JIGE 7 (4) (2026) 3569-3584
JURNAL ILMIAH GLOBAL EDUCATION
ejournal.nusantaraglobal.ac.id/index.php/jige
DOI: https://doi.org/10.55681/jige.v7i4.6954

Strategic Leadership and the Adaptation of Indonesia's National Defense Strategy in Addressing Multidimensional Security Threats

Animus Grahadi[1*], Sundring Pantja Djati[1], Joni Widjayanto[1], Guntur Eko Saputro[1], Asep Adang Supriyadi[1]

[1] Doctoral Program, Republic of Indonesia Defense University, Jakarta, Indonesia
**Corresponding author email: grahadianimus@gmail.com*

Article Info

Article history:

Received November 04, 2026
Approved November 20, 2026

Keywords:

Strategic Leadership, Defense Strategy Adaptation, Multidimensional Security Threats, Social Resilience, Non-Military Deterrence

ABSTRACT

This article examines the role of strategic leadership in adapting Indonesia's national defense strategy to multidimensional security threats. Using a qualitative conceptual design and narrative literature review, it synthesizes scholarship on strategic leadership, dynamic capabilities, civil-military relations, hybrid threats, cyber deterrence, collaborative governance, and social resilience. The study develops a model of non-military deterrence in which adaptive strategic leadership functions as the driver, social resilience and legitimacy as the foundation, and multidimensional policy integration as the enabler. Together, these components strengthen decision-making, public trust, cross-sector coordination, policy learning, and systemic resilience. The findings indicate that Indonesia should enhance interoperable coordination, real-time decision support, crisis exercises, digital literacy, strategic communication, and continuous evaluation.

Copyright © 2026, The Author(s).
This is an open access article under the CC–BY-SA license

How to cite: Grahadi, A., Djati, S. P., Joni Widjayanto, Saputro, G. E., & Supriyadi, A. A. (2026). Strategic Leadership and the Adaptation of Indonesia's National Defense Strategy in Addressing Multidimensional Security Threats. *Jurnal Ilmiah Global Education*, *7*(4), 3569–3584. https://doi.org/10.55681/jige.v7i4.6954

INTRODUCTION

Contemporary national security is undergoing a structural transformation characterized by a shift in the nature of threats from conventional to multidimensional. Threats no longer take the form solely of interstate military aggression but increasingly encompass non-military domains, including disinformation, cyberattacks, radicalization, public-health crises, and social fragmentation. This complexity generates an uncertain strategic environment and requires a fundamental change in how states formulate defense strategies. In this context, strategic leadership is a key variable that determines the state's capacity to adapt to evolving threats.

Strategic leadership in defense studies refers not merely to the formal positions occupied by state elites, but to the capacity to interpret environmental change, articulate a long-term vision, and orchestrate cross-sector resources effectively. Modern defense systems demonstrate that public trust, interagency coordination, and the ability to foster social cooperation are essential to sustaining national resilience in complex crises (Bengtsson & Brommesson, 2024). Strategic

leadership must therefore move beyond rigid bureaucratic approaches toward an adaptive model responsive to social, political, and technological change.

Changes in global threat characteristics indicate that contemporary conflict is hybrid, distributed, and nonlinear. Modern threats frequently begin not with open military confrontation, but with information penetration, perception manipulation, attacks on digital systems, and the exploitation of domestic social vulnerabilities. Developments in deterrence theory suggest that modern prevention can no longer rely exclusively on military power; it must incorporate social, psychological, and informational dimensions as components of national strategic capability (Nye, 2017; Taddeo, 2018). Accordingly, national defense strategy must shift from an exclusively hard-power orientation toward a more comprehensive and adaptive approach.

In Indonesia, national security challenges are especially complex because they are shaped by geographical, demographic, institutional, and sociocultural factors. As a large archipelagic state with substantial social heterogeneity, Indonesia is vulnerable to digital disinformation, horizontal conflict, identity polarization, and socioeconomic inequality, all of which can become serious sources of instability. Under such conditions, the effectiveness of the defense system depends heavily on the quality of civil-military relations managed through strong and adaptive strategic leadership capable of balancing civilian control with institutional effectiveness (Mukherjee, 2022). Without leadership that can unify strategic vision and coordination, the state's response to multidimensional threats is likely to remain fragmented.

Modern national security approaches also show that national defense can no longer be narrowly understood as the exclusive responsibility of the military sector. Energy resilience, economic stability, institutional capacity, and social cohesion are integral components of a state's strategic resilience. An effective defense system must therefore incorporate energy, economic, and social dimensions within an integrated national resilience framework (Christensen & Lægreid, 2007; Cutter et al., 2008). Strategic leadership in defense must consequently formulate policy directions that do not separate hard power from soft power, but combine them within a coherent national defense framework.

Social legitimacy is an increasingly important element in defense-strategy adaptation. In an uncertain security environment, the state requires not only coercive capacity but also social acceptance of its policies and institutions. Public compliance is influenced more strongly by perceptions of legitimate authority than by the threat of punishment alone (Tyler, 2006). In defense, social legitimacy provides a foundation for civic participation, compliance with emergency policies, support for security institutions, and the strengthening of citizen-based national resilience. Without public trust, even well-designed defense policies may encounter resistance, apathy, or delegitimation.

