IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

International Journal of Innovative Research and Scientific Studies
ONLINE ISSN : 2617-6548

Expanding the intelligence web model to address collaborative challenges in Indonesia

Oktora Aditia[1*], Amy Y. S. Rahayu[2], Roy V. Salomo[3]

[1,2,3]*Faculty of Administrative Sciences (FIA), University of Indonesia, Indonesia.*

Corresponding author: Oktora Aditia (*Email: oktoraaditia@gmail.com*)

Abstract

This study aims to propose an expansion of Gill and Phythian [2] Intelligence Web Model by introducing the Collaborative Intelligence Model, a framework adapted to Indonesia's fragmented intelligence structure and democratic context. Key innovations include the addition of a dedicated Collaboration Space, the separation of internal and external control mechanisms, and the integration of dual protective layers: secrecy and trust, and counterintelligence. Employing a constructivist paradigm, the study draws on twenty in-depth interviews with intelligence committee members, practitioners, academics, and oversight bodies. Findings reveal that Indonesian agencies operate under varying models, often without formalized planning, dedicated analysts, or standardized cycles, leading to redundancy, competition, and information politicization. The proposed model emphasizes shared planning, joint analysis through fusion centers, performance-based incentives, and a centralized intelligence memory to streamline coordination. By institutionalizing collaboration while safeguarding accountability and civil liberties, the Collaborative Intelligence Model offers a viable solution to the operational fragmentation and politicization of intelligence. Although developed for the Indonesian context, the model contributes broader theoretical insights for intelligence reform in democracies navigating multi-agency coordination. Further validation through comparative and quantitative studies is recommended.

Keywords: Collaboration, Indonesia, Intelligence cycle, Intelligence web, Model.

DOI: 10.53894/ijirss.v8i5.9372
Funding: This study received no specific financial support.
History: Received: 10 July 2025 / **Revised:** 12 August 2025 / **Accepted:** 14 August 2025 / **Published:** 19 August 2025

Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.
Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Publisher: Innovative Research Publishing

1. Introduction

The concept of the intelligence cycle has long served as a foundational model in understanding how intelligence is produced and utilized within state institutions. Traditionally, the cycle outlines a linear, sequential process from planning and data collection to analysis and dissemination. While this framework has provided analytical clarity and institutional structure, its practical application has come under increasing scrutiny. The digital transformation of the security landscape, combined with rising complexity in global threats, has rendered classical intelligence models increasingly inadequate in addressing contemporary challenges.

Critiques of the classical intelligence cycle point to its oversimplification of operational realities and its failure to accommodate the non-linear, iterative, and multi-directional nature of modern intelligence practices. Analysts have highlighted the cycle's rigidity, especially in crisis scenarios where rapid, collaborative responses are essential. In many democratic societies, intelligence work now demands adaptability, integration of diverse stakeholders, and mechanisms for real-time collaboration. Consequently, scholars have proposed alternative frameworks, including networked and web-based models, to better reflect the complex dynamics of modern intelligence systems.

In Indonesia, these theoretical tensions manifest acutely. The country's intelligence architecture is marked by fragmentation, with multiple agencies operating under divergent mandates and protocols. Although the 2011 National Intelligence Law designates the Badan Intelijen Negara (BIN) as the coordinating authority, many institutions function independently, with overlapping roles and limited interagency communication. This fragmentation undermines national security efforts, especially in responding to transnational threats, political crises, and regional conflicts that require unified strategic coordination [1].

Compounding these structural challenges is the politicization of intelligence in Indonesia's democratic context. Intelligence outputs are often filtered through partisan lenses, with agencies competing for executive favor. Such competition dilutes the objectivity of intelligence and diminishes its utility for policymaking. In an era of heightened security demands and complex societal risks, Indonesia urgently requires an updated intelligence framework that promotes collaborative governance, minimizes duplication, and enhances institutional trust.

The Intelligence Web Model, proposed by Gill and Phythian [2] offers a conceptual departure from rigid linear models by emphasizing multidirectional flows, institutional memory, and oversight mechanisms [2]. While promising, the model requires further adaptation to reflect Indonesia's contextual needs, particularly the need for an inclusive collaboration space and explicit safeguards to prevent abuse of power. The present study addresses this gap by proposing an expanded framework: the Collaborative Intelligence Model.

This model integrates elements from the Intelligence Web Model with critical modifications, including the introduction of a collaboration space, dual-layer protections (trust and counterintelligence), and clearer boundaries between internal and external oversight. It redefines intelligence not as a closed bureaucratic function but as a collaborative process involving analysts, policymakers, civil society, and external actors. By institutionalizing joint planning, shared analysis, and a centralized intelligence memory, the model seeks to harmonize operational practices while preserving accountability and secrecy.

