a major concern (Ariansyah et al., 2021).

The use of E-commerce certainly has positive and negative consequences for sellers and buyers. According to Sabadmin, the positive benefits of using E-commerce include reaching a wider market, flexibility in operations, increasing revenue, reducing the risk of additional costs, improving service quality, as well as receiving feedback in the form of reviews from buyers which can be used as an indicator of business success. Meanwhile, negative

aspects include its vulnerability to online fraud, potential theft of personal information, and service interruptions (Maskuroh et al., 2022).

According to Johnson, the ever-increasing adoption of E-commerce technology throughout the world has opened the door to various cybercrime activities. In a report published by Kominfo in 2022, the e-commerce sector recorded 29.8% of cybercrime cases. Meanwhile, government agencies 25.5%. Followed by financial services 17%, social media 6.4%, and telecommunications 4.3%. Apart from that, there are also cases where e-commerce data in Indonesia was hacked by hackers, and the data was bought and sold. In 2020, 91 million Tokopedia user data was leaked and traded on dark sites or the dark web (Hasbullah, 2022).

The most common and frequently occurring security threat is phishing attacks. These attacks often result in money theft and misuse of users' data. In a phishing attack, the attacker tries to trick users by sending fake messages or tricking them into revealing personal information, such as passwords and financial data. The impact of phishing attacks can be devastating for consumers and businesses. Apart from phishing attacks, hacking is another significant threat in e-commerce. Attackers try to hack e-commerce security systems, access sensitive data, or steal customer information. This can threaten integrity and trust in online businesses (Butt et al., 2023).

However, there are still many cases that have not been solved by the police, this can be seen in the graph below:

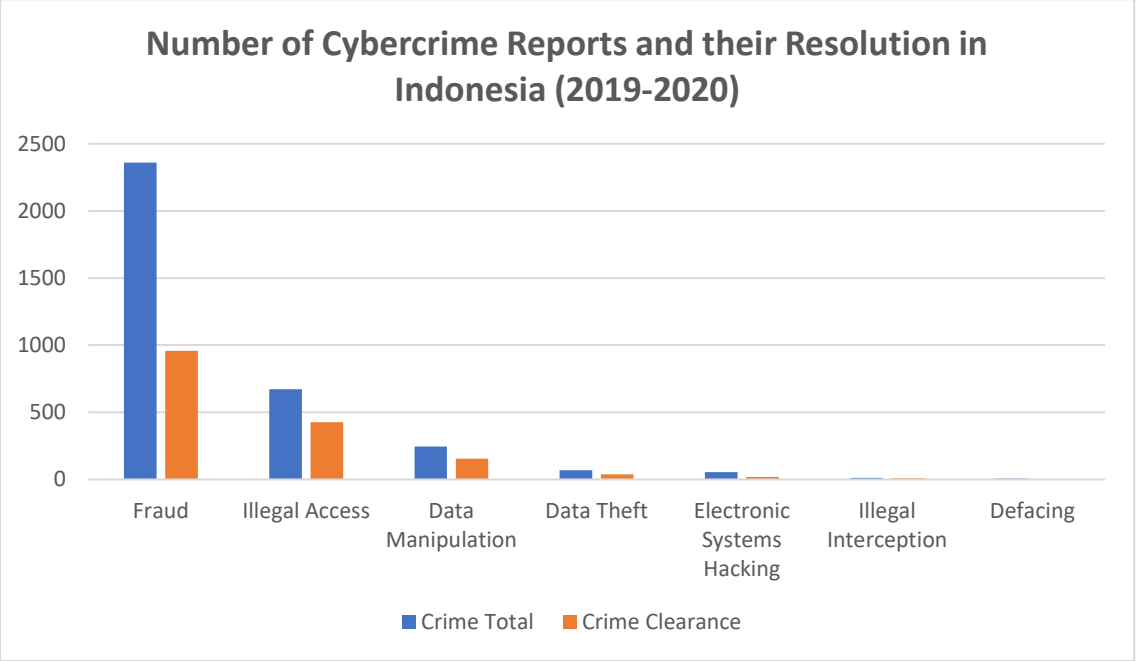

Figure 1. Number of Cybercrime Reports and Their Resolution in Indonesia

Based on the data above, we can see that the number of crime clearances is lower than the total crime, indicating that law enforcement in cyberspace has obstacles. According to Hendy Sumadi, the obstacles in overcoming cybercrime can be organized into several interrelated aspects. First, limited facilities and infrastructure in terms of technology and adequate human resources are the main obstacles. Police often face difficulties in accessing the tools and technology needed to identify and track increasingly sophisticated cybercriminals (Hounmenou & Toepp, 2023).

