Volume 6 Number 1 (2024)
January-June 2024
Page: 87-98

E-ISSN: 2686-4819
P-ISSN: 2686-1607
DOI: 10.37680/almanhaj.v6i1.4674

AL-MANHAJ
Jurnal Hukum dan Pranata Sosial Islam

Potential Cybercrime and Prevention in the Overseas Official Travel Approval Letter

Aas Rohmat[1], Hanuring Ayu Ardhiani Putri[2], Muhammad Muhtarom[3], Ismiyanto[4], Anies Fortina Febriani[5]

[1] Universitas Islam Batik, Surakarta, Indonesia; aasrohmat@gmail.com
[2] Universitas Islam Batik, Surakarta, Indonesia; Hanuringayu@gmail.com
[3] Universitas Islam Batik, Surakarta, Indonesia; mmmuhtarom@gmail.com
[4] Universitas Islam Batik, Surakarta, Indonesia; ismiyanto@student.uns.ac.id
[5] Universitas Sebelas Maret, Surakarta, Indonesia; aniesfortina@staff.uns.ac.id

Received: 05/11/2023 Revised: 28/01/2024 Accepted: 14/03/2024

Abstract

The aim of this research is to the potential for cybercrime and its prevention in foreign official travel approval letters. The research method used is normative juridical. The data collection technique is library research. The data analysis technique is descriptive qualitative which is used in the form of an interactive analysis model. The research results show that the potential for cybercrime in foreign official travel approval letters includes hacking, identity theft, data breaches, phishing, spamming, cyber vandalism, virus writers, XML injection, security configuration errors. To prevent cybercrime, the simple web application or https://simpel.setneg.go.id has data security, namely security testing by the state cyber and password agency, a captcha feature on the simple web, one time password feature on simple phones, application of certified digital signatures. The conclusion of this research is that the potential for cybercrime in overseas official travel approval letters is increasing. Prevention solutions can include educating users, using a hacker perspective, patch systems, policies, Intrusion Detection Systems bundled with Intrusion Prevention Systems, antivirus firewalls. Legal regulatory steps to support the implementation of cybercrime prevention solutions, namely Law No. 11 of 2008 concerning ITE and PP No. 82 of 2012 concerning the implementation of Electronic Systems and Transactions.

-Keywords Potency; Cyber Crime; Prevention; Approval letter; Overseas Service Travel

Corresponding Author
Aas Rohmat
Universitas Islam Batik, Surakarta, Indonesia; aasrohmat@gmail.com

1. INTRODUCTION

Cybercrime is an illegal criminal act and dangerous behavior involving the internet computer of Information Communication Technology that function as tools, targets or places where crimes occur. As an emerging social phenomenon in the information age, cybercrime has raised concerns throughout the world due to its high destructive power and widespread influence. Trust fraud, identity fraud, and other types of cybercrime are among them (Widijowati, 2022). Although computers or computer networks are the main components of cybercrime, it describes a more conventional criminal act in which

a computer or computer network is used to assist or enable the commission of a crime (Sumadinata, 2023).

The rapid development of ICT has become increasingly significant as well as the number of criminal acts. The government shows evidence of losses due to cybercrime (Widijowati, 2022). According to statistical data from *We Are Social and Hootsuite*, 5.07 billion people globally, or around 63.45% of the total world population of 7.99 billion people, are internet users as of October 2022 (Hardinato & Tata, 2023). The Internet facilitates or is necessary for almost all modern jobs. All computers in the world are connected via the internet, a worldwide network for communication, although using various hardware and operating systems (Hardinato & Tata, 2023).

Web-based applications are one way to use the internet. One of the main aspects of using web applications is how simple it is to get information from anywhere in the world via the internet (Styaningsih et al., 2023). Web servers and web pages form the two main parts of most web-based application systems. The most popular web server application according to Netcraft until December 2022 is Apache (Hardinato & Tata, 2023). Current advances in information technology seem to have two sides because apart from advancing human progress, prosperity, and civilization, they can also pose risks to the security of personal data (Nguyen, 2023).