Methodologically, this research is grounded in a constructivist paradigm and supported by qualitative data from twenty in-depth interviews with intelligence officials, oversight institutions, and academic experts. These informants offered valuable insights into Indonesia's current intelligence dynamics, challenges in interagency collaboration, and the practical feasibility of implementing collaborative intelligence structures. Document analysis further complemented the interviews, providing access to formal and informal records of intelligence processes and institutional coordination.

By addressing both structural and cultural impediments to intelligence reform, this study contributes to the growing body of literature on collaborative intelligence and security governance in democratic contexts. The Collaborative Intelligence Model is not merely an academic abstraction but a proposed operational tool for policymakers, security professionals, and reform advocates seeking to modernize intelligence practices in Indonesia and beyond.

2. Method

This study adopts a constructivist paradigm, focusing on the application of a collaborative intelligence model in Indonesia a nation confronting multifaceted threats, both domestic and external, that jeopardize national unity, economic development, political stability, and territorial integrity [3]. Such challenges necessitate collaborative efforts across all societal sectors to safeguard national interests and state sovereignty.

Data collection was conducted between 2024 and 2025, using two main techniques. In-depth interviews were conducted with 20 key informants, consisting of intelligence officials and practitioners from various institutions. The informants included 8 from intelligence agencies, 2 from the police, 3 active-duty military personnel, 1 from the Ministry of Home Affairs, 3 academics, and 3 representatives of non-state actors. All committee members were directly involved in intelligence planning, collection, analysis, counterintelligence operations, and product formulation. Interviews lasted an average of 90 minutes, preceded by a consent procedure and anonymity guarantees to protect participants' identities. Key informants were individuals who understood and implemented mechanisms and issues related to Indonesian intelligence. They were also involved in the Central Intelligence Committee (Kominpus), the Regional Intelligence Committee (Kominda), and the Strategic Analysis Council (DAS). Source triangulation was conducted by comparing informants' statements with other sources, such as statements from other informants, applicable mechanisms/regulations in Indonesia, formal documents, online/social media, and previous research.

Document analysis was performed, scrutinizing materials related to Indonesia's intelligence workflows, including both classified documents provided by informants and publicly accessible sources. Data analysis was conducted thematically and comparatively. This process involves three main stages: (1) Data reduction, filtering relevant information from interview results and documents, (2) Thematic categorization, by grouping data based on dimensions and important elements of the intelligence system, (3) Model reconstruction, compiling a new model based on empirical findings and theories that have been critically analyzed.

The development of the model also uses the principles of the ERM (Emergency Response Management) Life Cycle and the principles of international collaborative intelligence, which are then adapted to the Indonesian context. The final model is strengthened through simulations of information flows and logical tests of interactions between elements in the context of responding to national threats. Thus, this research method is not only oriented towards describing existing conditions but is also reconstructive-transformative, producing model innovations that are oriented towards systemic and applicable improvements to intelligence governance in Indonesia.

This research has passed the ethical review procedure for research protocols involving human subjects and was declared approved based on the Decree of the Chair of the Research Ethics Committee of the Faculty of Economics and Business, University of Indonesia, Number: S-011/UN2.F6.D2.LPM/PPM.KEP/IV/2025, on April 9, 2025, through an expedited review type.

3. Research Result

The study of intelligence cycles remains a perennially relevant topic, particularly in examining whether such models are actively operationalized as functional guides or merely retained as symbolic artifacts adorning the walls of intelligence institutions. Debates surrounding the practical relevance and applicability of these frameworks persist, reflecting unresolved tensions between theoretical constructs and real-world implementation. The intelligence cycle is defined through multiple interpretations, yet it has consistently been framed as a process comprising sequential stages or activities. This process-oriented model, often visualized as four or five interconnected phases (sometimes more), conceptually illustrates the relationships between actors within intelligence organizations across diverse scenarios [4]. The cycle operates iteratively, perpetually generating new informational demands and forming a feedback loop [5]. It is characterized by bidirectional interactions [6], resembling an endless chain where stages may be revisited multiple times [7]. Loch K. Johnson likens the cycle to the work of analysts who synthesize information from open and clandestine sources, subsequently delivering findings to policymakers via written or oral briefings [6].

The most universal explanation, as articulated by Gill and Phythian [2] begins with planning and direction, wherein intelligence consumers request insights on specific issues or targets. This is followed by data collection, succeeded by processing a pre-analytical phase involving filtering, codification, encryption, evaluation, translation, integration, and data reduction to prepare raw information for analysis. The subsequent analysis phase transforms processed data into actionable intelligence. The final stage, dissemination, distributes the refined intelligence back to the original requester, after which the cycle repeats.