Apart from that, the lack of personnel who have special skills in cybercrime investigations is also a serious problem. Second, the lack of legal awareness among the public is a significant obstacle. Many individuals do not fully understand the legal implications of their online actions, and thus often avoid appropriate legal action. Broader and more effective

legal education can help overcome these obstacles and increase awareness about the consequences of cybercrime (Cheurprakobkit & Lerwongrat, 2023).

Therefore, the Police cannot be alone in handling criminal acts related to e-commerce transactions. In this case, strategic intelligence analysis plays an important role in efforts to handle security threats in electronic commerce transactions by the National Police. Strategic intelligence analysis helps the National Police identify, understand, and anticipate various forms of threats that may arise in the context of electronic commerce (Spagnoletti et al., 2021). The police have collaborated with the OJK to form a Task Force to monitor electronic transactions. Apart from that, the Police have collaborated with the Coordinating Ministry for Political, Legal, and Security Affairs to form the National Cyber Agency. Meanwhile, with external parties, the Police have collaborated with external parties such as Night Fury Operation to enforce laws related to criminal acts whose intellectual actors come from abroad (Tran & Chuang, 2020).

In this case, strategic intelligence analysis can be a component in the National Police's efforts to maintain the security of electronic commerce transactions. By involving data and information collected from various sources, the National Police can have a deeper understanding of existing threats. This includes not only cybercriminals but also terrorist groups and foreign entities that may have an interest in destabilizing electronic commerce in Indonesia (Dolata & Schwabe, 2023). In an ever-growing digital world, criminals continue to look for loopholes to launch attacks. By using various modus operandi that have developed over time. Therefore, the National Police needs to have an accurate view of how criminal acts operate, what they target, and what methods they use. This allows the National Police to formulate effective strategies to deal with these threats (Begovic et al., 2023).

In addition, intelligence analysis also allows the National Police to identify trends and patterns in cybercrime activity. In doing so, they can take preventive measures to reduce risks and protect digital infrastructure, sensitive data, and businesses involved in electronic transactions. The importance of intelligence analysis is not only limited to law enforcement but also to protecting the country's national and economic interests (Cascavilla et al., 2021). Collaboration with related institutions is also an important component of this effort. The National Police needs to share information and coordinate well with parties who have relevant knowledge and intelligence resources. This allows for fast and accurate exchange of information, which can be used for more efficient law enforcement actions.

B. LITERATURE REVIEW

1. Intelligence Analysis

According to Law no. 17 of 2011 concerning State Intelligence, "Intelligence is knowledge, organization and activities related to the formulation of policies, national strategies and decision making based on analysis of information and facts collected through work methods for detection and early warning in the context of preventing, deterring and overcoming any threats to national security" (Alzoubi & Aziz, 2021).

The process of obtaining data and presenting it in the form of intelligence products, of course, refers to the intelligence circle scheme. The intelligence circle is generally divided into 4 (four) main elements, namely planning/directing, collection (gathering information), analysis (processing and producing reports), and policy-making so that intelligence works in an information business (Demestichas & Daskalakis, 2020). Intelligence analysis about the creation of intelligence products is also very vulnerable to information shortcuts called heuristics, meaning mental shortcuts which can then lead to deviations. Heuristics are the fastest possible way for someone to solve a problem and make new decisions more quickly and efficiently but are not relevant and accurate (Jain et al., 2023).