Multidimensional threats also require a reorientation of deterrence. Classical deterrence is limited when confronted with cyber threats that are ambiguous, transboundary, and involve multiple actors whose identities are difficult to establish with certainty (Taddeo, 2018). Under these conditions, defense strategy requires a form of non-military deterrence grounded in institutional capacity, social resilience, public literacy, and state credibility in crisis management. Strategic leadership plays a central role in designing policies that generate such deterrent effects because the effectiveness of modern deterrence depends heavily on shaping an adversary's perception that the state's institutions and society are sufficiently resilient to resist disruption.

In addition to social legitimacy, cross-sector collaboration is a critical component of modern defense. Contemporary crises cannot be managed effectively by a single institution.

Responses to multidimensional threats require synergy among government, the military, the private sector, academia, the media, and civil society. Interorganizational cooperation has been shown to strengthen collective capacity to address complex, uncertain, and rapidly evolving crises (Larsson et al., 2023). Strategic leadership must therefore be not only directive but also integrative, capable of building coordination, trust, and a clear division of roles among diverse actors.

Security threats are also becoming increasingly transnational. Terrorism, climate change, pandemics, cybercrime, and cross-border disinformation demonstrate that national security can no longer be fully contained within territorial boundaries. Modern deterrence is closely associated with representation, perception, and the ability of states to establish strategic positions within broader international interactions (Nye, 2017). Strategic leadership in defense must therefore incorporate an external dimension: the capacity to interpret the global environment, build cooperative networks, and translate international geopolitical developments into adaptive national policy.

A sociological approach to defense further supports the argument that society is not merely an object of protection but a principal actor in the construction of national resilience. Public trust in defense and security institutions increases when citizens perceive those institutions as effective, accountable, and aligned with the public interest (Tyler, 2006; Norris et al., 2008). This finding is important because it indicates that national defense resilience is strongly influenced by the quality of state-society relations. Strategic leadership must therefore frame defense as an inclusive national project rather than an agenda confined to state elites.

The evolution of hybrid threats also requires states to reconsider strategic frameworks that conventionally separate internal and external security. Digital disinformation, for example, may originate from foreign actors while operating through domestic social divisions. Cyberattacks on critical infrastructure can directly affect economic stability, public services, and public confidence in the state. Effective strategic leadership must therefore bridge these domains through an integrated and adaptive policy framework.

The dynamics of digital technology have further accelerated changes in the threat landscape. Social media platforms, artificial intelligence, and big data not only create opportunities but also open new avenues for non-state actors to influence national stability. Hoaxes and propaganda can be disseminated rapidly and at scale, requiring responses that are social as well as technical. Digital literacy and the public's ability to evaluate information must therefore be treated as integral components of defense strategy. Strategic leadership must promote the integration of education, public communication, and information-security policies within a unified defense framework.

Global experience also shows that states with high levels of social trust tend to be more resilient during crises. This was evident during pandemic responses, when public compliance was strongly influenced by trust in government and public institutions. Building trust is therefore not merely a social issue; it is a long-term component of national defense strategy.

In this context, strategic leadership must cultivate governance that is transparent, accountable, and inclusive. Policies must respond to societal needs while safeguarding national stability. This approach requires a paradigm shift from top-down leadership toward participatory and collaborative leadership.

The foregoing discussion indicates that Indonesia's adaptation of its national defense strategy to multidimensional security threats is inseparable from the quality of strategic

leadership. Adaptive, integrative, and socially legitimate leadership is essential to building a resilient defense system in an era of non-traditional threats. This article systematically examines the role of strategic leadership in adapting Indonesia's national defense strategy and develops a conceptual model that integrates military and non-military dimensions within a contemporary national security framework.

The article positions strategic leadership at the center of an analytical relationship linking threat dynamics, defense policy, and the state's social capacity to manage global uncertainty. Strategic leadership is understood not simply as an individual leader's competence, but as an institutional capacity to establish strategic direction, build consensus, and ensure effective policy implementation amid a complex security environment. This perspective is important because failures to integrate military and non-military dimensions often produce policy responses that are partial, reactive, and unsustainable.

This article also seeks to address a gap in defense literature that continues to separate hard-power and soft-power approaches. In contemporary practice, these approaches cannot be treated as a dichotomy; they must be combined within a holistic strategic framework. Multidimensional threats require states to manage military capability while simultaneously building social resilience, strengthening political legitimacy, and enhancing institutional adaptability. The principal contribution of this article is therefore the formulation of a conceptual framework that explains the relationship between strategic leadership and defense-strategy adaptation in an evolving threat environment.

It is also important to emphasize that the success of defense strategy depends not only on the quality of planning but also on effective implementation. Many states struggle to bridge the gap between centrally formulated policy and operational realities. Strategic leadership serves as the principal driver that translates strategic vision into coordinated action. This role includes the ability to communicate effectively, manage interagency conflicts of interest, and establish mechanisms for continuous evaluation.

Accordingly, the analysis is not merely descriptive; it seeks to generate a conceptual contribution relevant to the development of defense studies in Indonesia. The article is expected to provide a more comprehensive understanding of the importance of strategic leadership in addressing multidimensional threats while offering a new perspective for formulating more adaptive, inclusive, and sustainable defense strategies. Ultimately, strengthening strategic leadership is a prerequisite for a national defense system that is not only militarily capable but also socially and institutionally resilient in confronting future security challenges.

METHODS

This article employs a qualitative conceptual research design using a narrative literature review. This approach was selected to integrate diverse theoretical perspectives across the literature on strategic leadership, dynamic capabilities, civil-military relations, hybrid threats, cyber deterrence, collaborative governance, and social resilience. The literature review is treated as a research method for developing conceptual synthesis, identifying patterns of relationships among concepts, and formulating an agenda for theory development (Snyder, 2019; Torraco, 2016).

