Journal of Management and Administration Provision
Vol. 6, Issue 1, 2026
Page 068-079
DOI: https://doi.org/10.55885/jmap.v6i1.756

Critical Analysis of the Classical Intelligence Cycle Model in Facing Collaborative Challenges in Indonesia

Oktora Aditia[1], Amy Y. S. Rahayu[1], Roy Valiant Salomo[1]
[1]Administrative Science Program, Faculty of Administrative Sciences, Universitas Indonesia, Indonesia
Email: oktoraaditia@gmail.com

Abstract. *This study presents a critical analysis of the classical intelligence cycle model in addressing collaborative challenges among intelligence agencies in Indonesia. The analysis highlights the limitations of its linear, closed, and hierarchical structure within the context of increasingly complex and multidimensional threat landscapes. Using a qualitative descriptive approach, the study examines barriers to effective collaboration, such as overlapping mandates, lack of integrated information systems, and bureaucratic cultures resistant to openness. Based on interviews, document analysis, and literature review, the study proposes an adaptive and collaborative intelligence framework incorporating elements of intelligence fusion and real-time intelligence cycles. These models emphasize horizontal coordination, digital technology integration, and cross-sectoral partnerships. The research offers strategic recommendations for policy reform, including establishing a national integrated intelligence center, enhancing interagency data interoperability, and promoting collaborative organizational cultures. This study contributes to academic discourse and policy development by advocating for a modern, responsive, and synergistic national intelligence system tailored to Indonesia's unique institutional and socio-political context.*

Keywords: *Classical Intelligence, Intelligence Cycle, Collaborative Intelligence*

JEL Classification: *H56, H83, D83, O38, H11*

Received: September 1, 2025 Received in Revised: October 16, 2025 Accepted: January 30, 2026

INTRODUCTION

Intelligence plays a crucial role in supporting state policymaking, particularly concerning national security (Best, 2015; Gumenyuk et al., 2025). In complex environments like Indonesia, the need for an efficient and flexible intelligence system is increasingly urgent. However, the effectiveness of traditional intelligence approaches is being questioned in the face of rapidly evolving modern threats. The classical intelligence cycle model comprising planning, collection, processing, analysis, and dissemination has long been the primary operational framework for global intelligence agencies (Gill & Phythian, 2013; Mitchell, 2005).

Yet, scholars such as Hulnick (2006) argue that this model is overly linear, rigid, and fails to reflect actual operational dynamics. In practice, many functions within this cycle occur concurrently, overlap, and do not follow a systematic sequence. A key critique is its misalignment with rapidly changing, complex threats (Heracleous & Werres, 2016; Voelpel et al. 2006; Benbya & McKelvey, 2006). Challenges such as global terrorism, cyber warfare, pandemics, and social

E-ISSN: 2776-1290, P-ISSN: 2776-1282

media disinformation demand adaptive and collaborative intelligence responses. Hierarchical, compartmentalized intelligence models are inadequate for addressing these threats effectively.

In Indonesia, the intelligence system encompasses multiple organizations, including the State Intelligence Agency (BIN), the Indonesian Armed Forces Intelligence Agency (BAIS TNI), and the National Police Intelligence and Security Agency (Baintelkam Polri). However, fragmentation among these agencies creates significant challenges for collaboration and information integration. Akbar et al. (2025) Critical policies and decisions are often delayed due to insufficient synergy, exacerbated by sectoral egos, mutual distrust, and limited system interoperability.

Historical intelligence failures such as the 9/11 attacks in the United States or the 2002 Bali bombings underscore the urgency of developing open, collaborative intelligence approaches. Alternative models, such as Gill & Phythian's (2013) Intelligence Web Model, offer interactive, multidirectional networks connecting intelligence actors and stakeholders. Collaboration in intelligence extends beyond interagency information sharing to include private sector, academic, and civil society engagement, aligning with the global trend where security is a shared responsibility (Petersen & Tjalve, 2018; Vogel & Tyler, 2019; Santoso, 2024; Nte & Nte, 2025). Effective collaboration enhances early detection and response to national and international threats.

Nevertheless, implementing collaborative models faces structural, cultural, and legal obstacles (Farahani, 2024; Weare et al., 2014). For instance, the perception that information sharing equates to leaking state secrets persists strongly within intelligence organizations. Consequently, despite coordination forums like the Central Intelligence Committee (Kominpus) and Regional Intelligence Committees (Kominda), outcomes remain suboptimal due to partial information sharing. The classical cycle also fails to bridge the gap between intelligence collectors and policymakers.

Studies by Gentry (2019) and De (2021) indicate policymakers often seek analyses supporting predetermined policies over neutral intelligence, potentially politicizing intelligence outputs and undermining objectivity. Additionally, the model lacks agility; asymmetric threats like cyberattacks and disinformation require responsive, decentralized processes. Here, artificial intelligence-based digital systems and technology become vital for rapid detection and analysis (Djenna et al., 2023; Kumar et al., 2010; Adly et al., 2020; Sharma et al., 2022; Majeed & Hwang, 2021; Javaid et al., 2022) .

Resource disparities in human capital and technology among Indonesian intelligence agencies further impede information collection and verification (Wijaya et al., 2024; Ramadhianto et al., 2025; Awaludin et al., 2024). Collaboration is essential to complement resources, expertise, and access. Chen et al.'s (2008) Emergency Response Management (ERM) framework offers insights into crisis coordination through "many-second" (strategic) and "mini-second" (operational) cycles. This approach could inspire flexible, responsive intelligence coordination in Indonesia.