According to Mc Dowell, Intelligence and analysis is a broader problem-solving process that involves data collection and analysis, interpretation, and speculative consideration of future developments, patterns, threats, risks, and opportunities. According to Mc Dowell, strategic intelligence analysis is a term used to describe types of intelligence and analytical practices (Kotsias et al., 2023). If all intelligence is concerned with analyzing problems so that forecasts can be made, then strategic intelligence takes on a certain aura, aiming to provide the type of analysis that is directly related to achieving overall strategic organizational, corporate, and government goals. The key definitions of strategic intelligence analysis are the depth of study, the development of futuristic and holistic explanations and projections, and the purpose of using analytical results as a basis for actively planning for the future (Chatterjee & Dethlefs, 2021).

2. Strategy Theory

According to Syafi'i Antonio, specifically, the strategy includes determining the company's mission, identifying organizational goals by considering external and internal factors, as well as designing specific policies and strategies to achieve these goals and ensuring their effective implementation. This aims to ensure that the main goals and objectives of the organization can be achieved successfully (Mio et al., 2022).

According to White, Strategy is an intellectual activity: it is a level of effort that commands military behavior that must provide some, at least, consequences dictated by the political foundations of the policy objectives. According to Bernard Brodie, the approach to strategy is very simple but important. Strategy is the study of 'how to do it', a guide to achieving something and doing it efficiently (Morgan-Owen, 2020).

Strategy as a support for improving the performance of an organization cannot be separated from the performance achieved by an organization and the behavior of the organization's members. In the context of POLRI's efforts to handle security threats in electronic commerce/e-commerce transactions, strategy theory is used to discuss the concept of strategy formulation; namely how POLRI as an organization identifies and plans the steps needed to formulate an effective strategy to protect electronic commerce transactions from various threats. Strategy theory can help analyze how the National Police formulates this strategy (Doz, 2020).

3. E-commerce

According to Hartman, Amir, E-commerce can be defined as an electronic business mechanism that focuses on individual business transactions that use the internet as a medium for exchanging goods or services. Such transactions can occur between two institutions (B-to-B) or between institutions and consumers directly (B-to-C). In other words, E-commerce involves buying, selling, or exchanging goods and services online between various parties, including companies and consumers (Xie & Wang, 2021).

Meanwhile, according to Wong, E-commerce is the process of buying selling, and marketing goods and services through electronic systems, such as radio, television, computer networks, or the internet. In other words, E-commerce involves trade transactions and promotion of products and services electronically through various electronic channels and media (Asbari, 2023).

Both definitions emphasize the use of electronic technology, such as computers and the internet, in carrying out various aspects of business, including sales, marketing, and providing information to consumers (Rauschnabel et al., 2022)

4. Cybercrime and Security Threats in E-commerce Transactions

Wahid defines cybercrime as all forms of using computer network devices to commit crimes that take advantage of the freedom of digital technology irresponsibly. Along with the rapid flow of developments in electronic commerce or e-commerce transactions, there are several main threats; including misuse of personal data which has the potential to occur due to the negligence of the community itself. For example, when someone downloads an application that requires a user to input personal data, this could create a chance that the data cannot be accounted for properly, thus potentially having a negative impact on the data owner (Akhuai et al., 2022).

There are several forms of threats to electronic commerce that generally occur frequently, including:

a. DoS and DDoS attacks
b. Hacking
c. Phishing
d. Malware
e. Social Engineering (Aslan et al., 2023)

C. METHOD

The research method used in this research is a descriptive qualitative approach. According to Creswell (2010), qualitative methodology is seen as a form of research that produces descriptive data obtained through information obtained from research subjects, complemented by data sourced from document studies. In this research, the data collection method used was an interview with the Head of Sub-Directorate 2 I Dittipidsiber Bareskrim POLRI, AKBP I Putu Bayu Pati, S.I.K., M.H. regarding POLRI's handling efforts in dealing with threats in electronic commerce transactions. Collecting data from interviews is a method used for research regarding strategic intelligence analysis by the National Police in monitoring e-commerce activities.

D. RESULT AND DISCUSSION

1. Vulnerabilities in Electronic Commerce Transactions

Electronic commerce transactions or e-commerce have become an integral part of our lives. The ease of shopping online and accessing a variety of products and services has changed the way we interact with businesses. However, behind the convenience and efficiency offered by e-commerce, there are several vulnerabilities that we need to consider seriously.