The main targets of cybercrime attacks are institutions in the financial sector, transportation companies, IT companies, entertainment, health services, and government institutions based on statistical data published by Positive Technology in 2023. The National Cyber Security Agency Center through the National Cyber and Crypto Agency stated that the majority of cyber crime attacks in Indonesia target web applications, especially government sites (Sumadinata, 2023). Cybercrime via web applications is becoming more frequent and increasing every year. Web application security is a top priority for every individual, organization, or institution, especially web application users (Sumadinata, 2023).

Overseas Service Trips are assignments carried out by State Officials, Other Officials, Civil Servants, BUMN/BUMD Employees, or Indonesian Personnel given by State Institutions or Government Agencies, to carry out activities abroad at State expense (APBN/APBD), foreign/domestic donors, or at their own expense and who has undertaken an official trip abroad is required to make a written report regarding the implementation of their duties, by the provisions stated in the approval letter. Overseas official travel is carried out by an employee or employee of an institution or company related to official work duties. The use of Foreign Service Approval includes the legal basis for assignments, requirements for processing official passports, exit permits, and recommendations for service visas. The basis for providing facilitation for the payment of income tax for individuals who will depart abroad (fiscal) with applicable provisions, completeness of financial accountability

administration. Categories of types of overseas official travel letters are new applications, extensions, corrections, and cancellations (Qohary & Inarto, 2021).

The Foreign Cooperation Bureau is a focal point in the Ministry of Education, Culture, Research and Technology which has the task of processing every application submitted by each work unit within the Ministry of Education, Culture, Research and Technology. In implementing the administration process for approval letters for overseas official travel, the Foreign Cooperation Bureau coordinates with the Ministry of State Secretariat and the Ministry of Foreign Affairs, where both ministries have applications to simplify and speed up the process of overseas official travel. In line with this, the Ministry of Education, Culture, Research and Technology has an overseas official travel application that can be integrated with existing applications in the ministry (Megandi et al., 2023).

Submitting a letter of approval for an overseas official trip, several document requirements must be met by employees who will undertake an overseas official trip (Rohmat & Elisanti, 2021). In the implementation of approval for overseas official travel, problems often occur including incomplete overseas official travel documents, late submission of physical documents, and documents given to the focal point are illegible, resulting in delays in the process of applying for external service to the Ministry of State Secretariat and the Ministry of Foreign Affairs (Megandi et al. al., 2023).

The Foreign Cooperation Bureau already has the e-PDLN application, an information system service for Overseas Official Travel, to facilitate the submission of administrative documents for overseas official travel in the electronic delivery system for overseas official travel documents. The web-based external official travel administration system (e-PDLN) in the Administration Sub-Section of the Foreign Cooperation Bureau can simplify and speed up the process of administering approval letters for external official travel. The development of the e-PDLN application is not only limited to the administration mechanism for overseas official travel but is an effort to simplify the overseas official travel process. It is hoped that the existence of the SIMPLE web application will make it easier for PDLN service users to submit requests for official travel abroad and of course can improve services for handling official travel administration more quickly, precisely, transparently, and accountably (Pratama, 2018).

The main features in the overseas official travel information system application are login module, application in process, application approved, application returned, application archive, assignment results report, and helpdesk. The SIMPEL application is used in the process of overseas official travel using of a login module where the user can log in with a username in the form of a registered email and a password that has been previously set according to the user's wishes. Applications in the process contain applications with status in the state secretariat process along with details of the application. Users can click on the application if they want to see the details. Contains an application with approved

status along with details of the application. Users can click on the application if they want to see the details.

This approved application also has a Download Approval Letter and Assignment Results Report feature. If the user chooses to download the approval letter, the approval letter file in PDF format will automatically be downloaded to the user's device. When an overseas official trip has been carried out, users can report the results of their official trip. This feature contains requests that are returned as shown in the screenshot. This module is used to view details of PDLN applications that have been archived. This feature is used to submit assignment results reports, in the form of substance reports, financial realization reports, and document uploads. An overseas official trip can be carried out by several participants who are members of one group. The Assignment Results Report can be filled in by one of the participants in the group. This Helpdesk menu is connected to the State Secretariat Web link.