Principles from the U.S. National Strategy for Information Sharing (NSIS) and National Strategy for Information Sharing and Safeguarding (NSISS) provide valuable references, emphasizing information as a national asset underpinned by security and trust. Indonesia has initiated steps toward collaborative intelligence, such as establishing the Strategic Analysis Council (DAS) under BIN. However, this initiative lacks full integration into the national coordination system and has yet to achieve substantive collaboration.

Given escalating threat complexity, Indonesia must urgently reevaluate its dominant classical intelligence model (Bahriansyah et al., 2024; Sukma, 2024). Revisions or abandonment are necessary to adopt responsive, adaptive, and collaborative systems. Without this paradigm shift, Indonesian intelligence risks obsolescence in addressing evolving threats. Thus, critical

E-ISSN: 2776-1290, P-ISSN: 2776-1282

analysis of the classical model in Indonesia's collaborative context is imperative. Evaluating existing practices and developing context-appropriate alternatives must be prioritized in future intelligence reforms.

METHODS

This study employs a qualitative approach with an exploratory case study method to examine the limitations of the classical intelligence cycle model in addressing collaborative challenges in Indonesia. This approach was selected for its capacity to reveal social realities and complex intelligence coordination dynamics shaped by actors' perceptions and interactions. The constructivist paradigm underpins the research, positing that knowledge and meaning are socially constructed through intelligence actors' subjective experiences and interpretations. The research focuses on Indonesia's national intelligence coordination system, particularly the Central Intelligence Committee (Kominpus) and Regional Intelligence Committees (Kominda) from 2019–2024. Subjects include state intelligence agencies (BIN, BAIS TNI, Baintelkam Polri) and intelligence units of other ministries/agencies. Data was collected through in-depth interviews with key informants possessing strategic experience in intelligence coordination, document analysis of regulations, performance reports, policies, and literature on collaborative intelligence models. Informants were purposively selected based on expertise, experience, and strategic roles in intelligence decision-making and implementation. Thematic analysis identified patterns, themes, and relationships across data sources, reinforced by Chen et al.'s (2008) Emergency Response Management (ERM) framework and U.S. NSIS/NSISS principles. To enhance validity, triangulation was applied across data sources, collection methods, and interpretations. Interview results, policy documents, and literature were cross-compared for consistency. Finally, a collaborative intelligence model was reconstructed by adapting elements from the Intelligence Web Model, offering alternatives suited to Indonesia's threat landscape.

RESULTS AND DISCUSSION

The study reveals that the classical intelligence cycle model, used as Indonesia's operational reference, suffers from fundamental weaknesses in addressing interagency collaboration needs. Its linear, hierarchical operation fails to reflect the complexity and dynamism of coordination and decision-making amid evolving threats. Sequential stages (planning, collection, analysis, dissemination) lack the agility to respond to emergencies and uncertainties. Analysis of Indonesia's intelligence coordination practices (2019–2024) shows suboptimal performance in Kominpus and Kominda forums. Evaluations by BIN (as national coordinator) indicate stagnation and fluctuating performance due to low member attendance, inadequate follow-up on recommendations, and persistent sectoral egos. This reflects trust deficits and information compartmentalization. Data show that the State Intelligence Coordination indicator consistently scores lowest in the Intelligence Reform Index annually.

Despite policies like Law No. 17/2011 and Presidential Regulation No. 67/2013, coordination has not evolved into collaboration. Indonesian intelligence remains operationally siloed, lacking risk-sharing, joint decision-making, or comprehensive cross-agency information integration. The study further highlights Indonesia's limited adoption of collaborative principles (e.g., information as a national asset, shared risk management, data interoperability, non-state actor inclusion) from U.S. NSIS/NSISS frameworks. Although BIN established a Strategic Analysis Council (DAS) involving external experts, interactions remain limited and unsystematic. Coordination approaches also misalign with ERM's distinction between strategic ("many-second") and operational ("mini-second") coordination. Current practices inadequately delineate roles between central and regional actors during crises requiring rapid, integrated, real-time responses (Ansell et al., 2010; Bethune et al., 2022; Salvador-Carulla et al., 2020). The existence of 11 specialized intelligence agencies with disparate systems lacks collaborative structural support.

E-ISSN: 2776-1290, P-ISSN: 2776-1282

Uneven technological capabilities, budgets, and human resource competencies create intelligence product quality gaps, reducing decision-making effectiveness. Conservative bureaucratic cultures resistant to information openness reinforce "silo mentalities," hindering horizontal/vertical data sharing a core requirement for collaborative intelligence. The cultural perception that sharing equates to breaching state secrets remains a significant barrier. Kominda forum assessments reveal incremental but suboptimal synergy improvements. The absence of Kominpus-level evaluations indicates weak central monitoring mechanisms, reflecting deficient collaboration performance assessment systems. The study concludes that the classical model is inadequate for modern collaborative challenges and advocates for an adaptive, responsive, participatory model emphasizing cross-sector collaboration and dynamic information integration (Arslan et al., 2021; Bryson et al., 2015; Van et al., 2018; Wu et al., 2025).

The Classical Intelligence Model

In the 1970s, NATO disseminated an intelligence doctrine simplifying a four-step cycle model, highlighting the UK's consistency in using the DCPD formula for operational and tactical intelligence (Davies et al., 2013).

