Integrating Risk Intelligence into Defense Policy: A Strategic Risk Management Approach

Aris Sarjito
Fakultas Manajemen Pertahanan, Universitas Pertahanan Republik Indonesia, Indonesia
*E-mail: arissarjito@gmail.com

Abstract

The increasing complexity and unpredictability of global threats, including cyberattacks and hybrid warfare, necessitate the integration of risk intelligence into defense policy frameworks. Risk intelligence, a proactive tool for anticipating and mitigating risks, plays a crucial role in enhancing situational awareness, resource optimization, and decision-making in defense strategies. This research aims to explore the integration of risk intelligence into defense policies through a strategic risk management approach, highlighting its importance, challenges, and practical implementation. A qualitative methodology was adopted, utilizing secondary data from government policy documents, international defense reports, and scholarly articles. Findings reveal that while risk intelligence enhances preparedness and adaptability in defense policies, its implementation faces barriers such as technological limitations, data silos, and resistance to change. Enablers include advancements in artificial intelligence, inter-agency collaboration, and structured policy frameworks. The study concludes that integrating risk intelligence into defense policies requires establishing dedicated units, investing in technology and training, and fostering international partnerships to share intelligence. These measures can bridge existing gaps, ensuring defense policies are resilient and proactive in managing contemporary and emerging threats.

Keywords : *cybersecurity, defense policy, hybrid threats, risk intelligence, strategic risk management*

1. INTRODUCTION

Risk intelligence plays a pivotal role in anticipating and mitigating potential threats by enabling the collection, analysis, and application of data, especially in dynamic environments. In defense policy, this capability is increasingly vital due to the complex challenges nations face, requiring informed and strategic decision-making (Evans, 2015). Theoretical perspectives emphasize that risk intelligence supports defence organizations in understanding risks, prioritizing resources, and improving operational readiness (Craparo et al., 2018; Evans, 2015).

Advancements in data analytics and artificial intelligence have significantly expanded the potential applications of risk intelligence within defense strategies. These technologies provide

sophisticated tools to address both traditional and non-traditional security threats, further enhancing the adaptability of defense systems (Johnson, 2021). Experts argue that the integration of AI-driven analytics into risk intelligence processes can optimize resource allocation and strategic planning (MBN, n.d.; Metricstream, 2024).

In the context of defense policies, risk intelligence has become increasingly vital as nations face complex challenges that require informed decision-making (Evans, 2015). It enables defense organizations to better understand the nature of risks, prioritize resources, and enhance operational readiness (Craparo et al., 2018; Evans, 2015). With advancements in data analytics and artificial intelligence, the potential for leveraging risk intelligence in defense strategies has grown significantly, offering tools to address both traditional and non-traditional threats (J. Johnson, 2021).

Strategic risk management integrates risk intelligence into a cohesive framework that aligns with long-term defense objectives (Mızrak, 2023). It is particularly crucial in addressing contemporary threats such as cyberattacks, which can undermine critical infrastructure, and geopolitical instability, which can disrupt international alliances and global security. By employing strategic risk management, defense policies can proactively mitigate risks rather than respond reactively, thereby reducing vulnerabilities and ensuring national security (Dhlamini, 2022; Ige et al., 2024). The increasing frequency and complexity of hybrid threats further underscore the necessity of robust risk management frameworks in defense planning (Käihkö, 2021).

Despite the growing recognition of its importance, many defense policies lack the systematic integration of risk intelligence (Dorn, 2007; KOUKAKIS, 2024). Existing frameworks often focus on immediate tactical responses rather than long-term strategic preparation, leaving critical gaps in the ability to anticipate and adapt to emerging risks (Dieperink et al., 2016). Furthermore, challenges such as technological limitations, inter-agency coordination issues, and insufficient investment in risk intelligence tools hinder effective implementation (Abinesh Kamal & Divya, 2024). These gaps highlight the urgent need for a structured approach to incorporate comprehensive risk intelligence systems into defense policies.

Defense policymakers are increasingly confronted with the challenge of managing risks that are both complex and unpredictable. These risks often stem from hybrid threats, which combine traditional and non-traditional elements such as cyberattacks, disinformation campaigns, and

economic coercion. The interconnected nature of global systems amplifies the impact of such threats, making it difficult to predict and mitigate their effects (Käihkö, 2021). Furthermore, rapid technological advancements and the evolving geopolitical landscape add layers of uncertainty, requiring policymakers to anticipate risks in dynamic and volatile environments (J. Johnson, 2021). The inability to accurately forecast and respond to these multifaceted risks can compromise national security and destabilize defense strategies.