Security vulnerabilities in electronic commerce transactions are the most significant. Online fraud, data theft, and cyberattacks can threaten customers' personal and financial data. According to Subroto, the requirement for consumers to be able to make transactions in E-Commerce by handing over their data causes the vulnerability of personal data to be leaked, which of course will be detrimental to society.

E-commerce requires users to provide personal data, including name, address, credit card number, and more. This makes them vulnerable to data theft if security systems are inadequate. If customer data is stolen, the information can be used for fraudulent activities or fake identities. Apart from that, cyber-attacks, especially hacking, are one of the vulnerabilities in e-commerce platforms. Cybercriminals may try to trick users with phishing techniques, where they create fake websites that appear to be legitimate e-commerce sites to steal login or payment information. Additionally, man-in-the-middle attacks can intercept communications between customers and sellers, allowing attackers to access confidential information.

Cybercriminals often try to manipulate or exploit gaps in e-commerce security systems. This can include various types of fraud, such as stealing credit card information, accessing

illegal user accounts, or sending counterfeit products to customers. A discussion of security vulnerabilities in e-commerce provides an understanding that cybercriminals are continually evolving and refining their methods. This is why intelligence analysis is important. By collecting, analyzing, and understanding data related to cyber threats, e-commerce companies can gain deep insight into potential risks and weaknesses in their infrastructure.

2. Intelligence Resources

Cybercrime is the result of the phenomenon of globalization of crime, where crimes can be committed without any specific geographical or time limits. According to Muladi and Diah Sulistyani R.S., the rapid increase in transportation, communication, and modern information technology has created technological globalization which has a significant impact on the spread of crime globally (globalization of crime).

In dealing with cybercrime, a comprehensive approach is needed, both through criminal law aspects and criminal law channels. Crime prevention and control efforts are carried out through an integral approach that combines penal and non-penal policies. Although penal policies have several limitations and weaknesses, such as being pragmatic, and offender-oriented, tend to be more repressive, and require high-cost infrastructure. According to Hatta, tackling cybercrime is better done using non-penal policies that are preventive.

The National Police, as a law enforcement agency in Indonesia, has adopted a comprehensive strategy for dealing with cybercrime in electronic commerce (e-commerce) transactions. First of all, the National Police focuses on increasing intelligence capabilities to understand and identify crime patterns that develop in the digital world. By utilizing advanced technology, such as big data analysis and artificial intelligence, the National Police can effectively analyze electronic transaction data to detect suspicious activity.

According to Head of Unit 2 Sub-Directorate I Dittipidsiber Bareskrim POLRI, AKBP I Putu Bayu Pati, S.I.K., M.H. in an interview on November 15, 2023: *"In an effort to tackle cyber crime, DITTIPIDSIBER Bareskrim Polri has launched the website patrolsiber.id. This site is designed to receive online reports from the public as a cybercrime prevention measure. The main feature provided is LAPORKAN!, this allows people who are victims of cybercrime to submit information regarding the perpetrator, such as name, telephone number, account number, social media account, email, as well as providing a chronology of events and proof of transactions or evidence of the crime that occurred"*.

3. Website and Social Media Monitoring

The first stage of this process is data integration, where the information contained in the police report from the Dittipidsiber Subbagops Bareskrim Polri is effectively combined with public complaint reports submitted via the patrolsiber.id platform. This step provides a new dimension to the authorities' understanding of the cybercrime landscape by bringing together data from various sources.

Next, the analyst team uses various analytical tools and techniques to investigate the digital footprints and behavioral patterns of cyber criminals. By utilizing advanced technology, they can identify links between reported cases, identify attack patterns, and uncover potential groups or individuals behind the cybercrime.

The patrolsiber.id website not only functions as a forum for complaints but also as an information center that provides guidance to the public regarding good cyber security practices. Through educational campaigns and the information provided, it is hoped that the public will become more aware of the risks of cybercrime and take appropriate steps to protect themselves.