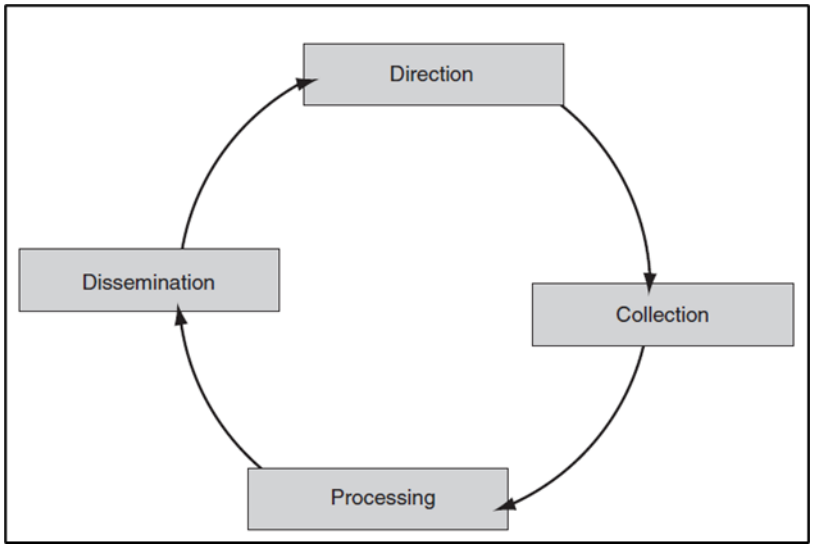

Figure 1. NATO's Classical DCPD Intelligence Cycle
Source: Canadian B-GJ-005-200/FP-000, 2003 (in Davies et al., 2013)

Practitioners used this four-stage model for decades in warfare contexts, rarely questioning its validity. However, environmental shifts information technology revolutions, changing national interests, threat complexity, and uncertainty have exposed its limitations (Syuntyurenko, 2022; Vecchiato, 2012; Dovers & Handmer, 1992). Warner (2013) argues it has passed its utility in enhancing effectiveness, while Richards (2013) and Hulnick (2006) note its failure to depict real-world processes. Digital revolutions have transformed intelligence collection, storage, and dissemination, prioritizing speed over linear sequences (Warner, 2013). Nanosecond-scale cyberattacks, for example, preclude sequential execution (Haeley, 2012). The intelligence cycle is now understood as a living organism producing outputs while reacting to stimuli and evolving within resource constraints. Conceptualists and proceduralists further debate its structure, offering critiques and refinements. Davies et al. (2013) analogize intelligence stages to research processes: conceptually, researchers self-assign tasks via plans, collect/process data, analyze to understand subjects, and disseminate findings. Procedurally, tasks may be delegated or consulted upon without altering the core conceptual logic.

Several critiques and proposed revisions of the intelligence cycle model have emerged. Warner (2013) contends that the model lacks clear delineation regarding the initiation and termination points of intelligence operations. Similarly, Davies et al. (2013) note the ambiguous

E-ISSN: 2776-1290, P-ISSN: 2776-1282

boundaries between its sequential stages. Richards (2013) further argues that its inherent linearity and rigidity reflect outdated Fordist and Taylorian principles, rendering it incompatible with postmodern operational realities. Moreover, critics highlight its failure to incorporate essential functions like secrecy, counter-intelligence, and oversight, thus inadequately reflecting real-world intelligence practice (Hulnick, 2006; Richards, 2013). Consequently, scholars such as Gill & Phythian (2013) conclude that the classical model requires substantial revision or complete abandonment.

A Collaborative Intelligence Model for Indonesia

Best practices from ERM Life Cycle and collaborative intelligence suggest that the four core elements of the *Intelligence Web Model* are applicable in Indonesia: (1) Planning/Direction; (2) Access/Collect; (3) Analyze/Elucidate; (4) Store/Memory

