International Journal of Technology and Education Research

https://e-journal.citakonsultindo.or.id/index.php/IJETER

E-ISSN: 2986-0733

# The Development Of Cybersecurity In Supporting Indonesia's Digital Transformation

**Harry Pratomo B.[1], Aulia Khamas H.[2], Rudy A.G. Gultom[3]**

[1,2] Cyber Defense Engineering, Faculty of Defense Engineering and Technology, Indonesian Defense University, Bogor, Indonesia

[3] Faculty of Defense Engineering and Technology, Indonesian Defense University, Bogor, Indonesia

Corresponding Author: harry.bagaskoro@tp.idu.ac.id

**Abstract**

*Indonesia's digital transformation has accelerated from early e-government implementation toward integrated digital public services, while cybersecurity has evolved into a more institutionalized national capability. This study examines the trajectory of Indonesia's digital transformation, the parallel development of cybersecurity capacity, and the extent to which both processes are aligned. Using qualitative document analysis supported by descriptive synthesis of policy documents, journal articles, and authoritative institutional reports, the study identifies four phases of digital transformation and a parallel strengthening of cybersecurity governance through BSSN and national cybersecurity policy. The findings show that policy-level alignment has improved, as reflected in SPBE development, the launch of INA Digital, and Indonesia's improved standing in the Global Cybersecurity Index. However, operational resilience remains uneven, particularly in coordination, backup readiness, human resources, and incident response. The study concludes that cybersecurity should be treated as a structural enabler of digital transformation and that secure-by-design principles are needed to ensure sustainable digital governance in Indonesia.*

**Keyword: digital transformation, cybersecurity, Indonesia, BSSN, SPBE, INA Digital.**

## INTRODUCTION

Indonesia has accelerated its digital transformation through regulatory reform, service integration, and the expansion of national digital infrastructure. Presidential Regulation No. 82



Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

of 2023 provides a legal basis for accelerating digital transformation and integrating national digital services, including priority SPBE applications and national interoperability arrangements (Government of Indonesia, 2023). In parallel, the government launched INA Digital as a GovTech platform to consolidate selected public services and reduce fragmentation across ministries and agencies (Government of Indonesia, 2024a, 2024b). These developments show a transition from isolated digitization initiatives toward a more integrated model of digital governance.

The progress of digital transformation is also visible in international assessment. The United Nations Department of Economic and Social Affairs reported that Indonesia's score in the UN E-Government Survey 2024 reached 0.7991, placing the country in the *Very High E-Government Development Index* category for the first time (United Nations Department of Economic and Social Affairs [UN DESA], 2024; Government of Indonesia, 2024c). This achievement reflects improvement in online service delivery, telecommunications infrastructure, and human capital. Studies on digital government also indicate that digital transformation in public services can improve efficiency, transparency, and accessibility when institutional and technological support are aligned (Syafarudin & Abd Haris, 2025; Baharuddin Kasim et al., 2025).

However, the acceleration of digital public services also increases dependency on secure data, reliable infrastructure, and trusted identity systems. As public administration, data exchange, and citizen services become more interconnected, cybersecurity becomes a core requirement for maintaining continuity and trust. Digital transformation without adequate cybersecurity may create faster services but also expand exposure to service disruption, data breaches, and identity misuse. Recent reviews of digital governance emphasize that the success of e-government depends not only on technology adoption but also on resilience, governance quality, and adaptation capacity (Syafarudin & Abd Haris, 2025; Baharuddin Kasim et al., 2025).

Indonesia has responded to these challenges through institutional and governance strengthening, especially through the National Cyber and Crypto Agency (BSSN). Previous studies show that BSSN plays an important role in cybersecurity governance, cyber sovereignty, and the coordination of national cyber policy (Chotimah, 2019; Aji, 2025). Other studies note that cybersecurity governance in Indonesia has historically been partial and sectoral, creating difficulties in integrating cyber defense across institutions (Sudarmadi & Runturambi, 2019). More recent work continues to underline the need for stronger regulatory coordination, improved capacity building, and more integrated cyber protection in the digital transformation era (Rahmawati et al., 2025; Aji, 2025). In short, the direction of policy is clear, but the alignment between digital expansion and cyber readiness remains uneven.



Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

Although prior studies have examined digital transformation and cybersecurity in Indonesia, these two streams are still often treated separately. Research on digital transformation tends to discuss policy evolution, service integration, and e-government development (Gusman, 2024; Angelica et al., 2024; Syafarudin & Abd Haris, 2025), while cybersecurity studies focus on BSSN, cyber governance, and threat response (Chotimah, 2019; Sudarmadi & Runturambi, 2019; Aji, 2025; Rahmawati et al., 2025). As a result, there is still a lack of integrated analysis showing how cybersecurity development supports Indonesia's digital transformation trajectory, where the alignment is already visible, and which capability gaps remain critical. This gap is important because digital transformation without sufficient cybersecurity may produce vulnerable systems, fragmented trust, and weak long-term resilience.

Therefore, this study examines the development of cybersecurity in supporting Indonesia's digital transformation through a structured review of policy, institutional, and capability-related evidence. The study aims to: (1) map the main stages of Indonesia's digital transformation from early e-government initiatives to integrated digital public services; (2) analyze the development of cybersecurity governance and national cybersecurity capacity; and (3) identify the alignment and remaining gaps between cybersecurity development and digital transformation requirements. By doing so, the study provides a concise analytical basis for understanding cybersecurity as an enabler of sustainable digital transformation in Indonesia.

## METHOD

This study employs a qualitative descriptive design based on document analysis and a targeted literature review. The purpose of this approach is to identify how cybersecurity development has supported Indonesia's digital transformation through policy, institutional, and capability-related evidence. This design is appropriate because the study focuses on interpreting documented developments rather than measuring primary data directly. Similar approaches have been used in studies of digital governance and cybersecurity policy when the objective is to map policy evolution, institutional roles, and capability gaps rather than to test causal relationships statistically (Syafarudin & Abd Haris, 2025; Aji, 2025; Ramadhan, 2025).

### Data Sources

The study relies on secondary sources from three groups. First, official policy documents and government publications were used to capture the legal and institutional context of digital transformation in Indonesia, including Presidential Regulation No. 82 of 2023, INA Digital policy



Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

materials, and the UN E-Government Survey 2024 (Government of Indonesia, 2023; Government of Indonesia, 2024a, 2024b, 2024c; UN DESA, 2024). Second, peer-reviewed journal articles with DOI were selected to support the academic discussion on digital transformation and cybersecurity governance, especially studies on e-government implementation, cyber sovereignty, and BSSN's institutional role (Chotimah, 2019; Gusman, 2024; Angelica et al., 2024; Syafarudin & Abd Haris, 2025; Aji, 2025; Ramadhan, 2025). Third, supporting review and policy-analysis articles were used to strengthen the synthesis of cybersecurity challenges in the digital transformation era (Rahmawati et al., 2025; Baharuddin Kasim et al., 2025).

**Selection Criteria**

The sources were selected using four criteria. Documents had to:

1. be directly relevant to Indonesia's digital transformation or cybersecurity development;
2. discuss policy, governance, institutional capacity, or service integration;
3. be published in an academic journal with DOI or issued by an official institution; and
4. provide sufficient information for thematic coding and comparison.

Sources that were too general, duplicated the same argument, or lacked clear relevance to Indonesia were excluded. This selective design keeps the article concise and ensures that the references are strong and traceable.

**Analytical Procedure**

The analysis was conducted in three steps. First, the documents were screened and grouped into two thematic domains: digital transformation and cybersecurity development. Second, the content of each source was coded into subthemes such as policy reform, digital service integration, institutional role, cybersecurity governance, capability development, and resilience. Third, the findings were compared to identify the points of alignment and the remaining gaps between digital transformation and cybersecurity support. For the synthesis stage, the study uses a simple comparative structure:

- a timeline of digital transformation milestones,
- a timeline of cybersecurity milestones, and
- a matrix of alignment between both domains.

