ASIAN DIGITAL GOVERNANCE PROBLEMS

e-ISSN 3048-0868 (online)

Volume 1, Issue 1 2024
Page 10-21

https://doi.org/10.71435/639167

Overcoming Security Challenges in Digital Government in West Papua

Ayu Sita Maharani[1]

[1]Department of Public Administration, Faculty of Social and Political Sciences, Universitas Papua, Manokwari, Indonesia

ARTICLE INFO

Received: 11 February 2024
Revised: 24 February 2024
Accepted: 19 March 2024
Available online: 22 March 2024

Keywords:
Digital Government
Security Challenges
West Papua
Quantitative Method
Government Employees

Corresponding Author:
Ayu Sita Maharani

Email:
ayusitamaharani@gmail.com

ABSTRACT

***Purpose**: This research aims to identify and analyze the security challenges faced by digital government initiatives in West Papua, Indonesia*

***Subjects and Methods:** The study employs a quantitative method, conducting surveys among government employees involved in digital transformation projects.*

***Results:** The results of the analysis indicate that there is still a low level of awareness and understanding of digital security among government employees in West Papua. These findings highlight the importance of increasing awareness and training on digital security for government employees involved in digital government initiatives.*

***Conclusions:** The conclusion of this research is the highlight several key findings regarding cybersecurity in digital governance in West Papua. There is a significant need for increased cybersecurity awareness and education, as well as greater investment in cybersecurity infrastructure and resources.*

INTRODUCTION

The advancement of information and communication technology has transformed how governments interact with citizens and provide public services. Digital governance has become a new paradigm that demands the integration of technology in governance to enhance efficiency, transparency, and public participation. However, like other technological advancements, digital governance also faces complex and evolving security challenges. In research by Malodia et al. (2021), digital government initiatives have become increasingly prevalent worldwide, offering government new avenues to enhance service delivery and engage with citizens. In Indonesia, these initiatives have gained momentum, aiming to improve governance and public service efficiency. However, the adoption of digital technologies in government processes also brings forth various challenges, especially concerning security (Toufaily et al., 2021). West Papua, a province in Indonesia with unique geographical and socio-political characteristics, faces its own set of challenges in implementing digital government securely (Christawan et al., 2023).

According by Skouby et al. (2022), security issues in West Papua's digital government initiatives encompass a wide array of concerns, including cybersecurity threats and data privacy issues. The region's remote and rugged terrain, coupled with limited infrastructure, further complicates efforts to secure digital systems and networks (Chaoub et al., 2021). Cyberattacks targeting government systems could disrupt services, compromise sensitive information, and undermine public trust in the government's digital initiatives (Lehto, 2022). West Papua, as a region with unique geographical and social challenges, has its own needs in addressing digital security challenges, according by Caraka et al. (2020). Factors such as limited infrastructure, lack of awareness about the importance of information security, and efforts from irresponsible parties to disrupt digital governance systems further add to the complexity of security issues in this region (Ksibi et al., 2023).

This research aims to address these security challenges by focusing on a quantitative analysis of the issues faced by digital government initiatives in West Papua. By employing a quantitative research method, this study seeks to provide a comprehensive understanding of the security landscape and offer recommendations to enhance security measures (Putro et al., 2023). Through surveys conducted among government employees involved in digital transformation projects, the research aims to gather insights into the perceptions and experiences related to digital security (Kraus et al., 2021). The quantitative approach adopted in this research allows for a systematic analysis of the security challenges faced by digital government initiatives in West Papua (Budi et al., 2020). By collecting and analyzing data from a large sample size, the study aims to identify trends, patterns, and critical issues that need to be addressed, according by Debrah et al. (2022). Additionally, the research intends to provide evidence-based recommendations to strengthen the security posture of digital government initiatives in West Papua.

