CAKRAWALA
JOURNAL OF CITIZENSHIP TEACHING AND LEARNING
ACADEMIC SOLUTION PUBLISHER

Defending The State in The Digital Domain: Between Cyber Threats and National Awareness

Rika Githamala Ginting[1], Gatot Teguh Arifyanto[2], Fauzan Ghafur[3]

[1,2,3]*Politeknik Negeri Medan, Indonesia*
[*]*Corresponding Author*: rikagithamalaginting@polmed.ac.id

Article Info

Article history:

Received : 20 April 2025
Accepteance : 20 May 2025
Published : 21 June 2025
Available online
http://aspublisher.co.id/index.php/cakrawala

E-ISSN: 3063-2447

How to cite:
Ginting, G. R., Arifyanto, T. G., & Ghafur, F (2025). "Defending The State in The Digital Domain: Between Cyber Threats and National Awareness," Cakrawala: Journal of Citizenship Teaching and Learning, vol. 3, no. 1, pp. 11-20, 2025.

ABSTRACK

Cyber threats are a big challenge for Indonesia along with the development of digital technology and dependence on cyberspace. This article aims to analyze the relationship between cyber threats and digital national defense and the role of national awareness in strengthening state resilience. This qualitative research with a literature analysis shows that Indonesia faces major challenges in digital resilience, such as low digital literacy, inadequate infrastructure, and limited experts in the field of cybersecurity. In conclusion, collaboration between the government, the private sector, and the community as well as increased digital literacy is needed to strengthen Indonesia's cyber resilience.

Keywords: *Digital State Defense, cyber threats, national awareness, digital literacy, cybersecurity policy*

1. INTRODUCTION

In the context of fast globalization and the digital revolution, Indonesia confronts increasingly intricate concerns, including the threat to national security emanating from cyberspace, referred to as cyber threats. This danger encompasses specific individuals or organizations and possesses the capacity to undermine the governmental framework, political stability, and the national economy. In this context, the notion of National Defense, established during Indonesia's fight for independence, necessitates an updating to address increasingly sophisticated and varied dangers, particularly cyber threats. Indonesia, the fourth most populous nation globally, with a steadily expanding population

of internet users, is more susceptible to cyber attacks that threaten national security and socio-economic stability (Yunita & Margiyanti, 2023).

The significance of recognizing National Defense in the digital realm has emerged as a problem that cannot be overlooked. Society, particularly the youth who are more engaged with the digital landscape, must cultivate a profound comprehension of their responsibilities in upholding national security in the digital domain. Cyber threats necessitate readiness to safeguard oneself, family, and the nation against potentially detrimental cyberattacks, including personal data breaches, dissemination of falsehoods, and assaults on important national infrastructure (Vasylkiv, 2023). Given the swift advancement of information technology, cyber dangers have emerged as a significant concern that must be confronted by the state through a methodical, organized strategy rooted in national awareness.

Cybersecurity, now international and ever evolving, necessitates a profound comprehension of technology's impact on national stability. Countries must implement adaptable policies and effective ways to address increasingly complex cyber threats. Consequently, a crucial element in mitigating this threat is national understanding regarding the need of cyber defense. This understanding must be cultivated not only at the governmental level but also throughout all strata of society. A robust comprehension of digital dangers and their mitigation can enhance the nation's resilience in cyberspace. In this instance, technology can be employed to enhance alertness and the ethos of national defense, given the widespread access to information via social media and other digital platforms.

Nonetheless, despite several initiatives to enhance public awareness regarding cyber risks, the fact remains that many young individuals possess a limited comprehension of the significance of safeguarding the nation in the digital realm. A study by Azzahra et al. (2023) indicates that public awareness, especially among Generation Z, remains significantly low about the rising cyber risks. This signifies a deficiency in awareness among the younger generation concerning digital hazards, resulting in an inadequate societal reaction to cyber threats. The information deficit may significantly contribute to the perception that cyber risks, despite their persistent escalation, are frequently relegated to a lower priority in everyday life.

This article seeks to examine the correlation between cyber dangers and the notion of National Defense in the digital age. This research will elucidate how efforts to augment national knowledge of digital risks might fortify the country's resilience in cyberspace. This article will examine the role of technology, specifically social media and digital literacy, in fostering awareness and the ethos of National Defense, particularly among the youth who are increasingly immersed in the digital realm (Nazira, Kholil, Rasyid, & Hutagalung, 2025). This discourse aims to generate concepts on utilizing digital media to cultivate a sense of nationalism pertinent to contemporary concerns.