Identification of "primary keys" such as the perpetrator's cellphone number and account number is used to direct the investigation. If there are similar cellphone numbers or account

numbers in different reports, this can increase the effectiveness of the investigation. The Analyst Team can request an inspection of the registration and CDR (Call Data Record) of the cellphone number as well as carry out financial transaction analysis through PPATK regarding the account number used. The data integration process is still carried out manually, causing a lack of monitoring of completed case handling in the Polda and Polres areas.

The second step in online inquiry involves data visualization. This is the process used to define and analyze data requirements, with the main goal of communicating information clearly and efficiently through various visual forms such as tables, graphs, or link charts. According to Head of Unit 2 Sub-Directorate I Dittipidsiber Bareskrim POLRI, AKBP I Putu Bayu Pati, S.I.K., M.H. in an interview on November 15, 2023: *"Dittipidsiber Subdit III Analyst Team uses the I2 analyst notebook application to describe networks based on OSINT and SIGINT data such as CDR cellphone numbers. Until now, the data source for analysis and visualization is still done manually, so it's not optimal"*.

4. Inter-Agency Coordination

Another step taken by POLRI in its strategy to deal with the threat of crime in e-commerce is to design close collaboration with various related parties, including financial institutions, e-commerce companies, and other related government institutions. This collaboration is important for the rapid and accurate exchange of information, enabling more efficient arrests of e-commerce criminals. This collaboration also enables the implementation of preventive measures, such as increasing the security of online payment systems and protecting customer data.

Efforts to handle criminal acts in the financial services sector have become more integrated and effective through close collaboration between the Financial Services Authority (OJK) and the Indonesian National Police (POLRI). The signing of a Memorandum of Understanding (MoU) between these two institutions is a concrete step to implement Law Number 21 of 2011 concerning the Financial Services Authority (UU OJK). The OJK Law mandates the OJK to investigate criminal acts in the financial services sector, while still giving the Police the authority to carry out investigations in this field.

According to Head of Unit 2 Sub-Directorate I Dittipidsiber Bareskrim POLRI, AKBP I Putu Bayu Pati, S.I.K., M.H. in an interview on November 15, 2023: *"...We are working with other state agencies, the private sector, and other stakeholders to share information and gain a comprehensive understanding of security threats in the E-commerce sphere...."*.

Collaboration between the OJK and the National Police is not just a formal implementation of the OJK Law but also aims to achieve synergy in carrying out the mandate of the law. With the MoU, the two can coordinate effectively, utilize their respective expertise, and increase efficiency in handling criminal acts in the financial services sector.

However, handling crime is not only limited to the conventional realm. In facing technological developments and new trends, POLRI understands the importance of education and public awareness. Therefore, the National Police has set a strategic focus on educational campaigns, which aim to increase public understanding of the risks and tactics used by criminals in electronic transactions.

The importance of education and public awareness in the context of e-commerce crimes is not only recognized by the National Police but is also realized through collaboration with well-known universities such as the University of Indonesia (UI) and Gadjah Mada University (UGM), as well as other educational institutions. Together, they are working to create special curricula and modules that cover critical aspects such as cyber security, cyber law, and cybercrime.

This step not only covers customers, but also small and medium businesses which are often easy targets for e-commerce criminals. By building solid understanding among the public and business people, POLRI hopes to reduce the potential for fraud and protect stakeholders in the e-commerce environment. This initiative reflects POLRI's commitment to creating a strong and sustainable digital security ecosystem.

5. Training and Skills Development

According to Head of Unit 2 Sub-Directorate I Dittipidsiber Bareskrim POLRI, AKBP I Putu Bayu Pati, S.I.K., M.H. in an interview on November 15, 2023: *"The National Police has also strengthened a special investigation unit that focuses on e-commerce crimes. Members of this unit are equipped with specialized skills and knowledge to investigate complex cases involving high technology. This in-depth investigation allows the National Police to collect strong evidence and ensure that e-commerce criminals are arrested and prosecuted following applicable laws".*

The National Police also understands that success in overcoming e-commerce crime does not only depend on an active response to cases that occur but also on the ability to anticipate and identify potential new security risks that emerge along with technological developments. Therefore, the National Police proactively monitors technological developments and new trends in electronic commerce.

