

National cyber security policy and its implications for Strategic defense

Restu Putri Pamungkas

Indonesia Defense University, Bogor, Indonesia

Asep Adang Supriyadi

Indonesia Defense University, Bogor, Indonesia

Tatar Bonar

Indonesia Defense University, Bogor, Indonesia

Novky Asmoro

Indonesia Defense University, Bogor, Indonesia

Corresponding Author: restu.pamungkas@doktoral.idu.ac.id

Abstract

The advance of digital technology has produced a new landscape for national security, in which threats are no longer only conventional but also originate in cyberspace. Attacks on strategic infrastructure, government data, and defense systems show that cyber security has become an inseparable part of national defense. National cyber security policy therefore matters for safeguarding digital sovereignty and for strengthening national resilience against non-traditional threats. This study analyses Indonesia's national cyber security policy and its implications for the country's strategic defense. It applies a systematic literature review guided by the PRISMA protocol; 602 records retrieved from the Dimensions database were screened, and 25 articles and policy documents published between 2020 and 2025 were selected and analysed thematically. The findings show that Indonesia has built a solid policy foundation through the establishment of the National Cyber and Crypto Agency (BSSN), the National Cyber Security Strategy, and regulations that protect vital information infrastructure. Persistent obstacles remain, however, in cross-sectoral coordination, the supply of skilled cyber personnel, and digital security awareness at both public and institutional levels. The implications for strategic defense are threefold: cyber defense needs to be integrated into the national defense system, detection and incident-response capacity needs to be enlarged, and synergy among the military, government, and the private sector needs

496



to be built deliberately rather than left to emerge on its own.

Keywords: BSSN; Cyber Defense; Cyber Security Policy; Digital Sovereignty; Strategic Defense.

INTRODUCTION

The advance of information and communication technology in the Fourth Industrial Revolution has changed the landscape of national security and strategic defense in a fundamental way. Digital transformation across the public and private sectors has made data more accessible, services more efficient, and electronic government systems more innovative. The same movement, however, has opened room for new non-conventional threats, particularly in the cyber domain (Budiyanto & Mabururi, 2025). Cyberspace is now a geopolitical arena in its own right, where attacks can inflict economic loss, disrupt vital infrastructure, and reach as far as national sovereignty (Saramuke et al., 2025).

Indonesia, with its high rate of technology adoption, faces the same challenges. The Global Cybersecurity Index published by the ITU records a year-on-year improvement in Indonesia's score, yet the country still trails several ASEAN neighbours (Cloramidine & Badaruddin, 2023). Progress in regulation and institution-building has therefore not yet translated into full national preparedness. BSSN reporting notes a marked rise in attacks on government portals and strategic sectors, finance and defense among them (Rizki & Aditya, 2024). The pattern underlines why national cyber security policy needs to be treated as an integral part of Indonesia's strategic defense system.

At the global level, the dynamics have grown more complex with the spread of state-sponsored operations and the involvement of non-state actors in digital sabotage (Saramuke et al., 2025). The United States, Russia, and China have each made cyber defense a central component of their national security strategies, and cyber warfare and information warfare have become instruments in the contest for information control and digital dominance (Qushayyi, 2025). In the regional context, ASEAN has begun to consolidate cooperation through the ASEAN Cybersecurity Cooperation Strategy, which encourages cross-border collaboration to raise digital resilience (Jamil, 2025).

Indonesia has responded by strengthening its institutional and policy framework. The establishment of the National Cyber and Crypto Agency (BSSN) under Presidential Regulation No. 53 of 2017 marked an important milestone in the coordination of national cyber security. BSSN



holds the mandate to manage, monitor, and protect vital national information infrastructure and to raise public awareness (Adma et al., 2023). The enactment of Law No. 27 of 2022 on Personal Data Protection reinforced the state's position in maintaining digital sovereignty and in guaranteeing citizens' rights over their personal data (Aji, 2023). This policy also carries consequences for defense management, since data protection now sits inside the national security strategy rather than beside it.