Shifts in the strategic landscape, such as the information-technology revolution, evolving national interests, escalating threat complexity, and heightened situational uncertainty, have rendered the classical intelligence cycle increasingly obsolete. The digital age has fundamentally altered how intelligence is gathered, utilized, stored, and disseminated, prioritizing rapid decision-making [8]. As Haeley notes, cyber threats now unfold in nanoseconds, rendering sequential intelligence cycles impractical [9]. The classical model has outlived its utility in enhancing operational efficacy [8], particularly given the reality that intelligence work rarely conforms to its idealized linearity [4, 10].

Warner’s critique resonates with our concerns: the cycle, as taught in foundational intelligence training [8], lacks clear operational start/end points and blurred interstage boundaries [5]. This oversimplification risks distorting practice, such as by enforcing rigid sequentiality between collection and analysis [10]. Furthermore, agencies adhering to non-risk-adapted models may exhibit reflexive biases, skewing judgments and influencing policymakers [11].

National approaches to the intelligence cycle vary significantly. The U.S. employs a five-stage framework (DCPAD: Directing, Collection, Processing, Analysis, Dissemination), while the U.K. condenses processing and analysis into a single phase, resulting in a four-stage model DCPD [5].

In Indonesia, most intelligence agencies do not formally endorse a specific model. This ambiguity has become more pressing under President Prabowo, whose military background has highlighted the challenges of fragmented intelligence coordination. With multiple agencies operating independently, including new entities outside the formal intelligence committee, information integration remains fraught. Since he began his leadership in 2025, President Prabowo has mandated interagency collaboration to produce inclusive, unified intelligence outputs.

Gill and Phythian [2] Intelligence Web Model aligns with Indonesia’s evolving practices and addresses critiques of classical frameworks. By introducing collaborative principles and nonlinear interactions, the model modernizes intelligence workflows. It acknowledges that contemporary intelligence is no longer a linear progression from planning to dissemination but a dynamic system of multidirectional engagement.

3.1. The Collaborative Intelligence Model

This study proposes a novel framework adaptable to diverse intelligence organizations, particularly in Indonesia. While the nation has excelled in collaborative governance, implementing collaborative intelligence under presidential mandate amidst institutional and cultural challenges remains an open question.

Despite extensive criticism and comparative analysis, it retains core elements of the classical cycle but enhances it with six innovations [2].

Store/Memory: A repository for information storage and processing. National Security/Organizational Culture: Institutional ideologies and principles shaping bureaucratic norms. External Liaison: Competitive and cooperative interactions with foreign intelligence entities. Ring of Secrecy: Protocols safeguarding intelligence from counterintelligence threats. Political Control: Accountability to elected officials regarding targets, methods, and legal compliance. Oversight:

Mechanisms to maintain public trust. The model incorporates bidirectional arrows symbolizing multidirectional interactions between elements, reflecting the complexity of modern intelligence ecosystems.

This study identifies eleven intelligence agencies within Indonesia's formal intelligence committee, chaired by the Head of BIN. Additionally, 15 government organizations operate intelligence units or functions outside this committee. Interviews with representatives from these agencies revealed divergent practices: some assert adherence to the DCPAD model, while others lack clarity on their operational frameworks.

The 2011 National Intelligence Law mandates BIN to coordinate Indonesia's intelligence system [12]. However, critical elements such as a standardized, binding intelligence cycle remain unregulated, relegating the cycle to a peripheral role in organizational workflows and structural development.

Work mechanisms vary significantly across agencies. When asked whether operations must begin with formal planning, responses diverged. Only informants from BIN, the National Counter Terrorism Agency, as well as the Drug & Food Oversight Agency, reported structured annual planning, later refined into detailed operational blueprints. These agencies are identified as "pure intelligence entities," whereas others functioning as subsidiary units within multifunctional parent organizations adopt ad hoc planning driven by emerging threats.

Regarding information collection, all informants agreed that analysts are prohibited from gathering raw data, contradicting Hulnick's advocacy for analyst-led open-source intelligence (OSINT) collection to expedite responses [10]. Notably, only BIN employs dedicated intelligence analysts. Other agencies assign analytical roles to personnel in legal, policing, policy, customs, or pharmaceutical fields, effectively merging collection and analysis duties, a practice that blurs professional boundaries.

Diverse conditions are not only evident in the operational mechanisms among intelligence agencies, but sectoral egos drive them to compete for the President's favor by submitting partial reports. This is akin to a shopper receiving numerous product brochures, each highlighting its own advantages. It becomes exceedingly challenging for the Indonesian President, who is inundated daily with a flood of information presenting varied facts and action recommendations.

