SITJOURNAL
Security Intelligence Terrorism Journal

Security Intelligence Terrorism Journal (SITJ), Vol. 03 No. 01 (2026), pp. 43-58
Research Article
doi: https://doi.org/10.70710/sitj.v3i1.88

Scenario Planning Model for Counterintelligence Strategy Against Foreign Intelligence Operations in Indonesia

Husein Sagaf[1,a,*]

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

Article Info
Received: 3-Feb-2026
Revised: 4-Feb-2026
Accepted: 4-Feb-2026

Keywords
Counterintelligence; Foreign Intelligence Operations; Intelligence Governance; National Vulnerability; Scenario Planning; TAIDA Framework

Abstract
Foreign intelligence operations continue to occur within Indonesian territory despite existing regulatory frameworks governing state intelligence. This phenomenon reveals Indonesia's territorial vulnerabilities driven by the attraction of natural resources and weaknesses in counterintelligence governance following the 1998 Reformasi. This study aims to analyze Indonesia's vulnerabilities to foreign intelligence operations and formulate a scenario planning-based counterintelligence strategy model. The research employs qualitative methods through in-depth interviews with national intelligence stakeholders, Focus Group Discussions (FGD), and document analysis. Data were analyzed using the TAIDA framework (Tracking, Analyzing, Imaging, Deciding, Acting). Interviews were conducted with representatives from various intelligence and national security agencies while maintaining informant confidentiality in accordance with research ethics. Findings reveal that Indonesia's vulnerabilities stem from three main factors: the attraction of natural resources, legal gaps in prosecuting espionage/sabotage, and institutional fragmentation characterized by sectoral intelligence governance. The scenario planning model identifies four scenarios based on two critical driving forces: internal intelligence governance cohesion and external foreign intelligence operation intensity. Based on current conditions and intelligence practitioners' perspectives, Indonesia is positioned in Scenario 2 (weak internal cohesion, high external intensity), indicating foreign intelligence dominance. The most relevant current strategies are strengthening BIN's coordination role and implementing reverse operations. This study recommends strengthening the legal foundation through revising the State Intelligence Law or creating a comprehensive National Security Law to establish espionage/sabotage as criminal offenses with clear sanctions.

1. Introduction

The dynamics of geopolitical competition at global, regional, and domestic levels have presented an increasingly complex threat landscape, including the intensification of foreign intelligence activities utilizing various instruments of influence, technology, and unconventional approaches (Lowenthal, 2020). The South China Sea conflict, tensions in the Taiwan Strait, and various regional territorial disputes demonstrate how intelligence operations have become critical instruments in strategic competition among nations (Darmawan, 2023). In such context, the conduct of state intelligence functions is required not only to be responsive but also capable of developing anticipatory capacity grounded in robust and proven analytical methodologies.

The phenomenon of foreign intelligence operations continues to occur within Indonesian territory, indicating territorial vulnerabilities despite the existence of Law Number 17 of 2011 on State Intelligence (Government of the Republic of Indonesia, 2011). Various media reports and academic studies indicate foreign intelligence collection activities in Indonesia, ranging from the use of diplomatic cover to the exploitation of cyber technology for strategic information gathering (Sumandoyo, 2016; Taher, 2022; Amin, 2022). This phenomenon suggests that Indonesia faces serious challenges in protecting its national interests from foreign intelligence operations.

As an archipelagic nation with abundant natural resources and a strategic geopolitical position, Indonesia becomes an attractive target for foreign intelligence operations. Indonesia's natural resource attractions, particularly in extractive industries, energy, and strategic minerals such as nickel, copper, and natural gas, create strong incentives for foreign countries to conduct intelligence operations to secure their national interests (Johnson, 2020). Indonesia's strategic geographical position as a connector between two oceans and along international trade routes also adds to Indonesia's strategic value in the geopolitical calculations of major powers.

However, Indonesia faces fundamental challenges in counterintelligence governance. Following the 1998 Reformasi Indonesia's democratic reform movement that ended President Suharto's authoritarian New Order regime (1966-1998) significant changes occurred in Indonesian intelligence governance. Elson (2001) documents how Suharto's 32-year rule had concentrated power through extensive security apparatus and repressive legislation. Aspinall (2005) demonstrates that the regime's collapse resulted from the convergence of mass protests, economic crisis, and elite defection, creating momentum for comprehensive political and legal reforms. Among these reforms was the repeal of the Anti-Subversion Law (Presidential Decree Number 11 of 1963), which had previously served as the legal basis for prosecuting espionage and sabotage activities (Government of the Republic of Indonesia, 1963).

Robison and Hadiz (2004) explain that post-Suharto Indonesia witnessed a reorganization of power structures, with reformers seeking to dismantle authoritarian legal instruments while establishing democratic governance frameworks. This repeal was conducted to eliminate legal instruments considered repressive from the previous authoritarian era and to signal a break from the New Order's surveillance state practices (Aspinall, 2005). Nevertheless, the resulting legal vacuum has created significant weaknesses in Indonesia's counterintelligence capacity. As Robison and Hadiz (2004) note, the challenge of transitioning from authoritarianism to democracy often involves overcorrection, where necessary security mechanisms are dismantled alongside repressive ones. Consequently, foreign intelligence agents cannot be prosecuted for espionage activities unless they commit common crimes that serve as investigation entry points a situation that reflects the unintended consequences of reform without adequate replacement legislation.

Furthermore, Indonesian intelligence governance tends to operate in a sectoral manner with coordination that still requires strengthening among various intelligence agencies. Although Law Number 17 of 2011 on State Intelligence has provided a coordination framework through BIN as the national intelligence coordinator, in practice, effective coordination still faces various challenges (Government of the Republic of Indonesia, 2011). This institutional fragmentation is reflected in the existence of various agencies with intelligence and counterintelligence functions such as BIN, BAIS TNI, BIK Polri, BSSN, and other agencies, each with their sectoral interests.

Facing this complex and uncertain situation, conventional strategic planning approaches that are reactive in nature are no longer adequate. A more sophisticated methodological approach is required that can accommodate uncertainty and assist decision-makers in anticipating various possible future developments. Scenario planning methodology offers a structured framework for understanding uncertainty and developing flexible and adaptive strategies (Lindgren & Bandhold, 2009). Scenario planning has proven effective in various strategic planning contexts, including in the security and defense sectors (Peterson et al., 2003; Volkery & Ribeiro, 2009).

By identifying critical driving forces and developing multiple future scenarios, scenario planning enables counterintelligence planners to prepare flexible strategies that remain effective across various possible futures. This approach is highly relevant for the counterintelligence context where threats are dynamic, uncertain, and often evolve in ways that cannot be predicted through traditional linear planning methods.