Implementation nevertheless meets several obstacles. Coordination between institutions remains less than optimal, technical expertise in the cyber field is in short supply, and awareness of digital security among the general public is low (Ikhssani et al., 2024). The involvement of the private sector and the national defense industry also needs reinforcement if an integrated cyber security ecosystem is to take shape (Adma et al., 2023). A further weakness lies in defense diplomacy and international cooperation, which have not been used to their full extent even though interaction in cyberspace is inherently cross-border (Ar Rahman, 2020).

Cyber threats carry destructive potential and can paralyse defense systems. Attacks on command and control systems, sabotage of military communication networks, or the theft of intelligence data would each threaten the integrity of national defense (Habibi et al., 2025). Cyber security therefore needs to be read not only as a technological issue but as a strategic one bearing on political, economic, and security stability (Hidayat & Radyawanto, 2025). Work by Rai et al. (2022) shows that cyber security and cyber resilience play a substantial part in shaping national resilience, especially against threats that cross domains.

Seen from a public policy angle, strengthening cyber security connects closely to good governance and transparency. Policies that are not integrated with digital government systems risk creating fresh security gaps (Ramadhan et al., 2024). Cyber security approaches accordingly need to be woven into governance policy and national development strategy, in the same way that offset policy has been used to build self-reliance in the wider defense sector (Mas et al., 2016).

Geopolitically, Indonesia also faces a dilemma between cyber sovereignty and global openness of information. Efforts to strengthen digital sovereignty cannot be separated from the dynamics of international relations and cross-border cooperation (Anwar & Nepri, 2025). Digital diplomacy is an important instrument for advancing national interests in global cyberspace governance (Lumintosari et al., 2024). Cooperation between Indonesia and other countries, such as South Korea through the Korea Internet and Security Agency, shows concrete steps towards adaptive technical and policy capability (Rizki & Aditya, 2024).



Transforming the national cyber defense system requires synergy between military and non-military sectors. BSSN acts as the coordinating hub linking the Ministry of Defense, law enforcement agencies, academia, and the technology industry (Alfi et al., 2023). Building cyber human resource capacity is unavoidable, particularly within the Indonesian National Armed Forces, which is now forming dedicated cyber units to handle digital threats (Habibi et al., 2025). Defense education also plays a strategic role in building national awareness of cyber threats (Tarom, 2025).

The policy framework is in place, but the challenges of implementation and integration remain substantial. They include developing a national strategy that adapts to technological change, establishing an early warning system for cyber attacks, and enforcing the law against cross-border cybercrime (Siti Maesaroh, 2024). Cooperation between states also needs continuous strengthening so that Indonesia becomes a subject rather than merely an object in international cyber security governance (Rosy, 2020).

From this description, the problem addressed in this article is how Indonesia's national cyber security policy is implemented and integrated in the context of strategic defense, together with the strategic implications of that policy for national security in the digital age. The study analyses the relationship between cyber security policy and Indonesia's strategic defense through a review of policy documents, official reports, and recent academic work published between 2020 and 2025. It is expected to offer a conceptual contribution to strengthening the national cyber security posture and to formulating a digital security strategy that is sovereign, adaptive, and sustainable.

METHODS

This study adopts a systematic literature review design. The approach was chosen for its capacity to identify, evaluate, and interpret critically the body of research relevant to a defined set of questions. Applied here, it maps the landscape of Indonesia's national cyber security policy and analyses the implications of that policy for defense doctrine and posture. The design keeps the resulting synthesis anchored in a structured and transparent reading of the current literature rather than in the selective coverage typical of a narrative review.

Data collection proceeded in stages following the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) protocol. The first stage, identification, searched the Dimensions database. The search strategy combined Boolean operators with keyword strings relevant to the topic: ("keamanan siber" OR "strategi siber" OR "kedaulatan digital" OR



“pertahanan siber”) AND (“Indonesia”) AND (“pertahanan” OR “militer” OR “TNI” OR “BSSN”). The search was restricted to material published between 2020 and 2025.

The second stage, screening, evaluated every identified record against inclusion and exclusion criteria set in advance, with attention to articles that explicitly address the intersection between national cyber policy and the Indonesian defense and military domain. Records that treated cyber security purely as a technical or commercial matter, without a policy or defense dimension, were excluded. Each article that passed screening was then processed through a structured extraction form capturing (a) author and year of publication; (b) title; (c) research design; (d) policy focus, such as regulation or data sovereignty; (e) the key actors studied, such as BSSN, the Indonesian National Armed Forces, or the ministry responsible for communications and informatics; and (f) key findings and the strategic implications identified.