The findings of this research are expected to contribute to the existing body of knowledge on digital governance and security (Milakovich, 2021). By highlighting the specific security challenges faced by digital government initiatives in West Papua, the study aims to inform policymakers, practitioners, and researchers about the importance of enhancing security measures (Wangge & Lawson, 2023). The recommendations proposed in this research may include the implementation of robust cybersecurity protocols, the establishment of data protection mechanisms, and the improvement of infrastructure to support digital services (Hasan et al., 2023). According by Wasistiono & Sartika (2022), the concept of digital governance in West Papua is relatively new, and its implementation is still in its early stages. As such, there is a need to address security challenges comprehensively to ensure the successful adoption and utilization of digital technologies in governance. Failure to do so could lead to vulnerabilities that may be exploited by malicious actors, compromising the integrity and effectiveness of digital government systems (Kitchin & Dodge, 2020).

One of the primary security challenges facing digital governance in West Papua is the lack of cybersecurity awareness and expertise among government officials and the general population (Christawan et al., 2023). Many are unaware of the potential risks associated with digital technologies and lack the knowledge to protect themselves and their systems from cyber threats (Rahman et al., 2020). Another significant challenge is the limited infrastructure and resources available for cybersecurity in the region (Djenna et al., 2021). West Papua lags behind other regions in terms of internet connectivity and technological infrastructure, making it more vulnerable to cyber-attacks and other digital security threats (Satriawan et al., 2023).

In research by Sawir et al. (2023), the remote and geographically dispersed nature of West Papua also presents challenges for securing digital government systems. The vast and rugged terrain makes it difficult to establish and maintain secure communication networks, leaving government agencies and citizens more susceptible to cyber threats (Rizi & Seno, 2022). The socio-political situation in West Papua adds another layer of complexity to digital governance and security, according by Fauzi et al. (2023). The region has a history of conflict and unrest, which can create a volatile environment for digital governance initiatives (Busby, 2021). Ensuring the security of digital systems in such an environment requires careful planning and coordination.

One specific security challenge in West Papua is the threat of misinformation and propaganda spread through digital channels, in research by Siagian et al. (2021). Malicious actors can use social media and other digital platforms to spread false information and manipulate public opinion, undermining the legitimacy of the government and creating social unrest (Sarts, 2021). Data privacy is also a significant concern in West Papua, as the region lacks comprehensive data protection regulations. This leaves citizens' personal information vulnerable to exploitation and misuse by both government and non-government entities (Speed et al., 2020). In addition to external threats, internal vulnerabilities also pose a challenge to digital governance security in West Papua. Insider threats, such as employees with access to sensitive information, can exploit their position to compromise digital systems and data, in research by Saxena et al. (2020). The lack of coordination and collaboration among government agencies and stakeholders is another obstacle to effective digital governance and security in West Papua (Sulaiman et al., 2023). A fragmented approach to cybersecurity can leave gaps in defense and make it easier for attackers to exploit vulnerabilities.

Despite these challenges, there are opportunities to enhance digital governance security in West Papua. Investing in cybersecurity education and training, improving infrastructure and resources, and fostering collaboration among stakeholders can help strengthen the region's digital resilience and ensure the successful implementation of digital governance initiatives (AlDaajeh et al., 2022). Another significant challenge for digital government initiatives in West Papua is the issue of digital inclusion. While digital technologies have the potential to improve access to government services and information, there is a risk that certain segments of the population may be left behind. This could exacerbate existing inequalities and create new barriers to access.

To address this challenge, it is essential to ensure that digital government initiatives are inclusive and accessible to all segments of the population, in research by Addo & Senyo (2021). This may require targeted efforts to provide training and support to marginalized groups, such as indigenous communities or people with disabilities, to help them access and use digital services effectively. Moreover, the sustainability of digital government initiatives in West Papua is a pressing concern. The region's limited resources and capacity pose challenges for maintaining and updating digital systems over time (Kabir et al., 2023). To ensure the long-term sustainability of these initiatives, it is crucial to develop robust governance structures and secure funding sources (Murphy et al., 2021).