Structurally, Indonesia's intelligence landscape is marked by multilayered complexity. Intelligence cycles operate not within a single locus but across dispersed levels and locations, mirroring the Nested Intelligence Cycles framework (Brunel Centre for Intelligence and Security Studies, BCISS) [5]. This fractal structure replicates DCPD/DCPAD phases at each hierarchical tier. Informants confirmed that strategic directives from leadership cascade into granular operational plans, with collection and analysis conducted in tiered phases. Intriguingly, field agents occasionally inject personal analytical insights when relaying information to analysts, a deviation from prescribed protocols.

Through our interview findings, we not only assessed existing models but also constructed the Intelligence Web Model to represent the complexity of Indonesia's intelligence processes. By integrating critical elements addressing collaborative intelligence challenges, we term this adapted framework The Collaborative Intelligence Model.

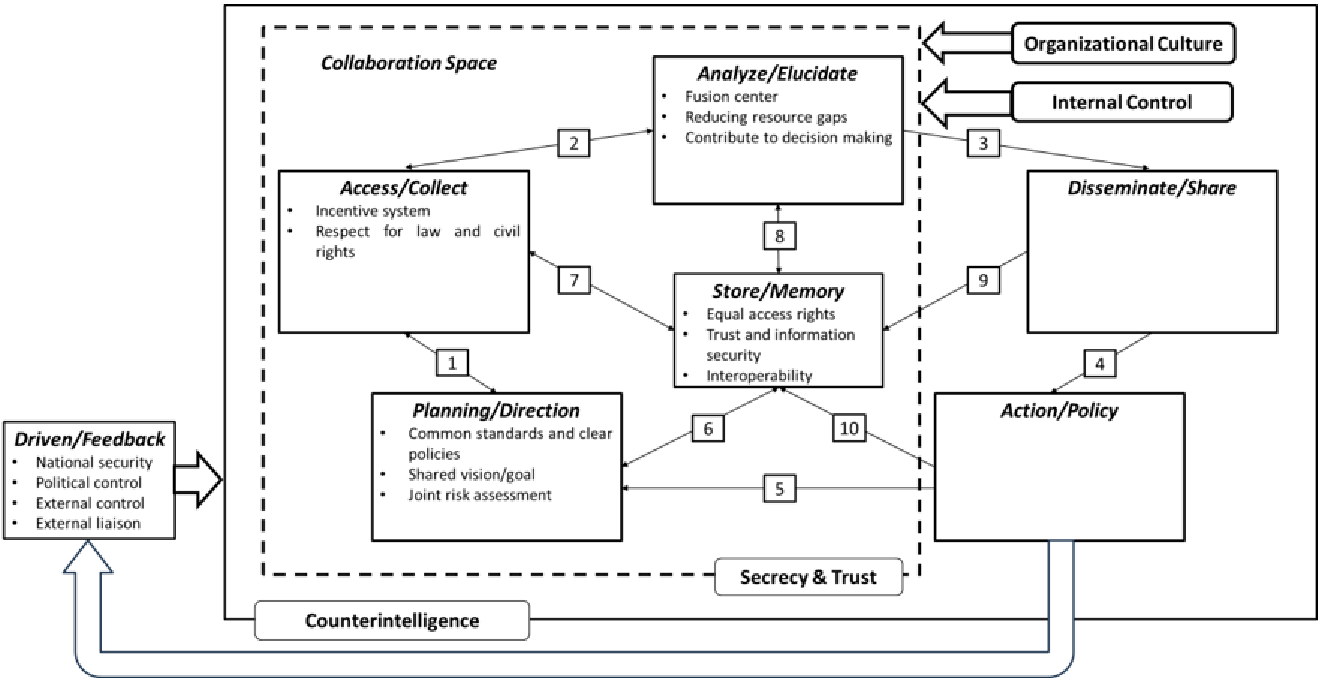

Figure 1.
The Collaborative Intelligence Model.

From the diagram above, intelligence-inclusive and integrated products can be produced through principles of collaboration and implementation with the following model formulation:

$$IIP = ColSp + (OC + IC - ST) + (DF\text{-}Ci)$$

The formulation of this model explains that in realizing Inclusive and Integrated Products (IIP), a Collaborative Space (ColSp) is needed, supported by a mature Organizational Culture (OC) that leads to the principle of collaboration in the four core elements (Planning/Direction, Access/Collect, Store/Memory, and Analyze/Elucidate). Furthermore, the collaboration space is strengthened by the Internal Control (IC) function, positioned above the internal control units within each collaboration member. These two supporting elements are protected by a ring of Secrecy from external threats and a ring of Trust (ST) between all the collaboration members. Inclusive products also consider the impact of actions or previous policies. Drivers and Feedback (DF), such as national security, political control, external control, and external liaison, are fenced by Counterintelligence (CI) elements before influencing the collaboration room and decision-making process.