This study employs a qualitative research method, utilizing a literature analysis that examines the policies and measures adopted by different countries to combat cyber threats. The author will examine the measures enacted by the Indonesian government about initiatives to combat cyber threats and improve National Defense awareness. The

findings of this research are anticipated to substantially enhance the formulation of national policies aimed at mitigating cyber risks and bolstering public awareness of National Defense. This essay seeks to enhance the literature on National Defense inside the digital realm and to outline the potential advancement of the relationship between cybersecurity and national resilience. The findings of this research can operate as a reference for the formulation of educational and training programs in diverse educational institutions and government organizations to enhance awareness regarding digital dangers and the significance of National Defense in the information technology era. It is crucial to guarantee that future generations comprehend the current challenges and may actively contribute to enhancing national resilience in cyberspace.

2. RESEARCH METHODE

This essay employs a qualitative research method, concentrating on literature review and policy analysis pertaining to National Defense and cyber threats. This qualitative research seeks to comprehensively analyze the correlation between national awareness of cyber dangers and initiatives in National Defense within the digital realm. This research included data from two categories of sources: primary and secondary. Primary sources encompass policy documents, government reports pertaining to cybersecurity policies, and pertinent international case studies. Countries such as Estonia and Singapore are recognized as exemplars of robust cyber security policy implementation and offer significant insights into policy execution in the digital realm (Luthfah, 2021). Secondary sources include scientific articles, media reports, and various publications addressing subjects such as National Defense, cyber threats, and digital policies, as analyzed by (Wibowo, 2025) regarding global threats to the digital economy, and (Nadhifah, 2020), who investigates Indonesia's cyber diplomacy in international forums.

Data collection methods involved systematic document reviews and the selection of case studies from nations with advanced cyber preparedness, such as Estonia and Singapore, which offer valuable insights into policy implementation in the digital realm (Launa, Mudjiyanto, & P. Roring, 2024). This research employs descriptive analysis to examine the correlation between national awareness and initiatives in National Defense against cyber threats. The author compares the approaches of countries that have effectively established strong digital national security programs. The analytical process entails identifying the principal themes of the policies and programs enacted by other countries, along with examining the deficiencies or opportunities for their implementation in Indonesia. This research, while not directly involving participants or samples, utilizes data from literature evaluation and policy analysis to yield valid and trustworthy findings on optimal tactics for enhancing digital national security awareness. This methodology aligns with the article's aims, which emphasize the role of public awareness in enhancing the nation's resilience in cyberspace (Lebo & Anwar, 2020).

3. RESULT AND ANALYSIS

The Correlation Between Cyber Threats and National Defense

Cyber attacks in the digital age provide a significant problem that assesses the resilience of nations in cyberspace. This threat encompasses not just technical assaults on the nation's key infrastructure but also extends to disinformation, public opinion manipulation, and personal data breaches that might jeopardize social and political stability. In this context, the notion of National Defense, traditionally perceived as the physical safeguarding of national sovereignty, must be broadened to encompass the preservation of the digital realm, which is as crucial. National security in the digital realm encompasses the safeguarding of information and communication technology employed for diverse governmental and economic operations. As noted by (Watney, 2022), challenges to this sector, including assaults on essential infrastructure, can result in extensive harm if not addressed with due seriousness. Cyberattacks on the energy or transportation sectors can suspend national operations for a lengthy duration, harm the economy, and jeopardize public safety. Moreover, assaults on banking infrastructures and personal information might diminish public confidence in governmental systems and heighten the risk of social unrest (Shandler & Gomez, 2023).

Cyber dangers originate not just from external entities but also from internal players who use vulnerabilities in national technological systems for their own goals. This threat is transnational and may involve extremely sophisticated international networks, as seen by numerous significant hacking incidents linked to specific nations. Consequently, national security in the digital age necessitates heightened understanding of the significance of cyber defense among the government, corporate sector, and the general populace. The execution of policies that foster collaboration between the public and private sectors is essential for establishing cyber resilience to safeguard the nation against emerging threats (Marta, 2023).

