SITJOURNAL
Security Intelligence Terrorism Journal

Security Intelligence Terrorism Journal (SITJ), Vol. 03 No. 02 (2026), pp. 93-98
Research Article
doi: https://doi.org/10.70710/sitj.v3i2.93

Data Sovereignty on the Brink: A Review of the Causes of Public Sector Data Leaks and Their Impact on Intelligence Stability

Sigit Setiono[1,a,*]

[1]Sekolah Tinggi Intelijen Negara, Indonesia
[a]sigit.setiono@gmail.com
*Corresponding author

Article Info
Received: 6-Mar-2026
Revised: 9-Mar-2026
Accepted: 30-June-2026

Keywords
Counterintelligence; Data Breach; Digital Sovereignty; National Security; Public Sector Intelligence

Abstract
Data leaks in the public sector have become an existential threat to Indonesia's digital sovereignty and national information amidst the massive digitization of bureaucracy through the Electronic-Based Government System (SPBE). While SPBE improves service efficiency, this integration simultaneously expands the attack surface for various threat actors. This research aims to analyze the systemic causes of data leaks in government agencies and their profound implications for the stability of the country's intelligence services. Using descriptive qualitative methods through a case study approach and a review of recent cyber incidents, this research identifies that the primary vulnerabilities stem from the human factor as the weakest link—reflected in low security literacy among state officials—and weak information security governance resulting from fragmented cyber infrastructure and inter-agency sectoral egos. Furthermore, the aggressiveness of Advanced Persistent Threat (APT) actors serves as an external catalyst that exacerbates this situation. The research findings indicate that the impact of data leaks goes beyond technical losses and individual privacy; they create systemic intelligence risks that undermine the country's counterintelligence and early detection functions. This phenomenon exposes strategic data to state-sponsored actors, facilitates cyber espionage, and delegitimizes public trust in the government. As a strategic solution, the author recommends strengthening national cyber resilience through the integration of a centralized security architecture integrated with intelligence functions, as well as regulatory reforms that are more responsive to the dynamics of hybrid threats to protect national digital sovereignty.

1. Introduction

The development of Information and Communication Technology (ICT) has transformed the paradigm of governance in Indonesia. As mandated by Presidential Regulation Number 95 of 2018 concerning the Electronic-Based Government System (SPBE), the digitalization of administrative processes aims to create clean, effective, and transparent governance (Ramadhani et al., 2025). However, this massive integration has created a new dependence on digital infrastructure that is highly vulnerable to cyberattacks.

Data in the public sector is not simply a collection of identities, but a strategic asset containing information about state power, population profiles, and even diplomatic secrets. When this data is leaked, national sovereignty is "on the line." The successive data breaches in various central and regional government agencies in recent years demonstrate that Indonesia's cyber defense posture remains reactive (Soleh & Tjenreng, 2025).

From an intelligence perspective, data breaches are a form of modern espionage. Adversaries no longer need to deploy physical agents in the field if they can hack government databases to obtain complete profiles of their targets. Therefore, the main problem discussed in this paper is: what are the multidimensional factors that cause data leaks in the public sector and how this phenomenon destabilizes the state intelligence function..

2. Literature Review

2.1. Information Security and the Onion Model

Information security in today's government ecosystem is no longer viewed as a static entity, but rather as a dynamic, multi-layered process. One of the most relevant frameworks for understanding this complexity is The Onion Model, also known as the Defense in Depth strategy. This model assumes that no single security control is perfect; therefore, defenses must be built in mutually supportive layers (Jou et al., 2024). From an intelligence and national security perspective, the layers of The Onion Model can be described in depth as follows:

a) The Human Layer (People/Personal Security)

Humans are the outermost and most crucial layer in this model. Referring to the findings of Xue et al. (2024), humans are often the weakest link in the information security chain. In the context of the Indonesian government, low security literacy among state officials and civil servants creates loopholes for social engineering attacks. Insider threats or negligence in the use of personal devices (BYOD) infected with malware can penetrate all existing technical layers. From an intelligence perspective, failure at this layer represents a failure in the personnel security function, which is the foundation of counterintelligence.

b) Physical Security

This layer includes protection against physical access to data centers, servers, and work terminals. Physical security ensures that threat actors cannot directly sabotage or steal hardware that stores strategic data. Reference documents highlight the importance of securing the country's vital information infrastructure as a vital national asset that must be maintained to clandestine intelligence standards.

c) Network and Perimeter Layer (Network & Perimeter Security)