Lastly, the issue of trust and transparency is critical for the success of digital government initiatives in West Papua. Citizens must have confidence in the security and integrity of digital systems to fully embrace digital services (Sule et al., 2021). This requires government agencies to be transparent about their data practices and to ensure that data is collected, stored, and used responsibly (Tenopir et al., 2020). Addressing the security challenges faced by digital government initiatives in West Papua is crucial for ensuring the success and sustainability of these initiatives. By focusing on a quantitative analysis, this research aims to provide valuable insights and recommendations to strengthen the security posture of digital government in West Papua. Through collaborative efforts and innovative solutions, West Papua can leverage digital technologies to enhance governance, improve service delivery, and foster development.

METHODOLOGY

This research will utilize a quantitative method involving data collection through structured surveys. The survey will be distributed to respondents consisting of government officials in West Papua involved in digital governance, as well as other stakeholders such as information security experts and users of digital public services. The survey instrument will be designed to identify security challenges faced in digital governance, the level of awareness regarding information security, and efforts that have been made or planned to address these challenges. Survey data will be analyzed using statistical techniques such as regression and analysis of variance to identify factors influencing digital governance security in West Papua.

RESULTS AND DISCUSSION

Respondent Demographics

Table 1. Respondent Demographics

No.	Age Group	Gender	Position	Years of Experience
1	25-34	Male	IT Manager	8
2	35-44	Female	Public Relations	12
3	45-54	Male	Govt. Official	20
4	35-44	Male	IT Specialist	15
5	25-34	Female	Research Analyst	5

Table 1 provides an overview of the demographic characteristics of the survey respondents, including their age group, gender, position, and years of experience. Understanding the demographics of the respondents is essential for contextualizing their responses and identifying any potential biases or trends based on their background. By analyzing this table, policymakers, and cybersecurity professionals can gain valuable insights into the demographic profile of stakeholders involved in digital governance in West Papua. This information can inform targeted strategies for improving cybersecurity awareness, training, and policy development tailored to the needs of different demographic groups.

Security Challenges

Table 2. Security Challenges in Digital Governance

No.	Security Challenge	Percentage of Respondents
1	Lack of Cybersecurity Awareness	45%
2	Insufficient Budget for Cybersecurity	30%
3	Inadequate Security Infrastructure	25%
4	Cybersecurity Skills Shortage	35%
5	Lack of Coordination between Agencies	20%

Table 2 presents the main security challenges identified by respondents in the context of digital governance in West Papua, along with the percentage of respondents who perceive each challenge as significant. The challenges listed in the table reflect the key concerns and priorities for stakeholders involved in digital governance.

Lack of Cybersecurity Awareness

This challenge is perceived by 45% of respondents as a significant issue. It indicates a need for education and awareness programs to enhance understanding of cybersecurity risks and best practices among government officials and stakeholders.

Insufficient Budget for Cybersecurity

30% of respondents highlight this challenge, suggesting a need for increased investment in cybersecurity infrastructure, training, and resources to strengthen the overall security posture of digital governance.

Inadequate Security Infrastructure

25% of respondents consider this a major challenge. This indicates a need for improvements in the technical aspects of cybersecurity, such as implementing robust security measures and protocols to protect digital assets.

Cybersecurity Skills Shortage

35% of respondents perceive this as a significant challenge. It underscores the importance of developing the cybersecurity workforce and building local capacity to address skill gaps in digital governance.

Lack of Coordination between Agencies

20% of respondents identify this as a major challenge. This highlights the need for better coordination and collaboration among government agencies to ensure a cohesive and effective approach to cybersecurity in digital governance.

By understanding these challenges and their respective proportions, policymakers and cybersecurity professionals can prioritize their efforts and resources to address the most pressing issues in digital governance security.