Based on the background above, this research addresses two main questions: (1) What factors cause Indonesia's vulnerability to foreign intelligence operations? (2) How can a counterintelligence strategy model be formulated using scenario planning to address foreign intelligence operations in Indonesia? Research objectives are: (1) To analyze the vulnerabilities of Indonesian territory to foreign intelligence operations from structural, legal, and institutional perspectives, and (2) To formulate a scenario planning-based counterintelligence strategy model that is anticipatory and adaptive to various possible future developments.

This research is important as it contributes to the development of more proactive and anticipatory Indonesian counterintelligence strategies. Additionally, it contributes to academic literature on the application of scenario planning in national security contexts, particularly counterintelligence, which remains limited in Indonesia.

2. Literature Review

2.1. Counterintelligence Theory

Counterintelligence is defined as information gathered and activities conducted to protect against espionage, sabotage, or assassinations conducted on behalf of foreign powers, organizations, or persons, as well as international terrorist activities (Lowenthal, 2020; Lowenthal & Clark, 2022). As a defensive function, counterintelligence serves as a protective shield that safeguards state secrets, operations, and personnel from intelligence collection efforts by adversaries. Gill and Phythian (2018) emphasize that in an insecure world, counterintelligence also encompasses efforts to detect, identify, exploit, disrupt, or neutralize evolving foreign intelligence threats.

According to Johnson (2020), counterintelligence encompasses three interrelated core functions. First, the collection function involves gathering information about foreign intelligence threats, including identifying foreign agents, their operational methods, and their targeted objectives. Second, the defensive function includes measures to protect against intelligence collection efforts through personnel security, physical security, communications security, and security awareness (Lowenthal & Clark, 2022). Third, the offensive function involves operations to disrupt and neutralize adversary intelligence activities, including through deception operations, disinformation, and penetration of foreign intelligence services (Gill & Phythian, 2018).

Prunckun (2019), in his analysis of scientific methods for intelligence analysis, emphasizes the importance of systematic approaches in counterintelligence. Effective counterintelligence requires not only technical capabilities but also deep understanding of adversary operational patterns, their motivations, and the strategic context in which they operate. Warner (2022), in his study of international security history, demonstrates that the evolution of intelligence threats necessitates the integration of various intelligence sources—from human intelligence (HUMINT) and signals intelligence (SIGINT) to cyber intelligence (CYBINT). Lowenthal and Clark (2022) further underscore that this multi-disciplinary integration is key to addressing the complexity of contemporary threats.

The taxonomy of counterintelligence activities includes five core components (Gill & Phythian, 2018; Warner, 2022): (1) Security awareness programs to educate personnel about intelligence threats and indicators of suspicious activities; (2) Counterespionage operations to detect and neutralize foreign agents through surveillance, investigation, and penetration of foreign intelligence networks; (3) Technical security measures to protect communications and information systems from interception and penetration; (4) Personnel security screening and monitoring to identify insider threat risks; and (5) Deception operations to mislead adversary intelligence services with manipulated information. Lowenthal and Clark (2022) affirm that effective counterintelligence requires the integration of all these elements within a well-coordinated institutional framework.

2.2. Intelligence Cycle Theory

The Intelligence Cycle provides a conceptual framework for understanding how intelligence is produced and distributed to decision-makers. According to Lowenthal (2020), the intelligence cycle

consists of five interrelated phases: planning and direction, collection, processing and exploitation, analysis and production, and dissemination. This cyclical process ensures that intelligence products meet the needs of policymakers and operational commanders in a timely and accurate manner.

The planning and direction phase involves identifying intelligence requirements and establishing collection priorities. The collection phase involves gathering raw information from various sources. The processing and exploitation phase converts raw data into analyzable formats. The analysis and production phase involves interpreting information and producing intelligence assessments. Finally, the dissemination phase ensures intelligence products reach the right users in useful formats (Bartes, 2013).

Understanding the intelligence cycle is crucial for counterintelligence planning. By understanding how adversaries plan, collect, analyze, and distribute intelligence, counterintelligence practitioners can identify vulnerabilities in adversary operations and develop targeted disruption strategies (Prunckun, 2019). This understanding also helps in designing protective measures at each phase where adversary collection might occur. For instance, operational security can be designed to frustrate the collection phase, while disinformation can target the analysis and production phase.

2.3. Strategic Intelligence Theory

Strategic intelligence focuses on long-term trends, patterns, and developments that affect national security interests. Kent (1949) in his seminal work asserts that strategic intelligence functions to inform high-level policy decisions and strategic planning. Unlike tactical or operational intelligence that addresses immediate threats and short-term situations, strategic intelligence provides context and forward-looking perspectives for long-term strategic positioning.

In the counterintelligence context, strategic intelligence involves comprehensive understanding of foreign intelligence service capabilities, intentions, and operational patterns, assessment of vulnerabilities in national security architecture, and projection of future threat scenarios. This strategic perspective is essential for developing proactive counterintelligence strategies rather than merely reactive responses to identified threats. Strategic intelligence enables anticipatory action and long-term capacity building in counterintelligence capabilities, as well as identification of emerging trends in foreign intelligence operation methods and targets.

2.4. Scenario Planning and the TAIDA Framework

Scenario planning is a strategic planning method used to create flexible long-term plans under conditions of high uncertainty. Lindgren and Bandhold (2009) explain scenario planning as a structured approach to thinking about and planning for the future by considering multiple plausible scenarios rather than relying on a single prediction. Amer, Daim, and Jetter (2013) in their comprehensive review emphasize that this method acknowledges the future cannot be predicted with certainty but can be anticipated by identifying key driving forces and developing coherent narratives about how the future might unfold. Chermack and Swanson (2017) further argue that scenario planning serves as a powerful model for organizational change by enabling decision-makers to reframe their understanding of strategic challenges and opportunities.

The TAIDA framework (Tracking, Analyzing, Imaging, Deciding, Acting) provides a structured methodology for implementing scenario planning (Lindgren & Bandhold, 2009). The Tracking phase involves continuous scanning of external and internal environments to identify changes, trends, and emerging issues that might shape the future. This includes monitoring relevant political, economic, social, technological, and security developments (Ramirez & Wilkinson, 2016). The Analyzing phase examines relationships among factors, identifies driving forces that will shape the future, and determines critical uncertainties that need to be considered in scenario development. Amer et al. (2013) note that rigorous analysis of driving forces and uncertainties is essential to ensure scenarios are both plausible and strategically relevant.