This model incorporates adjustments tailored to Indonesia's context, including the addition and removal of specific elements and directions, the creation of sub-elements within core components to clarify operational stages, and revisions to the directional interactions of lines L and M. The most significant addition is the Collaboration Space, which frames four core elements. All informants unanimously agreed that these elements, Planning/Direction, Access/Collect, Analyze/Elucidate, and Store/Memory, are the only phases suitable for collaboration, both among intelligence committee members and with external actors (e.g., private and public sectors). The Secrecy & Trust boundary (denoted by dashed lines in Figure 1) signifies that collaboration occurs semi-closed, balancing technological tools like OSINT and crowdsourcing with the need for trust amid member turnover. Trust was repeatedly emphasized by informants as a non-negotiable prerequisite for collaboration.

As illustrated in Figure 1, the Collaboration Space's four elements are further refined with sub-elements reflecting Indonesia's collaborative practices:

Planning/Direction includes Common Standards and Clear Policies. Indonesia's current intelligence policies remain limited to coordination. Implementing collaboration requires amending the State Intelligence Act to mandate information-sharing protocols, classification boundaries, and registration of all intelligence entities under the national committee. Criteria for recruiting private/public collaborators must also be clarified to prevent conflicts of interest and foster mutual trust. Shared Vision/Goals distinguish collaboration from coordination through interdependence, shared risks, and mutual support [13-16]. Joint Risk Assessment determines when operations should commence or terminate.

We added two sub-elements to the Access/Collect element. The Incentive System sub-element must be performance-based. Key informants emphasized that implementing performance management is highly feasible for task forces collaborating with external actors (e.g., private and public entities), as they are funded by state resources. Active contributors to information gathering and sharing should receive greater incentives compared to free riders or silent participants. The Respect for Rights and Law sub-element reinforces that civil rights, individual freedoms, and adherence to legal frameworks remain paramount constraints on intelligence activities during information collection. While collaboration strengthens intelligence agencies, expanded authority under ambiguous collaborative identities risks misuse, where powerful intelligence entities may act on behalf of arbitrary parties. A robust intelligence apparatus could also be exploited to perpetuate political power or ruling interests.

The most critical collaborative element is Analyze/Elucidate. Analysis is the core rationale for establishing collaborative intelligence. It integrates diverse expertise, experiences, tribal knowledge, and strategic considerations to produce inclusive, integrated intelligence outputs. This element requires support from a fusion center, analogous to a restaurant kitchen using premium ingredients to craft exceptional dishes. The fusion center would convene senior intelligence analysts, domain experts, community leaders, academics, and industry representatives recruited as collaborators. Here, collected data is rapidly processed, debated (e.g., theories, methodologies, language precision, policy recommendations), and refined before presentation to the President. Collaborative intelligence addresses the widening gap between intelligence capabilities and evolving threat complexity. Intelligence agencies cannot confront threats alone; modern intelligence products must enable policy decisions that mobilize national collective action.

A novel addition absent from classical intelligence cycle models is the Store/Memory element. This addresses challenges of the digital age and information revolution, answering whether information collection must await orders or occur proactively, stored in organizational memory. Analysts can directly access this shared repository to analyze cross-sector, cross-temporal, and multi-regional threats. Existing intelligence products presented to the President can also be updated with new analyses reflecting current developments.

This model significantly alters several lines from the original framework, reflecting intelligence's adaptation to rapid technological advancements and the challenges of implementing collaborative concepts. The modified connecting lines between elements signify shifts in how intelligence interacts, collects, stores, and disseminates its products.

Lines 1-2-3-4-5 represent processes common to classical cycles. In a collaborative context, Line 1 denotes joint planning by all collaboration members, informed by national security considerations, political decisions, or external environmental factors. It may also reflect feedback from field agents who refine plans upon identifying new situational developments such as emerging targets requiring specific attention that could impact operational success. Joint planning may further incorporate threat trends accessed from organizational memory. The bidirectional arrow on Line 2 allows analysts to clarify or request additional information from collectors for deeper exploration during or before analysis. Lines 3-4-5, unidirectional in nature, indicate that formal interactions must restart the cycle from Line 1. Reanalysis is not feasible once intelligence products are disseminated. Line 5, originally featuring bidirectional interaction between Action/Policy and Planning/Direction, should ideally be unidirectional. Informants agreed with Gill and Phythian [2] view: after policymakers act, they may require new intelligence, but reverse feedback (planning directly triggering policy/action) is invalid. If intelligence leaders advocate for new laws or policies (e.g., to enable future data collection in response to emerging technologies), this necessitates a new model beyond traditional intelligence-policymaker dynamics.