Awareness of Information Security

Table 3. Awareness of Information Security

No.	Level of Awareness	Percentage of Respondents
1	Low	20%
2	Moderate	50%
3	High	30%

Table 3 categorizes respondents based on their perceived level of awareness regarding information security into three groups: low, moderate, and high. The percentages indicate the distribution of respondents across these awareness levels, providing insights into the current state of information security awareness among stakeholders involved in digital governance in West Papua.

Low Awareness (20%)

Respondents in this category may have limited understanding of information security risks and best practices. They may require targeted education and training to improve their awareness and knowledge in this area.

Moderate Awareness (50%)

The majority of respondents fall into this category, indicating a moderate level of awareness regarding information security. While they may have some understanding of cybersecurity risks and practices, there is still room for improvement.

High Awareness (30%)

Respondents in this category demonstrate a high level of awareness regarding information security. They are likely well-informed about cybersecurity risks and best practices, suggesting that they may play a key role in promoting and implementing security measures in digital governance. By identifying the distribution of awareness levels, stakeholders can tailor their awareness campaigns and training programs to effectively target different groups based on their current level of understanding. This can help improve overall information security awareness and practices in digital governance in West Papua.

Efforts to Address Security Challenges

Table 4. Efforts to Address Security Challenges

No.	Effort	Percentage of Respondents
1	Increased Cybersecurity Training	40%

2	Enhanced Data Encryption	25%
3	Implementation of Secure Access Controls	35%
4	Regular Security Audits and Assessments	45%
5	Establishment of A Cybersecurity Task Force	20%

Table 4 outlines the efforts that respondents have taken or plan to take to address security challenges in digital governance. The percentages indicate the proportion of respondents who have implemented or are considering implementing each effort, providing insights into the strategies and measures being employed to enhance security in digital governance.

Increased Cybersecurity Training (40%)

This effort indicates a proactive approach by respondents to enhance cybersecurity awareness and skills among government officials and stakeholders. It suggests a recognition of the importance of education in addressing security challenges.

Enhanced Data Encryption (25%)

Data encryption is a critical security measure to protect sensitive information. The percentage of respondents considering this effort indicates a recognition of the need to strengthen data protection measures in digital governance.

Implementation of Secure Access Controls (35%)

Secure access controls help prevent unauthorized access to digital systems and data. The percentage of respondents planning to implement this effort suggests a focus on improving access security in digital governance.

Regular Security Audits and Assessments (45%)

Security audits and assessments help identify vulnerabilities and assess the effectiveness of security measures. The high percentage of respondents planning to conduct regular audits indicates a commitment to maintaining a strong security posture.

Establishment of A Cybersecurity Task Force (20%)

A cybersecurity task force can provide dedicated expertise and resources to address security challenges. While the percentage of respondents considering this effort is relatively low, it indicates a recognition of the need for specialized teams to manage cybersecurity risks.

By analyzing these efforts, stakeholders can gain insights into the strategies and measures that are being prioritized to address security challenges in digital governance. This can help inform future initiatives and investments to strengthen security practices and protect digital assets in West Papua.

Preferred Training Topics for Cybersecurity

Table 5. Preferred Training Topics for Cybersecurity

No.	Training Topic	Percentage of Respondents
1	Cybersecurity best practices	35%
2	Threat intelligence	25%
3	Incident response and management	30%
4	Security risk assessment and mitigation	40%
5	Secure coding practices	20%

Table 5 presents the preferred training topics for cybersecurity among respondents, along with the percentage of respondents who favor each topic. The table provides insights into the training

needs and priorities of stakeholders involved in digital governance in West Papua, highlighting the areas where additional education and training may be beneficial.

Cybersecurity Best Practices (35%)

This topic is favored by a significant portion of respondents, indicating a recognition of the importance of understanding and implementing best practices to enhance cybersecurity in digital governance.

Threat Intelligence (25%)

Threat intelligence refers to the knowledge and insights about potential cybersecurity threats. The percentage of respondents interested in this topic suggests a desire to stay informed about emerging threats and trends in cybersecurity.