The Imaging phase develops multiple distinct scenarios based on different combinations of driving forces and critical uncertainties. Each scenario must be internally consistent, different from one another, and relevant to the strategic decisions being faced (Ramirez & Wilkinson, 2016). The Deciding phase

evaluates strategies across various scenarios to identify robust options strategies that perform well across multiple possible futures. Chermack and Swanson (2017) emphasize that this phase facilitates organizational learning by challenging existing mental models and assumptions. Finally, the Acting phase implements chosen strategies, monitors developments, and adapts based on signals from the environment about which scenario is beginning to materialize.

Scenario planning is particularly appropriate for developing counterintelligence strategies because foreign intelligence operations are characterized by high uncertainty, non-linear dynamics, and unpredictable evolution. Traditional strategic planning methods that assume predictable environments are inadequate in addressing the complexity and ambiguity inherent in intelligence threats (Peterson et al., 2003; Volkery & Ribeiro, 2009). Ramirez and Wilkinson (2016) demonstrate that the strategic reframing approach enables organizations to navigate complex security environments by developing multiple perspectives on potential futures. By developing multiple scenarios based on critical driving forces, counterintelligence planners can prepare flexible strategies that remain effective across various possible futures, both optimistic and pessimistic (Amer et al., 2013; Chermack & Swanson, 2017).

2.5. Previous Research and Research Positioning

Kuswara (2019), in his research on evaluating Indonesian counterintelligence functions against foreign intelligence espionage, states that threat levels from foreign espionage can be measured, both from Human Intelligence (HUMINT) and Signal Intelligence (SIGINT). Caballero-Anthony (2016) frames such intelligence threats within the broader context of non-traditional security challenges that transcend national borders and require transnational approaches to mitigation. Kuswara emphasizes the need for establishing a more coordinated counterintelligence body and urges the government not to be reactive like 'firefighters' in addressing espionage threats. Emmers and Teo (2022) argue that middle powers in the Asia Pacific, including Indonesia, face unique security challenges requiring sophisticated strategic responses that balance cooperation and self-reliance. This research provides early warning about Indonesia's vulnerabilities and emphasizes the importance of institutional readiness in counterintelligence.

Lissofa (2016) examined the impact of NSA espionage on US-Japan diplomatic relations, demonstrating that espionage can damage relationships even with allied nations that have strong diplomatic and trade ties. The research reveals that the NSA had long monitored Japan, not only targeting influential politicians but also bankers and major corporations. This case study illustrates that espionage is a common practice in international relations, even among allies, and demonstrates the need for constant vigilance against foreign intelligence activities a reality that Caballero-Anthony (2016) identifies as part of the evolving transnational security landscape.

Anggraini et al. (2016) analyzed the abuse of diplomatic immunity in the context of gold smuggling by North Korean diplomatic officials in Bangladesh. The research shows that diplomatic cover can be misused for illegal activities, including possible intelligence operations. This study is relevant for understanding how foreign intelligence agents can exploit diplomatic status as operational protection.

In the context of scenario planning, several studies have demonstrated the effectiveness of this method in various fields. Peterson et al. (2003) demonstrated the use of scenario planning in conservation planning under uncertain environments. Volkery and Ribeiro (2009) analyzed the use of scenario planning in public policy and identified factors affecting its effectiveness. Kelly et al. (2023) applied scenario planning in post-pandemic policy planning contexts. Edgar et al. (2013) explained methodological challenges in applying scenario planning for regional development.

However, no research has specifically developed a scenario planning-based counterintelligence model for the Indonesian context. This research fills that gap by developing a scenario planning-based counterintelligence model specific to Indonesia's geopolitical, security, and institutional context. Emmers and Teo (2022) highlight that middle powers like Indonesia must develop context-specific security strategies that account for their unique position in regional power dynamics and evolving threat environments. Through the TAIDA framework and a four-quadrant scenario planning model, this research identifies strategic uncertainties and possible future threat scenarios. The counterintelligence strategies developed are based not only on actual threats but also on potential future threats, creating an anticipatory strategic posture. This represents a significant methodological advancement from reactive to proactive and

adaptive counterintelligence planning, aligning with Caballero-Anthony's (2016) call for comprehensive, transnational approaches to contemporary security challenges..

3. Method

This research employs an applied qualitative research approach designed to provide practical solutions to counterintelligence challenges. The qualitative method was chosen because counterintelligence issues are sensitive, classified, and contextual-strategic in nature, making quantitative data insufficient to capture foreign intelligence operation patterns, strategic decision-making logic, and security actor perceptions (Neuman, 2013).

3.1. Research Approach and Design

This research employs a qualitative approach with a descriptive-analytical design. The qualitative methodology was chosen because this research seeks to understand the complex phenomenon of foreign intelligence operations and counterintelligence governance involving multiple stakeholders, institutional dynamics, and contextual factors that cannot be adequately captured solely through quantitative measures (Creswell, 2002). The qualitative approach allows in-depth exploration of stakeholder perspectives, interpretation of meanings, and rich contextual understanding of the phenomenon being studied.

The analytical framework is based on the TAIDA methodology (Tracking, Analyzing, Imaging, Deciding, Acting) developed by Lindgren and Bandhold (2009) for scenario planning. This structured approach provides systematic steps for environmental scanning, driving force analysis, scenario development, strategy formulation, and implementation planning. Use of the TAIDA framework ensures methodological rigor in the scenario planning process and facilitates transparency in the analysis and conclusion-drawing process.

3.2. Informants and Data Collection Techniques

Data were collected through three main methods: in-depth interviews, Focus Group Discussions (FGD), and document analysis. In-depth interviews were conducted with key stakeholders from various agencies with roles in counterintelligence and foreign national oversight. Informant selection was conducted purposively based on criteria: (1) holding strategic positions or having experience in intelligence/counterintelligence, (2) possessing knowledge about Indonesian counterintelligence policies and operations, and (3) willing to participate with informed consent.

Interviews were conducted with representatives from the following institutions (specific informant identities are kept confidential according to research ethics):

- State Intelligence Agency (BIN): representatives from counterintelligence directorates
- TNI Strategic Intelligence Agency (BAIS TNI): representatives from related directorates
- National Police Intelligence and Security Agency (BIK Polri): representatives handling counterintelligence
- State Cyber and Crypto Agency (BSSN): representatives handling cyber threats
- Directorate General of Immigration: representatives handling foreign national oversight
- Ministry of Defense: representatives from defense intelligence units
- Attorney General's Office: representatives from intelligence divisions
- Commission I DPR RI: members overseeing intelligence and defense
- Ministry of Home Affairs: representatives from national vigilance directorates
- Academic experts in intelligence and national security studies

Interviews were conducted semi-structuredly with prepared interview guides while remaining flexible to explore in-depth information. Each interview lasted 60-90 minutes and was recorded with informant permission. Interview transcripts were then coded and analyzed to identify key themes, patterns, and strategic insights.