Lines 6-10 describe the interaction between the core elements and the Store/Memory element. In addition to accessing threat trends as material for planning on line 1, line 6 also explains that Store/Memory ideally stores joint planning documents that have been prepared for reuse when needed. Line 7 stores all information gathering results and allows for re-accessing them. Line 8 stores the analysis results and re-accesses them or accesses previously collected information by the collecting agent. Line 9 is not as explained in the original model, which is about how actors can explore information by accessing what is stored in intelligence memory after the intelligence product is disseminated, but rather only documents the list of intelligence product distribution or ensures that intelligence products have been received by collaboration members in a timely and targeted manner. Accessing intelligence memory to find additional information after receiving intelligence products is an information-gathering activity that has been explained in line 7. Similarly, line 10 only records what decisions and actions have been taken by policymakers, then stores them in intelligence memory.

We eliminated lines C and L from the original model; the informants share the same view that ideally, policymakers do not have direct relationships with collecting agents or analysts. Even in crisis situations, intelligence remains an organization with a leader who has the task of building communication with policymakers. In a collaborative context, policymakers only communicate with one intelligence official who has been selected as a trusted collaborator. Collaboration will be successful and provide added value when the identities of collaboration members are not disclosed. In addition to causing intelligence politicization, this also has the potential to increase institutional ego that is vying for praise from policymakers.

Although most informants agree with line D in the original model, which explains that in urgent and crisis conditions, some raw information from access or collection can be directly disseminated. They said that some events, such as natural disaster response, cyber-attacks, and increasing conflict tensions in Papua, do require direct hourly reports without going through an analysis process, although in the end, they still present a full analysis periodically. However, we found another fact that this is contrary to the policy on intelligence reporting systems, which stipulates that disseminated intelligence products must go through analysis first, so we decided to delete the line and direct it to pass through lines 2 to 3.

We also disagree with line G, which in the original model explains that in certain issues, when the intelligence leader and policymakers have the same preferences, analysts can directly provide analysis to confirm these preferences or provide assessments that align with what policymakers want to hear. Such practices, of course, cause bias in intelligence assessment. Intelligence must continue to present facts, even if they are not in line with what policymakers want to hear. For this reason, we changed the path through lines 6 to 8. Analysts cannot avoid the planning process; in addition to reducing the quality of products and control functions, analysis based on personal opinions, experiences, and interests of analysts in making intelligence products will only produce misleading products. By utilizing intelligence memory or other trusted open sources, this path will at least narrow the bias of intelligence assessment. Similarly, with line J, information obtained previously, dissemination of intelligence products to collaboration members simply utilizes intelligence memory facilities through lines 6 to 9.

The Collaboration Space environment and its success are directly shaped by Organizational Culture and Internal Control. Organizational Culture reflects the ethos, egos, and work ethics of collaborative members, influencing motivation and information flow. We bifurcated Oversight into Internal Control (technical oversight: performance targets, incentives, prioritization, risk management, secure resource sharing, and confidentiality) and External Control (strategic oversight by parliament, media, researchers, or external actors addressing human rights, leaks, or intelligence failures). External Control, alongside National Security, Political Control, and External Liaison, forms the Driven/Feedback sub-elements. All external inputs must pass through Counterintelligence and Secrecy & Trust layers before influencing the Collaboration Space, ensuring uncompromised security. We repositioned External Liaison as a Driven/Feedback sub-element in Indonesia's context, subject to dual protective layers (like External Control) before impacting the Collaboration Space agenda.

3.2. Implementation Challenges

Modern intelligence organizations globally have evolved through four successive conflicts. World Wars I and II positioned intelligence to fulfill informational demands about adversaries and leverage emerging technologies. The Cold War repurposed intelligence as a tool for power consolidation and rivalry between the Eastern and Western blocs. In today's Global War on Terror, intelligence agencies are compelled to collaborate with external actors to detect threats to national development and state sovereignty [11].

In democratic contexts like Indonesia, intelligence functions not as an instrument of political power but as a pillar of national defense and security [17]. Its role encompasses early-warning, early detection, and early prevention mechanisms. Ideally, intelligence agencies anticipate, identify, detect, and preemptively neutralize emerging threats within the strategic environment. The critical challenge lies in ensuring intelligence serves the public good rather than being co-opted for partisan political agendas.