The extracted data were synthesised through thematic analysis in three steps. Open coding labelled the textual data drawn from the key findings of each article according to substantive content. Axial categorisation grouped similar codes into broader categories. Theme formation then examined the relationships among those categories to identify recurring central themes, namely regulatory fragmentation and cyber sovereignty, the dual role of BSSN and the Indonesian National Armed Forces in the defense architecture, and the obstacles to policy implementation in cyber capability development. Figure 1 presents the outcome of the selection process.

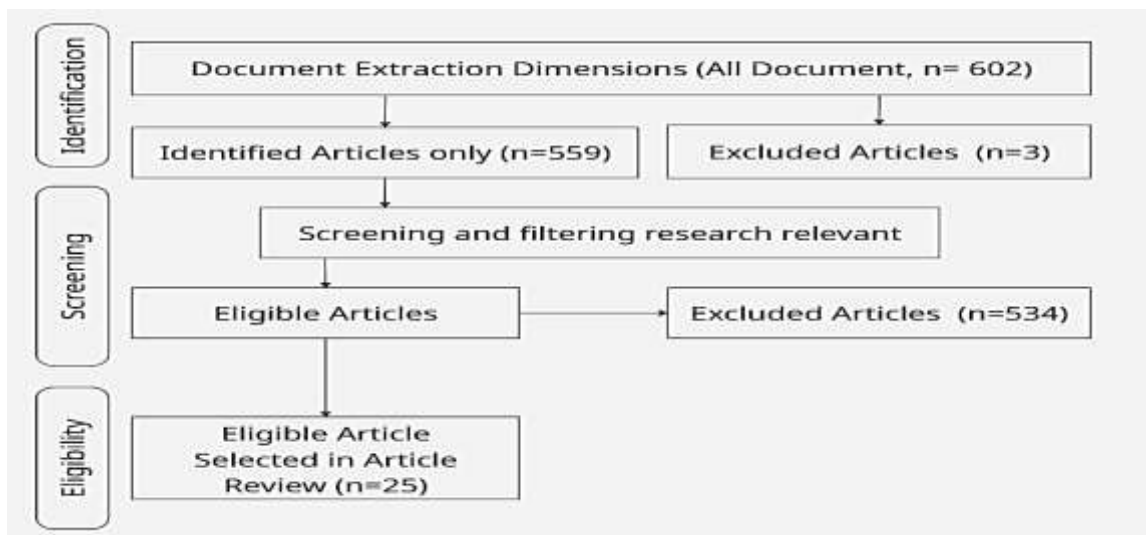


Figure 1. PRISMA Flow Diagram of Article Selection

RESULT AND DISCUSSION**Article Review**

Screening of 602 records produced a final corpus of 25 articles and policy documents. Thematic analysis of that corpus yielded five categories, summarised in Table 1 together with their key findings and strategic implications.

Table 1. Synthesis of Selected Articles

Category	Number of Studies	Key Findings	Strategic Implications
Transformation of the national cyber defense system	6	BSSN drives the transformation towards national cyber independence through regulation, infrastructure, and human resources (Adma et al., 2023; Delviana, 2024).	A comprehensive policy linking BSSN, the Ministry of Defense, and the Indonesian National Armed Forces is needed to develop a cyber defense force.
Cyber sovereignty and regulation	5	Harmonisation of digital law and national data sovereignty remains weak because regulations overlap (Aji, 2023; Anwar & Nepri, 2025; Siti Maesaroh, 2024).	The government needs a national cyber sovereignty framework that strengthens protection of strategic data and national security.
International cooperation and cyber diplomacy	4	Collaboration with partner countries such as the United Kingdom, South Korea, and the Netherlands strengthens cyber security capacity (Aksah & Nugraha, 2025; Qushayyi, 2025; Rizki & Aditya, 2024).	Indonesia needs to widen cyber diplomacy on the basis of strategic interest and defense technology transfer.
Technological	5	Building a human resource	Cyber education and



independence and cyber defense personnel		ecosystem and digital defense research is a priority for achieving cyber sovereignty (Ansori et al., 2025; Hidayat & Radyawanto, 2025).	research should be strengthened through the Indonesia Defense University, BSSN, and the national defense industry.
Cyber threats and risks to national defense	5	The intensity of attacks on critical defense and government infrastructure is rising (Alfi et al., 2023; Habibi et al., 2025).	An early detection system and an incident response team integrated with the national defense command system are needed.