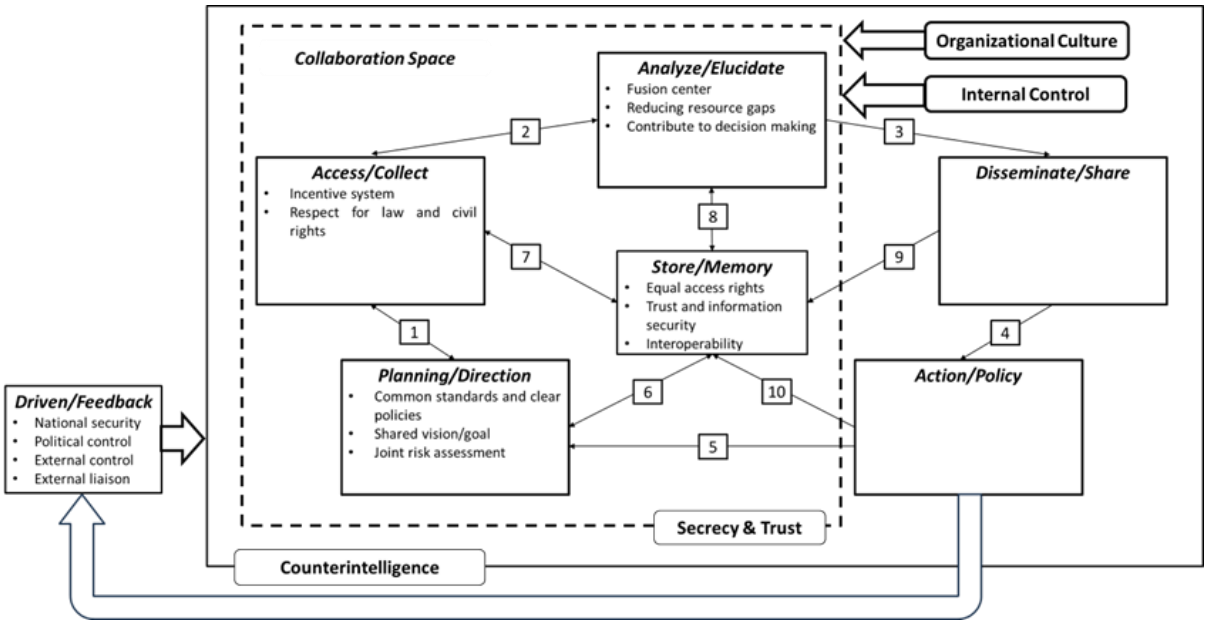

Figure 2. The Collaborative Intelligence Model

The model introduces a *Collaboration Space* framing these elements. Only the four core elements are collaborative among intelligence committee members or with private/public actors. Sub-elements refine collaborative principles for Indonesia: The Planning/Direction element necessitates establishing common standards and clear policies, particularly through amendments to the State Intelligence Law. Such revisions should explicitly govern interagency information sharing, define classification boundaries, and mandate the inclusion of all intelligence entities within formal coordination committees (Sandoval, 2013). Furthermore, this element requires articulating a shared vision and goal, which fundamentally distinguishes true collaboration characterized by interdependence, shared risk, and collective objectives from mere coordination involving independent goals. Joint risk assessment serves as a critical mechanism for determining the precise initiation and termination points of intelligence operations.

Finally, task decomposition, retained from Emergency Response Management (ERM) principles, ensures assignments are strategically aligned with specific expertise to prevent duplication of effort and mitigate operational conflicts. Within the Access/Collect function, the integration of multi-source information is paramount. This involves synthesizing Open-Source Intelligence (OSINT) with traditional Human Intelligence (HUMINT) methodologies, thereby enriching the foundational inputs available to analysts. Implementing a robust incentive system, structured around performance-based rewards, is essential to recognize active contributors and discourage passive participation ("free riding"). Crucially, all collection activities must operate

E-ISSN: 2776-1290, P-ISSN: 2776-1282

under the strict constraint of respect for rights and the law, ensuring adherence to civil liberties and legal frameworks throughout the information-gathering process.

The Analyze/Elucidate phase centers on the establishment of a fusion center. This integrative body synthesizes analyses from diverse stakeholders, including senior intelligence analysts, domain-specific experts, academics, and private sector actors, to generate comprehensive, inclusive, and policy-relevant intelligence products. Concurrently, a focus on reducing resource gaps fosters a unified national approach to collective threat response. This phase also demands an inclusive and integrated analytical methodology, ensuring cross-sectoral perspectives are incorporated and avoiding fragmented or partial reporting. The Store/Memory element addresses contemporary digital-era challenges. It moves beyond ad-hoc, task-specific collection by institutionalizing mechanisms for the continuous, systematic storage of intelligence information, thereby creating an organizational memory accessible for future analysis and strategic planning (Akter, M., & Kudapa, 2024; Niederman, 2021; Adabara et al., 2025).

Comparison: Classical vs. Collaborative Model

The classical model's linearity (Planning → Collection → Processing → Dissemination) inadequately represents real-world intelligence processes.

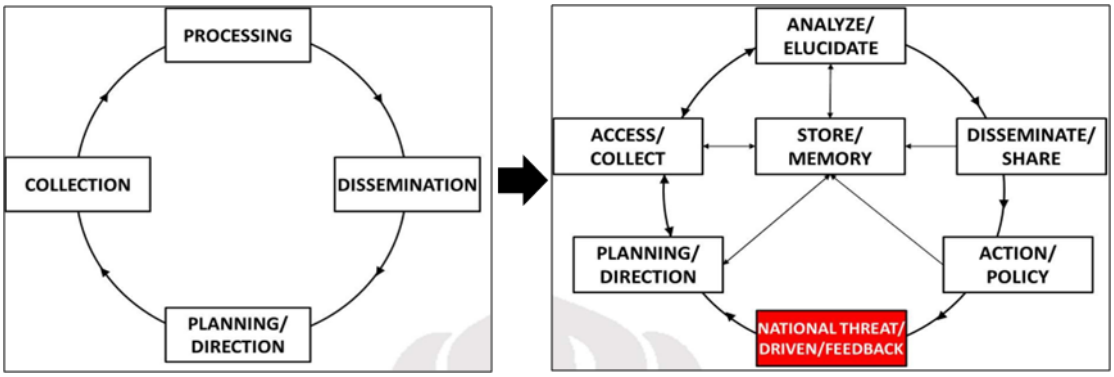

Figure 3. Addition of Store/Memory and National Threat Positioning
Source: Researchers' analysis, 2025

The classical model operates as a linear, unidirectional sequence comprising four distinct elements: it commences with planning and direction, proceeds to information collection, advances through processing (encompassing sorting, integration, and analysis), and culminates in intelligence dissemination to the President. Conversely, the Collaborative Intelligence Model offers a more realistic representation of operational dynamics. It accurately depicts bidirectional interactions, such as feedback loops between planning and collection phases, and reciprocal exchanges between collection and analysis activities. Furthermore, this model incorporates the essential Store/Memory element, facilitating iterative information flow across all stages with the exception of the Disseminate/Share and Action/Policy elements, which function exclusively as storage endpoints rather than access points.

