KRTHA BHAYANGKARA, Vol. 19, No. 3 (2025), pp. 665-690
ISSN 1978-8991 (print) | ISSN 2721-5784 (online)
Available online at: http://ejurnal.ubharajaya.ac.id/index.php/KRTHA

Counterintelligence in Legal Perspective: Balancing National Security and Human Rights in Indonesia

Stanislaus Riyanta
Graduate School of Sustainable Development, University of Indonesia
Email: stanislaus@ui.ac.id

Article info

Received: Sep 24, 2025	Revised: Nov 5, 2025	Accepted: Dec 20, 2025

DOI: https://doi.org/10.31599/krtha.v19i3.4528

Abstract : This study examines the crucial role of counterintelligence within the legal framework of Indonesia, focusing on the inherent tension between safeguarding national security and upholding human rights in the face of evolving contemporary threats. Utilizing a qualitative legal analysis approach, this research scrutinizes existing Indonesian laws, particularly the State Intelligence Law (Law No. 17/2011), to identify their adequacy, ambiguities, and potential for legal and ethical challenges in counterintelligence operations. It analyzes how core counterintelligence functions—such as intelligence gathering, surveillance, and neutralization—are regulated and the extent to which they align with international human rights standards. The study highlights critical legal gaps concerning privacy protection, accountability mechanisms, and oversight of intelligence agencies. Based on this analysis, it proposes concrete legal reforms and policy recommendations aimed at strengthening Indonesia's counterintelligence capabilities while ensuring robust adherence to democratic principles, rule of law, and fundamental human rights. This includes advocating for clearer legal mandates, enhanced independent oversight, and transparent accountability frameworks to foster public trust and legitimacy in counterintelligence practices.

Keywords : Counterintelligence, Intelligence Operations, National Security, Human Rights, Legal Framework, Indonesia

I. INTRODUCTION

The evolving landscape of national security threats, encompassing sophisticated foreign espionage, cyber warfare, and disinformation campaigns, necessitates robust counterintelligence capabilities for Indonesia. As a strategically vital nation, Indonesia faces persistent covert interference that demands proactive measures to protect its sovereignty and critical assets. However, the implementation of such measures inherently raises complex legal and ethical questions, particularly concerning the balance between national security imperatives and the protection of fundamental human rights.

Historically, intelligence and counterintelligence operations have often operated within a veil of secrecy, sometimes leading to concerns about accountability and adherence to legal norms. In Indonesia, the primary legal basis for intelligence activities is the State Intelligence Law (Law No. 17/2011). While this law grants broad mandates

to intelligence agencies, its provisions regarding the scope, limitations, and oversight of counterintelligence operations, especially those involving intrusive measures like surveillance or data collection, warrant critical examination. Incidents such as the alleged foreign intelligence intrusions, including cyber-attacks on Indonesian ministries, underscore the urgent need for effective counterintelligence. Yet, the legal mechanisms governing the response to such threats must be clear, proportionate, and compliant with democratic principles.

This study aims to comprehensively analyze the existing legal framework for counterintelligence in Indonesia, identify its strengths and weaknesses, and explore the legal and ethical challenges arising from its application. By scrutinizing relevant national laws and drawing comparisons with international best practices, this research seeks to propose actionable legal reforms that can enhance Indonesia's counterintelligence effectiveness while simultaneously ensuring robust protection for human rights and strengthening the rule of law. The central question guiding this inquiry is: How can Indonesia develop a resilient and effective counterintelligence apparatus that operates within a transparent, accountable, and human rights-compliant legal framework?

The Indonesia's national security faces an increasingly complex landscape of threats that make effective counterintelligence (CI) more critical than ever. As Southeast Asia's largest country, Indonesia occupies a strategic position that attracts intense geopolitical interest, which in turn heightens the risk of espionage and covert interference by foreign powers. Recognizing this, the Indonesian government has elevated security and intelligence improvements as a national priority, aiming to safeguard sovereignty and stability in the face of both traditional and non-traditional threats. In this context, counterintelligence as the practice of detecting and thwarting adversaries. It complements the country's intelligence gathering efforts to address challenges unique to the Indonesian environment.

Indonesia, in addressing these transformative challenges, must navigate a complex array of issues. This include geopolitical threats, technological vulnerabilities, and institutional challenges that underscore the urgent need for a robust counterintelligence strategy. On a specific note, World War II highlighted the pivotal role of intelligence in the Battle of Midway, where the U.S. Navy secured a significant victory by acting on approximately 60% of intercepted communications from the Imperial Japanese Navy, supplemented by an element of fortuitous circumstance. Geopolitically, Indonesia's non-aligned stance and leadership role in ASEAN have historically made it a target of espionage by major powers. For instance, covert operations by foreign intelligence agencies have been part of Indonesia's modern history, from the Cold War era such as the 1958 CIA mission in Ambon that led to the capture of American pilot Allen Pope, to more recent incidents like the 2009 revelation that Australia had intercepted communications of Indonesia's president. Technologically, Indonesia's rapid digital development has opened new avenues for espionage. A stark example came in 2021, when a Chinese state-linked cyber espionage group infiltrated the networks of Indonesian ministries, including the national intelligence agency (BIN), exposing critical vulnerabilities in cyber defense. These cases illustrate that Indonesia is not immune to

foreign intelligence intrusions, whether through traditional spying or advanced cyber-attacks, and that information has truly become a potent weapon in modern conflicts.

Over time, intelligence operations directed at Indonesia have contributed to its complex historical trajectory. A closer examination of individual cases reveals several key intelligence activities, which can foster a deeper understanding of the threats involved, the actors behind them, and the methods employed, outlined as follows:

Table 1. List of Intelligence Activities Conducted by Foreign Agents in Indonesia

No	Year	Incident	Country Involved
1	1958	Allan Pope (CIA) shot and killed personnel of the Indonesian National Armed Forces using airplanes in Ambon (sabotage).	United States of America (CIA)
2	1964	Classified documents were released in 2006 and 2007 on the CIA's official webpage regarding the situation in Indonesia throughout 1965.	United States of America (CIA)
3	1982	The Soviet Union managed to recruit an officer from the Indonesian Navy to steal maritime data.	Soviet Union / Russia
4	2005	John Perkins, a CIA recruit specializing in economic affairs, stated in his book "Confessions of an Economic Hit Man" that Indonesia was targeted by the U.S.	United States of America
5	2008	Tim Weiner, an author, stated the CIA's involvement in Indonesia after the coup known as G30S/PKI in his book "Legacy of Ashes: The History of the CIA."	United States of America
6	2009	Australia tapped the communication devices of the 6th President of Indonesia and his family, as reported by former NSA contractor Edward Snowden on Wikipedia.	Australia

In sum, the incidents underscore two critical insights. First, information serves as a powerful instrument of influence and control. Second, intelligence activities transcend borders, leaving no country untouched. Compounding these external threats are institutional challenges within Indonesia's security apparatus. Historically, Indonesia's intelligence community has prioritized information gathering and counter-terrorism, while counterintelligence has received comparatively less attention and development. This has resulted in gaps such as the absence of a dedicated counterintelligence agency and limited coordination specifically devoted to detecting and neutralizing espionage within Indonesia's borders. Such institutional vulnerabilities can be perilous – adversaries may exploit them to infiltrate agencies or recruit insiders, leading to leaks of confidential data or sabotage of critical infrastructure. In light of these factors, strengthening counterintelligence capabilities is imperative for Indonesia.