A nation's primary challenge in implementing collaborative intelligence lies in reforming policies to strengthen national security frameworks, align threat perceptions across stakeholders, and expand collaboration beyond mere information sharing. True collaboration entails unified efforts toward a singular objective: fostering a secure and resilient state.

Cultural diversity and the multi-threat landscape managed by numerous intelligence agencies further complicate implementation. Robust policies alone are insufficient; effective leadership capable of orchestrating collaboration is essential. Finally, internal oversight must strike a balance: rigorous enough to uphold secrecy and operational comfort, yet flexible enough to avoid stifling collaboration, ensuring intelligence fusion remains both secure and agile.

4. Discussion of Findings

The findings of this study reveal the fragmented and inconsistent application of intelligence models across agencies in Indonesia. While the classical DCPAD framework remains the most frequently cited, it is often implemented only in symbolic or partial forms. Many agencies operate without formal planning, assign intelligence functions to non-specialist personnel, and lack standardized procedures for information analysis and dissemination. These inconsistencies indicate that the classical model fails to reflect the real operational landscape, which is better characterized by nested, multi-layered, and sometimes ad hoc intelligence processes.

One of the most critical issues identified is the absence of a unified intelligence cycle model endorsed by all agencies. Despite the legal mandate assigning BIN as the coordinating body, agencies often operate independently, driven by institutional ego and competition for executive recognition. This leads to the submission of fragmented intelligence products to the President, often without cross-validation or collaborative analysis. The resulting information overload undermines the strategic value of intelligence and increases the risk of misinformed policy decisions. The lack of a formal collaboration framework further exacerbates these challenges. Informants consistently highlighted the need for a common platform where agencies can jointly plan, collect, analyze, and store intelligence data. The Collaborative Intelligence Model proposed in this study addresses this gap by introducing a Collaboration Space that houses four key stages: Planning/Direction, Access/Collect, Analyze/Elucidate, and Store/Memory, identified as suitable for interagency collaboration. This design encourages integrated decision-making and mutual trust among participating actors. A key innovation of the model is its emphasis on trust and secrecy as foundational elements of collaboration. While technology, such as open-source intelligence and crowdsourcing, can facilitate data access, informants emphasized that collaboration without trust is ineffective and even dangerous. The model, therefore, incorporates a dual-layer protection system: (1) trust and secrecy among collaborators, and (2) counterintelligence measures that filter and secure external and internal influences before they enter the collaborative space.

The separation between internal and external controls also marks a significant departure from existing models. Internal control mechanisms ensure technical compliance, performance monitoring, and protection of classified data, while external controls, including legislative oversight and public scrutiny, safeguard the democratic accountability of intelligence activities. By clearly defining these layers, the model enhances transparency without compromising operational security. Additionally, the inclusion of a centralized Store/Memory function reflects the realities of modern intelligence work, where information must be stored, accessed, and reused efficiently across temporal and organizational boundaries. This innovation allows for continuity in intelligence operations, enabling analysts to reference previous intelligence products, threat trends, and planning documents when developing new strategies.

Perhaps most importantly, the model redefines the role of analysis within the intelligence cycle. Instead of being a solitary process confined to a single agency, analysis is reframed as a collaborative task conducted through fusion centers. These centers bring together senior analysts, domain experts, academics, and representatives from civil society and the private sector to co-produce integrated intelligence products. This structure enhances the quality and relevance of intelligence, making it more reflective of the diverse and complex challenges facing Indonesian national security. In sum, the Collaborative Intelligence Model provides a practical and context-sensitive framework for reforming Indonesia’s intelligence system. It balances the need for interagency integration with safeguards against political misuse and institutional overreach. While further refinement and testing are necessary, especially through comparative studies, the model offers a solid foundation for enhancing intelligence governance in democratic settings.

5. Conclusion

This study critically examined the limitations of classical intelligence cycle models in the context of Indonesia's fragmented and multilayered intelligence landscape. Through qualitative inquiry involving twenty key informants and document analysis, it was found that Indonesian intelligence agencies operate under disparate frameworks, often lacking standardized planning, analytical clarity, and coordinated dissemination. These institutional inconsistencies contribute to redundancy, information politicization, and ineffective policymaking.

In response to these challenges, this study proposed the Collaborative Intelligence Model, an expanded version of Gill and Phythian [2] Intelligence Web Model tailored to Indonesia’s democratic governance and operational realities. The model introduces a structured Collaboration Space, delineates internal and external control mechanisms, embeds dual-layer protection (trust and counterintelligence), and emphasizes the centrality of shared analysis through fusion centers. The inclusion of a centralized Store/Memory further supports cross-agency continuity and institutional learning.