Incident Response and Management (30%)

Incident response and management training prepares individuals to effectively respond to and mitigate cybersecurity incidents. The percentage of respondents interested in this topic indicates a recognition of the importance of being prepared to handle cybersecurity incidents.

Security Risk Assessment and Mitigation (40%)

Security risk assessment and mitigation training helps individuals identify and mitigate potential security risks. The high percentage of respondents interested in this topic suggests a strong emphasis on proactive risk management in digital governance.

Secure Coding Practices (20%)

Secure coding practices are essential for developing secure software and applications. While the percentage of respondents interested in this topic is relatively low, it indicates a recognition of the importance of secure software development practices in cybersecurity.

By understanding the preferred training topics, stakeholders can tailor their training programs to meet the specific needs and priorities of individuals involved in digital governance. This can help improve overall cybersecurity awareness and practices in West Papua.

Perceived Impact of Cybersecurity Incidents

Table 6. Perceived Impact of Cybersecurity Incidents

No.	Impact Area	Percentage of Respondents
1	Financial losses	45%
2	Damage to reputation	30%
3	Loss of sensitive data	35%
4	Disruption of services	40%
5	Legal and regulatory penalties	25%

Table 6 outlines the perceived impact of cybersecurity incidents among respondents, along with the percentage of respondents who consider each impact area significant. The table provides insights into the potential consequences of cybersecurity incidents, which can help inform risk management strategies and mitigation efforts.

Financial Losses (45%)

Financial losses resulting from cybersecurity incidents can have a significant impact on organizations. The high percentage of respondents who consider this impact area significant highlights the importance of protecting against financial losses.

Damage to Reputation (30%)

Cybersecurity incidents can damage an organization's reputation and erode trust among stakeholders. The percentage of respondents who consider this impact area significant suggests a recognition of the importance of maintaining a positive reputation.

Loss of Sensitive Data (35%)

The loss of sensitive data can have serious consequences, including legal and regulatory penalties. The percentage of respondents who consider this impact area significant indicates a recognition of the importance of protecting sensitive information.

Disruption of Services (40%)

Cybersecurity incidents can disrupt services and operations, leading to downtime and reduced productivity. The high percentage of respondents who consider this impact area significant highlights the importance of maintaining service continuity.

Legal and Regulatory Penalties (25%)

Non-compliance with cybersecurity regulations can result in legal and regulatory penalties. The percentage of respondents who consider this impact area significant suggests a recognition of the importance of complying with relevant laws and regulations.

By understanding the perceived impact of cybersecurity incidents, stakeholders can prioritize their efforts and resources to mitigate the most significant consequences and protect against potential risks.

Perception of Government's Response to Cybersecurity

Table 7. Perception of Government's Response to Cybersecurity

No.	Response	Percentage of Respondents
1	Adequate	15%
2	Inadequate	65%
3	Unsure	20%

Table 7 presents the respondents' perception of the government's response to cybersecurity, along with the percentage of respondents who view the response as adequate, inadequate, or are unsure. The table provides insights into stakeholders' opinions regarding the effectiveness of the government's cybersecurity efforts, which can help identify areas for improvement and inform future policy decisions.

Adequate (15%)

The percentage of respondents who perceive the government's response to cybersecurity as adequate indicates a minority view. This suggests that there is room for improvement in the government's cybersecurity strategies and initiatives to better meet stakeholders' expectations.

Inadequate (65%)

The majority of respondents consider the government's response to cybersecurity as inadequate. This highlights a widespread perception among stakeholders that the government needs to do more to address cybersecurity challenges and enhance its response capabilities.

Unsure (20%)

A significant proportion of respondents are unsure about the government's response to cybersecurity. This indicates a lack of clarity or information regarding the government's cybersecurity efforts, highlighting a need for better communication and transparency in government cybersecurity initiatives.

By analyzing stakeholders' perceptions of the government's response to cybersecurity, policymakers and cybersecurity professionals can gain valuable insights into the effectiveness of current strategies and identify areas for improvement. This can help inform the development of more robust and comprehensive cybersecurity policies and initiatives to strengthen digital governance in West Papua.