Sources were purposively selected according to three criteria: direct relevance to the article's focus, theoretical contribution to explaining defense adaptation, and the traceability of scholarly publication. The material analyzed comprised journal articles and academic works

addressing strategic leadership, organizational learning, resilience, legitimacy, cross-sector collaboration, cybersecurity, and hybrid conflict. Foundational literature was used to establish the conceptual basis, while more recent publications were used to interpret developments in threat dynamics and defense governance.

The analysis was conducted in four stages. First, each source was reviewed to identify relevant concepts, arguments, and findings. Second, the information was grouped into themes: strategic leadership, multidimensional threats, strategy adaptation, legitimacy and social resilience, and policy integration. Third, relationships among themes were compared and synthesized using thematic-analysis principles to identify recurring patterns and explanatory relationships (Braun & Clarke, 2006). Fourth, the synthesis was translated into a strategic-leadership-based model of non-military deterrence and its policy implications.

Conceptual validity was maintained through cross-literature comparison, consistency between propositions and supporting sources, and examination of the relationship between theoretical dimensions and the Indonesian defense context. Because the study does not employ field data, its findings are positioned as a conceptual model requiring empirical testing through interviews, surveys, case studies, simulations, or mixed methods in future research.

RESULTS AND DISCUSSION

1. Conceptualizing Strategic Leadership in Defense.

In the context of national defense, strategic leadership is the capacity to direct, align, and integrate multiple instruments of national power in response to continuously evolving threats. It extends beyond elite-level decision-making to include the ability to articulate a long-term vision, establish cross-sector coordination, and ensure effective policy implementation. In modern defense literature, strategic leadership is understood as a dynamic process involving interactions among state actors, institutions, and society in responding to complex security environments (Bengtsson & Brommesson, 2024; Boal & Hooijberg, 2001; Ireland & Hitt, 2005).

Strategic leadership emphasizes sensemaking: the capacity of leaders to interpret ambiguous and complex changes in the strategic environment. In defense, sensemaking is critical because threats often do not appear in readily identifiable forms but are embedded in social and technological dynamics (Day & Schoemaker, 2006). Strategic leaders must integrate dispersed information, develop a shared understanding, and convert it into operational policy direction. This process requires advanced cognitive capacity, rapid information processing, and strategic communication capable of aligning diverse actors.

The concept of dynamic capabilities offers a strong theoretical framework for understanding the role of strategic leadership. Teece (2018) identifies three principal capabilities of adaptive organizations: sensing, seizing, and transforming. In defense, sensing refers to the early detection of threats through integrated multidomain intelligence; seizing concerns rapid response through cross-sector resource mobilization; and transforming involves structural changes in doctrine, organization, and defense governance. These capabilities are interdependent, iterative, and highly contingent on the quality of strategic leadership.

Strategic leadership is also closely linked to the capacity to manage uncertainty. Modern security environments are characterized by volatility, uncertainty, complexity, and ambiguity. Under such conditions, leaders cannot depend on linear planning. They instead require scenario-based approaches, policy experimentation, and rapid learning. Effective strategic leadership

balances exploration—the search for new options—with exploitation—the optimization of existing capabilities—in decision-making (March, 1991).

Beyond its cognitive and adaptive dimensions, strategic leadership also has a relational dimension. Leaders must build interagency trust, strengthen coordination, and reduce bureaucratic friction. In defense, cross-sector coordination encompasses the military, intelligence, cybersecurity, public communication, and economic sectors. Without strong relational capability, formulated strategies are unlikely to be implemented effectively.

The institutional dimension likewise shapes the effectiveness of strategic leadership. Leaders do not operate in a vacuum, but within institutions characterized by specific rules, cultures, and structures. Leadership success therefore depends on the ability both to leverage and transform institutions. The institutional-leadership perspective emphasizes the leader's role in shaping norms, incentives, and working mechanisms that support strategic adaptation.

Strategic leadership in defense also has a legitimacy dimension. Defense policies frequently involve the mobilization of substantial resources and, in some cases, restrictions on civil liberties. Leaders must therefore build legitimacy through transparency, accountability, and effective public communication. Legitimacy strengthens voluntary compliance and increases policy effectiveness without excessive dependence on coercion.

Finally, strategic leadership must be understood as a collective process. In modern defense systems, strategic decisions are rarely made by a single individual; rather, they emerge from interactions among multiple actors within policy networks. Strategic leadership therefore includes the capacity to govern networks, facilitate collaboration, and align objectives across actors.

Strategic leadership in defense thus encompasses cognitive, adaptive, relational, institutional, and legitimacy dimensions. The integration of these five dimensions determines a state's capacity to respond to multidimensional threats effectively and sustainably.

2. The Dynamics of Multidimensional Security Threats.

Multidimensional security threats reflect a fundamental paradigm shift in contemporary security studies. Traditional approaches centered on interstate military threats are no longer sufficient to explain the complexity of modern insecurity. Threats are no longer singular or isolated; instead, they arise from simultaneous interactions among military, economic, social, technological, and informational domains. These interconnections create a nonlinear threat landscape that is difficult to predict and often ambiguous with respect to actor identification and impact.