DISCUSSION

Across the 25 sources, the transformation of the national cyber defense system emerges as the dominant issue in Indonesia's cyber security policy. Consistent with Adma et al. (2023), the role of BSSN as a coordinating hub is to harmonise cyber security standards across agencies, build a national cryptographic system, and prepare a cyber defense command within the structure of the Indonesian National Armed Forces. Delviana (2024) reinforces the argument by pointing to the urgency of forming a cyber force as part of the restructuring of Indonesia's digital defense.

On digital sovereignty and law, Anwar and Nepri (2025) stress the need to harmonise international and national legal instruments so that personal data protection becomes a strategic matter rather than an administrative one. Aji (2023) adds that Indonesia's digital political economy remains weak at balancing security interests against openness to investment. What follows from both is the case for national cyber security legislation that integrates legal, economic, and defense considerations instead of treating them separately.

International cooperation and cyber diplomacy have proved effective in raising Indonesia's capability. Aksah and Nugraha (2025) and Qushayyi (2025) show that collaboration with the United Kingdom and the Netherlands opens opportunities for technology transfer, capacity building, and improved interoperability of digital defense systems. As Rosy (2020) cautions, however, such cooperation needs to be directed towards self-reliance rather than towards dependence on foreign technology.

On technological independence and defense personnel, Ansori et al. (2025) emphasise resilient cyber leadership as a condition for handling multidimensional threats in the digital space.



Hidayat and Radyawanto (2025) argue that the development of cyber sovereignty has to rest on digital defense research and education. Cyber education at the Indonesia Defense University and the training programmes run by BSSN are strategic steps in building that capacity, and defense education more broadly contributes to public awareness of cyber threats (Tarom, 2025).

Finally, threats and risks to national defense show an upward trend across military and government infrastructure. Alfi et al. (2023) identify weaknesses in the digital security of public services, while Habibi et al. (2025) find that the cyber unit of the Indonesian National Armed Forces needs stronger cyber information infrastructure if it is to detect cross-border threats in real time. This is consistent with the logic of cyber resilience, which calls for systems that are robust and adaptive in the face of dynamic attacks. Taken together, the synthesis indicates that Indonesia's national cyber security policy is in a stage of transformation towards digital independence, still constrained by incomplete legal harmonisation, a limited pool of skilled personnel, and reliance on foreign technology. Implementation of the national strategy accordingly needs to be directed towards inter-agency synergy, defense technology research, and cyber diplomacy at the global level.

These findings resonate with several theoretical frameworks in cyber security and international relations. The development of offensive-capable cyber capacity, such as the formation of a cyber force (Delviana, 2024), illustrates the cybersecurity dilemma described by Buchanan (2017), in which any increase in defensive capability may be read by other states as an offensive threat. That reading underlines the value of cyber diplomacy (Aksah & Nugraha, 2025; Qushayyi, 2025) as a mechanism of transparency and confidence-building that limits escalation. The tension between the pursuit of autonomy (Hidayat & Radyawanto, 2025) and the necessity of international cooperation (Rosy, 2020) reflects Nye's (2017) account of power in cyberspace, in which deterrence rests on entanglement and norms as much as on retaliation, and absolute digital sovereignty is not attainable. The urgency of protecting critical infrastructure (Alfi et al., 2023) and strengthening the cyber unit of the Indonesian National Armed Forces (Habibi et al., 2025) aligns with Dunn Cavelty (2008), who positions cyber resilience not merely as a technical capability but as a core function of state sovereignty in the twenty-first century.

CONCLUSION

Indonesia's national cyber security policy acts as the principal catalyst for a fundamental change in the country's strategic defense posture. That change appears most clearly in a dual institutional architecture centred on BSSN as national coordinator and the Indonesian National



Armed Forces as military operator, evidenced by the initiative to establish a cyber force. It also encompasses the adaptation of the universal defense doctrine to the cyber domain and the use of defense diplomacy to raise capability, all directed towards digital sovereignty. The strategic effect of these efforts remains constrained, however, by the incomplete harmonisation of a comprehensive national legal framework.