Indonesia's official planning documents, as a matter in fact, already hint at the importance of intelligence (and by extension, counterintelligence) in national security. The National Medium-Term Development Plan 2020–2024 (RPJMN) explicitly calls for

"strengthening the governance and coordination of state intelligence" and "increasing the professionalism of intelligence personnel" as part of its security objectives. Although counterintelligence is not named outright in the RPJMN, these priorities indicate a national commitment to bolstering intelligence capabilities, which inherently includes countering espionage and infiltration threats. Moreover, Indonesia's Defence White Paper (2015) identifies espionage as one of the key threats to the nation's security, alongside issues like terrorism, cyber attacks, and separatism. By acknowledging espionage as a security threat, the White Paper underscores the need for robust counterintelligence measures within defense and security policies. Integrating the development of counterintelligence efforts into policy bridges the gap between theory and practice: it ensures that the theoretical frameworks of deterrence, detection, deception, and neutralization discussed in this study translate into concrete government strategies for threat reduction. For instance, if counterintelligence capabilities are enhanced, they can inform national policy by providing early warning of foreign espionage plots or disinformation campaigns, thereby allowing policymakers to craft proactive measures in response. In addition, Indonesia's State Intelligence Agency (BIN) plays a central role in this integration. As the primary intelligence body, BIN is already charged with detecting and preventing threats to national stability – a mandate codified in the State Intelligence Law (No. 17/2011), which positions intelligence as the "first line of defense in the national security system". Developing a dedicated counterintelligence apparatus or strengthening BIN's counterintelligence capacity, by extension, significantly influence the formulation of future national security policies.

II. METODHOLOGY

This study employs a qualitative legal analysis approach, grounded in a comprehensive review of primary and secondary legal sources. The methodology is designed to critically examine the legal framework governing counterintelligence in Indonesia and its implications for human rights. The research process involves:

1. **Statutory Analysis:** In-depth examination of relevant Indonesian legislation, primarily Law No. 17/2011 on State Intelligence, along with other pertinent laws such as the Electronic Information and Transactions Law (Law No. 11/2008 as amended by Law No. 19/2016), the Criminal Procedure Code, and human rights instruments ratified by Indonesia. This analysis focuses on identifying legal mandates, limitations, and ambiguities related to counterintelligence operations.
2. **Case Law Review:** Where publicly available, analysis of judicial decisions or legal interpretations that shed light on the application and challenges of intelligence-related laws in practice.
3. **Comparative Legal Analysis:** Examination of legal frameworks for intelligence and counterintelligence oversight in selected democratic jurisdictions (e.g., the United States, United Kingdom, Germany) to identify best practices and potential models for reform concerning accountability, transparency, and human rights protection.

4. **Scholarly Literature Review:** Synthesis of academic works in intelligence studies, public law, human rights law, and national security to contextualize legal debates and theoretical underpinnings.

The analytical process involves identifying key legal principles, assessing the compatibility of existing laws with international human rights standards, and pinpointing areas where legal clarity, oversight, or accountability mechanisms are deficient. The ultimate goal is to formulate evidence-based recommendations for legal and policy reforms that can foster a more robust and rights-compliant counterintelligence system in Indonesia.

As for the literature review, it draws on a diverse range of sources selected through purposive sampling to ensure thematic relevance and analytical depth. The inclusion criteria prioritized:

1. Peer-reviewed academic journals in the fields of intelligence studies, political science, international security, and strategic defense.
2. Government and institutional policy documents, including Indonesia's RPJMN 2020–2024, the Defense White Paper, and legal texts such as Law No. 17/2011 on State Intelligence.
3. Credible non-academic sources such as declassified documents, expert-authored books (e.g., by Richard Betts and Mark Lowenthal), think-tank reports (e.g., RAND, CSIS), and intelligence agency briefings (e.g., MI5, FBI).
4. Contemporary news sources and investigative reports to illustrate real-world case studies such as foreign espionage in Indonesia or the cyber-espionage attack by Mustang Panda.
5. Geographic focus that primarily centered on Indonesia and Southeast Asia, with comparative cases from global intelligence practices to contextualize relevance and draw cross-regional insights.

The analytical process employed a thematic synthesis, organized around key principles of counterintelligence which is deterrence, detection, deception, and neutralization and the three supporting axioms: surprise, data collection, and targeting. Sources were categorized and analyzed to identify recurring themes, strategic models, institutional patterns, and policy linkages. This conceptual mapping approach allowed for an integrated synthesis of theoretical constructs and practical policy implications. It ensured that insights drawn from international best practices were critically adapted to the Indonesian security environment. The goal of the analysis was not only to identify theoretical patterns but also to formulate actionable recommendations that address Indonesia's unique counterintelligence gaps, such as the absence of a dedicated agency or the need for psychological support systems and technological readiness.

III. ANALYSIS

Counterintelligence refers to the spectrum of measures aimed at detecting, deterring, and disrupting adversary intelligence operations. Its key objectives include protecting agencies from infiltration, preventing the leakage of sensitive information, and securing vital

facilities, technologies, and resources against espionage, subversion, sabotage, or other threats. In essence, effective CI acts as a defensive shield for national security, ensuring that intelligence gains are not undermined by an opponent's covert actions.

More nations are relying on intelligence as a primary source for national security policy and offensive operations. This reliance can lead to information warfare characterized by asymmetric resources, potentially resulting in geopolitical crises and instability. To mitigate these impacts, effective countermeasures must be implemented to prevent leaks of critical military and national security information. These countermeasures, known as counterintelligence, involve efforts by a country to thwart intelligence gathering by adversary agencies or political movements. The primary objectives of counterintelligence include:

1. protecting an agency or client from adversary infiltration
2. preventing inadvertent leakage of confidential information
3. securing materials and installations against espionage, subversion, sabotage, terrorism, and other forms of politically motivated violence, as well as safeguarding key technologies and equipment.

Given the increasing importance of intelligence, robust counterintelligence capabilities are essential for protecting national security. Therefore, to achieve optimal outcomes, a dedicated counterintelligence agency should be established alongside the intelligence agency, as both play critical roles in addressing asymmetric information warfare. This study will examine the concepts, challenges, complexities, and strategic proposals surrounding the development of counterintelligence in Indonesia. It also aims to recommend the establishment of a counterintelligence agency to strengthen national security and prevent future intelligence leaks.

The Legal Basis of Counterintelligence in Indonesia

Counterintelligence activities in Indonesia are primarily governed by Law No. 17/2011 on State Intelligence (hereinafter, the 'State Intelligence Law'). This comprehensive legislation outlines the functions, authorities, and organizational structure of the State Intelligence Agency (BIN) and other intelligence entities. Article 1 defines intelligence as 'efforts, activities, and actions carried out to detect, identify, analyze, and provide early warnings to the government regarding various threats to national security.' While counterintelligence is not explicitly defined as a standalone function, its core activities—such as preventing espionage, subversion, and sabotage—are implicitly covered under BIN's general mandate to 'conduct intelligence operations to secure national interests' (Article 26).

However, the State Intelligence Law has been criticized for its broad and sometimes ambiguous provisions, particularly concerning the scope of intelligence operations and the protection of individual rights. For instance, Article 31 grants intelligence agencies the authority to 'collect information, conduct investigations, and carry out intelligence operations,' without clearly delineating the specific legal thresholds or judicial oversight required for intrusive measures like surveillance or interception of communications. This broad mandate raises concerns about potential abuses and the lack

of robust safeguards for privacy, a fundamental human right recognized under international law. As argued by Prunckun, 'the absence of clear legal definitions and limitations for intelligence activities can create a fertile ground for arbitrary actions and human rights violations.[1]

Furthermore, other relevant laws, such as the Electronic Information and Transactions Law (Law No. 11/2008 as amended by Law No. 19/2016), provide legal grounds for electronic surveillance and data collection. However, the coordination and hierarchy of these legal provisions in the context of counterintelligence operations remain complex and sometimes overlapping, leading to potential **jurisdictional ambiguities** among different law enforcement and intelligence agencies.[2] The Criminal Procedure Code (Law No. 8/1981) also governs aspects of investigation and evidence collection, but its provisions are primarily designed for criminal prosecution rather than proactive intelligence gathering, creating a gap in regulating preventive counterintelligence measures.