Hybrid warfare provides a central analytical framework for understanding these dynamics. It refers to the integrated use of military and non-military instruments to achieve strategic objectives without necessarily triggering open conflict. Actors conducting hybrid warfare exploit gaps in international law, domestic vulnerabilities, and the gray zone between war and peace (Rid, 2018; Lindsay, 2015). This strategy enables them to generate strategic effects at relatively low cost while controlling the risk of escalation.

A defining feature of multidimensional threats is their capacity to exploit systemic interdependence. An attack on a digital financial system, for example, may undermine economic stability, which can subsequently trigger social dissatisfaction and political instability. Threats are therefore no longer confined to a single sector but can produce extensive cascading effects.

Cyber threats are among the fastest-growing security dimensions of the past decade. State dependence on digital infrastructure has created a broad and complex attack surface. Energy, transportation, communication, and financial systems all rely on digital technologies vulnerable

to cyberattack. Such attacks may be conducted by state or non-state actors with a high degree of anonymity, complicating attribution and policy response (Nye, 2017; Taddeo, 2018).

Beyond their technical consequences, cyber threats also have strategic implications. Attacks on critical infrastructure can paralyze state functions, generate public panic, and erode trust in government. Cybersecurity is therefore not merely a technical issue but a political and social concern that requires a cross-sector approach.

Digital disinformation has likewise become a strategic instrument in modern conflict. False or misleading information can significantly influence public opinion. Social-media algorithms accelerate the circulation of unverified content, increasing the risk of large-scale information manipulation. Disinformation can intensify political polarization, weaken governmental legitimacy, and undermine trust in public institutions (Vosoughi et al., 2018; Tucker et al., 2018).

Disinformation is often systematically engineered through coordinated information operations. Actors employ bots, fabricated accounts, and microtargeting techniques to influence particular groups within society. Information threats have thus evolved into a sophisticated and structured form of warfare.

The social dimension of security threats has also become more prominent. Social inequality, identity conflict, and political polarization can become major sources of internal instability. Cederman et al. (2015) demonstrate that horizontal inequalities among social groups can increase the risk of conflict, while Norris et al. (2008) emphasize community resilience as an important capacity for managing both external and internal pressures.

Social threats are often intensified by economic factors. Economic inequality, unemployment, and inequitable resource distribution can create conditions susceptible to conflict. External actors may exploit these domestic tensions to advance their strategic objectives.

Globalization increases the complexity of threats through interdependence among states. Accelerating flows of goods, services, information, and people create both opportunities and vulnerabilities. Global crises such as the COVID-19 pandemic demonstrate how a public-health threat can rapidly develop into an economic and political crisis with global consequences.

Climate change is also an increasingly relevant non-traditional threat. Its consequences—including natural disasters, water scarcity, and forced migration—can generate regional instability and increase the risk of conflict. Environmental security must therefore be regarded as an integral component of national security.

Non-state actors also play an increasingly significant role in multidimensional threat dynamics. Terrorist groups, transnational criminal organizations, and even individuals with advanced technological capabilities can constitute serious threats. This development indicates that the state's monopoly over the use of force is increasingly contested.

The dynamics of multidimensional security threats therefore require a fundamental change in how states understand and address insecurity. Fragmented sectoral approaches are no longer effective. A systemic approach is required to integrate multiple threat dimensions within a unified analytical and policy framework.

3. Adaptation of National Defense Strategy.

Defense-strategy adaptation is a systemic response to the increasingly complex, dynamic, and cross-domain nature of threats. Modern defense strategy can no longer rely on assumptions of environmental stability or actor predictability. It must instead be designed to operate under conditions of high uncertainty, rapid change, and systemic interdependence. Farrell (2010)

emphasizes that military innovation and organizational learning are essential because organizations that learn more rapidly gain a strategic advantage.

The adaptive-strategy approach places flexibility at its core. Flexibility involves not only the ability to revise plans but also the capacity to design systems that are inherently prepared to adapt. Strategy is thus understood as a continuous process rather than a static product. March (1991) argues that organizations must balance exploration and exploitation: exploration concerns the pursuit of new ideas, technologies, and approaches, whereas exploitation concerns the optimization of existing capabilities. In defense, this balance is necessary to sustain operational effectiveness while avoiding technological and conceptual stagnation.

Defense-strategy adaptation also requires strong sensing capability. States must identify changes in the strategic environment at an early stage through integrated multidomain intelligence. This involves the simultaneous analysis of military, cyber, economic, and social threats. The resulting data and information must then be converted into strategic insight for decision-making. This capability depends heavily on the quality of intelligence systems and interagency coordination.

The next stage is seizing—the capacity to respond to change rapidly and appropriately. In defense, this includes resource mobilization, doctrinal adjustment, and effective decision-making under pressure. Speed is critical because delayed responses can amplify the effects of threats. Decision-making systems should therefore be designed to minimize bureaucratic obstacles that impede timely action.

Transforming represents a subsequent stage of strategic adaptation. At this stage, the state undertakes structural changes to sustain adaptive capacity. Transformation may include organizational reform, doctrinal renewal, and investment in emerging technologies. It is not a temporary adjustment but a continuous, long-term process.

Civil-military integration is a critical element of adaptive strategy. Brooks (2016) shows that collaboration between civilian and military sectors improves the effectiveness of crisis response. In the context of multidimensional threats, such integration extends to cooperation with the technology, communication, health, and economic sectors. A whole-of-government approach ensures coordinated action across state institutions, while a whole-of-society approach engages citizens and social actors in safeguarding national security (Christensen & Lægreid, 2007).