Cyber threats that challenge the nation's resilience in cyberspace necessitate a more comprehensive approach under the National Defense policy. Countries possessing explicit cybersecurity rules and robust infrastructure are generally more resilient to such threats (TANRIVERDIYEV, 2022). In Indonesia, despite several initiatives to implement cybersecurity legislation, the primary problems remain the scarcity of educated personnel and insufficient cooperation among relevant institutions. This study suggests that fostering national awareness of cyber dangers is the essential first step to enhance the nation's digital security (Misrah, Nurcahaya, Ismail, & Hutagalung, 2024).

Required Strategies and Policies

To confront the escalating complexity of cyber threats, Indonesia must formulate more systematic plans and policies to enhance the nation's resilience in cyberspace. An all-encompassing and cohesive policy is vital to address risks originating from cyberspace, which jeopardize not just individuals or companies but also the governmental framework, economic stability, and social cohesion. The formulation of cybersecurity policies that engage both public and commercial sectors is essential for establishing a successful cyber defense framework. Indonesia must develop policies that include the safeguarding of key

infrastructure, the management of sensitive data, and the establishment of mechanisms for the detection and response to cyber attacks (Syafi'i, Supriyadi, Prihanto, & Gultom, 2023). This policy must be founded on a thorough assessment of cyber threat threats to enhance national readiness. Moreover, enhancing legislation pertaining to personal data and national strategic information is crucial to prevent potential data breaches or manipulation by negligent entities, as articulated by (Li, Chen, & Huang, 2021).

Enhancing human resources (HR) in cybersecurity is crucial for addressing digital threats. Indonesia is presently experiencing a deficiency of qualified professionals in this domain. Consequently, the government must prioritize education and training in information technology and cybersecurity. Asserts that formal training and education at higher education institutions must prioritize the cultivation of abilities to combat cyber dangers. Furthermore, the incorporation of professional certification in cybersecurity into regulations is essential to guarantee internationally recognized quality and standards. The government should promote collaboration between the public and commercial sectors to strengthen human resource capabilities in safeguarding the nation's cybersecurity (Wibowo, 2025).

Furthermore, digital literacy education constitutes a vital component of this program. To enhance public knowledge of cyber risks and self-protection measures, digital literacy instruction must be implemented early in educational institutions. Proficient digital literacy within the populace can foster a culture of alertness against cyber risks and enhance public engagement in safeguarding the nation's digital security (Lailatul Fitria, Tjahjaningsih, Harmoko, Sabila, & Fawaitd, 2022). Moreover, public campaigns disseminated across all societal strata via social media and other digital platforms would significantly enhance awareness of the necessity of cybersecurity. Cooperation among the government, private sector, and educational institutions is essential for the implementation of this program.

Enhancing safe digital infrastructure is a crucial measure in bolstering cybersecurity policies. The state must guarantee that both public and private sectors possess sufficient systems to safeguard critical data and information, along with explicit processes for addressing cyberattacks. Given the nation's reliance on technology, safeguarding critical industries such as energy, finance, and healthcare is paramount. assert that enhancing legislation governing the protection of personal data and sensitive information, particularly in relation to national security, might mitigate the risk of assaults that may jeopardize economic and social stability (Polikanina, Polikanin, & Shaburova, 2022). Consequently, augmenting the technical infrastructure's capability via robust encryption systems and fortifying real-time detection and response to threats is an indispensable factor in bolstering Indonesia's digital resilience.

The Significance of National Awareness in Enhancing Digital Defense

The national awareness of cyber risks is crucial for enhancing digital national defense, particularly in Indonesia, which is becoming increasingly integrated into the cyber realm. The perpetually advancing cyber dangers can undermine national stability; thus, it is essential to cultivate a comprehensive awareness of cybersecurity across all societal strata.

Elevated digital awareness will enhance the capacity of individuals, corporations, and governments to confront cyber threats and safeguard personal data, along with the nation's key infrastructure. The national awareness of digital dangers should recognize that each citizen contributes significantly to the nation's digital resilience, rather than solely relying on the government or business sector (Srilaksmi et al., 2023). With the rise of public participation in digital activities, education and training on cyber dangers and their mitigation should be broadly implemented throughout all societal sectors, encompassing both children and adults (Aksenta et al., 2023)

Digital literacy education is an essential initial measure in fostering public awareness of cyber risks. The implementation of robust digital literacy programs in schools and universities is anticipated to cultivate a generation that is more cognizant and adequately equipped to confront cyber threats. Research conducted by Luić, Švelec-Juričić, and Mišević (2021) indicates that education focused on digital literacy at the elementary to middle school levels is crucial for enhancing knowledge regarding the significance of personal data protection and information security (Luić, Švelec-Juričić, & Mišević, 2021). Furthermore, the significance of imparting digital literacy training to the younger generation, who are more engaged with social media and information technology, is paramount (Andriani, Rahayu, & Prasetiyo, 2024).