Legal and Ethical Challenges in Counterintelligence Operations

The inherent secrecy and often intrusive nature of counterintelligence operations pose significant legal and ethical challenges, particularly in a democratic state committed to the rule of law and human rights. These challenges manifest in several key areas:

Privacy and Surveillance: One of the most contentious issues is the tension between the need for intelligence agencies to conduct surveillance to detect threats and the individual's right to privacy. While the State Intelligence Law permits intelligence operations, it lacks explicit provisions for independent judicial authorization or oversight for surveillance activities, including wiretapping and electronic data collection. This contrasts sharply with practices in many democratic countries, where such intrusive measures typically require a warrant from a specialized court or an independent oversight body.[3] The absence of such safeguards in Indonesia raises concerns about potential arbitrary surveillance, which can infringe upon the right to privacy guaranteed by Article 28G of the Indonesian Constitution and Article 17 of the International Covenant on Civil and Political Rights (ICCPR), to which Indonesia is a party.[4] As Lyon notes, the balance between security and privacy is a constant challenge, especially with evolving surveillance technologies[5]

Accountability and Oversight: The State Intelligence Law establishes internal and external oversight mechanisms, including parliamentary oversight by the House of

[1] Henry Prunckun, *Counterintelligence Theory and Practice*, 2nd ed. (Lanham, MD: Rowman & Littlefield, 2019), 25-27.

[2] Sulastri, Lusia. "Analisis Kewenangan Penyidikan Dalam Pelanggaran Wilayah Udara Indonesia (Tinjauan Peran Penyidik PNS dari Kementerian Perhubungan dan TNI AU)." KRTHA BHAYANGKARA 16, no. 2 (Desember 2022): 273-285.

[3] Sulastri, Lusia. "Analisis Kewenangan Penyidikan Dalam Pelanggaran Wilayah Udara Indonesia (Tinjauan Peran Penyidik PNS dari Kementerian Perhubungan dan TNI AU)." KRTHA BHAYANGKARA 16, no. 2 (Desember 2022): 273-285.

[4] Lucia Zedner, "Security, the State and the Citizen: The Changing Face of Security," *Theoretical Criminology* 13, no. 3 (August 2009): 305-307.

[5] United Nations, *International Covenant on Civil and Political Rights*, G.A. Res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), entered into force March 23, 1976, Article 17.

Representatives (DPR). However, the effectiveness of these mechanisms in ensuring genuine accountability for intelligence agencies remains a subject of debate. Critics argue that parliamentary oversight is often limited by the classified nature of intelligence operations and the lack of specialized expertise among parliamentarians.[6] As Haggerty and Ericson suggest, a lack of transparency can lead to public distrust and potential abuse of power.[7] Independent oversight bodies, common in other democracies to review intelligence activities and handle public complaints, are not explicitly mandated with strong powers under Indonesian law. This creates a 'democratic deficit' where the executive branch's intelligence powers may operate with insufficient checks and balances.[8]

Use of Force and Neutralization: Counterintelligence operations may involve measures to 'neutralize' threats, which can range from disrupting foreign intelligence networks to apprehending suspected agents. The legal boundaries for the use of force, detention, and interrogation in such contexts are critical. While the Criminal Procedure Code governs arrests and detentions for criminal offenses, the application of these provisions to intelligence-led operations, particularly those aimed at prevention rather than immediate prosecution, can be ambiguous. Concerns about the potential for arbitrary detention or coercive interrogation methods, even if not explicitly sanctioned, underscore the need for clear legal guidelines and strict adherence to human rights standards, including the absolute prohibition of torture.[9] Walzer emphasizes that actions taken in the name of security must always consider their impact on individuals and society.[10]

Disinformation and Freedom of Expression: In the era of cognitive warfare and disinformation, counterintelligence agencies are increasingly involved in countering foreign influence operations. While essential for national security, these efforts must be carefully balanced with the protection of freedom of expression and access to information. Legal provisions aimed at combating disinformation, such as those in the Electronic Information and Transactions Law, have sometimes been criticized for their potential to be used to suppress legitimate criticism or dissent.[11] A robust legal framework for counter-disinformation must clearly distinguish between harmful foreign propaganda and protected speech, ensuring that counterintelligence efforts do not inadvertently stifle democratic discourse. Putter highlights the growing importance of counterintelligence in cognitive warfare, which necessitates careful consideration of ethical boundaries.[12]

---

[6] David Lyon, *Surveillance as Social Sorting: Privacy*, Risk, and Digital Discrimination (London: Routledge, 2003), 88-90. Kevin D. Haggerty and Richard V. Ericson, "The Surveillant Assemblage*," British Journal of Sociology 51*, no. 4 (December 2000): 610-612.

[7] Haggerty and Ericson, "The Surveillant Assemblage," 615.

[8] Hans Born, Ian Leigh, and Aidan Wills, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (Oslo: Geneva Centre for the Democratic Control of Armed Forces (DCAF) and Norwegian Parliamentary Intelligence Oversight Committee, 2015), 45.

[9] Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations,* 5th ed. (New York: Basic Books, 2015), 134-136.

[10] Walzer*, Just and Unjust Wars*, 135.

[11] Lyon, *Surveillance as Social Sorting,* 95-97.

[12] Dries Putter, "Navigating the Interplay of Cognitive Warfare and Counterintelligence in African Security Strategies: Insights and Case Studies," *Journal of Policing, Intelligence and Counter Terrorism* 20, no. 2 (2024): 173-192.

Concepts and Classifications in Counterintelligence

Counterintelligence is defined as the activities involved in gathering information to thwart intelligence operations conducted by adversaries. More specifically, it encompasses efforts to protect against espionage and intelligence threats, particularly from adversaries. This definition emphasizes that counterintelligence is just as significant as intelligence itself. Unfortunately, it has historically received less attention, leading to its underdevelopment and, in some cases, being perceived as the "stepchild" of the intelligence community. This situation arises because counterintelligence efforts often concentrate on specific espionage cases and terrorist prevention, rather than on its broader role in shaping national security policy.

Counterintelligence operations, much like broader intelligence functions, are riddled with multifaceted challenges. These challenges become even more acute in a national context such as Indonesia, where institutional limitations, legal ambiguities, and internal political dynamics pose significant constraints on the effective development and execution of counterintelligence strategies. One of the most pressing issues is the lack of a clear legal and institutional framework specifically dedicated to counterintelligence. While Indonesia has a State Intelligence Law (Law No. 17/2011) that outlines the mandates of agencies like BIN, the law does not sufficiently define counterintelligence as a standalone strategic function, nor does it provide legal clarity regarding the scope, authority, and limits of counterintelligence operations. This legal ambiguity can discourage proactive counterintelligence efforts, especially when actions risk being perceived as violations of civil liberties or due process, issues that are especially sensitive in democratic transition contexts like Indonesia.

Moreover, institutional overlap and fragmentation among security and intelligence agencies in Indonesia, such as BIN, BSSN (National Cyber and Crypto Agency), BAIS (Military Intelligence), and even Polri's Intelligence Directorate create siloed operations and communication gaps. These gaps present opportunities for hostile actors to exploit blind spots between agencies, particularly when inter-agency trust is low or when jurisdictional boundaries are unclear. The lack of an integrated counterintelligence command structure weakens Indonesia's ability to detect and respond to internal threats swiftly and comprehensively. In essence, Indonesia's counterintelligence faces not only external operational threats but also a dense web of internal vulnerabilities. These include legal uncertainty, inter-agency fragmentation, internal corruption risks, inadequate psychological monitoring, and a persistent gap in cyber-defensive capabilities. Addressing these challenges requires not only structural reforms but also a reimagining of counterintelligence as a strategic pillar of national security policy, with dedicated resources, legal mandate, and institutional authority. By localizing the analysis of challenges to Indonesia's unique security and governance context, this study affirms the necessity for a grounded, context-aware approach to counterintelligence reform.