Defense-strategy adaptation also requires changes in policy design. Policies can no longer remain rigid and long-term without review; they must be designed as adaptive instruments that can be periodically revised through evaluation and learning. Dunlop (2017) identifies policy learning as an important mechanism for improving effectiveness. Through policy learning, states can identify weaknesses, refine strategies, and avoid repeating past failures.

Data-driven approaches are another important element of defense adaptation. Big data and analytics enable states to identify threat patterns with greater precision. Data can support crisis forecasting, vulnerability assessment, and policy evaluation, thereby improving decision quality and reducing uncertainty.

Organizational culture also plays an important role in strategy adaptation. Rigid and highly hierarchical organizations often struggle to respond to change. A culture that supports innovation, learning, and collaboration is therefore essential. Strategic leaders help shape such a culture through open and inclusive leadership.

Risk management is equally important. Modern defense strategy must manage risk proactively through risk identification, impact analysis, and the development of effective

mitigation measures. This approach enables the state not only to react to threats but also to anticipate them and minimize their consequences.

Adaptation of national defense strategy is therefore a multidimensional process involving innovation, learning, integration, and transformation. An adaptive strategy enables the state to remain relevant amid evolving threats and to enhance the effectiveness of national-security protection.

4. The Role of Social Legitimacy and Social Resilience.

Social legitimacy is a key determinant of defense-strategy effectiveness because it shapes the extent to which state policies are accepted, obeyed, and supported by the public. In uncertain modern security environments, compliance based primarily on coercion is not sustainable. Tyler (2006) shows that legitimacy promotes non-coercive compliance through perceptions of procedural fairness, trust, and rightful authority. When citizens perceive state institutions as fair, transparent, and accountable, they are more likely to comply with policy even during crises. In defense, this affects successful resource mobilization, adherence to emergency protocols, and support for security operations.

Social legitimacy is not created instantaneously; it develops over time through policy consistency, the quality of public services, and effective communication. Public trust in state institutions is the principal foundation of legitimacy and is shaped by perceptions of institutional performance, integrity, and competence. Defense strategy must therefore incorporate governance dimensions, including transparent decision-making, policy accountability, and public participation in policy formulation.

Alongside legitimacy, social resilience is a central pillar in addressing multidimensional threats. It refers to society's capacity to absorb shocks, adapt to change, and recover rapidly from crises. Adger (2000) and Folke (2006) emphasize that adaptive social systems are better able to withstand external and internal pressures. In defense, social resilience strengthens resistance to disinformation, internal conflict, and external pressure.

Social cohesion and solidarity are core elements of social resilience. Social cohesion refers to the degree of connectedness and trust among members of society, while solidarity refers to their willingness to support one another during crises. Societies with high levels of cohesion are generally better able to maintain stability and reduce conflict risk. Fragmented societies, by contrast, are more vulnerable to manipulation and provocation.

Social resilience is also influenced by economic conditions and inequality. High levels of inequality can erode social cohesion and increase the potential for conflict. Defense policy must therefore incorporate welfare considerations as part of security strategy. This perspective affirms that security concerns not only protection from external threats but also the strengthening of domestic social structures.

In the digital era, digital literacy is a critical component of social resilience. Guess et al. (2020) show that digital education can reduce the impact of disinformation by strengthening citizens' ability to evaluate information. Digital literacy includes the ability to assess sources, recognize bias, and verify content. In the context of information threats, it functions as a community-based first line of defense.

Digital literacy extends beyond individuals to the broader information ecosystem. Media platforms, content-distribution algorithms, and regulatory frameworks all shape the information environment. Defense strategy must therefore incorporate proactive, transparent, and data-informed public communication policies to counter disinformation effectively.

Collaborative relationships between the state and society are essential to building legitimacy and social resilience. Ansell and Gash (2008) demonstrate that collaborative governance improves policy effectiveness by involving non-state actors in decision-making. Such collaboration fosters a sense of ownership over policy, thereby strengthening legitimacy and compliance.

In practice, collaborative approaches can be implemented through partnerships among government, the private sector, academia, and civil society. Each actor contributes to social resilience through education, innovation, or resource provision. Collaboration also facilitates faster and more accurate information exchange, improving the quality of crisis response.

Effective public communication is another important instrument for building legitimacy and social resilience. Clear, consistent, and evidence-based communication can increase public trust and reduce uncertainty. Conversely, opaque or contradictory communication can erode legitimacy and amplify the risk of disinformation.

Strategic leadership is crucial in this context. Leaders must construct credible narratives, reconcile the interests of diverse actors, and ensure policy consistency. Communicative and inclusive leadership can strengthen legitimacy and enhance the effectiveness of defense strategy.

Social legitimacy and social resilience are therefore not merely supporting factors but core components of modern defense strategy. Integrating both dimensions into defense policy will strengthen the state's capacity to withstand multidimensional threats and improve the effectiveness of crisis response.

5. A Strategic-Leadership-Based Model of Non-Military Deterrence.

The conceptual model proposed in this article integrates three principal components: adaptive strategic leadership, social resilience and legitimacy, and multidimensional policy integration. These components form an interactive and mutually reinforcing system that generates credible and sustainable non-military deterrence. The model conceptualizes deterrence not solely as a function of military capability but as the outcome of cross-domain orchestration that shapes an adversary's perception of the resilience of the state system.