The potential for cybercrime in the e-PDLN application, a website-based external official travel information system service on external official travel approval letters, is very possible. Several things that need to be studied about the emergence of applications (software) which are becoming more sophisticated day by day are related to privacy in cyberspace, including protection from spying, protection of personal data, and positional privacy. Every agreement regarding automatic downloads has provided an opening for application owners to hack personal data or track the whereabouts of application downloaders (Mohd. Yusuf DM et al., 2022).

The research aims to determine the potential for cybercrime and its prevention in approval letters for overseas official travel. Researchers chose this topic because this topic is very urgent to research regarding the increasing number of cybercrime problems and to provide solutions related to potential cybercrime problems in the SIMPLE application in overseas official travel application letters. Regulatory policies support the implementation of cybercrime prevention solutions.

Several countries have long paid more attention to the security of data in cyberspace. The implementation of these concerns is contained in national regulations related to information technology. Indonesia stipulates all rights and obligations related to cyber law in Law Number 19 of 2016 concerning Electronic Information and Transactions, abbreviated as the ITE Law (Nugraha, 2021). National legal regulations, bilateral agreements, and international legal regulations related to data are expected to be able to overcome problems related to the privacy aspects of potential cybercrime and prevention of cyber crime in foreign official travel approval letters (Destyarini et al., 2023; Dewi, 2022).

This research contributes to existing literature related to cybercrime as well as to the wider community with solutions to preventing cyber crime. Legal regulatory policies and also legal certainty regarding cybercrimes. Many criminal acts related specifically to cyber crimes carried out using cyber internet technology are closely related to the SIMPEL application system in the process of overseas

official travel which needs to be studied further. This research is important to carry out with the title "Potential Cybercrime and its Prevention in Approval Letters for Overseas Official Travel".

2. METHOD

The research method used is normative juridical. This type of secondary data comes from data that has been documented in the form of legal materials. The data collection technique is library research. Data collection will be carried out through library research collected through library research, namely by studying the provisions of the law regarding the analysis of potential cybercrime and its prevention in overseas official travel documents. All data collected is analyzed using interpretation techniques and then interpreted and described descriptively in accordance with the cases studied with the provisions of relevant laws and regulations and theories.

3. FINDINGS AND DISCUSSION

3.1. Potential for cybercrime in the approval letter for overseas official travel.

Cybercrime is a criminal activity in which a computer or computer network becomes a tool, target, or place of crime. As has been mentioned, cybercrime emerged along with the increasing intensity of digital, communication and information technology. Cybercrime is an unlawful act carried out using internet access which is based on sophisticated computer and telecommunications technology (Pervaiz et al., 2023). Analysis of the potential for cybercrime on the e-PDLN application, website-based Overseas Official Travel information system service on approval letters for overseas official travel is very likely to occur. The increasing development of cybercrime is now not limited to illegal access (Sabillon et al., 2016). Some potential cyber crimes in overseas official travel approval letters through the Overseas Official Travel information system service application in the form of SIMPLE or https://simpel.setneg.go.id are as follows:

Hacking is the activity of breaking into someone else's computer program. Most of the online activities of hackers are legal and illegal. Hacking becomes illegal once it is used for unauthorized access to a computer system (Artikov, 2021). Ilegal hacking activities are usually part of organized crime networks, with specific motives and a high level of sophistication (Suci Meinarni & Sari, 2020). There are many categories of hackers, these categories include different terminology and iconography which gives rise to controversy over the term computer attacker. The media and general public call the people responsible for attacking and destroying computer systems hackers (Wijoseno & Widhiyaastuti, 2023). A hacker is someone who likes computer exploration, has the skills to create and read certain programs, and is obsessed with monitoring security. There are 2 categories of hackers, namely White Hat and Black Hat.