This is where technologies such as firewalls, intrusion detection systems (IDS), and encryption come into play. In the era of bureaucratic digitalization (SPBE), this layer serves as the primary gateway for detecting and containing Advanced Persistent Threat (APT) attacks. However, the fragmentation of cyber infrastructure across various government agencies often makes this perimeter layer inconsistent, creating blind spots that are easily exploited by state-sponsored actors (Soleh & Tjenreng, 2025).

d) Data Layer (Data Security)

As the core of the "onion," data is an asset whose confidentiality, integrity, and availability must be protected. From an intelligence perspective, data at this deepest layer is the primary target for cyber espionage. When the outer layers fail, strong data encryption and a zero-trust policy become the last line of defense to prevent sensitive state information from being misused for national destabilization.

The implementation of the Onion Model in the public sector must be accompanied by intelligence awareness. Information security is not simply about installing hardware; it must also include early detection (early warning) capabilities to identify attack patterns before they reach the deepest data layers. The synergy between these layers determines the resilience of a country's digital sovereignty in the face of hybrid threats (Ramadhani, Enriko & Sari, 2025).

2.2. Data Sovereignty from a Strategic Intelligence Perspective

Data sovereignty is not simply a technical issue regarding server storage location, but rather a manifestation of state sovereignty in cyberspace. In strategic intelligence discourse, public sector data is viewed as a national asset that determines a country's competitive advantage and resilience (Soleh & Tjenreng, 2025).

a) Data as an Instrument of National Power.

In strategic intelligence theory, information is a key element of National Power. Data sovereignty refers to a state's ability to regulate, manage, and protect its citizens' data from foreign jurisdiction and exploitation. Reference documents state that digitization through SPBE has consolidated strategic data that, if not sovereign, could become a primary target for espionage by state-sponsored actors to map national vulnerabilities (Ramadhani, Enriko & Sari, 2025).

b) The Counterintelligence Perspective on Data Protection.

Data sovereignty is closely related to the function of Counterintelligence. Counterintelligence aims to neutralize espionage, sabotage, and solicitation efforts by adversaries. Leaks of public sector data, such as population data or civil servant data, from the intelligence perspective represent a form of adversary penetration into vital information infrastructure. Without strong data sovereignty, a state's early detection function is weakened because adversaries can gain access to strategic personnel profiles and confidential state communication patterns (Xue et al., 2024).

c) Hybrid Threats and National Security

Data sovereignty is being tested by the emergence of hybrid threats, where cyberattacks are used for political and destabilizing purposes. Referring to the data leak phenomenon in Indonesia, the loss of data sovereignty leaves the country vulnerable to Information Warfare. Leaked data can be processed using artificial intelligence algorithms by adversary intelligence agencies to conduct psychological operations and delegitimize the government in the public eye (Jou et al., 2024).

d) Legal Framework and Security Intelligence

The implementation of the Personal Data Protection Law (PDP Law) and regulations regarding national cybersecurity must be viewed as security intelligence instruments. Reference documents emphasize that data protection must be part of the national security doctrine. Data sovereignty demands technological independence (local technology) to minimize backdoors in foreign software or hardware that could exploit sensitive state information for foreign espionage.

3. Method

This research uses a qualitative approach with an interpretive phenomenological method. The primary data sources come from national cyber incident report documents, draft cybersecurity policy research, and case studies of cyber attacks that occurred in the 2022-2024 period (including the hacking of the Temporary National Data Center/PDNS). Data analysis techniques are carried out in three stages: (1) Data reduction to filter the most significant causal factors; (2) Data presentation in the categories of People, Process, and Technology; and (3) Drawing conclusions based on the impact on national intelligence stability.

4. Results and Discussion

4.1. Analysis of Factors Causing Public Sector Data Leaks

Based on the analyzed data, the factors causing data leaks can be classified into four main pillars:

a) Human Factors (The Weakest Link)
Data shows that the majority of data leaks originate from personal devices of civil servants infected with stealer malware. The use of pirated software and the habit of accessing unsecured websites using office networks are the main entry points. Low cybersecurity literacy makes personnel unable to detect phishing attempts by hackers.

b) Process and Governance Factors
Regulatory and operational fragmentation exists between institutions. Sectoral egos often hinder the sharing of threat information. Furthermore, many government agencies do not comply with minimum information security standards (ISO 27001) and ignore early warnings from the National Agency for the Protection of Information and Communication Technology (BSSN) due to limited skilled human resources.

c) Technology and Infrastructure Factors
Many government information systems are built using legacy architectures without adequate encryption. Furthermore, reliance on third-party vendors whose security is not rigorously audited creates vulnerabilities in the supply chain (supply chain attacks).

d) Structural and Budgetary Factors
Budget allocations for cybersecurity in government agencies are still very minimal compared to hardware procurement budgets. This often results in delayed system maintenance and patch management.