This structure is useful for a short technical article because it allows the reader to see the evolution of both domains side by side without requiring quantitative modeling.

**Analytical Focus**

The analysis is centered on three levels. The first is the policy level, which includes legal



Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

and strategic directions for digital government and cybersecurity. The second is the institutional level, which includes the role of BSSN and the coordination of ministries and agencies. The third is the capability level, which includes infrastructure readiness, governance maturity, cyber resilience, and the extent to which digital transformation is supported by secure systems. This layered focus is consistent with current literature showing that digital governance outcomes depend not only on technology, but also on institutional coordination and cybersecurity capacity (Chotimah, 2019; Sudarmadi & Runturambi, 2019; Aji, 2025; Ramadhan, 2025).

## RESULTS AND DISCUSSION

### Trajectory of Digital Transformation in Indonesia

The literature indicates that Indonesia's digital transformation has progressed through several discernible phases. The early phase was dominated by e-government adoption and the institutionalization of the Electronic-Based Government System (SPBE), which established a formal basis for digitizing bureaucratic processes and public service delivery (Angelica et al., 2024; Government of Indonesia, 2018; Government of Indonesia, 2023). This stage was followed by a broader push toward digital infrastructure expansion and service digitalization, including national connectivity initiatives and the widening use of online public services (Gusman et al., 2024; ERIA, 2023).

**Table 1. Trajectory of Digital Transformation and Cybersecurity in Indonesia**

| Phase | Digital Transformation Development | Cybersecurity Development | Main Interpretation |
|---|---|---|---|
| **Phase 1: Early e-government** | Introduction of e-government policy and SPBE as a basis for administrative digitization (Angelica et al., 2024; Government of Indonesia, 2018). | Cybersecurity was still fragmented and not yet strongly institutionalized. | Digital transformation started earlier than a robust cybersecurity architecture. |
| **Phase 2: Infrastructure expansion** | Expansion of digital infrastructure and online public services (Gusman et al., 2024; ERIA, 2023). | BSSN was strengthened as the central cybersecurity institution (Sudarmadi & Runturambi, 2019; | Cybersecurity began to become a supporting pillar of digital expansion. |



Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Technology and Education Research

https://e-journal.citakonsultindo.or.id/index.php/IJETER

E-ISSN: 2986-0733

| Phase | Digital Transformation Development | Cybersecurity Development | Main Interpretation |
|---|---|---|---|
| | | Haryanto & Sutra, 2023). | |
| **Phase 3: Service integration** | Development of IKD and INA Digital for integrated public services (Zainudin, 2025; Government of Indonesia, 2024a; Government of Indonesia, 2024b). | Indonesia's GCI score increased from 94.88 in 2020 to 100 in 2024 (ITU, 2024; Statbase, 2026). | Policy-level alignment became stronger, but implementation pressure also increased. |
| **Phase 4: Consolidation and resilience** | Focus shifted to interoperability, platform integration, and unified service delivery (Government of Indonesia, 2024a; Indonesia Baik, 2024). | Remaining issues include incident response, backup readiness, and coordination gaps (Meliala, 2024; Rahmawati et al., 2025). | Cybersecurity is now a prerequisite for sustainable digital governance. |

A later phase is characterized by service integration and digital identity development, especially through the Indonesian Digital Identity (IKD) policy and the GovTech initiative INA Digital. These developments indicate that the policy direction has shifted from isolated digitalization efforts toward a more integrated digital public-service ecosystem (Zainudin, 2025; Government of Indonesia, 2024a; Government of Indonesia, 2024b; Indonesia Baik, 2024). In the United Nations E-Government Survey 2024, Indonesia is also reported to have moved into the very high EGDI group, which suggests that its digital government capacity has improved in formal terms (UN DESA, 2024).