1. White Hat Hackers are individuals with hacking skills who act to protect a network in a defensive manner. They work in a corporate environment as security. Notify the admin whose computer has been breached, that there are weaknesses in the program they own and have the potential to be compromised. The characteristics of white hat hackers are providing non-destructive information that will definitely benefit/help the victim.
2. Black Hat Hackers are individuals who break into other people's programs to damage, manipulate/alter, and steal their data. Hackers with extraordinary computing skills who are interested in malicious activities. Their motives are to cause damage, steal information, destroy data, and make money. The characteristic of Black Hat Hackers is that they carry out criminal activities that will harm their victims (Sabillon et al., 2016).

Identity theft or identity theft is a cybercrime crime of stealing someone's identity. An attacker pretends to be a different person to gain financial gain. Identity theft leads to identity fraud that exploits crimes such as financial identity theft, business identity theft, and criminal identity theft (Wijoseno & Widhiyaastuti, 2023). A data breach is the disclosure of data or information that violates confidentiality leading to distribution in the public domain. Leaks can occur by insider agents or hacker attacks. Damage can affect or trigger a company's reputation, financial losses, lawsuits, stock prices, fraud, and physical assets (Sabillon et al., 2016).

Phishing is the activity of luring internet users in the hope that the user will unconsciously provide user data and password information on a website that has been defaced. Fraudulent processes that steal confidential information from end users. Phishing usually involves using fake websites. Phishers configure universal man-in-the-middle phishing kits to enable real-time URLs that interact with valid websites (Hermawan, 2013). Spamming is the sending of unwanted news messages, images, and advertisements via electronic mail (e-mail), search engines, instant messages (IM), and smartphones. Spammers use botnets and virus-infected networks to distribute spam. However, many people are also affected and become victims (Wijoseno & Widhiyaastuti, 2023).

Cybervandalism is vandalism that occurs using computer technology. The most common attacks are website defacement, data deletion malware, DDoS, and social media account hijacking (Sabillon et al., 2016). Virus Writers are a group that tends to exploit weaknesses found by hackers, then code methods to execute computer weaknesses. XML injection: eXtensible Markup Language injection attacks are similar to SQL injection attacks. The primary vulnerabilities include code insertion to enter or export database data. Additionally, the XML query language XPath can be included using query statements for data retrieval or modification (Sabillon et al., 2016). Security misconfiguration is where web applications are often deployed by utilizing incorrect, default, or compromised configurations to access systems, networks, computers, servers, mobile devices, or interconnect devices that may have

security holes. System managers who do not change the default configuration can open vulnerabilities to hackers (Wijoseno & Widhiyaastuti, 2023).

Legal aspects can be used to overcome and prevent potential cybercrimes, which requires cyber law. Cyber Law is a legal aspect whose term comes from Cyberspace Law, the scope of which covers every aspect related to individuals or legal subjects who use and utilize internet/electronic technology starting when they go "online" and enter the cyber world. Cyber Law in Indonesia related to cyber crime is Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE).

Legal concepts used in discussing potential cybercrime crimes. Law is a system created to limit human behavior so that human behavior can be controlled. Law is certain written or unwritten rules or provisions that regulate people's lives and provide sanctions for violators. The law functions to protect the interests of internet service users and take firm action against perpetrators of cyber crime. The government needs to enact Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, which monitors blocking fraud sites and designs a good system to protect the public from the threat of cybercrime.

3.2. Prevention of cyber crimes in foreign official travel approval letters.

Submission of Official Travel Approval Letters which used to be manually changed to an electronic process. SIMPLE application that is not limited to the process of digitizing work mechanisms. SIMPLE is an online licensing web application built to improve the quality of public services in the issuance of government approval letters for overseas official travel (PDLN) carried out by State Officials, other Officials, Civil Servants, BUMN/BUMD Employees, and Indonesian Personnel assigned by State Institutions or Government Agencies, funded by APBN/APBD or by technical cooperation partners. The SIMPEL Mobile application can also be downloaded via the Android Play Store and iOS App Store. In the future, the SIMPEL application will continue to be developed to improve the quality and governance of overseas official travel licensing services.