A comprehensive national awareness of cyber dangers necessitates effective public campaigns to improve the public's comprehension of the measures required to safeguard personal data and prevent prospective assaults. Campaigns employing social media and influencers are highly effective in engaging a broader audience, particularly among the youth active on digital platforms (Najmi Nuji, Ali, Wan Noordin, Mohamed Thaheer, & Mathiew, 2023). This campaign must elucidate the risks associated with cyber threats and offer guidance on safeguarding oneself, family, and personal data from cyber attacks (Putri, Nurbaiti, & Nasution, 2022).

Enhancing public understanding of the significance of national defense in the digital realm necessitates the involvement of both the commercial sector and the government. Cooperation among the government, commercial sector, and community will establish a more secure environment in addressing digital threats. The government must promote cybersecurity training across all sectors, including education, industry, and public domains. Research by Górka indicates that collaboration between the public and business sectors in formulating inclusive and awareness-driven cybersecurity policies can strengthen national cyber resilience (Górka, 2022). By enhancing public awareness, Indonesia can cultivate improved digital resilience against cyber threats and bolster a sense of national defense pertinent to the problems of the digital era. The significance of technology and social media as instruments for fostering national consciousness in preserving the country's sovereignty in cyberspace is evident.

Challenges and Hindrances

Confronted with increasingly intricate cyber threats, Indonesia faces significant obstacles in enhancing the nation's digital resilience. A primary difficulty is the insufficient infrastructure to facilitate effective cybersecurity measures. The susceptibility of

infrastructure to cyberattacks, in both public and commercial sectors, constitutes a substantial obstacle to safeguarding information security and personal data in Indonesia. Research by Syafi'i et al, indicates that despite Indonesia's efforts to enhance its information technology industry, critical areas such as energy, banking, and other public services continue to exhibit vulnerabilities in their cybersecurity frameworks. This generates vulnerabilities that can be exploited by nefarious entities to execute harmful assaults (Syafi'i et al., 2023).

Furthermore, Indonesia confronts the difficulty of insufficient public knowledge concerning the significance of cybersecurity. Despite the continuous evolution of cyber dangers, public understanding of the significance of personal data protection and methods to mitigate potential cyber risks remains markedly insufficient (Gille & Brall, 2021). The insufficient comprehension of the risks associated with cyber attacks at both individual and community levels aggravates the issue, as these attacks frequently originate from users' irresponsibility in handling personal data or engaging with digital platforms unsafely. A significant enhancement of digital literacy across all societal strata is urgently required. A notable difficulty is the scarcity of expertise in the field of cybersecurity in Indonesia. Wibowo asserts that, despite the growing interest in the information technology sector, the quantity of individuals skilled in cybersecurity remains inadequate to address current threats (Wibowo, 2025). This necessitates that the government and commercial sector intensify their efforts in providing training and education programs in this domain. Both formal and informal education aimed at cultivating pertinent technological skills is essential for producing specialists adept at addressing progressively complex cyber threats.

Furthermore, Indonesia encounters difficulties regarding inter-institutional and inter-sectoral coordination. A primary hurdle is the insufficient collaboration among the public, business, and community sectors in combating cyber threats. Research by Trein et al. (2021) indicates that despite the issuance of numerous government policies, their execution is frequently obstructed by coordination challenges among the pertinent agencies (Trein et al., 2021) For instance, numerous governmental organizations addressing cyber matters sometimes lack effective communication routes, which may impede a prompt response to cyber threats. Consequently, it is imperative for the Indonesian government to enhance collaboration among agencies and sectors to fortify cybersecurity policy.

Addressing this dilemma necessitates the implementation of more cohesive policies, which include fortifying security infrastructure, augmenting digital literacy education, and fostering intersectoral collaboration. By implementing more comprehensive and coordinated measures, Indonesia can enhance its digital resilience and mitigate the effects of cyber threats.