The model also rectifies a significant ambiguity in the classical framework regarding the positioning of national threats. The classical model misleadingly implies that planning and direction occur after intelligence dissemination, contingent upon the President's subsequent assessment of threats. In reality, planning and direction are continuously informed by real-time national threat levels, alongside Driven/Feedback mechanisms including political control, external oversight, and liaison functions.

E-ISSN: 2776-1290, P-ISSN: 2776-1282

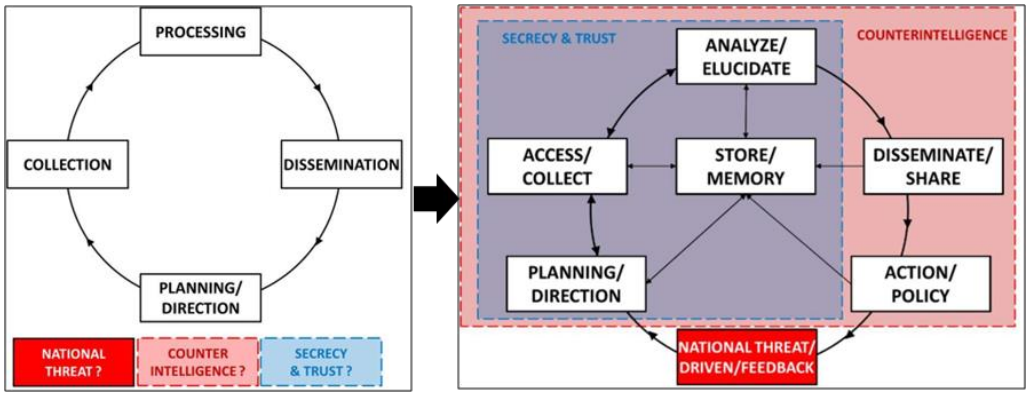

Figure 4. Addition of Secrecy & Trust and Counterintelligence
Source: Researchers' analysis, 2025

The Collaborative Intelligence Model establishes a rigorous confidentiality perimeter, explicitly defining all processes within the intelligence collaboration framework as protected by protocols of secrecy and trust. In contrast, the Disseminate/Share and Action/Policy elements operate beyond this confidential domain, as intelligence products at this stage have been transferred to the President and entered the non-classified realm of policy deliberation. Crucially, the Counterintelligence element safeguards the entire operational continuum including dissemination, policy action, and Driven/Feedback mechanisms against threat intervention. This protective function creates a critical filtration system: political controls, external oversight, and liaison activities cannot directly influence collaborative intelligence processes or their intrinsic values. Instead, such influences must first traverse the counterintelligence layer for threat mitigation, followed by evaluation against confidentiality and trust protocols as a secondary protective tier.

Challenges to Collaborative Intelligence in Indonesia

Within Indonesia's democratic framework, intelligence serves as a vital instrument of national defense and security, providing essential early warning, detection, and prevention capabilities. Ideally, intelligence agencies should proactively anticipate, identify, detect, and mitigate emerging threats within the strategic environment. A fundamental challenge lies in ensuring intelligence is utilized appropriately by policymakerswhether it genuinely serves national interests or is instrumentalized for partisan political purposes. The primary challenge in implementing a collaborative intelligence model involves navigating public opinion during policy formulation, enactment, and execution. Public perceptions remain highly susceptible to inflammatory narratives, particularly given historical experiences with intelligence institutions. This necessitates proactive governmental communication strategies that clearly articulate the objective of enhancing national security stability without ulterior motives.

Concurrently, institutional egoism among state intelligence actors presents a significant impediment, as agencies may compete for jurisdictional primacy a dynamic potentially emerging during initial policy deliberations. Achieving consensus across societal stakeholders, including the global intelligence community, requires considerable time and sustained effort. Ultimately, collaboration can only be deemed successful when it transcends perceptions of serving elite, military, or ruling-class interests or being reduced to a technical information-sharing mechanism. Its broader legitimacy derives from demonstrably contributing to national security and establishing the collaborative model as a trusted governance framework for intelligence oversight. Further complexity arises from harmonizing diverse organizational cultures amid multifaceted threats. This demands not only robust policy frameworks but skilled leadership capable of orchestrating multiple stakeholders across cultural boundaries.

E-ISSN: 2776-1290, P-ISSN: 2776-1282

Effective internal oversight mechanisms are equally critical to maintain operational equilibrium; such supervision should safeguard collaborative endeavors without unduly constraining them, respecting confidentiality imperatives and participant engagement while enabling intelligence fusion. Implementation faces particular difficulty in standardizing information classification protocols among all collaborative participants. Aligning classification standards between state intelligence entities, private sector actors, and civil society introduces significant complexity. Subsequent challenges include securing data, information systems, and networks especially given recurring governmental cybersecurity failures. Finally, persistent budgetary constraints for funding advanced technologies, systems, and infrastructure remain a classic impediment to comprehensive reform.

This research emphasizes that the traditional intelligence cycle model, historically serving as the primary framework for intelligence agencies in Indonesia, is no longer sufficient to address the diverse nature of contemporary threats and collaborative requirements. Such models exhibit linearity, hierarchy, and rigidity attributes starkly contrasted with modern challenges demanding rapid, adaptable, and cooperative responses. Within a context where threats manifest asymmetrically, such as in cyberattacks, disinformation campaigns, transnational terrorism, and pandemics, inflexible intelligence methodologies significantly hinder the efficacy of policy and operational responses.