It is hoped that the SIMPLE web application can make it easier for PDLN service users to submit requests for overseas official travel and of course can improve the service for handling official travel administration more quickly, precisely, transparently and accountably. The approval letter for overseas official travel uses the Overseas Official Travel information system service application in the form of SIMPLE or https://simpel.setneg.go.id which has been created by the Ministry of State Secretary. Simple data in there is a database, namely 1) Data Base of list of officials/employees of all K/Ls, 2) Data Base of PDLN reports for all K/Ls, 3) Data Base of PDLN budget usage.

Various technological products such as computers, for example, have been used as media for global information purposes, and these technological products also facilitate the rise of cybercrime (Wu et al.,

2023). Cybercrime takes quite several victims, especially from a personal and financial perspective. Most victims can only regret what happened. They hope to learn a lot from their experience. What needs to be done now is to prevent possibilities that could harm us as IT practitioners (Hall & Ziemer, 2023). Cybercrime is a complex and external phenomenon, the proliferation of mobile devices, Wi-Fi networks, and the openness of the internet has increased the expansion of cyber attacks, cybercrime, and cyber victimization (Sugiarto & Qurratulaini, 2020).

Prevention of cybercrime attacks on foreign service approval letters for web applications used by a website that is the target of attacks (Agung et al., 2022). The SIMPLE web application or https://simpel.setneg.go.id is an external official travel information service. The SIMPLE web application or https://simpel.setneg.go.id contains Security Data, namely 1) Security Test by the National Cyber and Crypto Agency, 2) Captcha feature on SIMPEL Web, 3) One Time Password (OTP) feature on SIMPEL Mobile , 4) Implementation of Certified Digital Signature.

Cybercrime prevention can take the form of:

1. Educate User (providing new knowledge about Cybercrime and the internet world)
2. Use hacker's perspective (using thinking from the hacker's side to protect your system)
3. Patch System (covers weaknesses in the system)
4. Policy (determines policies and rules that protect your system from unauthorized people)
5. IDS (Intrusion Detection System) bundled with IPS (Intrusion Prevention System)
6. AntiVirus Firewall.

Cybercrime security prevention efforts are mainly focused on implementing technical approaches such as Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), firewalls, and anti-virus software to reduce the threat of cyber attacks (Agung et al., 2022). This is in accordance with research studies that show that these methods can help to some extent reduce the adverse impact of cybercrime on both organizations and individuals (Mohd. Yusuf DM et al., 2022).

Protective prevention against cybercrime begins with taking personal measures for protection and then escalates to the organizational, societal, corporate, national, military, and international levels (Artikov, 2021). Deep cybersecurity defenses at all levels will minimize, prevent, and slow cyber attacks. (Sumadinata, 2023). The creation of national governance to combat cybercrime, international cooperation to prosecute cyber criminals, strengthening laws for prosecution, additional academic research, and a participating cyber security industry are just some of the areas that need improvement (Rosy, 2020) .

Solutions for preventing cyber crimes in foreign official travel approval letters include:

1. User education

   User education is still lacking and there is a lack of human resources (HR). Public education and literacy regarding cyber needs to be improved. To be smarter in using information and communication technology. Minimizing the occurrence of cyber crimes such as *hacking, phishing, identity theft, cybervandalism.* The education and literacy provided must be easily understood by the public so that cyber crimes do not occur again in the future.

2. System Mapping

   Crime system mapping is used by analysts in law enforcement agencies to map, visualize, and analyze crime incident patterns. Key components of CompStat crime analysis and policing strategies. Mapping crime using geographic information systems (GIS) allows crime analysts to identify crime hot spots along with trends and patterns.

3. Policy

   National positive legal instrument legal policy related to the use of information technology in Indonesia Law no. 11 of 2008 concerning Information and Electronic Transactions (UU ITE) as the first legal umbrella to regulate the cyber world (cyberlaw) and regulate actions committed in cyberspace as criminal acts.

4. Governance and technology are related to legal principles that apply to crime prevention. The approach to governance and information security technology, the approach is carried out through an information security management system as well as through a technological approach that is careful, accurate, and up-to-date to close every loophole that can be used to carry out attacks in the cyber world.