In addition, the global relevance of this finding is particularly noteworthy, as it highlights the critical role of counterintelligence on an international scale. For instance, Lieutenant General Oleg Gribanov established key milestones for counterintelligence in the Soviet Union but was later removed from his position for unclear reasons. He sought

to raise public awareness about the importance of counterintelligence through his fictional works; however, his efforts were insufficient. The landscape shifted dramatically after the September 11 attacks on the United States, which prompted security intelligence analysts to recognize the critical role of counterintelligence in minimizing or preventing intelligence failures. In discussing counterintelligence, the analysis within this domain are categorized into four types:

1. Type One: Foreign Intelligence Threat Analysis
2. Type Two: Counter-Counterintelligence Analysis
3. Type Three: Operational and Investigative Analysis
4. Type Four: Strategic Foreign Intelligence Analysis

Foreign intelligence threat analysis focuses on assessing risks to friendly interests posed by foreign intelligence activities. This prevalent form of counterintelligence analysis systematically examines the operational modalities of foreign intelligence systems within targeted sovereign states. Its utility extends across a broad spectrum of stakeholders, from tactical operatives to strategic policymakers. Specifically, its beneficiaries include military decision-makers, who leverage such analysis to mitigate threats to their operations, critical infrastructure, and personnel; senior government officials, for whom it provides essential insights for personal security protocols during international engagements; governmental agencies, in their imperative to safeguard their workforce from hostile espionage; and the research, development, and acquisition communities, for whom the protection of proprietary and critical technologies is paramount.

In summary, foreign intelligence threat analysis provides valuable counterintelligence insights to non-intelligence sectors. Counter-counterintelligence analysis provides guidance and direction to intelligence collectors, helping them avoid foreign counterintelligence activities. Unlike the previous type, this analysis focuses on how foreign counterintelligence services attempt to neutralize intelligence operations within the targeted country. Consequently, the primary users of this analysis are intelligence collectors from the targeted nation. Key aspects of this type of counterintelligence include: (1) information gathered by friendly intelligence units to identify vulnerabilities and hostile capabilities for exploitation; (2) counterintelligence reviews of human intelligence (HUMINT) activities; (3) assessments of damage caused by counterintelligence efforts; and (4) asset validation. Essentially, this type of counterintelligence parallels operations security analysis, as both aim to identify elements of friendly operations that may be vulnerable to foreign observation and neutralization.

Counterintelligence operational and investigative analysis provides crucial insights that support the investigative and operational functions of counterintelligence, including information assurance efforts. This analysis seeks to determine how domestic counterintelligence initiatives can neutralize foreign counterintelligence threats. Its main focus is opportunity analysis, which identifies the right venues, assets, scenarios, targets, and passage materials to bolster friendly counterintelligence activities. Additionally, it may guide the development of evidence to support counterintelligence investigations. The primary users of this analysis are insiders within the Intelligence Community, who work to prevent foreign intelligence from compromising friendly operations. Furthermore, this

type of counterintelligence targets the most significant foreign intelligence threats, which require substantial resources for effective counteraction.

Lastly, strategic foreign intelligence analysis examines the relationship between foreign intelligence activities and the strategic decision-making processes that guide them. This type of counterintelligence is closely linked to strategic political and military analysis, as it seeks to answer two key questions: (1) the missions assigned by adversaries to their intelligence resources, and (2) the intelligence priorities and overarching strategic mindset of the adversary. The primary goal of this analysis is to identify why a country targets specific individuals or entities with its foreign intelligence or clandestine activities and what these choices reveal about its policies. Thus, while this type of counterintelligence shares similarities with earlier types, it serves a distinct purpose: to provide insights into the strategic thinking behind intelligence operations, focusing on the adversaries' intentions.

Counterintelligence Principles and Commandments

Thoroughly understanding the definition and classification of counterintelligence serves as a foundation for grasping its core aspects. These core aspects comprise the principles and commandments of counterintelligence activities. While they may seem separate, both are complementary. Specifically, counterintelligence principles guide the execution of counterintelligence activities, while commandments direct analysts and practitioners in fulfilling their roles and responsibilities. The interplay between these principles and commandments is crucial, as they work together to safeguard vital intelligence through their complementary characteristics. Therefore, focusing on these principles and commandments is essential for developing effective and credible counterintelligence practices.

In general, there are two types of counterintelligence principles: defensive and offensive. These can be further categorized as follows: (1) defensive counterintelligence principles, which include deterrence and detection, and (2) offensive counterintelligence principles, which comprise deception and neutralization. Deterrence aims to discourage adversaries from conducting penetration operations or to deny them data gathering after such operations. For deterrence to be effective, three premises must be met: (1) the organization must be capable of inflicting unacceptable damage on the adversary; (2) the threat must be perceived by the adversary; and (3) the threat must be credible. In summary, the first premise pertains to the capability to deliver unacceptable harm, the second concerns the intention to do so, and the third addresses the credibility of the threat. This highlights why deterrence is a fundamental component of defensive counterintelligence, which includes physical security, information security, personnel security, and communications security.

In relation to deterrence, detection is also vital. Detection involves confirming whether a breach or potential breach of confidential information has occurred. The detection process consists of five key premises that analysts should consider: (1) identifying the event of concern; (2) identifying the individuals involved; (3) determining their organizational affiliations; (4) identifying their current locations; and (5) gathering evidence indicating their involvement in the event of concern. An "event of concern"

refers to any occurrence related to information-gathering operations conducted by adversaries or hostile intelligence agencies. Examples include the transfer of information from employees to opposing entities or unauthorized surveillance of confidential information. Together with deterrence, effective detection can discourage adversaries from launching operations, enabling counterintelligence to better assess future threats to confidential information.

In contrast to defensive counterintelligence principles, offensive counterintelligence principles aim to thwart adversaries' information-gathering efforts. By launching offensive operations, the goal is to protect vital or confidential information before adversaries can exploit it. Deception plays a key role in this context by misleading adversary decision-makers regarding the operations, capabilities, and intentions of domestic intelligence. The ultimate objective of deception is to create a false perception that leads adversaries to take actions that ultimately prove futile. This confusion delays their ability to respond effectively and wastes their time and resources, allowing friendly intelligence to strengthen its position against hostile forces. A notable example is Operation Bodyguard, which successfully misled the Nazis about the D-Day invasion, contributing to the Allied Nations' victory.

The final component of offensive counterintelligence principles is neutralization. Like detection, which complements deterrence, neutralization works alongside deception. In this context, neutralization involves blocking adversary intelligence operations based on the concept of "defeat," which can manifest as collapse, failure, rout, or ruin. Neutralization means that adversary intelligence efforts can be thwarted through destruction or paralysis. By effectively implementing neutralization, adversaries may lose interest in their operations, and friendly intelligence can undermine their confidence. Destruction can include actions such as dismantling forward observation posts or arresting spy networks. Ultimately, the paralysis created by neutralization encourages adversaries to cease their operations, allowing friendly intelligence to undertake preemptive measures.

The four counterintelligence principles—deterrence, detection, deception, and neutralization—function based on three axioms: the axiom of surprise, the axiom of data collection, and the axiom of targeting. The axiom of surprise asserts that the purpose of counterintelligence is to support intelligence functions in achieving the optimum element of surprise. This element may involve attacks on physical facilities, such as public places or military sites, or bluffing by foreign leaders regarding geopolitical issues. By achieving surprise, an agency can create secure conditions and effectively manage potential threats. The axiom of data collection posits that adversaries will use various methods to gather information about an agency's operations. This implies that adversaries may employ all available data-gathering techniques—whether ethical or unethical, legal or illegal—to ensure the success of their operations. As a result, counterintelligence analysts and officers must anticipate dangerous attack vectors to formulate potential solutions for prevention. According to the axiom of targeting, adversaries focus their data collection efforts on understanding how an agency operates and the services it protects. Hostile information collection targets data that reveals the agency's structure, scope, influence, current capabilities, and future intentions. This focus is critical, as targeted areas for hostile

information collection can lead to unexpected surprises for the agency, causing significant damage and providing adversaries with a substantial advantage that jeopardizes both operations and clients.

In addition to the principles and axioms of counterintelligence, several commandments warrant attention. Specifically, ten commandments should guide counterintelligence analysts and practitioners: (1) Be offensive; (2) Honor your professionals; (3) Own the street; (4) Know your history; (5) Do not ignore analysis; (6) Do not be parochial; (7) Train your people; (8) Do not be sidelined; (9) Do not overstay; and (10) Never give up. The command "Be Offensive" emphasizes that passive counterintelligence efforts are vulnerable to failure and may squander valuable resources. Therefore, counterintelligence must operate aggressively against adversaries. The command "Honor Your Professionals" suggests that counterintelligence officers and analysts deserve recognition and rewards for their contributions, as they provide critical early warnings of potential breaches. Unfortunately, many view counterintelligence personnel as only delivering bad news. In reality, they are often blamed for failing to signal such news. Shifting this perception is essential for enabling counterintelligence analysts and officers to perform optimally and effectively prevent intelligence failures.