Focus Group Discussions (FGD) were conducted with intelligence practitioners and academics to validate findings, deepen understanding of counterintelligence dynamics, and discuss strategic implications of various scenarios. FGD involved 8-12 participants with diverse backgrounds to ensure representation of different perspectives. Discussions were facilitated using scenario planning techniques to develop and evaluate possible scenarios.

Document analysis was conducted on various sources: (1) Regulations and policies: Law Number 17 of 2011 on State Intelligence, Presidential Decree Number 11 of 1963 on Eradication of Subversive Activities, and other related publicly available policy documents, (2) Academic literature: scientific journals, textbooks, and academic publications on counterintelligence, scenario planning, and national security, (3) Media reports: news and investigative reports on foreign intelligence operation phenomena in Indonesia from credible sources. The entire research process was conducted within academic, methodological, and ethical boundaries, without involving sensitive information or state secrets.

3.3. Research Ethics and Informant Protection

This research adheres to strict research ethics principles, particularly regarding confidentiality and informant protection. Each informant was provided informed consent explaining the research purpose, data use, and confidentiality guarantees. Specific informant identities, including names, detailed positions, and information that could personally identify them, are kept confidential in all publications of this research.

In presenting research results, informant quotes or views are referenced with general codes such as 'representative from intelligence agency', 'counterintelligence practitioner', 'intelligence studies academic', or 'stakeholder from institution X' without mentioning names or specific positions. Sensitive data or data that could endanger national security are not included in this research. The entire data collection and analysis process was conducted with topic sensitivity and informants' strategic positions in mind.

3.4. TAIDA Analytical Framework

Data analysis employed the TAIDA framework adapted from the intelligence cycle. The TAIDA framework consists of five interrelated stages forming a systematic analytical process (Bartes, 2013):

1. Tracking: This stage identifies and documents foreign intelligence operations that have occurred in Indonesian territory post-1998 Reformation. The tracking process includes tracing exposed cases, operational patterns employed, and evolving modus operandi. Data were collected from various sources including intelligence agency reports, immigration documentation, mass media reports, and cases handled by law enforcement. This stage produced a comprehensive database on foreign intelligence operation characteristics in Indonesia.
2. Analysing: This stage conducts in-depth examination of factors causing Indonesia's vulnerability and identified vulnerability patterns. The analysis employs scenario planning methodology to identify driving forces affecting Indonesia's counterintelligence condition. Driving forces are grouped into internal factors (intelligence governance) and external factors (foreign intelligence operation intensity). The analysis stage also examines causal relationships between various factors and identifies leverage points for strategic intervention.
3. Imaging: The imaging stage formulates four possible scenarios based on two identified critical driving forces. These four scenarios encompass the best condition (Indonesian Intelligence Superiority), worst condition (Foreign Intelligence Dominance), and two intermediate scenarios (Intelligence Warfare and Mutual Respect). Each scenario is then mapped in a 2x2 matrix for easy visualization and understanding. The imaging process involved brainstorming with stakeholders to ensure realistic and relevant scenarios.
4. Deciding: Based on scenario analysis, this stage determines appropriate strategy options for each scenario. Formulated strategies must be adaptive and adjustable to changing conditions. Each strategy is evaluated based on implementation feasibility, potential effectiveness, resource requirements, and compatibility with Indonesia's political-legal context. Strategy prioritization is conducted based on urgency and expected impact.
5. Acting: The final stage recommends concrete implementation steps and necessary policies to execute formulated strategies. Recommendations cover regulatory, institutional, operational, and

capacity development aspects. Each recommendation includes timelines, responsible actors, and success indicators to facilitate implementation and monitoring.

Scenario planning was specifically chosen for this research due to its suitability in analyzing foreign intelligence operations characterized by: (1) high uncertainty regarding when, where, and how operations will be conducted, (2) multiple interacting driving forces from both internal and external factors, (3) long-term national security impacts requiring strategic anticipation, and (4) need for adaptive strategies adjustable to changing global and domestic geopolitical conditions (Edgar et al., 2013).

3.5. Data Validation

Data credibility was ensured through three validation techniques (Sujarweni, 2014): First, source triangulation was conducted by cross-verifying information from various intelligence stakeholders. For each key question, information was collected from at least three different sources to ensure consistency and accuracy. Second, methodological triangulation was performed by combining various data collection methods in-depth interviews, document analysis, and FGD so that weaknesses of one method could be compensated by strengths of others. Third, member checking was conducted by confirming interpretations and research findings with original informants to ensure accuracy and authenticity of collected data and prevent misinterpretation. This validation process is crucial given the research topic's sensitivity and limited access to classified state information.

4. Results and Discussion

4.1. Patterns of Foreign Intelligence Operations in Indonesia

Based on document analysis, stakeholder interviews, and FGD, this research reveals that Indonesia's vulnerability to foreign intelligence operations stems from three interrelated and mutually reinforcing factors:

1. Attraction of Natural Resources and Strategic Position

   Indonesia possesses abundant natural resources including strategic minerals (nickel, copper, tin, bauxite), energy reserves (natural gas, coal), and critical materials for modern technology highly important for the economic and technological development of advanced nations. As stated by a representative from an intelligence agency: “Our natural resource wealth becomes both an attraction and a weakness. Foreign countries have interests in knowing our resource potential, exact locations, extraction processes, and government policies regarding resource management.”

   Indonesia's strategic geographical position as a connector between two oceans (Pacific and Indian) and located on international trade routes also adds to Indonesia's strategic value. As articulated by an intelligence studies academic: “Indonesia is not only a target because of its natural resources, but also because of its strategic geopolitical position. Control over Indonesia or even just influence over Indonesian foreign policy can provide significant strategic advantages in regional and global geopolitical competition”.

2. Legal Gaps in Prosecuting Espionage and Sabotage

   The repeal of Presidential Decree Number 11 of 1963 on Eradication of Subversive Activities in 1998 created a significant legal gap in prosecuting espionage and sabotage (Government of the Republic of Indonesia, 1963). This Presidential Decree previously served as the legal basis for prosecuting espionage, sabotage, and subversion activities with clear sanctions. However, its repeal was conducted as part of post New Order legal reform to eliminate legal instruments considered repressive and often misused to silence political opposition.

   A practitioner from a law enforcement agency stated: “Currently we face difficulties in prosecuting activities that are clearly espionage because there is no specific legal umbrella. We can only prosecute if there are common crimes committed, such as document forgery or immigration

violations. The intelligence collection activity itself cannot be legally processed". This legal gap severely limits Indonesian counterintelligence effectiveness because many intelligence activities threatening national security cannot be legally prosecuted.