By actively engaging in understanding technological developments, the National Police can identify potential new security risks before they become real threats. This allows this institution to adapt strategies for handling e-commerce crimes quickly and effectively so that it remains relevant in facing the ever-growing challenges in the digital world.

6. Strategic Intelligence Analysis

Based on the description above, researchers carried out an analysis of POLRI's intelligence steps in carrying out efforts to deal with security threats in electronic trading transactions.

a. Planning/Directing:
   The National Police adopts a comprehensive approach to dealing with cybercrime in e-commerce transactions. The first focus is to improve intelligence capabilities to understand and identify crime patterns in the digital world. By using advanced technology such as big data analysis and artificial intelligence, the National Police can analyze electronic transaction data to detect suspicious activity.
b. Collection (Gathering Information):
   The National Police involves the public in efforts to prevent cybercrime through the website patrolsiber.id. This site allows the public to report cyber crimes and provide information regarding the perpetrators. Information received from the public is combined with police reports, creating a broader understanding of the cybercrime landscape.
c. Data Analysis:
   The analyst team at the National Police uses various analytical tools and techniques to investigate the digital traces and behavioral patterns of cyber criminals. They also perform data visualization to understand the relationship between reported cases and identify attack patterns. Even though the data integration process is still carried out manually, the National Police is trying to increase efficiency in data analysis.
d. Policy Making:
   The National Police plans close collaboration with various related parties, including financial institutions, e-commerce companies, and related government agencies. This

collaboration enables fast and accurate exchange of information, making it easier to catch e-commerce criminals. In addition, the National Police is focusing on educational campaigns and collaboration with educational institutions to increase public understanding of the risks of cybercrime.

E. CONCLUSION

Cybercrime is becoming increasingly relevant and complex along with the growth of electronic commerce, and therefore, the National Police needs to take comprehensive steps to address this threat. One of the key steps that the National Police can take is to strengthen cooperation with various related parties, including financial institutions, e-commerce companies, and related government agencies. This collaboration is key to the rapid and accurate exchange of information, enabling more efficient arrests of e-commerce criminals. This collaboration also enables the implementation of preventive measures, such as increasing the security of online payment systems and protecting customer data. Polri must ensure that this cooperation is strengthened through formal agreements and Memorandums of Understanding (MoUs) to ensure effective implementation. In addition, the National Police must continue to invest in advanced technology such as big data analysis and artificial intelligence. This allows them to conduct more effective data analysis, detect suspicious activity, and identify emerging crime patterns in the digital world. Automation of the data integration process should also be considered to increase efficiency in combining information from various sources. Overall, by taking these steps, the National Police can improve their ability to tackle cybercrime in e-commerce transactions. This not only protects society but also creates a more resilient and sustainable digital security ecosystem. The National Police continues to adapt to technological developments and new trends so that it remains effective in facing ever-growing threats.

REFERENCES

1. Akhuai, W., Nugraha, A. A., Lukitaningtyas, Y. K. R. D., Ridho, A., Wulansari, H., & Al Romadhona, R. A. (2022). Social Capital of Pancasila Education in Smart Education with Social Media in Cybercrime Prevention in the Industrial Revolution Era 4.0. *Jurnal Panjar: Pengabdian Bidang Pembelajaran*, *4*(2).
2. Alzoubi, H. M., & Aziz, R. (2021). Does emotional intelligence contribute to quality of strategic decisions? The mediating role of open innovation. *Journal of Open Innovation: Technology, Market, and Complexity*, *7*(2), 130.
3. Ariansyah, K., Sirait, E. R. E., Nugroho, B. A., & Suryanegara, M. (2021). Drivers of and barriers to e-commerce adoption in Indonesia: Individuals' perspectives and the implications. *Telecommunications Policy*, *45*(8), 102219.
4. Asbari, M. (2023). Scope of e-Business & e-Commerce to Business and Modern Life. *Journal of Information Systems and Management (JISMA)*, *2*(1), 33-38.
5. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.
6. Begovic, K., Al-Ali, A., & Malluhi, Q. (2023). Cryptographic ransomware encryption detection: Survey. *Computers & Security*, 103349.
7. Butt, U. A., Amin, R., Aldabbas, H., Mohan, S., Alouffi, B., & Ahmadian, A. (2023). Cloud-based email phishing attack using machine and deep learning algorithm. *Complex & Intelligent Systems*, *9*(3), 3043-3070.
8. Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security*, *105*, 102258.