The deficiencies of the classical model are evidenced by suboptimal coordination performance indicators within the national intelligence reform index. Empirical data from the Regional Intelligence Committee (Kominda) reveals that the effectiveness of intelligence synergy is subject to fluctuations and fails to fully embody collaborative efforts. This observation suggests that formal coordination mechanisms have yet to evolve into trust-based partnerships, risk frameworks, and integrated information exchange across agencies. Low performance metrics further signify a deficit of trust among intelligence entities and a prevailing tendency towards closed operational frameworks, consequently impairing early detection capabilities and informed decision-making.

Furthermore, the research illustrates that collaboration must extend beyond state institutions to include the participation of the private sector, academic institutions, and civil society. In this regard, the "Intelligence Web" model, integrating core principles of Emergency Response Management (ERM) and the National Strategy for Information Sharing and Security (NSISS), emerges as a more appropriate representation of Indonesia's requirements. This model facilitates horizontal coordination, data interoperability, and systematic, outcome-oriented engagement with diverse stakeholders.

Nevertheless, significant implementation challenges persist. These include bureaucratic cultural resistance to information transparency, the prevalent notion that data sharing equates to disclosing state secrets, and the divergent interests and hierarchical structures inherent among various agencies. Even following the establishment of the Strategic Analysis Council (DAS) by BIN, integration within the national coordination framework remains superficial. This indicates that merely establishing new structures is insufficient; transformative change in operational paradigms and mechanisms is necessary to cultivate mutual trust and a sense of equality among stakeholders.

The importance of technology is paramount within the collaborative model. The incorporation of Open-Source Intelligence (OSINT), advanced data analytics, artificial intelligence, and the creation of fusion centers can accelerate information collection, analysis, and dissemination processes. However, this technological evolution must be complemented by robust institutional reform and legal frameworks. Enhancing human resource capabilities and establishing clear information classification standards are also urgent necessities to ensure collaboration proceeds securely and purposefully.

E-ISSN: 2776-1290, P-ISSN: 2776-1282

The collaborative model proposed in this analysis introduces components such as Store/Memory and Secrecy & Trust into the intelligence cycle, asserting that information storage management and the cultivation of trust are fundamental foundations of contemporary intelligence practice. Additionally, integrating Counterintelligence elements serves as a protective barrier against political influence and external threats, thereby providing a vital layer of security to maintain the integrity of intelligence processes. The research concludes that a successful transition towards a collaborative intelligence framework critically depends on national leadership that embodies a clear vision and possesses the capacity to align diverse actors with varying cultures, interests, and capabilities. Such leadership must reconcile differences, forge a collective vision, and enforce principles of accountability and legality throughout every phase of intelligence operations. Without this essential leadership, reform efforts are likely to remain normative, yielding minimal impact on national security.

CONCLUSION

This research contends that the traditional intelligence cycle model, characterized by linearity and hierarchical structure, has become obsolete in effectively addressing the imperative for cross-agency collaboration amidst Indonesia's complex contemporary national security threat landscape. This model inadequately captures the dynamic, responsive, and multi-dimensional operational context essential for confronting challenges such as terrorism, cyber threats, disinformation, and complex disasters. Findings indicate that the efficacy of intelligence coordination through the Kominda forum remains inconsistent and has yet to demonstrate significant collaborative effort. Coordination indicators within the Intelligence Reform Index persistently rank as the lowest-scoring component, reflecting deficits in synergy, interagency distrust, and evident sectoral compartmentalization. This underscores the reality that Indonesia's intelligence apparatus continues to operate in sectoral silos and has not established a robust collaborative architectural framework. Reform initiatives, exemplified by the establishment of coordination forums and analytical bodies such as the Strategic Analysis Council, remain largely confined to structural dimensions and have not initiated the necessary paradigm shift. Effective collaborative intelligence requires cross-sectoral integration, the engagement of non-state actors, information system interoperability, and trust-based methodologies characterized by secure and measurable transparency. Given these deficiencies, alternative frameworks such as the Intelligence Web Model and the National Strategy for Information Sharing and Security (NSISS) gain relevance for adaptation to the Indonesian context. These models are inherently more adaptable to rapid transformation and facilitate coordinated, evidence-based decision-making processes.

Conflict of Interest

The authors declare no conflict of interest.

REFERENCES

Adabara, I., Sadiq, B. O., Shuaibu, A. N., Danjuma, Y. I., & Maninti, V. (2025). Trustworthy agentic AI systems: a cross-layer review of architectures, threat models, and governance strategies for real-world deployment. *F1000Research*, *14*(905), 905.

Adly, A. S., Adly, A. S., & Adly, M. S. (2020). Approaches based on artificial intelligence and the internet of intelligent things to prevent the spread of COVID-19: scoping review. *Journal of medical Internet research*, *22*(8), e19104. https://doi.org/10.2196/19104

Akbar, G. G., Muchtar, M., Pundenswari, P., & Ginting, S. (2025). Mapping poverty alleviation in Garut Regency: An Actor-Network Theory perspective on collaboration and actor interactions. *International Journal of Science and Environment (IJSE)*, *5*(1), 47-63. https://doi.org/10.51601/ijse.v5i1.147

E-ISSN: 2776-1290, P-ISSN: 2776-1282

Akter, M., & Kudapa, S. P. (2024). A comparative analysis of artificial intelligence-integrated bi dashboards for real-time decision support in operations. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 158-191. https://doi.org/10.63125/47jjv310