A representative from the House of Representatives overseeing defense and intelligence added: "We are aware of this legal gap and there have been discussions to revise the State Intelligence Law or even create a more comprehensive National Security Law. However, the process requires caution because we must balance national security needs with human rights protection. We do not want to repeat past abuses".

3. Institutional Fragmentation in Intelligence Governance

Indonesian intelligence architecture is characterized by sectoral fragmentation with coordination that still requires strengthening. Although Law Number 17 of 2011 designates BIN as the national intelligence coordinator, in practice effective coordination still faces various challenges (Government of the Republic of Indonesia, 2011). Various agencies have intelligence and counterintelligence functions: BIN (State Intelligence Agency), BAIS TNI (TNI Strategic Intelligence Agency), BIK Polri (National Police Intelligence and Security Agency), BSSN (State Cyber and Crypto Agency), intelligence units in various ministries, and others.

A representative from an intelligence agency stated: "Each agency has its own tasks and functions based on law. But in practice, coordination does not always run optimally. Sometimes there is sectoral ego, sometimes there are differences in interpreting authority, sometimes there is reluctance to share information. This makes our response to foreign intelligence threats not as integrated as it should be".

FGD results confirmed that this fragmentation is a serious challenge. An FGD participant from academia observed: "Unlike some countries that have a strong central counterintelligence body, Indonesia is still spread across various agencies. This can be a strength if coordination is good (there are multiple layers of defense). But it can also be a weakness if not coordinated (there are gaps that can be exploited by foreign intelligence)".

These three factors: attraction of natural resources, legal gaps, and institutional fragmentation mutually reinforce each other and create conditions of significant vulnerability. The attraction of natural resources creates incentives for foreign intelligence operations, while legal gaps make prosecution difficult, and institutional fragmentation weakens coordinated defensive responses. The combination of these three factors places Indonesia in a position vulnerable to exploitation by foreign intelligence services.

4.2 Identification of Driving Forces

Through systematic analysis of interview data, FGD, document review, and literature examination, two critical driving forces were identified that will shape Indonesia's counterintelligence landscape in the future:

1. Internal Driving Force: Intelligence Governance Cohesion

This driving force refers to the level of coordination, integration, and harmonization among Indonesian intelligence agencies in executing counterintelligence functions. This governance cohesion can vary from weak to strong. Under weak conditions, governance is characterized by: high sectoral fragmentation, limited inter-agency information sharing, poorly coordinated operations, duplication of efforts and resource inefficiency, and unclear division of tasks and responsibilities in certain situations.

Conversely, under strong conditions, governance is characterized by: effective coordination with clear mechanisms, integrated intelligence systems with smooth information sharing, well-coordinated joint operations, optimized resource use through clear task division, and strong unity of effort in addressing foreign intelligence threats. A representative from a coordination agency

stated: “Intelligence governance cohesion is key. It's not about creating one super large agency that handles everything, but about making various agencies work together effectively like a harmonious orchestra”.

2. External Driving Force: Foreign Intelligence Operation Intensity

This driving force refers to the scale, sophistication, and frequency of foreign intelligence operations targeting Indonesia. This intensity can range from minimal to massive. Under minimal conditions, foreign intelligence operations are relatively limited in scale and scope, use conventional methods that are relatively easy to detect, are conducted by a limited number of actors, and target specific and limited areas.

Under massive conditions, foreign intelligence operations are widespread with multiple targets, use advanced technologies including cyber intelligence and technical surveillance, are conducted by various countries and actors with possible coordination, cover various strategic sectors (economic, political, military, technology), and employ multiple methodologies from traditional HUMINT to sophisticated SIGINT and CYBINT. A counterintelligence practitioner explained: “We face increasingly sophisticated threats. Not just suspicious diplomats or overly curious businessmen. Now there is cyber espionage, subtle influence operations, use of technology we may not be able to detect”.

These two driving forces were selected as the basis for scenario development because they have characteristics of: high impact, high uncertainty, and independence. The combination of these two driving forces creates four different possible future states with unique strategic implications for Indonesian counterintelligence.

4.3. Scenario Planning Model: Four Strategic Scenarios

Based on the TAIDA analytical framework and stakeholder interview results, this research developed a scenario planning model employing two critical driving forces as scenario-forming axes. These two driving forces were selected based on: (1) highly significant influence level on Indonesia's counterintelligence condition, (2) high uncertainty level in future development predictions, and (3) relatively independent nature enabling formation of distinct scenario combinations.

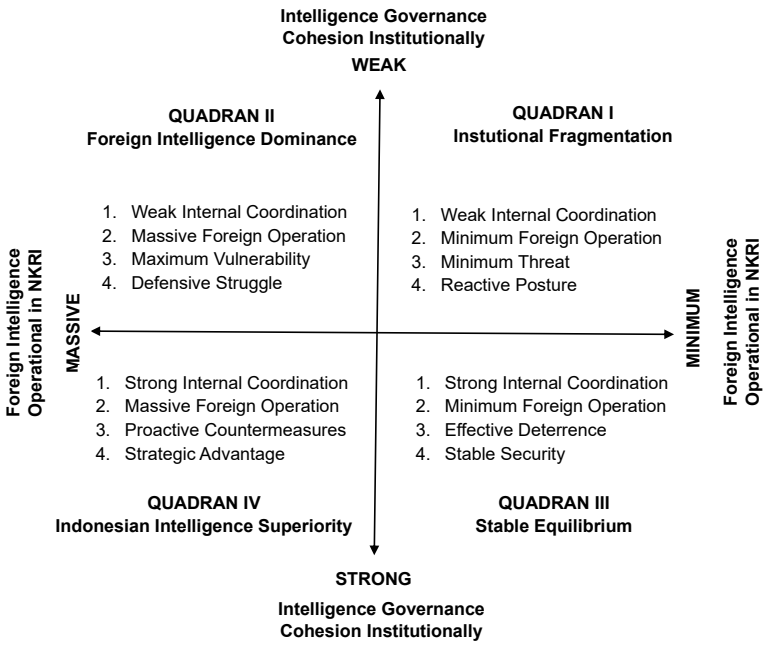

Figure 1. Counterintelligence Scenario Planning Model Against Foreign Intelligence Operations

As illustrated in Figure 1, these two axes generate a 2x2 matrix with four quadrants, each representing different scenarios with unique characteristics and strategic implications. Figure 1 presents a comprehensive Counterintelligence Scenario Planning Model that visualizes Indonesia's intelligence posture through four distinct scenarios, constructed around two critical variables positioned as the horizontal and vertical axes: the intensity of foreign intelligence operations (ranging from low to high) and the state of Indonesian intelligence governance (ranging from fragmented to unified). The matrix depicted in Figure 1 employs a quadrant approach to illustrate different strategic positions and their corresponding implications for national security, with each quadrant representing a distinct combination of external threat levels and internal institutional capacity.