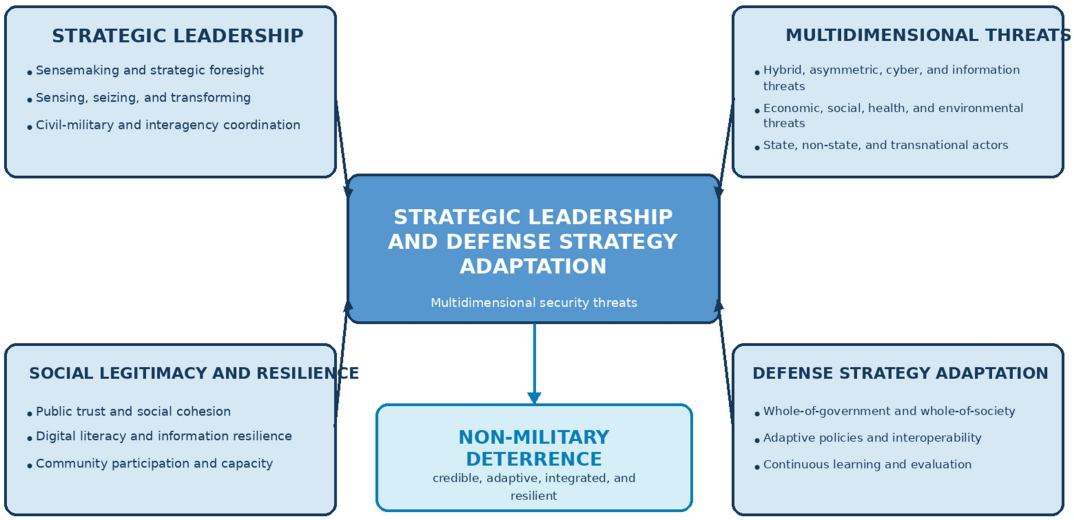


Figure 1. Analytical framework of strategic leadership and defense-strategy adaptation

Adaptive strategic leadership functions as the principal driver that orchestrates sensing, seizing, and transforming. During sensing, leaders consolidate multisource intelligence—military, cyber, social, and economic—through an integrated analytical center to identify weak signals, trends, and anomalies. During seizing, they rapidly activate cross-sector policies through integrated coordination mechanisms, including crisis protocols, emergency budgeting, and interagency tasking. During transforming, they promote structural changes in doctrine, organization, and governance to align the defense system with emerging threat characteristics. This process is cyclical, iterative, and learning-based.

To strengthen this driver function, strategic leadership requires supporting infrastructure, including data-driven decision-support systems, real-time situational dashboards, and rapid decision-making mechanisms that minimize bureaucratic bottlenecks. Leadership competencies must also encompass scenario planning, risk-based decision-making, and strategic communication across stakeholder groups.

Social resilience and legitimacy function as the model's foundation. This dimension includes public trust, social cohesion, digital literacy, and community capacity to absorb shocks and recover rapidly. Legitimacy encourages non-coercive compliance, reduces enforcement costs, and improves the effectiveness of crisis response. Within the deterrence framework, legitimacy creates the perception that society is resistant to provocation and that state institutions are credible. This perception is critical because many contemporary threats seek to divide society before targeting formal institutions.

This foundation is strengthened by policy consistency, transparency, and public participation in policy processes. Practical interventions include national digital-literacy programs, evidence-based communication campaigns, and the strengthening of local community networks as social first responders. Social resilience is also supported by equitable resource distribution and access to public services, which reduce vulnerability to exploitation by external actors.

Multidimensional policy integration functions as an enabler that unifies military and non-military instruments within a single policy architecture. It is operationalized through whole-of-government and whole-of-society approaches, supported by data-interoperability standards, interministerial coordination procedures, and consistent public communication platforms. Integration ensures that the state's response is not fragmented and can operate synchronously across domains.

Operationally, this enabling mechanism requires a clear governance architecture consisting of: (1) a cross-sector command center; (2) secure and rapid data-sharing protocols; (3) system-interoperability standards; and (4) decision-escalation mechanisms. A regulatory framework is also required to enable collaboration with the private sector and civil society, particularly in the cyber and information domains.

The model can be represented as a closed cycle: strategic leadership directs policy integration; policy integration strengthens social resilience; social resilience increases deterrence credibility; and credible deterrence, in turn, reinforces strategic leadership in managing threats. This reinforcing loop increases the resilience of the defense system. It also produces a psychological deterrent effect by leading adversaries to assess the costs of intervention as greater than its potential benefits.

To improve implementation precision, the model requires key performance indicators (KPIs) for each component. Strategic-leadership indicators include decision-making speed, the

quality of cross-sector coordination, and organizational adaptability. Social-resilience indicators include public-trust levels, digital-literacy indices, social cohesion, and community-response capacity. Policy-integration indicators include data interoperability, interagency response time, consistency of public communication, and cross-sector compliance.

In addition to KPIs, the model requires data-driven monitoring and evaluation that combines quantitative and qualitative indicators. Post-crisis audits, periodic tabletop exercises, and system stress tests are important instruments for assessing readiness and identifying gaps.

The model is also compatible with policy-learning frameworks. Each crisis cycle generates feedback that can be used to improve doctrine, procedures, and institutional design. Learning may be single-loop, involving procedural correction, or double-loop, involving changes in assumptions and paradigms. Non-military deterrence is therefore not static; it evolves through experience and collective learning.