Law No. 11 of 2008 concerning the ITE Law and PP No. 82 of 2012 concerning the Implementation of Electronic Systems and Transactions, one of which is policies and regulations in the field of information security to support the implementation of cyber crime prevention solutions.

4. CONCLUSION

Based on the findings of the research study, it was concluded that the potential for cybercrime in approval letters for overseas official travel through the Overseas Official Travel information system service application in the form of SIMPLE or https://simpel.setneg.go.id includes hacking, identity theft, data breach, phishing, spamming, cybervandalism, virus writers, XML injection, security misconfiguration. Prevention of cyber crime in external service approval letters, namely Data Security, namely 1) Security Test by the National Cyber and Crypto Agency, 2) Captcha feature on SIMPEL Web, 3) One Time Password (OTP) feature on SIMPEL Mobile. 4) The application of Certified Digital

Signature in preventing cybercrime can take the form of preventing it by educating users, using a hacker's perspective, patch system, policy, IDS (Intrusion Detection System) bundled with IPS (Intrusion Prevention System), antivirus firewall. The suggestion from this research is that cyber crimes in the e-PDLN application, website-based external official travel information system services on external official travel approval letters must be handled immediately. Preventive protection against cybercrime begins with taking personal action for protection and then escalates to the organizational, societal, corporate or institutional, national, military and international levels. The government is increasing cooperation between countries, both bilaterally, regionally, and multilaterally, in efforts to handle and prevent cybercrime. Carrying out intensive outreach to organizations, communities, companies or institutions that use the e-PDLN application, website-based external official travel information system services on approval letters for external official travel specifically for preventing or dealing with cybercrime. Legal or regulatory steps to support the implementation of cyber crime prevention solutions, namely Law No. 11 of 2008 concerning ITE and PP No. 82 of 2012 concerning Implementation of Electronic Systems and Transactions.

REFERENCES

Agung, A., Hafrida, H., & Erwin, E. (2022). Crime Prevention Against Cybercrime. *PAMPAS : Journal Of Criminal Justice* , *3* (2), 212–222.

Artikov, A. K. (2021). Cybercrime As a Threat To Public Safety. *Texas Journal of Multidisciplinary Studies* , *1* , 171–178. https://doi.org/10.31085/2310-8681-2021-1-204-171-178

Destyarini, N., Prastyanti, RA, & Elisanti, E. (2023). Legal Study of Kradenan Village Regulations, Kaliwungu District, Semarang Regency No. 11 of 2022 concerning Village Market Levies. *Al-Manhaj: Journal of Islamic Law and Social Institutions* , *5* (2), 2093–2114. https://doi.org/10.37680/almanhaj.v5i2.3088

Dewi, MC (2022). Cyber Espionage in National and Global Perspective: How does Indonesia Deal with this issue? *International Law Discourse in Southeast Asia* , *1* (1), 1–22. https://doi.org/10.15294/ildisea.v1i1.56874

Hall, T., & Ziemer, U. (2023). Exploring the relationship between IT development, poverty and cybercrime : an Armenian case study. *Journal of Cyber Policy ISSN:* , *7* (3), 353–374. https://doi.org/10.1080/23738871.2023.2192234

Hardinato, H., & Tata, S. (2023). Analysis of Cyber Crime handling in Web Applications with WAF ModSecurity. *PETIR: Journal of the Study and Application of Informatics Engineering* , *16* (1), 91–99.

Hermawan, R. (2013). Readiness of Government Apparatus in Facing Cyber Crime in Indonesia. *Journal of Information Engineering* , *6* (1), 43–50.

Megandi, M., Susanty, M., & Setiawan, E. (2023). Classification of Business Travel Expenditure Items Using Recurrent Neural Network and Long Short-Term Memory. *PETIR: Journal of the Study and Application of Informatics Engineering* , *16* (1), 11–18.