The command "Own the Street" emphasizes the need for counterintelligence to be supported by a robust network. This network should be established, developed, and maintained at a reasonable cost to ensure optimal surveillance capabilities. With these capabilities, counterintelligence can effectively monitor adversary activities, leading to the identification of surveillance on key meeting areas, participant recognition, and evidence collection. The command "Know Your History" underscores that counterintelligence analysts and officers must have a deep understanding of their field's history. This knowledge is critical for avoiding intelligence failures. Awareness of past failures, as well as counterintelligence history, is essential for adhering to this command. The command "Do Not Ignore Analysis" asserts that analysts must thoroughly review each case to make informed decisions. This requires dedicating adequate resources to key sources, such as reports, signals intelligence, audio and telephone tapping, maps, travel data, and surveillance. These resources enable counterintelligence personnel to uncover clues, draw connections, and target the most productive areas for their activities.

The command "Do Not Be Parochial" emphasizes that counterintelligence analysts and officers should not view themselves as superior to other agencies. Such an attitude can create vulnerabilities, allowing adversary intelligence to exploit gaps and launch operations. It also undermines cooperation and synergy between counterintelligence and other departments, fostering internal conflicts that adversaries can manipulate. Counterintelligence personnel must work collaboratively with other agencies to achieve optimal results. The command "Train Your People" highlights the need for adequate training and education for counterintelligence analysts and officers. This is essential, as counterintelligence is a specialized discipline requiring distinct skills. Comprehensive training enables personnel to sharpen their abilities to observe and analyze intelligence effectively. The command "Do Not Be Shoved Aside" stresses the importance of persistence in carrying out duties, especially in safeguarding the agency. This command is crucial because counterintelligence often faces scrutiny following

operational failures or breaches. While this responsibility can be challenging, it is essential for preventing intelligence failures, which adversaries strive to exploit.

The command "Do Not Stay Too Long" emphasizes that counterintelligence analysts and officers should be refreshed with new talent. This infusion of fresh perspectives helps create a more effective counterintelligence environment, enabling the agency to adapt to emerging challenges. New talent can also mitigate potential pitfalls, such as: (1) the school of doublethink; (2) the us-against-them mindset; (3) the nothing-is-what-it-seems syndrome; and (4) the wilderness of mirrors. The command "Never Give Up" underscores the importance of persistence in counterintelligence tasks. While developing counterintelligence strategies can be time-consuming, the rewards are substantial upon successful completion. Through perseverance, the agency can achieve optimal performance. By executing these commands effectively, counterintelligence analysts and officers can fulfill their responsibilities and safeguard their agency from adversary breaches.

Challenges and Complexities in Counterintelligence

Counterintelligence faces numerous challenges and complexities, similar to other intelligence fields. For instance, the Federal Bureau of Investigation (FBI) has historically struggled with public scrutiny when covert activities were leaked, often due to the determined efforts of reformers and revolutionaries. This situation can be viewed as retaliation since FBI agents had previously infiltrated these groups. Agencies must recognize that they can overlook critical details in their operations, which adversaries may exploit. Therefore, protecting vital information during counterintelligence operations is a top priority.

Moreover, intelligence failures can still occur despite proactive counterintelligence initiatives. A prime example is the reunification of Germany and the subsequent fall of the Soviet Union. Before reunification, the Soviet Union orchestrated an elaborate program aimed at undermining the U.S. intelligence system in West Germany through manipulation and misdirection, leading to misguided and futile operations fueled by disinformation. While these counterintelligence methods effectively safeguarded Soviet operations, they ultimately failed to prevent German reunification. Decades later, declassified documents revealed that strict counterintelligence measures were compromised by mandates from higher authorities. In summary, although the Soviet Union may have succeeded in clandestine operations, they ultimately lost the broader conflict.

The challenges and complexities of counterintelligence are significantly influenced by advancements in knowledge and technology. Learning from past mistakes, Russia—as the successor to the Soviet Union—has developed a more effective intelligence and counterintelligence apparatus. This evolution is evident in the ongoing war with Ukraine, which has inflicted severe devastation in the region. The conflict underscores the critical roles of intelligence and counterintelligence, alongside the innovations and transformations that have taken place over the past few decades. The importance of counterintelligence is particularly highlighted by recent events, such as the surge in investigations and the arrests of senior Ukrainian national security officials for treason on

behalf of Russia. Additionally, the widespread dismissal of Russian intelligence officers operating under diplomatic cover worldwide reflects Russia's extensive counterintelligence efforts.

Adversary intelligence operations are often as vigorous as those of friendly intelligence, and adversaries frequently disregard standard protocols. Unfortunately, counterintelligence is commonly regarded as the "stepson" of intelligence, despite its equally vital role in safeguarding critical information. Two main factors contribute to the slower development of counterintelligence compared to intelligence: (1) the sensitive nature of counterintelligence, which focuses on internal affairs and leads to reluctance in open discussions, and (2) a general lack of understanding regarding its contributions to national security. This situation can have serious consequences, as any surprise attacks by adversaries—stemming from misunderstandings or neglect—may lead to intelligence failures that jeopardize national security.

In light of the previous discussion, two critical concepts warrant attention: false negatives (Type I Error) and false positives (Type II Error). False positives refer to risks of omission, while false negatives concern risks of commission. The risk of omission occurs when counterintelligence fails to prevent an undesired event due to an analyst or officer not following up on a clue or signal. Conversely, the risk of commission arises when counterintelligence intentionally dismisses warnings from other departments. Together, Type I and II Errors can have fatal consequences for domestic intelligence operations, which helps explain the continued prevalence of espionage in certain regions, particularly Europe. Agents recruited as part of counterintelligence initiatives may betray their own states or friendly intelligence organizations. These agents often align with motives related to MICE (Money, Ideology, Coercion, and Ego), complicating counterintelligence efforts further.

In authoritarian regimes, the situation becomes even more complicated due to rigid governance structures. Such rigidity can lead to overconfidence in intelligence activities, resulting in several vulnerabilities: (1) counterintelligence assessments may be manipulated in favor of the regime due to loyalty or fear; (2) traditional threats might be overestimated while emerging threats are underestimated; (3) regime leaders often act as apologists, reinforcing biases and state propaganda; (4) there is a focus on internal coups over popular revolts, leading to the formation of multiple internal security services to prevent any single agency from gaining too much power; (5) regimes echo the paranoia of their leaders, filled with suspicions of disloyalty and fears of violent uprisings; (6) dependence on external intelligence services may lead to ineffective monitoring and harassment of domestic anti-regime activists; and (7) power is highly concentrated within these regimes. Authoritarian regimes often reject intelligence reports that do not align with their ideals. These vulnerabilities hinder counterintelligence functions, allowing adversaries to manipulate and penetrate regime intelligence, ultimately leading to the regime's downfall.

Counterintelligence faces several challenges, including covert operations, moles, defectors, and deceptions. These factors share a common goal: to undermine domestic intelligence's ability to detect adversary activities. This highlights that adversary

intelligence operations can be as formidable as counterintelligence efforts. A notable example is the effective use of the "sunlight method" in countering Russian interference in the 2020 U.S. election. Exposing such covert operations presents challenges, as the U.S. intelligence community feared that Russian actions could alter election outcomes and undermine democracy. However, U.S. intelligence ultimately managed to mitigate these risks for two main reasons: (1) the identity of the source impacts how information is perceived, and (2) exposure can negatively influence public opinion towards the intended beneficiaries of the leaks. Additionally, it is crucial to recognize that adversarial intelligence efforts are often as vigorous as those of domestic intelligence. This means that while counterintelligence seeks to protect vital information, adversaries will not follow standard protocols.