While this model is grounded in the Indonesian context, its theoretical innovations, such as redefining trust, oversight, and collaboration in intelligence, offer broader relevance to countries facing similar multi-agency coordination challenges. Future research should further test and refine the model through comparative, quantitative, or policy-implementation studies.

The Indonesian government needs to enhance the inter-organizational relationship (IoR) of the intelligence organization. It begins with establishing policies that clearly regulate the roles and authorities of each organization in efforts to maintain national security, which is balanced between civil and military, including regulating the balance of ranks and positions within collaboration forums. The policy should also eliminate overlapping and duplication of efforts within the framework of national security. This is expected to minimize the issue of the superiority of one institution over another, as well as a common view on integrated work systems and inclusive intelligence products.

Ultimately, the Collaborative Intelligence Model provides a practical framework for improving interagency coordination, reducing intelligence politicization, and enhancing the strategic value of intelligence in democratic settings. It is a timely contribution to ongoing debates on intelligence reform in the digital age.

References

[1] C. Rui, R. Sharman, H. R. Rao, and S. J. Upadhyaya, "Coordination in emergency response management," *Communication ACM,* vol. 51, no. 5, pp. 66–73, 2008. https://doi.org/10.1145/1342327.1342340

[2] P. Gill and M. Phythian, "From intelligence cycle to web of intelligence: Complexity and the conceptualisation of intelligence 1," in Understanding the intelligence cycle: Routledge, 2013, pp. 21-42.

[3] P. Gill and A. Wilson, "Intelligence and security-sector reform in Indonesia," University of Salford, Manchester, UK, 2013. https://www.researchgate.net/publication/290098556

[4] J. Richards, *Pedalling hard: Further questions about the intelligence cycle in the contemporary era. In M. Phythian*. New York: Understanding the Intelligence Cycle, 2013.

[5] P. H. J. Davies, K. Gustafson, and I. Rigden, *The intelligence cycle is dead, long live the intelligence cycle: Rethinking intelligence fundamentals for a new intelligence doctrine. In M. Phythian* London; Milton Park, Abingdon, Oxon, UK: Understanding the intelligence cycle 2013. https://doi.org/10.4324/9780203558478

[6] L. K. Johnson, "Sketches for a theory of strategic intelligence," in Intelligence Theory. London New York: Routledge, 2008, pp. 47-67.

[7] M. Warner, "The past and future of the intelligence cycle," in Understanding the Intelligence Cycle. London & Milton Park: Routledge, 2013, pp. 9-20.

[8] M. Warner, *The past and future of the intelligence cycle. In M. Phythian* London: Understanding the Intelligence Cycle, 2013.

[9] J. Healey, "Claiming the lost cyber heritage," *Strategic Studies Quarterly,* vol. 6, no. 3, pp. 11-19, 2012.

[10] A. S. Hulnick, "What's wrong with the intelligence cycle," *Intelligence and National Security,* vol. 21, no. 6, pp. 959-979, 2006. https://doi.org/10.1080/02684520601046291

[11] P. Gill, S. Marrin, and M. Phythian, *Intelligence theory: Key questions and debates*. London & New York: : Routledge, 2009.

[12] Republic of Indonesia, *Undang-undang republik indonesia nomor 17 tahun 2011* Citra Umbara: Tentang Intelijen Negara, 2011.

[13] C. Whelan, "Managing dynamic security networks: Towards the strategic managing of cooperation, coordination and collaboration," *Security Journal,* vol. 30, no. 1, pp. 310-327, 2017. https://doi.org/10.1057/sj.2014.20

[14] H. Zhong, R. R. Levalle, M. Moghaddam, and S. Y. Nof, "Collaborative intelligence-definition and measured impacts on internetworked e-work," *Management and Production Engineering Review*, vol. 6, no. 1, pp. 67–78, 2015.

[15] D. Sedgwick, "Managingcollaborative paradox: Examining collaboration between head start and the virginia preschool initiative," *Administration & Society,* vol. 48, no. 2, pp. 190-215, 2016. https://doi.org/10.1177/0095399714532269

[16] X. Castañer and N. Oliveira, "Collaboration, coordination, and cooperation among organizations: Establishing the distinctive meanings of these terms through a systematic literature review," *Journal of Management*, vol. 46, no. 6, pp. 965-1001, 2020. https://doi.org/10.1177/0149206320901565

[17] I. N. Bhakti, *Intelligence in the vortex of democracy in post-New Order Indonesia*. Yogyakarta: Andi, 2017.