Scenario 1: Intelligence Warfare (Quadrant I)

As shown in the upper-right quadrant of Figure 1, the first scenario represents a condition of intelligence warfare characterized by high foreign intelligence operation intensity coupled with unified Indonesian intelligence governance. In this situation, both sides possess strong capabilities, creating an active intelligence competition. The consequences of this scenario manifest as intense yet controlled intelligence rivalry, where Indonesia demonstrates the capacity to identify, prevent, and counter foreign intelligence operations effectively. The relevant strategies for this quadrant emphasize reverse operations, strengthening BIN coordination, and intelligence force consolidation. This scenario reflects a mature intelligence environment where Indonesia can engage adversaries on relatively equal footing, demonstrating that strong institutional coordination serves as the foundation for effective counterintelligence operations even under conditions of heightened foreign intelligence activity.

Scenario 2: Foreign Intelligence Dominance (Quadrant II) - The Current Condition

Positioned in the upper-left quadrant of Figure 1, the second scenario depicts the most vulnerable situation and represents Indonesia's current condition according to the matrix. This scenario combines high foreign intelligence operation intensity with fragmented Indonesian intelligence governance, creating a particularly precarious situation for national security. Under these circumstances, Indonesia becomes an exposed target of foreign intelligence operations without possessing the coordinated response capacity necessary to defend its interests effectively. The consequences are severe, resulting in significant strategic losses for the nation. The relevant strategies identified for addressing this critical situation prioritize strengthening BIN coordination as the most urgent action, supplemented by reverse operations, strengthening espionage and sabotage capabilities, and establishing a robust legal basis for intelligence activities. This scenario underscores the urgent need for comprehensive intelligence reform and institutional consolidation to address the fundamental vulnerability arising from governance fragmentation.

Scenario 3: Mutual Respect and Deterrence (Quadrant III)

Located in the lower-left quadrant of Figure 1, the third scenario presents a condition of mutual respect and deterrence achieved through low foreign intelligence operation intensity and fragmented Indonesian intelligence governance. This scenario represents a temporary equilibrium that, while appearing relatively safe, remains fundamentally fragile. The minimal threats faced by Indonesia in this scenario stem not from Indonesian strength but rather from external factors that limit foreign intelligence activities. The consequences reveal a precarious peace where Indonesia's security depends more on circumstances than capabilities. The relevant strategies focus on intelligence institutional strengthening, human resource capacity building, and system modernization to transform this temporary respite into sustainable security. This scenario serves as a reminder that apparent calm should not breed complacency in intelligence development, as the underlying structural weaknesses in governance remain unaddressed and could quickly become critical if external conditions change.

Scenario 4: Indonesian Intelligence Superiority (Quadrant IV) - The Target Condition

Represented in the lower-right quadrant of Figure 1, the fourth scenario represents the ideal target condition characterized by low foreign intelligence operation intensity combined with unified Indonesian intelligence governance. This optimal situation demonstrates effective deterrence, where foreign intelligence operations are reduced due to Indonesia's strong counterintelligence capabilities. The consequences of achieving this scenario include a substantial reduction in foreign intelligence activities,

driven by recognition of Indonesia's robust defensive and offensive intelligence capabilities. The relevant strategies for maintaining this advantageous position include capacity maintenance, technology innovation, intelligence diplomacy, and regional cooperation. This scenario represents the strategic endpoint toward which Indonesian intelligence reform efforts should be directed, embodying the principle that superior intelligence governance creates inherent deterrence effects that reduce the need for reactive counterintelligence operations.

Current Position and Strategic Implications

Based on interview data analysis and documents, validated through Focus Group Discussion (FGD) with stakeholders, Indonesia currently occupies Quadrant II (Foreign Intelligence Dominance) in Figure 1. This condition is characterized by high foreign intelligence operation intensity confirmed by all informants from various agencies, while Indonesian intelligence governance remains fragmentary with suboptimal coordination. Position confirmation was obtained through consensus from all interviewed stakeholders and supported by empirical evidence of ongoing foreign intelligence operation cases without effective legal enforcement.

The scenario planning model presented in Figure 1 fundamentally illustrates that Indonesia occupies the least favorable strategic position and must undertake systematic efforts to transition toward Scenario 4, the ideal condition represented in Quadrant IV. This transition requires comprehensive reform of intelligence governance, with particular emphasis on strengthening coordination mechanisms and establishing BIN as the central focal point for national intelligence coordination. The pathway from the current vulnerable state to the target state of superiority demands sustained commitment to institutional development, technological advancement, legal framework enhancement, and human capital investment in the intelligence sector. The urgency of this transition is underscored by the demonstrated gap between the intensity of foreign intelligence threats and Indonesia's current capacity to mount coordinated, effective responses, as clearly visualized in the matrix structure of Figure 1.

4.5. Strategic Recommendations: Transition from Quadrant II to Quadrant IV

Based on Indonesia's current position in Quadrant II, the research recommends phased strategies to achieve Quadrant IV (Indonesian Intelligence Superiority). These strategies are divided into two phases: short-term strategies for current situation stabilization, and medium-to-long-term strategies for fundamental structural transformation.

4.5.1. Short-Term Strategies (1-2 Years)

Strengthening BIN's Coordination Role (Primary Priority Strategy): Operationalizing BIN's mandate as national intelligence coordinator based on Law No. 17 of 2011 Article 10. Based on research findings analysis, effective coordination is key to addressing institutional fragmentation as the main weakness of Indonesia's counterintelligence system. Concrete steps required include: (1) forming an Integrated Counterintelligence Task Force involving BIN, BAIS TNI, BIK Polri, Attorney General's Office, BSSN, and Immigration with weekly coordination meetings to discuss actual cases and share information in real-time, (2) developing an Integrated Intelligence Information System enabling inter-agency data exchange while maintaining information security through layered access systems and strong encryption, (3) establishing joint Standard Operating Procedures (SOPs) for handling suspected espionage cases from early detection, further investigation, evidence collection, to enforcement or deportation, and (4) forming joint assessment mechanisms for foreign intelligence threat assessments collaboratively conducted by analysts from various agencies, producing more comprehensive threat assessments.