4. CONCLUSION

This study effectively recognized the problems and potential in enhancing Indonesia's digital national defense, emphasizing cyber dangers and the importance of national awareness. The primary findings reveal that national knowledge of cyber dangers remains

inadequate, notwithstanding the swift advancement of digital technology and its considerable influence on national resilience. This signifies that augmenting public digital literacy, fortifying cybersecurity legislation, and fostering cross-sector collaboration are essential for bolstering the nation's digital defense. This research enhances the idea of National Defense inside the digital realm and addresses the deficiency in the literature of the formulation of policies and training pertinent to cybersecurity in Indonesia. The social ramifications of these findings necessitate enhanced education on digital hazards to increase awareness among the youth, while the cultural implications require the cultivation of a vigilant ethos against cyber threats. This research is limited by the extent of data and methodologies employed; hence, additional investigation is necessary to examine wider variables in enhancing digital resilience.

This report recommends collaboration among the government, commercial sector, and educational institutions to fortify cybersecurity policies and improve digital literacy throughout society, particularly among the youth. Technology practitioners must intensify their training on cyber threat mitigation, while academics should concentrate on creating courses pertinent to contemporary digital concerns. Future study may investigate triangulation methods to achieve a more holistic picture and use empirical analysis to assess the efficacy of current policy. Future study should focus on exploring the cultural and socioeconomic determinants of digital awareness in Indonesia and assessing the effects of emerging technologies, such as artificial intelligence, on cybersecurity.

References

Aksenta, A., Irmawati, Hayati, N., Sepriano, Herlinah, Silalahi, A. T., ... Ginting, T. W. (2023). LITERASI DIGITAL: Pengetahuan & Transformasi Terkini Teknologi Digital Era Industri 4.0 dan Sociaty 5.0. In Perspektif (Vol. 1).

Andriani, D. R. P., Rahayu, P., & Prasetiyo, P. (2024). Effectiveness of Bottle Size Variation on the Growth of Dendrobium Striaenopsis Orchid Plantlets. Jurnal Pembelajaran Dan Biologi Nukleus, 10(1), 143–153. https://doi.org/10.36987/jpbn.v10i1.5325

Gille, F., & Brall, C. (2021). Limits of data anonymity: lack of public awareness risks trust in health system activities. Life Sciences, Society and Policy, 17(1), 7. https://doi.org/10.1186/s40504-021-00115-9

Górka, M. (2022). Cybersecurity culture in the public and private sector area in the Central European region. Nowa Polityka Wschodnia, 35(1), 51–71. https://doi.org/10.15804/npw20223503

Lailatul Fitria, N. J., Tjahjaningsih, Y. S., Harmoko, H., Sabila, S. M., & Fawaitd, G. F. I. (2022). SOSIALISASI LITERASI DIGITAL TERKAIT CYBER CRIME BAGI KARANG TARUNA GAGAK RIMANG DI DESA PABEAN. Abdimas Galuh, 4(2), 1240. https://doi.org/10.25157/ag.v4i2.8485

Launa, Mudjiyanto, B., & P. Roring, F. (2024). Tendensi Politik Kejahatan Dunia Maya. JIKA (Jurnal Ilmu Komunikasi Andalan), 7(1), 26–51. https://doi.org/10.31949/jika.v7i1.8762

Lebo, D., & Anwar, S. (2020). Pemberdayaan komunitas siber oleh Pemerintah Republik Indonesia dari perspektif Strategi Perang Semesta. Jurnal Strategi Pertahanan Semesta, 6(1), 101–127.

Li, S.-C., Chen, Y.-W., & Huang, Y. (2021). Examining Compliance with Personal Data Protection Regulations in Interorganizational Data Analysis. Sustainability, 13(20), 11459. https://doi.org/10.3390/su132011459

Luić, L., Švelec-Juričić, D., & Mišević, P. (2021). The Impact of Knowledge of the Issue of Identification and Authentication on the Information Security of Adolescents in the Virtual Space. WSEAS TRANSACTIONS ON SYSTEMS AND CONTROL, 16, 527–533. https://doi.org/10.37394/23203.2021.16.49

Luthfah, D. (2021). Serangan Siber Sebagai Penggunaan Kekuatan Bersenjata dalam Perspektif Hukum Keamanan Nasional Indonesia (Cyber Attacks as the Use of Force in the Perspective of Indonesia National Security Law). TerAs Law Review : Jurnal Hukum Humaniter Dan HAM, 3(1), 11–22. https://doi.org/10.25105/teras-lrev.v3i1.10742

Marta, R. F. (2023). STRATEGI MEDIA KOMUNIKASI DI MASA PANDEMI. Bandung: WIDINA BHAKTI PERSADA.