However, the reviewed studies also show that this progression is not uniform. Although policy integration has accelerated, implementation challenges remain, particularly in interoperability, institutional coordination, data governance, and organizational readiness (Frinaldi et al., 2024; Angelica et al., 2024; Hamda & Wahyudi, 2025). This means that Indonesia's digital transformation is no longer merely a matter of digitizing services, but increasingly a matter of sustaining an integrated, secure, and reliable digital ecosystem.



Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Technology and Education Research

https://e-journal.citakonsultindo.or.id/index.php/IJETER

E-ISSN: 2986-0733

**Development of Cybersecurity Capacity in Indonesia**

The findings also show that Indonesia's cybersecurity landscape has evolved from a fragmented policy environment into a more institutionalized system. The establishment and strengthening of the National Cyber and Crypto Agency (BSSN) represent a major milestone in national cybersecurity governance, as BSSN functions as the central coordinating body for cybersecurity policy, technical development, and inter-agency collaboration (Sudarmadi & Runturambi, 2019; Haryanto & Sutra, 2023; Chotimah, 2019; Hamda & Wahyudi, 2025). The literature also shows that BSSN's role is increasingly linked to human-capital development, cyber diplomacy, and coordination with domestic and international stakeholders (BSSN, 2024; A. R. Hamda & Wahyudi, 2025).

At the international level, Indonesia's cybersecurity capacity has improved substantially. The Global Cybersecurity Index (GCI) shows that Indonesia's score increased from 94.88 in 2020 to 100 in 2024, placing the country in Tier 1 (role-modelling) in the latest ITU classification (ITU, 2024; Statbase, 2026; Meutya Hafid, 2025). This upward trend suggests stronger commitment in legal, technical, organizational, capacity-building, and cooperative dimensions of cybersecurity (Haryanto & Sutra, 2023; ITU, 2024).

Nevertheless, the literature also warns that these improvements should not be interpreted as complete operational maturity. Several studies note continuing issues related to fragmented coordination, shortage of skilled cybersecurity personnel, limited backup readiness, and reactive responses to major incidents (Khoirunnisa & Jubaidi, 2024; Rahmawati et al., 2025; Meliala, 2024). In other words, Indonesia's cybersecurity posture has improved at the policy and institutional level, but operational resilience still requires further strengthening.

**Alignment Between Digital Transformation and Cybersecurity**

The central finding of this study is that Indonesia's cybersecurity development increasingly supports digital transformation, but the alignment remains incomplete. At the policy level, both domains have advanced in parallel: digital transformation has moved toward integrated public services, while cybersecurity has matured through BSSN, regulatory expansion, and improved international index performance (Angelica et al., 2024; Government of Indonesia, 2024a; ITU, 2024). The launch of INA Digital and the broader SPBE integration agenda illustrate the government's effort to build a unified digital service architecture, which in turn increases the need for stronger security controls and governance (Government of Indonesia, 2024a; Government of Indonesia, 2024b; Indonesia Baik, 2024).

At the implementation level, however, cybersecurity often appears as a reactive



Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

safeguard rather than an embedded design principle. The literature repeatedly identifies gaps in preparedness, backup systems, inter-agency coordination, and human resources, particularly when large-scale digital public systems are disrupted (Rahmawati et al., 2025; Meliala, 2024; Sudarmadi & Runturambi, 2019). This is important because the more integrated the digital ecosystem becomes, the greater the potential impact of security failures.

Accordingly, cybersecurity should be treated not as an auxiliary feature but as a structural enabler of digital transformation. Digital identity systems, integrated government platforms, and cross-ministerial service portals require secure-by-design architecture, strong governance, and continuous operational readiness. Without these foundations, the gains of digital transformation may be offset by heightened exposure to cyber incidents, data breaches, and service disruption (Zainudin, 2025; Rahmawati et al., 2025; Government of Indonesia, 2024a).