Two recommendations follow. In policy terms, the government and the legislature should treat the synchronisation of cyber security legislation, including the draft Cyber Security Bill, as an urgent priority, so as to provide legal certainty and a clear demarcation of authority among BSSN, the Indonesian National Armed Forces, and other stakeholders. Academically, further research should move towards empirical methods, including qualitative interviews and quantitative analysis, in order to test the effectiveness of BSSN–TNI institutional synergy in practice and to measure the actual readiness of Indonesia's cyber defense capability.

The study has limitations. It rests on a single bibliographic database and on published material, so unpublished operational documents and classified defense practice fall outside its reach. The corpus is also dominated by Indonesian-language sources, which strengthens contextual depth while limiting comparative scope. Future work drawing on multiple databases and on primary data from the institutions concerned would test and extend the conclusions offered here.

REFERENCES

- Adma, A., Surbakti, Y. M., & Sari, P. (2023). Transformasi sistem pertahanan siber Indonesia dengan BSSN sebagai poros dan motor penggerak menuju angkatan siber mandiri di masa depan. *Jurnal Kajian Strategik Ketahanan Nasional*, 6(1), Article 7. <https://doi.org/10.7454/jkskn.v6i1.10077>
- Aji, M. P. (2023). Sistem keamanan siber dan kedaulatan data di Indonesia dalam perspektif ekonomi politik (studi kasus perlindungan data pribadi). *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, 13(2), 222–238. <https://doi.org/10.22212/jp.v13i2.3299>
- Aksah, N. S. M., & Nugraha, I. F. (2025). Kerja sama Indonesia dan Inggris dalam upaya meningkatkan kapabilitas keamanan siber. *Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi*, 2(3), 1–16. <https://doi.org/10.62383/konsensus.v2i3.831>
- Alfi, M., Yundari, N. P., & Tsaqif, A. (2023). Analisis risiko keamanan siber dalam transformasi digital pelayanan publik di Indonesia. *Jurnal Kajian Strategik Ketahanan Nasional*, 6(2),



- Article 5. <https://doi.org/10.7454/jkskn.v6i2.10082>
- Ansori, A., Ali, K., Susilo, T., Hadisuseno, B., & Amperawan, C. (2025). Cyber leadership in the digital age: Building a resilient Indonesian defense in cyberspace. *Indonesian Journal of Interdisciplinary Research in Science and Technology*, 3(9), 915–932.
- Anwar, S., & Nepri, J. E. (2025). Harmonisasi hukum digital: Tantangan global dan strategi adaptif Indonesia dalam era kedaulatan siber. *Hutanasyah: Jurnal Hukum Tata Negara*, 4(1), 69–88. <https://doi.org/10.37092/hutanasyah.v4i1.1297>
- Ar Rahman, L. L. (2020). Implikasi diplomasi pertahanan terhadap keamanan siber dalam konteks politik keamanan. *Jurnal Diplomasi Pertahanan*. <https://files.core.ac.uk/download/pdf/595551633.pdf>
- Buchanan, B. (2017). *The cybersecurity dilemma: Hacking, trust and fear between nations*. Oxford University Press.
- Budiyanto, D., & Mabruri, M. (2025). Pentingnya keamanan siber dalam era digital: Tinjauan global dan kondisi di Indonesia. *Prosiding Seminar Nasional Sains dan Teknologi (SainTek)*, 2(1), 981–994. <https://conference.ut.ac.id/index.php/saintek/article/view/5134>
- Cloramidine, F., & Badaruddin, M. (2023). Mengukur keamanan siber Indonesia melalui indikator pilar kerjasama dalam Global Cybersecurity Index (GCI). *Jurnal Sosial dan Humaniora*, 8(1), 57–73. <https://doi.org/10.47313/pjsh.v8i1.1957>
- Delviana, N. (2024). Inisiasi pembentukan angkatan siber dan digital dalam organisasi Tentara Nasional Indonesia. *Jurnal Syntax Admiration*, 5(2), 392–402. <https://doi.org/10.46799/jsa.v4i12.1016>
- Dunn Cavelty, M. (2008). *Cyber-security and threat politics: US efforts to secure the information age*. Routledge.
- Habibi, H., Widodo, P., & Sianturi, D. (2025). Strategi satuan siber Tentara Nasional Indonesia dalam penguatan infrastruktur informasi siber. *Journal of Current Research in Management, Policy, and Social Studies*. <https://ejournal.hakhara-institute.com/MPSS/article/view/78>
- Hidayat, S., & Radyawanto, A. S. (2025). Kemandirian siber Indonesia: Tantangan dan peluang menuju kedaulatan digital. *International Journal of Social and Management Studies*, 6(5), 98–102. <https://www.ijosmas.org/index.php/ijosmas/article/view/537>
- Ikhssani, A., Mudra, C., & Prasidya, F. G. (2024). Cybersecurity dan tata kelola intelijen. *Jurnal Kajian Strategik Ketahanan Nasional*, 7(1), Article 2. <https://doi.org/10.7454/jkskn.v7i1.10086>