Misrah, Nurcahaya, Ismail, & Hutagalung, S. A. (2024). From Classroom to Ideological Space: The Formation of Radicalism in the Academic Environment. 23(3).

Nadhifah, H. N. (2020). Diplomasi Siber Indonesia dalam United Nations Group of Governmental Experts on Development in the Field of Information and Telecommunication in the Context of International Security 2012-2019. Repository.Uinjkt.Ac.Id, i–140. Retrieved from https://repository.uinjkt.ac.id/dspace/handle/123456789/59997

Najmi Nuji, M. N., Ali, A., Wan Noordin, W. N., Mohamed Thaheer, B. A. N., & Mathiew, V. (2023). Of Trust and Influence: A Look At Social Media Influencers and Brand Promotion. International Journal of Academic Research in Business and Social Sciences, 13(6). https://doi.org/10.6007/IJARBSS/v13-i6/15444

Nazira, S., Kholil, S., Rasyid, A., & Hutagalung, S. A. (2025). Komunikasi Interpersonal Himpunan Mahasiswa Islam (HMI) dalam Membentuk Soft Skill Mahasiswa Ilmu Komunikasi Universitas Islam Negeri Sumatera Utara Medan. Polyscopia, 2(2), 122–129. https://doi.org/10.57251/polyscopia.v2i2.1682

Polikanina, O. A., Polikanin, A. N., & Shaburova, A. V. (2022). Organization of personal data protection in state and municipal information systems. Interexpo GEO-Siberia, 6, 197–203. https://doi.org/10.33764/2618-981X-2022-6-197-203

Putri, T. A., Nurbaiti, & Nasution, J. (2022). Pengaruh Norma Subjektif dan Persepsi Manfaat Terhadap Intensitas Menggunakan Fintech Payment dengan Sikap Pengguna Sebagai Variabel Intervening (Studi Kasus: Mahasiswa Fakultas Ekonomi dan Bisnis Islam UIN Sumatera. Braz Dent J., 33(1), 1–12.

Shandler, R., & Gomez, M. A. (2023). The hidden threat of cyber-attacks – undermining public confidence in government. Journal of Information Technology & Politics, 20(4), 359–374. https://doi.org/10.1080/19331681.2022.2112796

Srilaksmi, N. K. T., Irnadianis, B., Estiningtyas, D., Delareiza, M., Sulistiowati, S., &

Nilam, A. (2023). State Defense: Challenges Towards Digitalization. Journal of Digital Law and Policy, 2(2), 81–92. https://doi.org/10.58982/jdlp.v2i2.313

Syafi'i, M. H., Supriyadi, A. A., Prihanto, Y., & Gultom, R. A. G. (2023). Kajian Ilmu Pertahanan dalam Strategi Pertahanan Negara Guna Menghadapi Ancaman Teknologi Digital di Indonesia. Journal on Education, 5(2), 4063–4076. https://doi.org/10.31004/joe.v5i2.1100

TANRIVERDIYEV, E. (2022). THE STATE OF THE CYBER ENVIRONMENT AND NATIONAL CYBERSECURITY STRATEGY IN DEVELOPED COUNTRIES. National Security Studies, 23(1), 19–26. https://doi.org/10.37055/sbn/149510

Trein, P., Biesbroek, R., Bolognesi, T., Cejudo, G. M., Duffy, R., Hustedt, T., & Meyer, I. (2021). Policy Coordination and Integration: A Research Agenda. Public Administration Review, 81(5), 973–977. https://doi.org/10.1111/puar.13180

Vasylkiv, B. (2023). CYBER SECURITY AS A DIRECTION OF PROTECTION OF THE INFORMATION AND COMMUNICATION SECTOR IN MODERN CONDITIONS. Business Navigator, (1(71)). https://doi.org/10.32782/business-navigator.71-3

Watney, M. (2022). Cybersecurity Threats to and Cyberattacks on Critical Infrastructure: a Legal Perspective. European Conference on Cyber Warfare and Security, 21(1), 319–327. https://doi.org/10.34190/eccws.21.1.196

Wibowo, A. (2025). DISRUPSI TATA KELOLA GLOBAL EKONOMI DIGITAL Era Perang Tarif Amerika - China 2025. Semarang: Yayasan Prima Agus Teknik Bekerja Sama dengan Universitas STEKOM.