**Table 2. Alignment and Gap Between Digital Transformation and Cybersecurity**

| Dimension | Finding | Implication |
|---|---|---|
| **Policy** | **Digital transformation and cybersecurity both show clear policy advancement (Angelica et al., 2024; Haryanto & Sutra, 2023; Government of Indonesia, 2024a).** | **National policy direction is broadly supportive of secure digitalization.** |
| **Institutions** | **BSSN has become a central coordinating actor in cybersecurity governance (Chotimah, 2019; Hamda & Wahyudi, 2025).** | **Institutional foundations exist, but coordination must remain consistent.** |
| **International index** | **Indonesia's GCI increased from 94.88 in 2020 to 100 in 2024 (ITU, 2024; Statbase, 2026).** | **Formal cybersecurity capacity has improved significantly.** |
| **Operational resilience** | **Fragmentation, skill shortages, and weak recovery mechanisms remain recurring concerns (Meliala, 2024; Rahmawati et al., 2025; Hakim, 2025).** | **Operational readiness remains a gap despite better formal indicators.** |
| **Overall relationship** | **Cybersecurity increasingly supports digital transformation, but not always from the design stage (Zainudin, 2025; Rahmawati et al., 2025).** | **Secure-by-design integration is still needed.** |



Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Technology and Education Research

https://e-journal.citakonsultindo.or.id/index.php/IJETER

E-ISSN: 2986-0733

**Gap Analysis**

The reviewed literature reveals four main gaps. First, many studies discuss digital transformation and cybersecurity separately, leaving the relationship between them underexplored (Angelica et al., 2024; Haryanto & Sutra, 2023; Hakim, 2025). Second, cybersecurity improvement is often measured by policy or index-based indicators, while operational resilience is less frequently examined (ITU, 2024; Statbase, 2026; Rahmawati et al., 2025). Third, sector-specific evidence remains limited, especially regarding how cybersecurity supports the digital transformation of government services, identity systems, and integrated public platforms (Zainudin, 2025; Government of Indonesia, 2024a; Government of Indonesia, 2024b). Fourth, human-resource readiness and organizational culture are acknowledged as important but rarely integrated into a single explanatory framework (Frinaldi et al., 2024; Meliala, 2024; BSSN, 2024).

These gaps suggest that future research should move beyond descriptive parallel accounts and develop integrative models that connect policy development, institutional capacity, operational resilience, and service-level outcomes. For Indonesia, this is especially relevant because digital transformation is proceeding rapidly while cybersecurity demands are rising simultaneously.

**Implications**

The findings imply that Indonesia needs a more explicit secure-by-design approach in its digital transformation agenda. This means that cybersecurity requirements should be embedded from the beginning in the design of digital public services, rather than added after implementation. Such an approach would help ensure that integration, interoperability, and efficiency are matched by confidentiality, integrity, availability, and recovery capability (Rahmawati et al., 2025; Zainudin, 2025; Government of Indonesia, 2024a).

The findings also suggest that global indicators such as the GCI should be interpreted cautiously. A high GCI score is important, but it does not by itself guarantee full operational resilience. For this reason, future evaluations of digital transformation should combine policy indicators, technical readiness, incident-response capability, and service continuity measures (ITU, 2024; Statbase, 2026; Meutya Hafid, 2025).



Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Technology and Education Research

https://e-journal.citakonsultindo.or.id/index.php/IJETER

E-ISSN: 2986-0733




**Figure 1. Conceptual framework of the relationship between Indonesia's digital transformation and cybersecurity development**

## CONCLUSION

This study shows that Indonesia's digital transformation has progressed from early e-government implementation toward more integrated and service-oriented digital governance, as reflected in SPBE development, digital identity policy, and the launch of INA Digital. In parallel, Indonesia's cybersecurity capacity has become more institutionalized through the strengthening of BSSN and the improvement of the country's Global Cybersecurity Index score, which indicates stronger formal commitment to cybersecurity governance.

However, the study also finds that the alignment between digital transformation and



Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

cybersecurity remains incomplete. Although policy direction, institutional capacity, and international index performance have improved, operational resilience still faces important challenges, particularly in coordination, human resources, backup readiness, and incident response. These gaps suggest that cybersecurity is not yet fully embedded as a secure-by-design principle in the implementation of digital public services.