Ansell, C., Boin, A., & Keller, A. (2010). Managing transboundary crises: Identifying the building blocks of an effective response system. *Journal of contingencies and crisis management*, *18*(4), 195-207. https://doi.org/10.1111/j.1468-5973.2010.00620.x

Arslan, A., Golgeci, I., Khan, Z., Al-Tabbaa, O., & Hurmelinna-Laukkanen, P. (2021). Adaptive learning in cross-sector collaboration during global emergency: conceptual insights in the context of COVID-19 pandemic. *Multinational Business Review*, *29*(1), 21-42. https://doi.org/10.1108/MBR-07-2020-0153

Awaludin, M., Yasin, V., & Risyda, F. (2024). The influence of artificial intelligence technology, infrastructure and human resource competence on Internet access networks. *Inform: Jurnal Ilmiah Bidang Teknologi Informasi Dan Komunikasi*, *9*(2), 111-120. https://doi.org/10.25139/inform.v9i2.8109

Bahriansyah, I. M., Supriyadi, A. A., & Nurisnaeny, P. S. (2024). Anticipating the impact of artificial intelligence to increase national vigilance against terrorism attacks in Indonesia. *Remote Sensing Technology in Defense and Environment*, *1*(2), 86-97.

Benbya, H., & McKelvey, B. (2006). Using coevolutionary and complexity theories to improve IS alignment: A multi–level approach. *Journal of Information technology*, *21*(4), 284-298. https://doi.org/10.1057/palgrave.jit.2000080

Best Jr, R. A. (2015). Intelligence and US national security policy. *International Journal of Intelligence and Counterintelligence*, *28*(3), 449-467. https://doi.org/10.1080/08850607.2015.1022460

Bethune, E., Buhalis, D., & Miles, L. (2022). Real time response (RTR): Conceptualizing a smart systems approach to destination resilience. *Journal of Destination Marketing & Management*, *23*, 100687. https://doi.org/10.1016/j.jdmm.2021.100687

Bryson, J. M., Crosby, B. C., & Stone, M. M. (2015). Designing and implementing cross-sector collaborations: Needed and challenging. *Public administration review*, *75*(5), 647-663. https://doi.org/10.1111/puar.12432

Chen, R., Sharman, R., Rao, H. R., & Upadhyaya, S. (2008). *Coordination in emergency response management*. Communications of the ACM, 51(5), 66–73. https://doi.org/10.1145/1342327.1342340

Davies, P. H., Gustafson, K., & Rigden, I. (2013). The intelligence cycle is dead, long live the intelligence cycle: rethinking intelligence fundamentals for a new intelligence doctrine. In *Understanding the intelligence cycle* (pp. 56-75). London: Routledge.

De Werd, P. (2021). Reflexive intelligence and converging knowledge regimes. *Intelligence and National Security*, *36*(4), 512-526. https://doi.org/10.1080/02684527.2021.1893073

Djenna, A., Bouridane, A., Rubab, S., & Marou, I. M. (2023). Artificial intelligence-based malware detection, analysis, and mitigation. *Symmetry*, *15*(3), 677. https://doi.org/10.3390/sym15030677

Dovers, S. R., & Handmer, J. W. (1992). Uncertainty, sustainability and change. *Global environmental change*, *2*(4), 262-276. https://doi.org/10.1016/0959-3780(92)90044-8

Farahani, F. M. (2024). Challenges and Barriers to Implementing Collaborative Governance for Linking Education and Industry. *Management Strategies and Engineering Sciences*, *6*(3), 164-173. https://doi.org/10.61838/msesj.6.3.16

E-ISSN: 2776-1290, P-ISSN: 2776-1282

Gentry, J. A. (2019). "Truth" as a Tool of the Politicization of Intelligence. *International Journal of Intelligence and CounterIntelligence*, *32*(2), 217-247. https://doi.org/10.1080/08850607.2019.1565265

Gill, P., & Phythian, M. (2013). From Intelligence Cycle to web of intelligence: Complexity and the conceptualisation of intelligence 1. In *Understanding the intelligence cycle* (pp. 21-42). London: Routledge. https://doi.org/10.4324/9780203558478

Gumenyuk, V., Nikitin, A., Bondar, O., Zhydovtsev, I., & Yermakova, H. (2025). The role and significance of state-building as ensuring national security in the context of artificial intelligence development. *AI Magazine*, *46*(1), e12207. https://doi.org/10.1002/aaai.12207

Healey, J. (2012). Claiming the Lost Cyber Heritage. *Strategic Studies Quarterly*, *6*(3), 11-19.

Heracleous, L., & Werres, K. (2016). On the road to disaster: Strategic misalignments and corporate failure. *Long Range Planning*, *49*(4), 491-506. https://doi.org/10.1016/j.lrp.2015.08.006

Hulnick, A. S. (2006). What's wrong with the intelligence cycle. *Intelligence and National Security*, 21(6), 959–979. https://doi.org/10.1080/02684520601046210

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2022). Artificial intelligence applications for industry 4.0: A literature-based study. *Journal of Industrial Integration and Management*, *7*(01), 83-111. https://doi.org/10.1142/S2424862221300040

Kumar, G., Kumar, K., & Sachdeva, M. (2010). The use of artificial intelligence based techniques for intrusion detection: a review. *Artificial Intelligence Review*, *34*(4), 369-387. https://doi.org/10.1007/s10462-010-9179-5

Majeed, A., & Hwang, S. O. (2021). Data-driven analytics leveraging artificial intelligence in the era of COVID-19: an insightful review of recent developments. *Symmetry*, *14*(1), 16. https://doi.org/10.3390/sym14010016

Mitchell, B. (2005). The intelligence cycle and an information management process model: A comparative analysis. *Journal of the Australian Institute of Professional Intelligence Officers*, *14*(2), 14-27.