9. Chatterjee, J., & Dethlefs, N. (2021). Scientometric review of artificial intelligence for operations & maintenance of wind turbines: The past, present and future. *Renewable and Sustainable Energy Reviews*, *144*, 111051.
10. Cheurprakobkit, S., & Lerwongrat, K. (2023). Criminal justice officials' attitudes towards addressing computer crimes in Thailand: Difficulties and recommendations. *Trends in Organized Crime*, 1-21.
11. Creswell, J. W. (2010). Research design pendekatan kualitatif, kuantitatif, dan mixed. *Yogyakarta: pustaka pelajar*.
12. Demestichas, K., & Daskalakis, E. (2020). Information and communication technology solutions for the circular economy. *Sustainability*, *12*(18), 7272.
13. Dolata, M., & Schwabe, G. (2023). Moving beyond privacy and airspace safety: Guidelines for just drones in policing. *Government Information Quarterly*, *40*(4), 101874.
14. Doz, Y. (2020). Fostering strategic agility: How individual executives and human resource practices contribute. *Human Resource Management Review*, *30*(1), 100693.
15. Hasbullah, M. A. (2022). Strategies and Best Practices Firms Should Adopt in Compliance with Business Competition Law: The Role of Cybercrime in Indonesian Perspective. *International Journal of Cyber Criminology*, *16*(2), 87-103.
16. Hounmenou, C., & Toepp, S. (2023). Exploring private investigation agencies' experience of collaboration with law enforcement in Investigations of human trafficking cases. *Societies*, *13*(2), 44.
17. Jain, J., Walia, N., Singla, H., Singh, S., Sood, K., & Grima, S. (2023). Heuristic Biases as Mental Shortcuts to Investment Decision-Making: A Mediation Analysis of Risk Perception. *Risks*, *11*(4), 72.
18. Kotsias, J., Ahmad, A., & Scheepers, R. (2023). Adopting and integrating cyber-threat intelligence in a commercial organisation. *European Journal of Information Systems*, *32*(1), 35-51.
19. Maskuroh, N., Fahlevi, M., Irma, D., Rita, R., & Rabiah, A. (2022). Social media as a bridge to e-commerce adoption in Indonesia: A research framework for repurchase intention. *International Journal of Data and Network Science*, *6*(1), 107-114.
20. Mio, C., Costantini, A., & Panfilo, S. (2022). Performance measurement tools for sustainable business: A systematic literature review on the sustainability balanced scorecard use. *Corporate social responsibility and environmental management*, *29*(2), 367-384.
21. Morgan-Owen, D. G. (2020). History and the perils of grand strategy. *The Journal of Modern History*, *92*(2), 351-385.
22. Rauschnabel, P. A., Babin, B. J., tom Dieck, M. C., Krey, N., & Jung, T. (2022). What is augmented reality marketing? Its definition, complexity, and future. *Journal of business research*, *142*, 1140-1150.
23. Schwob, A., de Kervenoael, R., Kirova, V., & Vo-Thanh, T. (2023). Casual selling practice: a qualitative study of non-professional sellers' involvement on C2C social commerce platforms. *Information Technology & People*, *36*(2), 940-965.
24. Spagnoletti, P., Ceci, F., & Bygstad, B. (2021). Online black-markets: An investigation of a digital infrastructure in the dark. *Information Systems Frontiers*, 1-16.
25. Tran, E., & Chuang, Y. H. (2020). Social relays of China's power projection? Overseas Chinese collective actions for security in France. *International Migration*, *58*(3), 101-117.
26. Xiao, L., Cheng, X., & Mou, J. (2022). Understanding global e-commerce development during the COVID-19 pandemic: Technology-Organization-Environment perspective. *Journal of Global Information Technology Management*, *25*(1), 1-6.

27. Xie, J., & Wang, L. (2021). Collaborative innovation of E-Commerce enterprises based on FPGA and convolutional neural network. *Microprocessors and Microsystems*, *80*, 103595.