The main implication is that cybersecurity should be treated as a structural enabler of digital transformation rather than as a supplementary response after system deployment. For Indonesia, sustainable digital transformation requires integrated governance, stronger technical readiness, continuous capacity building, and resilience-oriented service design. Future studies should therefore move beyond parallel descriptions of digitalization and cybersecurity and examine their relationship through sector-specific and operational indicators.

**REFERENCE**

Angelica, et al. (2024). Trajectory of digital transformation policy in Indonesia from 2003 to 2024.

Chotimah, H. C. (2019). Tata kelola keamanan siber dan diplomasi siber Indonesia di bawah kelembagaan Badan Siber dan Sandi Negara. Politica, 10(2), 163–180.

ERIA. (2023). Accelerating digital transformation in Indonesia: Technology, market, and policy.

Frinaldi, et al. (2024). Digital transformation of government administration: Analysis of efficiency, transparency, and challenges in Indonesia.

Government of Indonesia. (2018). Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.

Government of Indonesia. (2023). Peraturan Presiden Republik Indonesia Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional.

Government of Indonesia. (2024a, May 27). President Jokowi launches INA Digital. Sekretariat Kabinet Republik Indonesia.

Government of Indonesia. (2024b). SPBE Summit 2024 materials and announcements.

Gusman, et al. (2024). Development of the Indonesian government's digital transformation.

Hafid, M. (2025). Remarks on Indonesia's GCI ranking improvement.

Hakim, A. (2025). Understanding Indonesia's cyber security policies: Opportunities and challenges in the digitalization transformation era.

Haryanto, A., & Sutra, S. M. (2023). Upaya peningkatan keamanan siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) tahun 2017–2020. Global Political Studies Journal, 7(1). https://doi.org/10.34010/gpsjournal.v7i1.8141

Indonesia Baik. (2024). Luncurkan Govtech INA Digital, apa tuh?.



Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Telecommunication Union. (2024). Global cybersecurity index 2024.

Khoirunnisa, & Jubaidi. (2024). Indonesia's cyber security strategy: Countering the threats of cybercrime and cyberterrorism.

Meliala, B. N. (2024). Indonesia cybersecurity policy toward data and privacy protection: Literature review study. International Journal of Research and Applied Technology, 4(2), 354–361. https://ojs.unikom.ac.id/index.php/injuratech/article/view/19664

MENPANRB. (2024, September 20). Indonesia naik 13 peringkat pada UN E-Government Survey 2024.

Rahmawati, et al. (2025). Keamanan siber: Respon strategis Indonesia terhadap eskalasi ancaman digital.

Statbase. (2026). Global cybersecurity index | Indonesia (2020–2024).

Sudarmadi, D. A., & Runturambi, A. J. S. (2019). Strategi Badan Siber dan Sandi Negara (BSSN) dalam menghadapi ancaman siber di Indonesia. Jurnal Kajian Stratejik Ketahanan Nasional, 2(2). https://doi.org/10.7454/jkskn.v2i2.10028

United Nations. (2024). UN e-government survey 2024.

Zainudin, et al. (2025). Digital ID policy in support of digital transformation in Indonesia.

Aji, M. P. (2025). Cybersecurity politics in building cyber sovereignty in Indonesia. Society.

Angelica, L., Soenarto, N. A., & Salsabila, N. (2024). Trajectory of digital transformation policy in Indonesia from 2003 to 2024: Analysis of trends and policy contents. Proceedings of the Indonesian Association for Public Administration (IAPA).

Baharuddin Kasim, B., Ferriswara, D., & Haryati, E. (2025). Digital transformation in public services: A literature review on bureaucratic innovation and adaptation in the era of digital government. International Journal of Social Science and Humanity.

Chotimah, H. C. (2019). Tata kelola keamanan siber dan diplomasi siber Indonesia di bawah kelembagaan Badan Siber dan Sandi Negara. Politica, 10(2), 163–180.