Factors Influencing Cybersecurity Preparedness

Table 8. Factors Influencing Cybersecurity Preparedness

No.	Factor	Percentage of Respondents
1	Lack of funding	45%
2	Limited expertise in cybersecurity	30%
3	Insufficient government support	25%
4	Complexity of cybersecurity threats	35%
5	Inadequate cybersecurity policies and regulations	20%

Table 8 presents the factors that influence cybersecurity preparedness among respondents, along with the percentage of respondents who consider each factor significant. The table provides insights into the challenges and barriers faced by stakeholders in enhancing cybersecurity in digital governance in West Papua.

Lack of Funding (45%)

The percentage of respondents who identify lack of funding as a significant factor influencing cybersecurity preparedness indicates a widespread challenge. This suggests a need for increased investment in cybersecurity initiatives and resources to address this issue.

Limited Expertise in Cybersecurity (30%)

The percentage of respondents who perceive limited expertise in cybersecurity as a significant factor highlights the importance of building local capacity and expertise in cybersecurity. This can be achieved through training programs and knowledge-sharing initiatives.

Insufficient Government Support (25%)

The percentage of respondents who consider insufficient government support as a significant factor suggests a need for stronger government commitment and leadership in promoting cybersecurity initiatives. This can include developing and implementing cybersecurity policies and regulations.

Complexity of Cybersecurity Threats (35%)

The complexity of cybersecurity threats is a significant concern for respondents, indicating the evolving nature of cyber threats and the challenges in keeping pace with new and emerging threats. This underscores the need for continuous monitoring and adaptation of cybersecurity strategies.

Inadequate Cybersecurity Policies and Regulations (20%)

The percentage of respondents who identify inadequate cybersecurity policies and regulations as a significant factor suggests a need for the development and implementation of robust cybersecurity frameworks. This can help provide clear guidelines and standards for cybersecurity practices in digital governance.

By understanding these factors, stakeholders can prioritize their efforts and resources to address the most significant challenges and barriers to cybersecurity preparedness. This can help strengthen cybersecurity practices and resilience in digital governance in West Papua.

CONCLUSION

The research findings reveal critical challenges in digital governance in West Papua, primarily centered around a lack of cybersecurity awareness (45%) and a cybersecurity skills shortage (35%), which highlight the need for targeted education and workforce development. Respondents also emphasized the importance of increased cybersecurity training (40%) and regular security audits (45%) to address these gaps. Despite efforts to improve cybersecurity, a significant portion of respondents (65%) perceive the government's response as inadequate, suggesting that stronger government action, clearer communication, and enhanced inter-agency collaboration are necessary. Furthermore, the lack of coordination between agencies (20%) and the complexity of cybersecurity threats (35%) underscore the importance of developing a more cohesive, adaptive approach to cybersecurity. These insights indicate a need for greater investment in cybersecurity resources, policy development, and collaborative frameworks to strengthen the digital governance infrastructure in West Papua.

REFERENCES

Addo, A., & Senyo, P. K. (2021). Advancing E-governance for development: Digital identification and its link to socioeconomic inclusion. *Government Information Quarterly*, *38*(2), 101568. https://doi.org/10.1016/j.giq.2021.101568

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, *119*, 102754. https://doi.org/10.1016/j.cose.2022.102754

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & security*, *99*, 102030. https://doi.org/10.1016/j.cose.2020.102030

Budi, N. F. A., Fitriani, W. R., Hidayanto, A. N., Kurnia, S., & Inan, D. I. (2020). A study of government 2.0 implementation in Indonesia. *Socio-Economic Planning Sciences*, *72*, 100920. https://doi.org/10.1016/j.seps.2020.100920

Busby, J. W. (2021). Beyond internal conflict: The emergent practice of climate security. *Journal of Peace Research*, *58*(1), 186-194. https://doi.org/10.1177/0022343320971019