Niederman, F. (2021). Project management: openings for disruption from AI and advanced analytics. *Information Technology & People*, *34*(6), 1570-1599. https://doi.org/10.1108/ITP-09-2020-0639

Nte, N. D., & Nte, U. N. (2025). The Intelligence-Led Risk Management for National Security sand Public Safety in Nigeria: Strengthening the Collaborative Continuum for Optimum Efficiency. *Jurnal Ilmu Sosial Politik dan Humaniora*, *8*(1), 1-21. https://doi.org/10.36624/jisora.v8i1.164

Petersen, K. L., & Tjalve, V. S. (2018). Intelligence expertise in the age of information sharing: public–private 'collection'and its challenges to democratic control and accountability. *Intelligence and National Security*, *33*(1), 21-35. https://doi.org/10.1080/02684527.2017.1316956

Ramadhianto, R., Rezasyah, T., Kertopati, S. N. H., Estrada, M. A. R., & Kanellopoulos, A. N. (2025). Strengthening management of non-military intelligence organizations in detecting cyber threats to support national security. *Advanced Research in Intelligence and National Security*, *1*(1), 90-121.

Ratner, B. D., Meinzen-Dick, R., Hellin, J., Mapedza, E., Unruh, J., Veening, W., ... & Bruch, C. (2017). Addressing conflict through collective action in natural resource management. *International Journal of the Commons*, *11*(2).

E-ISSN: 2776-1290, P-ISSN: 2776-1282

Richards, J. (2013). Pedalling hard: Further questions about the intelligence cycle in the contemporary era. In *Understanding the intelligence cycle* (pp. 43-55). London: Routledge. https://doi.org/10.4324/9780203558478

Salvador-Carulla, L., Rosenberg, S., Mendoza, J., Tabatabaei-Jafari, H., & Network, P. M. H. I. (2020). Rapid response to crisis: Health system lessons from the active period of COVID-19. *Health Policy and Technology*, *9*(4), 578-586. https://doi.org/10.1016/j.hlpt.2020.08.011

Sandoval, C. C. (2013). *Federal interagency intelligence and information sharing: A matter of mission, a function of trust and leadership* (Doctoral dissertation, University of Phoenix).

Santoso, P. A. (2024). The Role of Threat Intelligence Sharing in Strengthening Collective Cyber Defense Across Organizations. *Global Research Perspectives on Cybersecurity Governance, Policy, and Management*, *8*(12), 24-33.

Sharma, A., Sharma, V., Jaiswal, M., Wang, H. C., Jayakody, D. N. K., Basnayaka, C. M. W., & Muthanna, A. (2022). Recent trends in AI-based intelligent sensing. *Electronics*, *11*(10), 1661. https://doi.org/10.3390/electronics11101661

Sukma, I. M. (2024). Techno-realism: Navigating new challenges in the contemporary role of technology in politics. *Security and Defence Quarterly*, *46*(2), 24-46.

Syuntyurenko, O. V. (2022). Predicting potential threats and megarisks in information technology development. *Scientific and Technical Information Processing*, *49*(1), 48-59. https://doi.org/10.3103/S0147688222010130

Van Tulder, R., & Keen, N. (2018). Capturing collaborative challenges: Designing complexity-sensitive theories of change for cross-sector partnerships. *Journal of Business Ethics*, *150*(2), 315-332. https://doi.org/10.1007/s10551-018-3857-7

Vecchiato, R. (2012). Environmental uncertainty, foresight and strategic decision making: An integrated study. *Technological Forecasting and Social Change*, *79*(3), 436-447. https://doi.org/10.1016/j.techfore.2011.07.010

Voelpel, S. C., Leibold, M., & Tekie, E. B. (2006). Managing purposeful organizational misfit: Exploring the nature of industry and organizational misfit to enable strategic change. *Journal of Change Management*, *6*(3), 257-276. https://doi.org/10.1080/14697010600963076

Vogel, K. M., & Tyler, B. B. (2019). Interdisciplinary, cross-sector collaboration in the US Intelligence Community: lessons learned from past and present efforts. *Intelligence and National Security*, *34*(6), 851-880. https://doi.org/10.1080/02684527.2019.1620545

Warner, Michael. (2013). The Past and Future of the Intelligence Cycle. In Phythian, M. (Eds.), *Understanding the Intelligence Cycle*. New York: Routledge. https://doi.org/10.4324/9780203558478

Weare, C., Lichterman, P., & Esparza, N. (2014). Collaboration and culture: Organizational culture and the dynamics of collaborative policy networks. *Policy Studies Journal*, *42*(4), 590-619. https://doi.org/10.1111/psj.12077

Wijaya, S. G., Suwadi, P., & Rustamaji, M. (2024). The Justification for Enhancing the Attorney General's Intelligence Authority in Human Rights-Oriented Law Enforcement in Indonesia. *Contemp. Readings L. & Soc. Just.*, *16*, 338.

Wu, G., Hu, Z., Wang, H., & Liu, B. (2025). Adding sectors or strengthening ties? Adaptive strategies for cross-sector collaboration in disaster governance. *Public Management Review*, *27*(9), 2007-2029. https://doi.org/10.1080/14719037.2024.2315563

E-ISSN: 2776-1290, P-ISSN: 2776-1282