In authoritarian regimes, the situation grows more complex due to rigid governance structures, which may lead to overconfidence in intelligence activities. This creates vulnerabilities, including: (1) the potential manipulation of counterintelligence assessments to favor regime narratives; (2) overestimating traditional threats while overlooking emerging ones; (3) leaders acting as apologists for state propaganda; (4) an emphasis on internal threats over popular dissent, resulting in the formation of multiple internal security services; (5) a culture of paranoia surrounding disloyalty; and (6) reliance on weaker external intelligence services, which may hinder effective monitoring of anti-regime activists. Authoritarian regimes tend to reject intelligence reports that do not align with their ideals, hampering counterintelligence functions. This allows adversaries to manipulate and penetrate regime intelligence, ultimately leading to the regime's downfall.

In the contemporary era of technological advancement, disinformation remains a potent tool for deceiving target audiences. Disinformation is typically defined as a specific type of engineered information designed with the intent to mislead recipients. The primary goal of deploying disinformation is to imbue recipients with seemingly valid knowledge, whether useless or detrimental, which can subsequently prompt them to make erroneous decisions, thus benefiting the adversary. Disinformation becomes even more effective when aligned with the vulnerabilities of the targeted intelligence entity. This was notably evident in the USSR's intelligence activities against the United States during the Cold War. The USSR effectively exploited U.S. vulnerabilities by dispatching agents to identify and capitalize on these weaknesses, a strategy tracing back to the KGB operations during the Rome Olympic Games. This case exemplifies how active counterintelligence measures often capitalize on the shortcomings of domestic intelligence agencies.

The challenges and complexities within counterintelligence can be inwardly destructive. The search for moles or defectors may lead to doubts about the loyalty of subordinates, creating vulnerabilities that adversaries can exploit to destabilize operations. Such uncertainties give rise to five significant security threats: (1) penetration by adversaries; (2) technical collection of electronic, telephonic, or face-to-face communications; (3) direct observation of the suspected agent; (4) passive observation of the agent's activities in hostile territories, whether controlled by adversaries or their allies; and (5) exposure of the agent's actions. Investigating loyalty can be detrimental, especially if it ultimately confirms that the agency's loyalty is intact. This leads to the possibility that

the loyalty question was disinformation from adversaries. It is vital to avoid such internal conflicts to ensure counterintelligence can effectively counter threats.

Another significant challenge is the legal system. The secrecy and deception inherent in counterintelligence often clash with laws and regulations governing intelligence operations. This tension may force counterintelligence to take unlawful measures to neutralize threats. While counterintelligence and the legal system share a common goal of maintaining national security, their approaches can conflict. These challenges can hinder counterintelligence performance and raise questions about the effectiveness of its strategies. Therefore, establishing strong networks with other security-related departments is crucial. Through these collaborative efforts, counterintelligence can address the challenges and complexities it faces more effectively.

Proposed Legal Reforms and Policy Recommendations

To address the identified legal and ethical challenges, and to strengthen Indonesia's counterintelligence capabilities within a robust rule of law framework, several legal reforms and policy recommendations are proposed:

Amending the State Intelligence Law: The State Intelligence Law (Law No. 17/2011) should be amended to include clearer definitions of counterintelligence functions and specific legal thresholds for intrusive operations. This includes:

- Judicial Authorization for Surveillance: Mandating prior judicial authorization (e.g., from a specialized intelligence court or a high court judge) for all intrusive surveillance measures, including wiretapping, electronic data interception, and bulk data collection. This would align Indonesia with international best practices and strengthen privacy protections.[13]
- Clearer Mandates and Limitations: Precisely defining the scope of intelligence operations to prevent overreach and ensure that activities are strictly necessary and proportionate to the threat.
- Data Protection Provisions: Incorporating explicit provisions: for the collection, storage, use, and sharing of personal data by intelligence agencies, in line with comprehensive data protection principles, as advocated by international human rights bodies.[14]

Strengthening Oversight and Accountability Mechanisms:

- **Independent Oversight Body:** Establishing an independent oversight body with powers to review intelligence activities, investigate complaints, and ensure compliance with legal and human rights standards. This body should have adequate resources, access to classified information, and the authority to make binding recommendations, as suggested by Born, Leigh, and Wills.[15]

[13] Zedner, "Security, the State and the Citizen," 308.

[14] United Nations, *General Assembly Resolution 68/167: The Right to Privacy in the Digital Age,* A/RES/68/167 (December 18, 2013).

[15] Born, Leigh, and Wills, *Making Intelligence Accountable*, 60-65.

- **Enhanced Parliamentary Oversight:** Strengthening the capacity of parliamentary committees responsible for intelligence oversight through specialized training, access to expert advice, and regular, substantive reporting from intelligence agencies (while respecting necessary classification).
- **Public Reporting:** Mandating periodic, declassified public reports on intelligence activities, including statistics on surveillance authorizations and human rights compliance, to enhance transparency and public trust.[16]

Human Rights Training and Compliance:

- **Mandatory Human Rights Training:** Implementing mandatory and regular human rights training for all intelligence personnel, focusing on international human rights law, ethical conduct, and the principles of necessity and proportionality.
- **Internal Compliance Mechanisms:** Establishing robust internal compliance and ethics units within intelligence agencies to monitor adherence to legal and ethical standards and to investigate alleged misconduct.

Legal Framework for Cyber Counterintelligence:

- Developing a dedicated legal framework for cyber counterintelligence that addresses the unique challenges of the digital domain, including cross-border data flows, attribution of cyber-attacks, and the legal use of offensive cyber capabilities, all while ensuring compliance with international law.[17]

These reforms are crucial not only for upholding democratic values but also for enhancing the legitimacy and effectiveness of Indonesia's counterintelligence apparatus. A counterintelligence system that operates within a clear, accountable, and rights-respecting legal framework is more likely to gain public trust and international cooperation, both of which are vital for national security in the contemporary era.

Future Directions for Counterintelligence

Counterintelligence today must evolve beyond traditional paradigms, particularly in light of the challenges posed by cyber operations, disinformation warfare, and insider threats. As outlined in this study, four key initiatives are proposed to enhance counterintelligence effectiveness: capacity building, outreach programs, psychological support, and technological integration. However, these initiatives must be critically assessed within the context of Indonesia's unique institutional landscape, resource constraints, and socio-political environment, to ensure their feasibility and sustainable implementation.

A key strategy for addressing these challenges is to adopt innovative methods for modern counterintelligence. One proposed approach involves expanding the scope of personnel background checks and profiling by incorporating various aspects of agents'

[16] Haggerty and Ericson, "The Surveillant Assemblage," 615.
[17] Putter, "Navigating the Interplay of Cognitive Warfare and Counterintelligence," 185-187.

lives, including understanding about key variables in the counterintelligence model. The institution-level theoretical approach to counterintelligence, as illustrated in the chart and derived from Miron Varouhakis's framework, conceptualizes counterintelligence (CI) not merely as a reactive security function but as a systemic and strategic institutional process. These include six key domains: family, workplace, friends, finance, habits, and travel. From a counterintelligence perspective, these variables represent potential entry points for adversarial influence, manipulation, surveillance, or exploitation. Each arrow pointing toward the "Individual" underscores how these seemingly personal or civilian aspects of life can become vectors of vulnerability. For instance, an individual's financial stress could be leveraged for coercion, while travel patterns might reveal predictability or access points for physical surveillance. Likewise, relationships with friends or colleagues might offer adversaries indirect access through social engineering or infiltration. In institutional counterintelligence, understanding these personal dimensions allows for more accurate threat assessments, insider risk evaluations, and tailored protective measures. By embedding such variables into a structured model, institutions can develop behavioral baselines, anomaly detection protocols, and proactive interventions that align with the broader CI principles—deterrence, detection, deception, and neutralization.