Caraka, R. E., Lee, Y., Chen, R. C., Toharudin, T., Gio, P. U., Kurniawan, R., & Pardamean, B. (2020). Cluster around latent variable for vulnerability towards natural hazards, non-natural hazards, social hazards in West Papua. *Ieee Access*, *9*, 1972-1986. https://doi.org/10.1109/ACCESS.2020.3038883

Chaoub, A., Giordani, M., Lall, B., Bhatia, V., Kliks, A., Mendes, L., ... & Zorzi, M. (2021). 6G for bridging the digital divide: Wireless connectivity to remote areas. *IEEE Wireless Communications*, *29*(1), 160-168. https://doi.org/10.1109/MWC.001.2100137

Christawan, E., Perwita, A. A. B., Midhio, I. W., Hendra, A., & Risman, H. (2023). Implementation of the Total People's War Strategy to Suppress Papua Separatist Movement. https://doi.org/10.31219/osf.io/8y2q7

Debrah, C., Chan, A. P., & Darko, A. (2022). Artificial intelligence in green building. *Automation in Construction*, *137*, 104192. https://doi.org/10.1016/j.autcon.2022.104192

Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences*, *11*(10), 4580. https://doi.org/10.3390/app11104580

Fauzi, F. Z., Mayor, D. E., & Liauw, G. (2023). The Direction of Papua Development: Is A New Autonomous Region the Answer?. *Policy & Governance Review*, *7*(1), 1-20. https://doi.org/10.30589/pgr.v7i1.609

Hasan, M. K., Habib, A. A., Shukur, Z., Ibrahim, F., Islam, S., & Razzaque, M. A. (2023). Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. *Journal of Network and Computer Applications*, *209*, 103540. https://doi.org/10.1016/j.jnca.2022.103540

Kabir, H., Tham, M. L., & Chang, Y. C. (2023). Internet of robotic things for mobile robots: concepts, technologies, challenges, applications, and future directions. *Digital Communications and Networks*. https://doi.org/10.1016/j.dcan.2023.05.006

Kitchin, R., & Dodge, M. (2020). The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention. In *Smart cities and innovative Urban technologies* (pp. 47-65). Routledge. https://doi.org/10.4324/9781003132851

Kraus, S., Jones, P., Kailer, N., Weinmann, A., Chaparro-Banegas, N., & Roig-Tierno, N. (2021). Digital transformation: An overview of the current state of the art of research. *Sage Open*, *11*(3), 21582440211047576. https://doi.org/10.1177/21582440211047576

Ksibi, S., Jaidi, F., & Bouhoula, A. (2023). A comprehensive study of security and cyber-security risk management within e-Health systems: Synthesis, analysis and a novel quantified approach. *Mobile Networks and Applications*, *28*(1), 107-127. https://doi.org/10.1007/s11036-022-02042-1

Lehto, M. (2022). Cyber-attacks against critical infrastructure. In *Cyber security: Critical infrastructure protection* (pp. 3-42). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-91293-2_1

Malodia, S., Dhir, A., Mishra, M., & Bhatti, Z. A. (2021). Future of e-Government: An integrated conceptual framework. *Technological Forecasting and Social Change*, *173*, 121102. https://doi.org/10.1016/j.techfore.2021.121102

Milakovich, M. E. (2021). *Digital governance: Applying advanced technologies to improve public service*. Routledge. https://doi.org/10.4324/9781003215875

Murphy, S. E., Farmer, G., Katz, L., Troëng, S., Henderson, S., Erdmann, M. V., ... & Putra, K. S. (2021). Fifteen years of lessons from the Seascape approach: A framework for improving ocean management at scale. *Conservation Science and Practice*, *3*(6), e423. https://doi.org/10.1111/csp2.423