The model also accounts for risk and limitations. Major risks include fragmented coordination, information overload, and organizational resistance to change. Implementation design should therefore incorporate mitigation strategies such as streamlined decision pathways, data prioritization, and incentives for cross-sector collaboration.

Finally, the model provides a framework that can be operationalized through a phased roadmap: an initial stage focused on developing foundations and standards; an intermediate stage centered on system integration and capacity enhancement; and an advanced stage devoted to optimization and continuous learning. This phased approach supports implementation sustainability and reduces the risk of systemic failure.

Table 1. Operational components of the non-military deterrence model

Component	Function	Key elements	Performance indicators
Adaptive strategic leadership	Driver	Sensing, seizing, transforming; foresight; rapid decision-making	Decision speed; coordination quality; adaptive capacity
Social resilience and legitimacy	Foundation	Public trust; social cohesion; digital literacy; community capacity	Trust index; digital literacy; cohesion; community preparedness
Multidimensional policy integration	Enabler	Whole-of-government; whole-of-society; interoperability; public communication	Data interoperability; response time; communication consistency; cross-sector compliance

6. Strategic Implications and Model Strengthening.

The first implication is the need to establish an integrated national coordination architecture as the backbone of responses to multidimensional threats. The government should establish a cross-sector national coordination center linking defense, cybersecurity, public communication, intelligence, and crisis management within a unified system. This architecture should be supported by real-time data-sharing protocols, interagency interoperability, and an integrated analytical platform for data-informed decision-making. Clear lines of authority and decision-escalation mechanisms are also necessary to prevent overlapping mandates from delaying response.

The second implication is the strengthening of strategic-leadership capacity through the development of key competencies such as sensemaking, foresight, and decision-making under high uncertainty. Leadership-development programs should be competency-based, emphasizing cross-domain analysis, scenario planning, adaptive leadership, and crisis management. In addition to formal training, experiential learning mechanisms such as crisis simulations, war games, and cross-sector exercises are required. Cross-institutional rotations can also broaden leaders' perspectives and enhance their coordination capacity within complex systems.

The third implication is systematic investment in social resilience as the foundation of non-military defense. The state should expand national digital-literacy programs, improve the quality of public communication through transparency and speed, and strengthen the capacity of local communities as first actors in crisis response. These interventions should be supported by inclusive policies that reduce social inequality and strengthen cohesion. Society would thereby become not merely an object of protection but an active subject within the national defense system.

The fourth implication is policy reform toward multidimensional integration. Defense planning should be aligned with economic, energy, health, and technology policies within a unified strategic framework. This requires cross-sector planning based on risk assessment and scenario analysis. Budgeting should also move toward performance-based arrangements linking cross-sector outputs to national-security outcomes, thereby improving resource-use efficiency and effectiveness.

The fifth implication is the continuous strengthening of evaluation and policy-learning mechanisms. Every crisis response should be followed by a policy audit, indicator-based performance evaluation, and the revision of doctrine and procedures. This approach enables the defense system to learn continuously and adapt to evolving threats. A knowledge-management system should also document experience and best practices for use in future decision-making.

The sixth implication is the strengthening of the technology and innovation ecosystem in defense. The state should promote collaboration with the private sector, technology start-ups, and research institutions to develop innovative solutions in cybersecurity, data analytics, and early-warning systems. Investment in technology not only improves technical capacity but also strengthens the state's strategic competitiveness in confronting global threats.

The seventh implication is to strengthen strategic communication as an instrument of defense. The state must be able to construct consistent, credible, and fact-based narratives to sustain public trust and counter disinformation. Strategic communication should be designed as an integral component of defense policy rather than an auxiliary function.

In conclusion to the discussion, the effectiveness of modern defense strategy depends greatly on a state's ability to integrate strategic leadership, social resilience, and multidimensional policy within a coherent framework. These elements are interdependent and mutually reinforcing in producing an adaptive and resilient defense system. A state capable of building cross-sector coordination, strengthening public legitimacy, and developing continuous policy-learning capacity will possess a strategic advantage in addressing complex threats. Strengthening the non-military dimension of defense is therefore no longer optional, but a strategic necessity in the contemporary security environment.

CONCLUSION

Strategic leadership plays a fundamental role in determining the direction and effectiveness of national defense strategy in an era of multidimensional threats. The increasingly complex, dynamic, and unpredictable character of threats requires a fundamental transformation in national defense. An approach once centered primarily on military power must evolve into a multidimensional framework that integrates social, economic, technological, and institutional dimensions. This shift requires a systemic understanding of security as the outcome of cross-sector interaction rather than solely a product of military superiority.

The analysis demonstrates that strategic leadership functions not only as a decision-making authority but also as a central actor in adapting the defense system. Effective leadership identifies changes in the strategic environment, anticipates threats, and formulates adaptive and sustainable policies. Strategic leadership thereby connects policy vision with implementation in the field. This role includes aligning cross-sector actors, managing uncertainty, and ensuring consistency between strategic objectives and operational action.

The dynamics of multidimensional threats also confirm that national security cannot be separated from the social condition of the population. Disinformation, social conflict, and global crises demonstrate that national stability depends heavily on social strength and institutional legitimacy. Defense strategy must therefore build public trust, strengthen social cohesion, and enhance citizens' capacity to resist information manipulation. Without a strong social foundation, defense policy risks losing both effectiveness and public support.