Strategy implementation requires strong political will support from the highest state leadership. Based on stakeholder recommendations, particularly former senior intelligence officials, the President must explicitly affirm that BIN is the coordinator possessing authority to coordinate all intelligence agencies, and all agencies must comply with this coordination mechanism. Without affirmation from the highest national leadership level, coordination will remain difficult due to each agency's sectoral ego.

Reverse Operations: Implementing offensive counterintelligence operations that not only detect and prevent but also exploit foreign intelligence operations for Indonesian benefit. This strategy shifts the

paradigm from defensive to offensive counterintelligence. Required steps include: (1) systematic identification and monitoring of individuals or organizations suspected of conducting foreign intelligence operations through rigorous surveillance and activity pattern analysis, (2) turning operations where identified foreign intelligence agents become double agents working for Indonesian interests by providing seemingly credible but actually controlled information, (3) deception operations providing seemingly valuable but actually disinformation designed to mislead foreign intelligence and cause them to make incorrect decisions, and (4) intelligence exploitation using foreign intelligence operations as information sources about capabilities, methods, priorities, and organizational structures of foreign intelligence services.

4.5.2. Medium-to-Long-Term Strategies (3-5 Years)

Strengthening Legal Basis for Espionage and Sabotage: This is the most crucial transformative strategy for moving Indonesia from Quadrant II to Quadrant IV. Based on comprehensive research findings analysis, without a strong legal basis, Indonesian counterintelligence operations will always be hindered and unable to provide adequate deterrent effects. The research recommends two alternatives for policymakers:

Alternative 1: Comprehensive Revision of Law No. 17 of 2011 on State Intelligence to add a special Chapter on Espionage and Sabotage Criminal Offenses. This revision must include: (1) clear operational definitions of espionage (collection of state secret information by foreign parties or their agents) and sabotage (destructive acts or disruption of state strategic interests), (2) establishing espionage and sabotage as criminal offenses with minimum 5 years and maximum 20 years imprisonment depending on damage level, plus significant fines, (3) special authorities for intelligence agencies to conduct wiretapping, searches, and arrests of espionage suspects with special court authorization understanding national security issues, and (4) clear prosecution procedures with specially trained prosecutors possessing security clearance to handle cases involving classified state information.

Alternative 2: Enacting a new comprehensive National Security Law covering various national security threats including espionage, sabotage, terrorism, separatism, and subversion in one integrated legal framework. This law can adopt best practices from other countries such as Singapore's National Security Law or the United Kingdom's Official Secrets Act with Indonesian contextual adjustments respecting human rights and democratic principles. This approach's advantage is providing broader, more integrated legal frameworks for coherently addressing the entire national security threat spectrum. This law can also regulate establishment of National Security Courts specifically handling national security cases with judges and prosecutors possessing deep understanding of strategic issues and state security.

Intelligence Institutional Consolidation: Restructuring Indonesia's intelligence architecture to reduce fragmentation and enhance long-term synergy. Required steps include: (1) comprehensive evaluation and restructuring of overlapping intelligence functions among agencies to identify redundancies and coverage gaps, (2) establishing clear task divisions based on operational domains domestic versus foreign, civilian versus military, preventive versus repressive so each agency has clear focus without overlap, (3) strengthening BIN's capacity as coordinator with qualified human resource additions, adequate budget, and firmer authority in coordinating other intelligence agencies, and (4) forming a National Intelligence Council directly led by the President or at minimum the Vice President to ensure strategic coordination at the highest level and rapid decision-making in facing urgent threats.

Intelligence Technology Modernization: Integrating modern technologies such as Artificial Intelligence (AI) for pattern analysis, big data analytics for processing large information volumes, facial recognition for foreign operative identification, and cyber intelligence for digital activity monitoring in counterintelligence operations. Technology investment will enhance early detection capabilities through sophisticated early warning systems, predictive analysis to anticipate foreign intelligence operations before occurrence, and rapid response through integrated command and control systems. Indonesia needs to allocate significant budget for intelligence technology development and personnel training to operate these technologies effectively.

4.6. Theoretical and Practical Contributions

This research provides significant contributions at three interrelated levels:

1. Theoretical Contribution: This research advances scenario planning methodology application in counterintelligence strategy formulation, an area still rarely researched in Indonesian intelligence literature. The TAIDA framework integration with scenario planning produces structured yet flexible analytical models replicable for other intelligence challenges such as counter-terrorism, industrial counter-espionage, or counter-radicalization. This research also enriches national threat and vulnerability theory by identifying that vulnerability is not solely a function of external threats but also internal governance weaknesses enabling threat development. These findings are consistent with securitization literature emphasizing that security is a socio-political construction involving complex interactions among actors, threats, and institutional contexts.
2. Methodological Contribution: This research demonstrates multi-stakeholder perspective value in sensitive intelligence research. Triangulation across ten intelligence and security agencies produces far more comprehensive understanding than single-source analysis prone to sectoral bias. This method also overcomes data access limitations in intelligence research by leveraging various viewpoints to build more complete and accurate pictures. FGD use in intelligence research context also constitutes methodological innovation enabling dialogue among agencies typically working separately and even competitively, creating space for mutual understanding of respective perspectives and building consensus on joint strategies.
3. Practical Contribution: This research provides Indonesian policymakers and intelligence practitioners with actionable strategic frameworks for responding to foreign intelligence operations. The four-scenario model enables adaptive strategy selection based on evolving conditions, both increasing and decreasing threat intensity. Generated specific recommendations particularly regarding strengthening BIN coordination and espionage legal basis strengthening have received positive responses from interviewed stakeholders and are deemed feasible for implementation. This research can provide input for policymakers at Commission I DPR RI in conducting State Intelligence Law revisions or National Security Bill discussions, as well as for executive agencies in formulating more effective operational counterintelligence policies.

5. Conclusion

This research demonstrates that Indonesia's vulnerability to foreign intelligence operations stems from the convergence of three mutually reinforcing factors: abundant and strategic natural resource attractiveness, legal vacuum for prosecuting espionage and sabotage following the de facto repeal of Presidential Decree No. 11/1963, and sectoral intelligence governance fragmentation with suboptimal coordination. The scenario planning model developed based on the TAIDA framework identifies four possible scenarios with two main driving forces: intelligence governance cohesion as an internal factor and foreign intelligence operation intensity as an external factor.

Based on in-depth analysis of data from ten national intelligence and security agencies confirmed through source and method triangulation, Indonesia currently occupies Quadrant II position indicating Foreign Intelligence Dominance condition. This is the most vulnerable condition among four existing scenarios as it shows Indonesia faces high foreign intelligence operation intensity but lacks coordinated response capacity to address it. This condition requires immediate strategic intervention to prevent further losses to Indonesian national interests whether in terms of strategic information loss, natural resource exploitation, or potential sabotage of critical infrastructure.