Putro, A. N. S., Mokodenseho, S., Hunawa, N. A., Mokoginta, M., & Marjoni, E. R. M. (2023). Enhancing security and reliability of information systems through blockchain technology: a case study on impacts and potential. *West Science Information System and Technology*, *1*(01), 35-43. https://doi.org/10.58812/wsist.v1i01.166

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378-382. https://doi.org/10.18178/ijiet.2020.10.5.1393

Rizi, M. H. P., & Seno, S. A. H. (2022). A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city. *Internet of Things*, *20*, 100584. https://doi.org/10.1016/j.iot.2022.100584

Sarts, J. (2021). Disinformation as a threat to national security. *Disinformation and Fake News*, 23-33. https://doi.org/10.1007/978-981-15-5876-4_2

Satriawan, I., Elven, T. M. A., & Lailam, T. (2023). Internet Shutdown in Indonesia: An Appropriate Response or A Threat to Human Rights?. *Sriwijaya Law Review*, *7*(1), 19-46. https://doii.org/10.28946/slrev.Vol7.Iss1.1018.pp19-46

Sawir, M., Robo, S., Abubakar, F., & Kamaluddin, S. (2023). Implementation Of Public Services In The Digital Era As A Public Information Media Regional Government Of Jayapura Regency, Papua Province. *Jurnal Manajemen Pelayanan Publik*, *6*(2), 212. http://dx.doi.org/10.24198/jmpp.v6i2.45532

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. *Electronics*, *9*(9), 1460. https://doi.org/10.3390/electronics9091460

Siagian, M. U. H. N. I. Z. A. R., & Yuliarti, M. S. (2021). Papua's Internet Ban 2020: Politics, information democracy, and digital literacy. *Jurnal Komunikasi: Malaysian Journal of Communication*, *37*(3), 304-316. https://doi.org/10.17576/JKMJC-2021-3703-18

Skouby, K. E., Dhotre, P., Williams, I., & Hiran, K. (Eds.). (2022). *5G, Cybersecurity and Privacy in Developing Countries*. CRC Press. https://doi.org/10.4324/9781003374664

Speed, A., Thomson, C., & Richardson, K. (2020). Stay home, stay safe, save lives? An analysis of the impact of COVID-19 on the ability of victims of gender-based violence to access justice. *The Journal of Criminal Law*, *84*(6), 539-572. https://doi.org/10.1177/0022018320948280

Sulaiman, A., Dwilaksana, C., & Muta'ali, A. (2023). Synergy between the Police, TNI, Local Government, and the Community to Promote Diversity and Improve Security and National Unity in the Papua Region. *International Journal of Social Science Research and Review*, *6*(5), 436-448. https://doi.org/10.47814/ijssrr.v6i5.1317

Sule, M. J., Zennaro, M., & Thomas, G. (2021). Cybersecurity through the lens of digital identity and data protection: issues and trends. *Technology in Society*, *67*, 101734. https://doi.org/10.1016/j.techsoc.2021.101734

Tenopir, C., Rice, N. M., Allard, S., Baird, L., Borycz, J., Christian, L., ... & Sandusky, R. J. (2020). Data sharing, management, use, and reuse: Practices and perceptions of scientists worldwide. *PloS one*, *15*(3), e0229003. https://doi.org/10.1371/journal.pone.0229003

Toufaily, E., Zalan, T., & Dhaou, S. B. (2021). A framework of blockchain technology adoption: An investigation of challenges and expected value. *Information & Management*, *58*(3), 103444. https://doi.org/10.1016/j.im.2021.103444

Wangge, H. R., & Lawson, S. (2023). The West Papua issue in Pacific regional politics: explaining Indonesia's foreign policy failure. *The Pacific Review*, *36*(1), 61-89. https://doi.org/10.1080/09512748.2021.1931417

Wasistiono, S., & Sartika, I. (2022). Model Evaluation of Papua and West Papua Province's Special Autonomous. *Bestuurskunde: Journal of Governmental Studies*, *2*(1), 73-88. https://doi.org/10.53013/bestuurskunde.2.1.73-88