The conceptual model developed in this article contributes to the advancement of defense studies by demonstrating that modern deterrence depends not only on military power but also on the state's capacity to build legitimacy and social resilience. The interaction of strategic leadership, social resilience, and policy integration creates a more adaptive and resilient defense system. The model also highlights the importance of a continuous approach in which policy learning and evaluation are integral to strategic adaptation.

The model has theoretical implications because it extends deterrence into the non-military domain and integrates strategic-leadership and social-resilience theories within a single analytical framework. Practically, it guides policymakers in designing more holistic, responsive, and cross-sector collaborative defense strategies. This is particularly relevant in a global environment characterized by high uncertainty and complexity.

The practical implications indicate that the state must develop strategic-leadership capacity capable of bridging sectors and interests. Defense policy should be designed holistically and grounded in cross-sector collaboration. This approach will improve the effectiveness of defense strategy in addressing multidimensional threats. The state should also strengthen coordination mechanisms, increase investment in technology and human resources, and establish adaptive evaluation systems.

The success of defense strategy is determined not only by state capacity but also by the quality of state-society relations. Strengthening legitimacy and public participation must therefore be integral to defense strategy. This approach will produce a defense system that is structurally strong and socially resilient.

Strengthening strategic leadership is therefore a principal prerequisite for building a resilient defense system. Without adaptive, integrative, and legitimacy-based leadership, defense strategy will struggle to achieve optimal effectiveness. This article is expected to contribute theoretically and practically to the development of defense strategies more relevant to contemporary security challenges and to provide a foundation for further research on multidimensional defense.

REFERENCES

Adger, W. N. (2000). Social and ecological resilience: Are they related? Progress in Human Geography, 24(3), 347–364.

Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. Journal of Public Administration Research and Theory, 18(4), 543–571.

Bengtsson, R., & Brommesson, D. (2024). Trust and security in complex governance systems. Cooperation and Conflict. Advance online publication.

Boal, K. B., & Hooijberg, R. (2001). Strategic leadership research: Moving on. The Leadership Quarterly, 11(4), 515–549.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101.

Brooks, R. A. (2016). Civil-military relations and military effectiveness: Past, present, and future. Annual Review of Political Science, 19, 1–19.

Cederman, L.-E., Weidmann, N. B., & Gleditsch, K. S. (2015). Horizontal inequalities and civil conflict: A global comparison. American Political Science Review, 105(3), 478–495.

Christensen, T., & Lægreid, P. (2007). The whole-of-government approach to public sector reform. Public Administration Review, 67(6), 1059–1066.

Cutter, S. L., Burton, C. G., & Emrich, C. T. (2008). Disaster resilience indicators for benchmarking baseline conditions. Journal of Homeland Security and Emergency Management, 5(1), Article 51.

Day, G. S., & Schoemaker, P. J. H. (2006). Peripheral vision: Detecting weak signals that will make or break organizations. Harvard Business Review, 84(11), 117–124.

Dunlop, C. A. (2017). Policy learning and policy failure. Policy & Politics, 45(1), 3–20.

Farrell, T. (2010). Military adaptation in war: Learning from experience. Journal of Strategic Studies, 33(4), 567–594.

Folke, C. (2006). Resilience: The emergence of a perspective for social-ecological systems analysis. Global Environmental Change, 16(3), 253–267.

Guess, A. M., Nyhan, B., & Reifler, J. (2020). Exposure to misinformation in digital environments. Nature Human Behaviour, 4(5), 472–480.

Hall, P. A. (1993). Policy paradigms, social learning, and the state. Comparative Politics, 25(3), 275–296.

Ireland, R. D., & Hitt, M. A. (2005). Achieving strategic competitiveness through leadership. Academy of Management Executive, 19(4), 63–77.

Larsson, G., Alvinius, A., Bakken, B., & Hœrem, T. (2023). Inter-organizational collaboration in total defence systems. International Journal of Organizational Analysis, 31(3), 693–709.

Lindsay, J. R. (2015). Cybersecurity and state conflict dynamics. International Security, 39(3), 7–47.

March, J. G. (1991). Exploration and exploitation in organizational learning. Organization Science, 2(1), 71–87.

Mukherjee, A. (2022). Civil-military relations in emerging democracies. Journal of Strategic Studies, 45(6–7), 820–842.

Norris, F. H., Stevens, S. P., Pfefferbaum, B., Wyche, K. F., & Pfefferbaum, R. L. (2008). Community resilience as a strategic capacity. American Journal of Community Psychology, 41(1–2), 127–150.

Nye, J. S., Jr. (2017). Deterrence and dissuasion in cyberspace. International Security, 41(3), 44–71.

Rid, T. (2018). Rethinking cyber conflict. Journal of Strategic Studies, 41(1–2), 5–32.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333–339.

Taddeo, M. (2018). Cyber deterrence theory and practice. Philosophy & Technology, 31(3), 339–355.

Teece, D. J. (2018). Dynamic capabilities and strategic management. Long Range Planning, 51(1), 40–49.

Torraco, R. J. (2016). Writing integrative literature reviews: Using the past and present to explore the future. Human Resource Development Review, 15(4), 404–428.

Tucker, J. A., Guess, A., Barbera, P., Vaccari, C., Siegel, A., Sanovich, S., Stukal, D., & Nyhan, B. (2018). Social media and political polarization. Political Science Quarterly, 133(2), 1–32.

Tyler, T. R. (2006). Psychological perspectives on legitimacy and compliance. Annual Review of Psychology, 57, 375–400.

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of misinformation online. Science, 359(6380), 1146–1151.