4.2. Impact on the Stability of National Intelligence

Data leaks are not merely an administrative issue, but a direct attack on the country's intelligence architecture:

a) Erosion of Counterintelligence
Leaked population, passport, and civil servant data allow foreign intelligence agents to map strategic Indonesian personnel. Using big data analytics techniques, adversaries can identify who has access to state secrets, thus facilitating close approaches or blackmail operations.

b) Influence Operations
Leaked data is often published with a narrative that distorts the facts to create social unrest. This aims to undermine public trust in the government (public distrust) and create domestic political instability.

c) Threats to Critical Infrastructure
Leaked government administrative credentials (usernames/passwords) provide an avenue for foreign state actors to sabotage vital infrastructure, from energy systems to the national financial system.

5. Conclusion

5.1. Synthesis of Findings

Sovereignty Under Threat Based on the multidimensional analysis presented, this study concludes that Indonesia's data sovereignty is currently in a highly vulnerable state. The digitization of the bureaucracy through SPBE, while providing administrative efficiency, has created new points of vulnerability that the current cybersecurity posture fails to mitigate. Data leaks in the public sector are no

longer simply technical incidents of data loss, but rather represent asymmetric penetration by threat actors into the heart of the nation's information. The human factor, as the weakest link, exacerbated by a low security culture among bureaucrats, serves as a primary entry point for foreign intelligence operations and cybercriminal groups.

5.2. Implications for National Intelligence Stability

This study confirms that the most dangerous impact of government data leaks is the destabilization of the national intelligence function. Three systemic impacts are identified:

a) Counterintelligence Paralysis
   Leaked data provides a "roadmap" for foreign intelligence agents to profile strategic personnel, identify command gaps, and design more targeted infiltration operations.

b) Erosion of Public Trust as an Intelligence Target
   Massive data leaks are used as a provocative tool in information warfare to create public distrust of the state, which is the ultimate goal of enemy intelligence destabilization operations.

c) Weakness of Early Detection
   Fragmentation of cyber infrastructure and sectoral egos between institutions have led to the loss of the state's ability to provide early warning, leaving the state in a reactive, rather than proactive, position.

5.3. Strategic Recommendations (Strategic Outlook)

To restore data sovereignty and maintain intelligence stability, this study recommends the following transformative steps:

a) Doctrine Repositioning
   Shifting the information security paradigm from merely technical security to being part of the National Defense and Intelligence doctrine. Data must be categorized as a vital national asset with protection equivalent to that of military installations.

b) Cyber Command Integration
   Eliminating sectoral egos by establishing an integrated cyber command center that combines the technical capabilities of the National Civil Service Agency (BSSN) with the analytical capabilities of strategic intelligence (BIN/TNI).

c) Technological Independence
   Reducing dependence on foreign vendors in vital government information infrastructure to minimize the risk of backdoors and ensure full sovereignty over the hardware and software used.

d) Intelligence-Based Human Resource Empowerment
   Cybersecurity training for civil servants should not be solely technical but should also address intelligence awareness to prevent manipulation through social engineering methods.

5.3. Limitations and Suggestions for Future Research

This research focuses on a qualitative analysis of past data breach incidents. Further research is expected to conduct quantitative analyses of the long-term economic and political losses resulting from government data leaks, as well as examine the effectiveness of the implementation of the Personal Data Protection Law (PDP Law) in mitigating intelligence risks in the public sector.

References

Jou, M., et al. (2024). Digital Transformation and Information Security in Public Sector. Journal of Government Technology.

Ramadhani, Enriko, & Sari. (2025). Implementasi SPBE dan Tantangan Keamanan Siber di Indonesia. Jurnal Tata Kelola Elektronik.

Soleh, A., & Tjenreng. (2025). Keamanan Nasional dan Kedaulatan Data di Era Disrupsi. Jurnal Intelijen Strategis.

Xue, L., et al. (2024). Cyber Threats in Modern Public Administration. International Journal of Information Management.

Laporan Analisis Serangan Siber. (2024). Evaluasi Insiden PDNS dan Dampaknya pada Sektor Publik.

BSSN. (2023). Laporan Tahunan Keamanan Siber Indonesia.

BSSN. (2024). Laporan Tahunan Keamanan Siber Indonesia.

BSSN. (2025). Laporan Tahunan Keamanan Siber Indonesia.