- Jamil, M. (2025). Strategi siber Indonesia dalam kerja sama ASEAN untuk menjaga kedaulatan digital. E-Journal APPISI. <https://ejournal.appisi.or.id/index.php/Komunikasi/article/view/421>
- Lumintosari, F. R., Santoso, M. P. T., & Hakiem, F. N. (2024). Peluang dan tantangan diplomasi digital dalam meningkatkan keamanan siber Indonesia. *Innovative: Journal of Social Science Research*, 4(3), 746–754. <https://doi.org/10.31004/innovative.v4i3.10537>
- Mas, R., Indrawan, J., & Widiyanto, D. B. (2016). Kebijakan offset dalam membangun kemandirian pertahanan negara. *Jurnal Pertahanan dan Bela Negara*, 6(2), 29–50. <https://doi.org/10.33172/jpbh.v6i2.306>
- Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security*, 41(3), 44–71. https://doi.org/10.1162/ISEC_a_00266
- Qushayyi, M. F. (2025). The dynamics of cyber security cooperation between countries: A case study of Indonesia and the Netherlands. *Journal of Peace, Security and Democracy*, 1(1), 37–56. <https://doi.org/10.63280/jpsd.v1i1.42626>
- Rai, I. N. A. S., Heryadi, D., & Kamaluddin, N. A. (2022). The role of Indonesia to create security and resilience in cyber spaces. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, 13(1), 43–66. <https://doi.org/10.22212/jp.v13i1.2641>
- Ramadhan, T., Pujiyanto, R., & Santoso, F. B. (2024). Strategi penanganan keamanan siber di Indonesia. *Journal of Informatic and Information Security*, 5(2), 307–320. <https://doi.org/10.31599/v0xr7273>
- Rizki, D. P., & Aditya, R. (2024). Kerjasama Badan Siber dan Sandi Negara (BSSN) dan Korea Internet and Security Agency (KISA) dalam meningkatkan keamanan cyber di Indonesia (2022). *Global Mind*, 6(2), 43–55. <https://doi.org/10.53675/jgm.v6i2.1362>
- Rosy, A. F. (2020). Kerjasama internasional Indonesia: Memperkuat keamanan nasional di bidang keamanan siber. *Journal of Government Science (GovSci): Jurnal Ilmu Pemerintahan*, 1(2), 118–129. <https://doi.org/10.54144/govsci.v1i2.12>
- Saramuke, S. S., Putri, V. A., Sormin, A. M., & Nugraha, M. (2025). Ancaman keamanan siber dan peran aktor non-negara di dunia digital. *Syntax Idea*, 7(2), 141–152. <https://jurnal.syntax-idea.co.id/index.php/syntax-idea/article/view/12437>
- Siti Maesaroh, R. (2024). Tantangan keamanan siber dan implikasinya terhadap hukum kenegaraan: Tinjauan atas peran negara dalam menjamin ketahanan digital. *Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam*, 4(2), 255–274. <https://doi.org/10.14421/3n8bxw79>



Tarom, M. (2025). The strategic role of defense education in strengthening Indonesia's national security system. *Jurnal Pendidikan dan Pengembangan Sumber Daya Pertahanan*, 2(1), 12–19. <https://doi.org/10.63210/jp3.v2i1.138>