In addition to earlier developments, an institutional-level analysis of workplace variables in the counterintelligence model is also crucial. This model explains a hierarchical framework for understanding how institutional factors within the workplace can escalate or mitigate espionage risk among employees. At the top of the model lies the workplace or agency itself, emphasizing the macro-environment in which all organizational dynamics are situated. From this foundation, the model flows downward through increasingly specific and influential layers: management philosophy, organizational culture, quality of work life, and finally the individual level, where worker performance, satisfaction, and espionage risk are directly impacted. Each layer represents a structural determinant that shapes the attitudes, behaviors, and motivations of individuals within the institution. Such analysis model is necessary because factors in the workplace, particularly employee dissatisfaction, can motivate agents to commit espionage against their own agency. This form of espionage can be highly detrimental, as involved agents often possess critical information. In today's era, particularly with the rise of disinformation, counterintelligence capabilities must be enhanced. One effective approach is to establish a counterintelligence outreach program, which involves building and utilizing functional relationships to support operational objectives. Key building blocks for this initiative include: (1) outreach encompasses a complex bundle of resources and capabilities; (2) information and knowledge are critical organizational assets; (3) developing and managing relationships should be prioritized; and (4) cultivating a competent counterintelligence workforce is essential.

These elements establish the foundation for creating an effective counterintelligence outreach program in the form of hierarchical relationships in the counterintelligence outreach program. This analysis framework is presented as a pyramid, with "Outreach" at the base and "Agency" at the apex, signifying a layered approach to relationship-building and operational alignment. At the foundational level, outreach efforts represent the initial contact point, typically involving engagement with external

stakeholders, awareness campaigns, or community-based interactions aimed at cultivating trust and promoting counterintelligence awareness. These outreach activities are designed not only to disseminate information but also to generate reciprocal channels for intelligence sharing, risk identification, and proactive collaboration. As outreach initiatives evolve, they give rise to relationships—the intermediate layer in the hierarchy—which signify the transition from transactional engagement to sustained, trust-based partnerships. These relationships are vital for ensuring consistency, credibility, and continuity in counterintelligence objectives. Above this layer are the partners, encompassing both governmental and non-governmental entities that share aligned security interests and contribute to the execution and reinforcement of CI mandates. At the top of the pyramid resides the agency, which serves as the central coordinating body that governs strategic intent, allocates resources, sets policy frameworks, and ensures that the outreach-to-agency continuum functions cohesively. The model reinforces the notion that effective counterintelligence is not a unilateral effort, but a multi-tiered collaboration, where success depends on the integrity and synchronization of relationships across all organizational levels.

In developing counterintelligence capabilities, several key principles must be prioritized: (1) effective communication; (2) establishing a robust multilateral information exchange network; (3) conducting outreach within transparent legal, political, and social norms; (4) leveraging the headquarters' central position; (5) collaborating with commercial sector partners; (6) implementing effective interventions; (7) measuring the effectiveness of outreach activities; and (8) managing risks associated with counterintelligence outreach. Adherence to these principles is vital for preventing intelligence failures. They should be continuously reinforced among counterintelligence personnel, as this domain increasingly intertwines with political and organizational issues. Strategies must be developed to ensure optimal operations, focusing on: (1) addressing essential organizational questions; (2) valuing simplicity in strategy; (3) aligning with national security goals and command intent; (4) recognizing constraints at leadership and operational levels; and (5) utilizing straightforward frameworks for strategy formulation.

Additionally, enhancing counterintelligence capacities is crucial for future effectiveness, particularly the ability to detect and neutralize Type I (false positive) and Type II (false negative) errors. This is essential, especially since counterintelligence is often viewed as the "stepson" of the intelligence community—crucial for identifying adversary activities yet lacking strong ties with other departments, particularly legal ones. To address these issues, collaboration across departments is necessary, as they share a common goal: to thwart adversary intelligence operations. This can be achieved by identifying spies within adversary ranks and gathering intelligence from them. Moreover, learning from past mistakes and fostering cooperation with foreign services can significantly enhance counterintelligence capabilities, especially when domestic and foreign entities confront the same adversaries.

Furthermore, counterintelligence today must evolve beyond traditional paradigms, particularly in light of the challenges posed by cyber operations, disinformation warfare, and insider threats. As outlined in this study, four key initiatives are proposed to enhance counterintelligence effectiveness: capacity building, outreach

programs, psychological support, and technological integration. However, these initiatives must be critically assessed within the context of Indonesia's unique institutional landscape, resource constraints, and socio-political environment, to ensure their feasibility and sustainable implementation. A phased institutional reform could begin by establishing an inter-agency Counterintelligence Coordination Task Force under the National Security Council (Wantannas). This entity would promote joint training, standard operating procedures (SOPs), and inter-operability protocols, without immediately disrupting existing agency hierarchies. Embedding capacity-building goals into national policy documents such as the RPJMN follow-up or Defense White Paper revisions can also help legitimize institutional change.

In addition, outreach programs are crucial for fostering strategic relationships across security, defense, civilian, and private sectors—particularly in a digital environment where information security is decentralized. However, public mistrust toward intelligence agencies, limited civil society involvement, and the absence of legal safeguards for engagement protocols may hinder the successful deployment of outreach activities. Moreover, pilot outreach programs can be done in sectors with clear national interest alignment, such as cyber defense cooperation with technology firms, academic partnerships for intelligence education, or information-sharing protocols with critical infrastructure operators. Establishing Memorandum of Understanding (MoUs) across ministries and private entities with oversight from Komnas HAM or civil liberty watchdogs can help balance effectiveness with transparency and accountability.

Establishing a robust counterintelligence structure, is indeed, essential for mitigating threats from moles, defectors, and disinformation, which can undermine national security. For example, Iran's Ministry of Intelligence and Security (MOIS) employs a unique candidate screening process. Applicants are selected based on specific academic backgrounds and undergo investigations lasting from nine to twenty-four months. After passing two tests, they receive specialized training at designated universities before being assigned to provincial intelligence services. A similar structure exists within the Irish Republican Army (IRA), where operatives are prohibited from disclosing their affiliation with the organization. This secrecy enhances their counterintelligence methods involving informants, agents, surveillance, and interrogation, making the IRA a formidable adversary to the British government. With such a strong framework, the IRA effectively adapts to the challenges posed by British intelligence operations.

The counterintelligence department's structure and strategic partnerships with other agencies should focus on one goal: thwarting adversarial operations. Developing these partnerships requires mutual understanding to prevent overlap and miscommunication regarding responsibilities. Key considerations include: (1) historical context; (2) internal political dynamics; (3) social characteristics; (4) international practices in information security; (5) current capabilities; and (6) future needs. Furthermore, counterintelligence measures must be improved to create an effective structure. This includes: (1) establishing operational standards; (2) defining leadership responsibilities; (3) enhancing staff training; and (4) promoting transparency. By focusing on these elements, the counterintelligence department can better manage threats. In an era of rapid technological advancement, addressing these challenges is vital, as threats can emerge

from conventional and non-conventional sources, including cyberspace, leading to espionage, subversion, assassination, terrorism, and hybrid operations.

A crucial aspect of counterintelligence development is psychological support. Often overlooked, this support is essential for effective background checks and profiling. It enhances operational psychology through systematic inquiry and relevant research. Psychological support is vital in the operational functions of intelligence and counterintelligence, encompassing risk assessment, recruitment, management, and elicitation. It significantly contributes to counterespionage and counterterrorism efforts. By utilizing effective psychological strategies, counterintelligence can optimize its performance in preventing threats, thereby reducing the risk of large-scale attacks, such as those in Mumbai in 1993 and 2008. Both attacks share three key similarities: (1) they were planned outside India's borders with local support; (2) they aimed to undermine India's economic stability; and (3) both were executed via seaborne operations. Had counterintelligence been given more time for investigation, psychological profiling could have identified the attackers and their local collaborators, potentially preventing the later attack.

While this study adopts the widely accepted framework of deterrence, detection, deception, and neutralization as core principles of counterintelligence, it is important to acknowledge that the field is not without scholarly contention and theoretical debate. A more nuanced analysis reveals divergent perspectives on the relevance, sequencing, and ethical implications of these principles, particularly as they are applied across varying political systems and strategic environments. For instance, proponents of offensive counterintelligence argue for the centrality of deception and neutralization in neutralizing adversary threats before they fully materialize. Yet, this view has been challenged by critics who caution against overdependence on deception, especially in democratic societies. In such contexts, covert operations aimed at misleading external or internal actors may conflict with democratic norms of transparency and civil accountability. This concern is particularly relevant for Indonesia, where public trust in state institutions—including intelligence bodies—has historically been fragile due to perceived politicization and lack of oversight. Hence, blindly importing deception-heavy models from more authoritarian intelligence systems may produce unintended consequences and erode domestic legitimacy.