The most applicable strategies for the current situation are: first, strengthening BIN's coordination role as national intelligence coordinator by forming an Integrated Counterintelligence Task Force, developing integrated information sharing systems, and establishing joint SOPs for handling espionage cases; second, implementing reverse operations that are not only defensive but also offensive to identify, monitor, and exploit foreign intelligence operations for Indonesian interests through agent turning, deception operations, and intelligence exploitation. To achieve the ideal condition in Quadrant IV (Indonesian Intelligence Superiority) characterized by effective deterrence and reduced foreign intelligence operations, fundamental transformation through legal basis strengthening is required. The research recommends two selectable alternatives: comprehensive revision of Law No. 17 of 2011 to add a

special chapter on espionage and sabotage criminal offenses with clear sanctions, or enacting a new National Security Law comprehensively regulating the entire national security threat spectrum including espionage and sabotage with firm criminal sanctions, clear prosecution procedures, and establishment of special national security courts.

The scenario planning approach employed in this research provides Indonesia's intelligence community with adaptive strategic frameworks capable of responding to dynamic operational environments. The TAIDA-based methodology integrated with scenario planning proves effective in analyzing complex problems involving multiple variables, high uncertainty, and long-term strategy needs requiring flexibility, thus replicable for addressing other national security challenges such as terrorism threats, radicalization, separatism, or cyber threats.

Future research is recommended to: (1) examine detailed specific implementation mechanisms of recommended strategies including required budget aspects, human resource needs with certain qualifications, and technologies needing adoption, (2) conduct comparative analysis with counterintelligence approaches in countries with similar geopolitical positions such as Singapore, Malaysia, Philippines, or Thailand to identify adoptable best practices with Indonesian contextual adjustments, (3) develop quantitative metrics and indicators to assess counterintelligence strategy effectiveness enabling objective measurement and continuous improvement, and (4) research modern technology aspects such as AI, machine learning, and cyber intelligence in Indonesian counterintelligence context to identify capability enhancement opportunities through technology adoption.

References

Amin, I. (2022, July 26). *TNI–Polri diminta telusuri WNI yang menjadi intelijen asing*. Tirto.id. https://tirto.id/tni-polri-diminta-telusuri-wni-yang-menjadi-intelijen-asing-gutx

Anggraini, C., Susetyorini, P., & Roisah, K. (2016). Penyalahgunaan hak kekebalan diplomatik ditinjau dari Konvensi Wina 1961 (studi kasus penyelundupan emas oleh pejabat diplomatik Korea Utara di Bangladesh). *Diponegoro Law Journal*, 5(3), 1–17.

Aspinall, E. (2005). *Opposing Suharto: Compromise, resistance, and regime change in Indonesia.* Stanford University Press.

Bartes, F. (2013). Five-phase model of the intelligence cycle of competitive intelligence. *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis*, 61(2), 283–288. https://doi.org/10.11118/actaun201361020283

Creswell, J. W. (2002). *Research design: Qualitative, quantitative, and mixed methods approaches (2nd ed.).* Sage Publications.

Darmawan, A. (2023). Konflik Laut Cina Selatan dan implikasinya terhadap keamanan regional. Jurnal Hubungan Internasional, 11(2), 145–162.

Edgar, B., Abouzeedan, A., Hedner, T., Maack, K., & Lundqvist, M. (2013). Using scenario planning in regional development context: The challenges and opportunities. *World Journal of Science, Technology and Sustainable Development,* 10(2), 75–94. https://doi.org/10.1108/20425941311323118

Elson, R. E. (2001). *Suharto: A political biography. Cambridge* University Press.

Gill, P., & Phythian, M. (2018). *Intelligence in an insecure world (3rd ed.).* Polity Press.

Government of the Republic of Indonesia. (1963). *Presidential Decree Number 11 of 1963 on the eradication of subversive activities*.

Government of the Republic of Indonesia. (2011). *Law Number 17 of 2011 on state intelligence*.

Johnson, L. K. (2020). *National security intelligence (2nd ed.).* Polity Press.

Kelly, P., Smith, R., & Anderson, T. (2023). Scenario planning in post-pandemic policy development. *Policy Studies Journal*, 51(3), 412–431. https://doi.org/10.1111/psj.12500

Kent, S. (1949*). Strategic intelligence for American world policy*. Princeton University Press.

Kuswara, Y. B. (2019). Evaluasi fungsi kontra intelijen Indonesia dalam menghadapi spionase intelijen asing. *Jurnal Intelijen*, 8(1), 23–45.

Lindgren, M., & Bandhold, H. (2009). *Scenario planning: The link between future and strategy (2nd ed.)*. Palgrave

Macmillan.

Lissofa, N. (2016). Dampak spionase NSA (National Security Agency) terhadap hubungan diplomatik Amerika dan Jepang. *Jurnal Hubungan Internasional*, 5(1), 67–82.

Lowenthal, M. M. (2020). *Intelligence: From secrets to policy (8th ed.).* CQ Press.

Lowenthal, M. M., & Clark, R. M. (2022). *The five disciplines of intelligence collection (3rd ed.).* CQ Press.

Neuman, W. L. (2013). *Social research methods: Qualitative and quantitative approaches (7th ed.).* Pearson Education.

Peterson, G. D., Cumming, G. S., & Carpenter, S. R. (2003). Scenario planning: A tool for conservation in an uncertain world. *Conservation Biology*, 17(2), 358–366. https://doi.org/10.1046/j.1523-1739.2003.01491.x

Prunckun, H. (2019). *Handbook of scientific methods of inquiry for intelligence analysis (3rd ed.).* Rowman & Littlefield.

Robison, R., & Hadiz, V. R. (2004). *Reorganising power in Indonesia: The politics of oligarchy in an age of markets*. RoutledgeCurzon.

Sujarweni, V. W. (2014). *Metodologi penelitian: Lengkap, praktis, dan mudah dipahami*. Pustaka Baru Press.

Sumandoyo, A. (2016). *Jejak operasi intelijen asing di Indonesia*. Kompas.

Taher, A. P. (2022). *Waspada infiltrasi intelijen asing di Indonesia.* Media Indonesia.

Volkery, A., & Ribeiro, T. (2009). Scenario planning in public policy: Understanding use, impacts, and the role of institutional context factors. *Technological Forecasting and Social Change*, 76(9), 1198–1207. https://doi.org/10.1016/j.techfore.2009.04.002

Warner, M. (2022). *The rise and fall of intelligence: An international security history*. Georgetown University Press.