Mohd. Yusuf DM, Vivi Yola, Destin Maiharani, & Egi Dwi. (2022). Analysis of Modes in Cyber Crime Law. *Journal of Law, Politics And Social Sciences* , *1* (2), 64–70. https://doi.org/10.55606/jhpis.v1i2.725

Nguyen, N.T. (2023). A Review Of Cyber Crime. *Journal Of Social Review and Development* , *2* (1), 1–3. https://dzarc.com/social/article/view/244/230

Nugraha, R. (2021). Indonesian Legal Perspective (Cyberlaw) Handling Cyber Cases in Indonesia. *Scientific Journal of Aerospace Law* , *11* (2), 44–56.

Pervaiz, H.S., Bhatti, S.H., Words, K., Security, C., Assets, C., Technologies, N., Network, S., & Pervaiz, H.S. (2023). Analysis of Cybercrime Regulations Falling behind New Technologies. *Journal of Social Sciences Review (JSSR)* , *3* (1), 460–469.

Pratama, RH (2018). Analysis of the Information System for Payment of Official Travel Expenses at the Soekarno Hatta Type C Customs and Excise Main Service Office. *Substance: Article Source Accounting Auditing and Vocational Finance* , *2* (1), 77. https://doi.org/10.35837/subs.v2i1.274

Qohary, Y., & Inarto, A. (2021). Overseas Official Travel Management at the Maritime and Fisheries Research and Human Resources Agency. *Journal of Business Administration Economics & Entrepreneurship* , *3* (1), 9–21.

Rohmat, A., & Elisanti, E. (2021). Analysis of Public Services to Bureaucracy Changes in the Covid-19 Pandemic Era. *Public Spirit: Journal of Public Administration* , *16* (2), 161. https://doi.org/10.20961/sp.v16i2.52390

Rosy, A. F. (2020). Indonesian International Cooperation: Strengthening National Security in the Field of Cyber Security. *Journal of Government Science (GovSci) : Journal of Government Studies* , *1* (2), 118–129. https://doi.org/10.54144/govsci.v1i2.12

Sabillon, R., Cano, J., Cavaller, V., & Serra, J. (2016). Cybercrime and Cybercriminals: A Comprehensive Study. *International Journal of Computer Networks and Communications Security* , *4* (6), 165–176. www.ijcncs.org

Styaningsih, RU, Destyarini, N., Aryono, A., & Elisanti, E. (2023). Implementation of Village-Owned Wealth Management as Mandated in Article 77 Paragraph (1) of Law Number 6 of 2014. *AL-MANHAJ: Journal of Islamic Law and Social Institutions* , *5* (2), 2205–2224. https://doi.org/10.37680/almanhaj.v5i2.3478

Suci Meinarni, NP, & Sari, HB (2020). Analysis of Potential Crime in Cyberspace Related to Data. *Kertha Wicaksana* , *14* (April 2019), 9–15.

Sugiarto, S., & Qurratulaini, R. (2020). Criminal Potential of Cyber Crime in Memes: A Forensic

Linguistic Study. *Deiksis: Journal of Indonesian Language and Literature Education* , *7* (1), 46. https://doi.org/10.33603/deiksis.v7i1.2495

Sumadinata, WS (2023). Cybercrime And Global Security Threats : A Challenge In International Law. *Russian Law Journal* , *XI* (3), 438–444.

Widijowati, RD (2022). Analysis of the Development of Cyber Crime in Indonesia. *International Journal of Artificial Intelligence Research* , *6* (1), 1–8.

Wijoseno, BA, & Widhiyaastuti, IGAAD (2023). Criminal Traps Against Perpetrators of Illegal Hacking of Computer Systems (Hackers) from the Perspective of Indonesian Criminal Law. *Kertha Desa Journal* , *11* (3), 2031–2041.

Wu, L., Peng, Q., & Lemke, M. (2023). Research Trends in Cybercrime and Cybersecurity : A Review Based on Web of Science Core Collection Database Research Trends in Cybercrime and Cybersecurity : A Review Based on Web of Science Core Collection Database. *International Journal of Cybersecurity Intelligence and Cybercrime* , *6* (1), 5–28.