Economic Research Institute for ASEAN and East Asia (ERIA). (2023). Accelerating digital transformation in Indonesia: Technology, market, and policy.

Frinaldi, A., et al. (2024). Digital transformation of government administration: Analysis of efficiency, transparency, and challenges in Indonesia. Proceedings of the Indonesian Association for Public Administration (IAPA).

Government of Indonesia. (2018). Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.

Government of Indonesia. (2023). Peraturan Presiden Republik Indonesia Nomor 82 Tahun 2023



Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional.

Government of Indonesia. (2024a, May 27). President Jokowi launches INA Digital to transform public services. Sekretariat Kabinet Republik Indonesia.

Government of Indonesia. (2024b). SPBE Summit 2024: Materials and announcements. Ministry of Administrative and Bureaucratic Reform.

Gusman, S. W., et al. (2024). Development of the Indonesian government's digital transformation. Dinasti International Journal of Education Management and Social Science.

Hafid, M. (2025). Remarks on Indonesia's Global Cybersecurity Index ranking improvement. Ministry of Communication and Digital.

Hakim, A. (2025). Understanding Indonesia's cyber security policies: Opportunities and challenges in the digitalization transformation era. Journal of Law and Social Policy.

Hamda, A. R., & Wahyudi, R. (2025). Literasi digital: Cyber security sebagai fondasi ketahanan nasional di era transformasi digital. Literasiana: Jurnal Kajian Literasi dan Edukasi.

Haryanto, A., & Sutra, S. M. (2023). Upaya peningkatan keamanan siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) tahun 2017–2020. Global Political Studies Journal, 7(1). https://doi.org/10.34010/gpsjournal.v7i1.8141

Indonesia Baik. (2024). Luncurkan Govtech INA Digital, apa tuh? https://indonesiabaik.id

International Telecommunication Union. (2024). Global Cybersecurity Index 2024. Geneva: ITU.

Khoirunnisa, I., & Jubaidi, R. (2024). Indonesia's cyber security strategy: Countering the threats of cybercrime and cyberterrorism. International Journal of Security Studies.

Meliala, B. N. (2024). Indonesia cybersecurity policy toward data and privacy protection: Literature review study. International Journal of Research and Applied Technology, 4(2), 354–361. https://ojs.unikom.ac.id/index.php/injuratech/article/view/19664

Ministry of Administrative and Bureaucratic Reform of the Republic of Indonesia (PANRB). (2024, September 20). Indonesia naik 13 peringkat pada UN E-Government Survey 2024. https://www.menpan.go.id

National Cyber and Crypto Agency (BSSN). (2024). National cybersecurity strategy and incident management framework [policy document].

Rahmawati, R., Bintang Semesta, B. F., & colleagues. (2025). Keamanan siber: Respon strategis Indonesia terhadap eskalasi ancaman digital. Triwikrama: Jurnal Multidisiplin Ilmu Sosial.

Ramadhan, G. (2025). Analisis strategi keamanan nasional Indonesia dalam menghadapi ancaman siber. Jurnal Ilmu Pengetahuan dan Keamanan Nasional.

Statbase. (2026). Global Cybersecurity Index | Indonesia (2020–2024). https://statbase.org



Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

Sudarmadi, D. A., & Runturambi, A. J. S. (2019). Strategi Badan Siber dan Sandi Negara (BSSN) dalam menghadapi ancaman siber di Indonesia. Jurnal Kajian Stratejik Ketahanan Nasional, 2(2). https://doi.org/10.7454/jkskn.v2i2.10028

Syafarudin, S., & Abd Haris. (2025). Digital transformation in public services: A study of e-government implementation in Indonesia. International Journal of Law and Society, 2(4), 169–179. https://doi.org/10.62951/ijls.v2i4.797

United Nations Department of Economic and Social Affairs (UN DESA). (2024). United Nations E-Government Survey 2024. New York, NY: UN DESA.

Zainudin, A., et al. (2025). Digital ID policy in support of digital transformation in Indonesia. Jurnal Bina Praja.



Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.