Additionally, scholars like Hulnick (2006) question the utility of the traditional intelligence cycle that underpins many counterintelligence doctrines. He argues that the linear model which is collection, analysis, dissemination, and feedback oversimplifies the chaotic nature of intelligence work, which is often iterative, adaptive, and influenced by political pressures. Applying this to counterintelligence, it becomes evident that a rigid adherence to doctrine may fail in fluid threat environments, such as cyberspace or social media manipulation, where threats evolve faster than bureaucratic processes.

Nevertheless, advancements in technology, particularly in biotechnology and communication, must be prioritized in counterintelligence development. Focusing on biotechnology is essential due to its implications for economic competitiveness, food security, and public health. The risk of developing biochemical weapons presents a

significant threat to safety. Conversely, communication technology enables disinformation campaigns that can mislead both domestic intelligence and adversaries, especially through media channels. This misrepresentation of intelligence activities, often dramatized in popular culture, distorts perceptions and misleads adversaries in their counterintelligence efforts against domestic agencies, ultimately jeopardizing vital information and national security. Therefore, effective counterintelligence requires collaboration among stakeholders and relevant agencies to achieve optimal results in safeguarding national security.

IV. CONCLUSION

This study has underscored the indispensable role of counterintelligence in safeguarding Indonesia's national security against a complex array of contemporary threats. However, it has critically demonstrated that the effectiveness and legitimacy of counterintelligence operations are inextricably linked to a robust and human rights-compliant legal framework. Our analysis of Indonesia's existing legal landscape, particularly the State Intelligence Law (Law No. 17/2011), reveals significant ambiguities and gaps concerning privacy protection, accountability, and independent oversight, which pose considerable legal and ethical challenges.

The tension between national security imperatives and fundamental human rights is a universal challenge for intelligence agencies worldwide. For Indonesia, navigating this tension requires a deliberate and comprehensive approach to legal reform. As argued by Lowenthal, 'effective intelligence oversight is not a hindrance to national security, but rather a prerequisite for its long-term legitimacy and public support.'[18] Without clear legal mandates, strong independent oversight, and transparent accountability mechanisms, counterintelligence operations risk operating in a 'legal grey zone,' potentially eroding public trust and undermining democratic principles.

Therefore, the proposed legal reforms—including mandating judicial authorization for intrusive surveillance, establishing a truly independent oversight body, and strengthening data protection provisions—are not merely procedural adjustments. They represent a fundamental shift towards a counterintelligence system that is both effective in countering threats and fully compliant with the rule of law and human rights standards. By embracing these reforms, Indonesia can build a resilient and legitimate counterintelligence apparatus that serves to protect the nation's security while upholding the democratic values upon which it is founded. This commitment to legal clarity and accountability will ultimately enhance Indonesia's standing as a responsible actor in the global security landscape.

This study has examined the evolving role of counterintelligence in national security strategy, with a specific focus on Indonesia’s vulnerabilities and institutional context. Through a conceptual analytical approach, it has highlighted four core counterintelligence principles which is deterrence, detection, deception, and

[18] Mark M. Lowenthal, *Intelligence: From Secrets to Policy,* 9th ed. (Thousand Oaks, CA: CQ Press, 2022), 250.

neutralization as essential tools for mitigating modern threats such as espionage, disinformation, and cyber intrusion. Drawing from global case studies and rooted in Indonesia's geopolitical, technological, and institutional landscape, the study underscores that counterintelligence is not merely a support function but a strategic necessity in safeguarding state sovereignty and stability. This study has also examined the evolving landscape of counterintelligence, highlighting its principles and addressing the complex challenges it faces today. The research questions regarding the effectiveness of counterintelligence strategies in countering espionage and the role of psychological support in enhancing operational capacity have been thoroughly analyzed. Findings indicate that proactive strategies, such as robust personnel training and the establishment of strong networks, significantly enhance the ability to thwart espionage efforts. Furthermore, psychological support is crucial in fostering resilience among counterintelligence personnel, enabling them to perform effectively and maintain operational vigilance.

These insights resonate with broader theories in intelligence studies, particularly the perspectives of Richard Betts (1978), who posits that intelligence failures often stem from a lack of adaptability and a failure to learn from historical mistakes. Betts emphasizes integrating lessons from past experiences into current practices. Similarly, Mark Lowenthal (2022) highlights the imperative for counterintelligence to adapt to the challenges posed by technological advancements, recognizing that adversaries exploit new technologies to undermine intelligence agencies.

The interplay between intelligence and counterintelligence remains vital in a landscape characterized by rapid change and disinformation. Strengthening inter-agency collaboration is crucial for effective counterintelligence, reflecting both Betts' and Lowenthal's assertions that coherence and adaptability are essential for addressing complex security challenges. Moreover, to translate these findings into actionable policy, several priority steps are recommended for the Indonesian government and its national security stakeholders. First, Establish a dedicated counterintelligence agency or create a permanent inter-agency counterintelligence coordination task force to bridge existing gaps among BIN, BSSN, BAIS, and Polri. This would ensure coherent strategy, reduce fragmentation, and improve detection of internal threats. Second, Embed counterintelligence objectives into national security documents such as future iterations of the RPJMN and the Defense White Paper. These policies should include measurable targets for counterintelligence capability development, such as personnel training, inter-agency protocols, and psychological screening mechanisms. Third, Public-Private and Regional Collaboration: Initiate pilot outreach programs that engage academic, private, and regional stakeholders, particularly in the cybersecurity domain. These programs should focus on building trust, securing digital infrastructure, and enhancing inter-operability between sectors. In addition, as a conceptual study, this research is inherently limited by the absence of primary field data and empirical validation specific to Indonesia's classified counterintelligence environment. Many of the operational cases, while illustrative, are based on secondary sources due to the restricted nature of intelligence disclosure. Ultimately, as adversaries become more sophisticated, counterintelligence must anticipate challenges by leveraging new technologies and

methodologies. By embracing these principles and fostering collaborative networks, counterintelligence agencies can significantly enhance their effectiveness in safeguarding national security. This research contributes to the ongoing discourse in intelligence studies by offering actionable recommendations for advancing counterintelligence practices.

REFERANCE

Born, Hans, Ian Leigh, and Aidan Wills (2015), Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies. Oslo: Geneva Centre for the Democratic Control of Armed Forces (DCAF) and Norwegian Parliamentary Intelligence Oversight Committee.

Haggerty, Kevin D, and Richard V. Ericson (2000). "The Surveillant Assemblage." British Journal of Sociology 51, no. 4 (December 2000): 605–22.

Lowenthal, Mark M. (2022). Intelligence: From Secrets to Policy. 9th ed. Thousand Oaks, CA: CQ Press.

Lyon, David. (2003). Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination. London: Routledge.

Prunckun, Henry (2019). Counterintelligence Theory and Practice. 2nd ed. Lanham, MD: Rowman & Littlefield.

Putter, Dries (2024). "Navigating the Interplay of Cognitive Warfare and Counterintelligence in African Security Strategies: Insights and Case Studies." Journal of Policing, Intelligence and Counter Terrorism 20, no. 2: 173–92.

Sulastri, Lusia (2022). "Analisis Kewenangan Penyidikan Dalam Pelanggaran Wilayah Udara Indonesia (Tinjauan Peran Penyidik PNS dari Kementerian Perhubungan dan TNI AU)." KRTHA BHAYANGKARA 16, no. 2 (Desember 2022): 273-285.

United Nations (2013). General Assembly Resolution 68/167: The Right to Privacy in the Digital Age. A/RES/68/167. December 18, 2013.

———. International Covenant on Civil and Political Rights. G.A. Res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966). Entered into force March 23, 1976.

Walzer, Michael. (2015). Just and Unjust Wars: A Moral Argument with Historical Illustrations. 5th ed. New York: Basic Books.

Zedner, Lucia. (2009) "Security, the State and the Citizen: The Changing Face of Security." Theoretical Criminology 13, no. 3 (August 2009): 299–318.