Despite the growing relevance of risk intelligence, its systematic integration into defense decision-making frameworks remains insufficient. Many existing policies are reactive rather than proactive, focusing on immediate responses rather than long-term strategic planning (Dieperink et al., 2016). This gap is further exacerbated by siloed approaches within defense institutions, where information and resources are not effectively shared or utilized to form a cohesive risk management strategy (Abinesh Kamal & Divya, 2024; Mandel & Irwin, 2021). Moreover, limited investment in advanced analytics and data-driven tools has hindered the ability to transform raw data into actionable insights, leaving decision-makers ill-equipped to address emerging risks comprehensively (Dhlamini, 2022; Ige et al., 2024). Addressing these shortcomings requires a structured and integrated approach to embedding risk intelligence in defense policy frameworks.

This research aims to explore how risk intelligence can be effectively integrated into defense policies by investigating methods, tools, and processes that bridge the gap between risk intelligence capabilities and defense strategies. It seeks to identify best practices, challenges, and enabling factors that ensure a comprehensive approach to managing risks. Additionally, the study analyzes the benefits of adopting a strategic risk management framework, evaluating how it enhances preparedness, resource allocation, and decision-making, particularly in addressing emerging threats such as cyberattacks and geopolitical instability. Finally, the research proposes a structured and practical framework for embedding risk intelligence into defense strategies, providing policymakers with actionable guidelines to improve risk anticipation, assessment, and mitigation in defense operations.

This research seeks to address three key questions: First, what is the role of risk intelligence in modern defense policies, particularly in providing insights into threat anticipation, resource optimization, and enhancing operational effectiveness in complex security environments? Second,

how can a strategic risk management approach improve decision-making by facilitating risk prioritization and aligning actions with long-term defense objectives? Third, what are the key challenges and enablers, such as technological limitations, organizational barriers, advanced analytics, and inter-agency collaboration, that impact the successful integration of risk intelligence into defense policy frameworks?

2. RESEARCH METHOD

This study adopts a qualitative research design that emphasizes in-depth understanding of the integration of risk intelligence into defense policies. A qualitative approach is appropriate because it allows for the exploration of complex and contextual factors that influence policy development and implementation. Specifically, secondary data analysis is utilized to extract relevant information from a range of pre-existing sources. According to Creswell (2014), qualitative research is particularly effective for investigating social phenomena and understanding processes, which aligns with the study's focus on policy integration and strategic risk management.

The data for this study is drawn from diverse secondary sources to provide a comprehensive perspective on the integration of risk intelligence into defense policies. Government defense policy documents offer insights into national strategies, legislative frameworks, and current approaches (Käihkö, 2021). Reports from international defense organizations, including NATO and the United Nations, present a global perspective on best practices and benchmarks (T. Johnson, 2021). Additionally, peer-reviewed scholarly articles and case studies provide theoretical underpinnings and contextualize findings by examining successful and unsuccessful implementations (Ige et al., 2024).

Thematic analysis is employed in this study to identify recurring patterns, themes, and insights from the collected data. As outlined by Braun & Clarke (2006), this method is particularly effective in qualitative research because it allows for the categorization of complex data into meaningful and organized themes. This study focuses on key themes such as the role of risk intelligence in defense policies, the challenges associated with its integration, and the strategic benefits it offers. By exploring these themes in depth, thematic analysis provides a comprehensive understanding of how risk intelligence can influence defense policy formulation and implementation.

3. FINDINGS AND DISCUSSION

3.1. Research Findings

Below is a summary table of the key findings related to the role of risk intelligence, strategic risk management, and challenges and enablers in defense policy. This table provides a concise overview of the insights gathered from the analysis.

Table 1. Summary of Research Findings

Aspect	Key Insights	Sources
The Role of Risk Intelligence	- Enhances situational awareness by leveraging diverse data sources (e.g., cyber networks, satellite imagery). - Supports strategic resource allocation to mitigate significant threats. - Fosters inter-agency collaboration for cohesive operations.	Craparo et al. (2018); (Evans (2015); Johnson (2021); Käihkö (2021); Dieperink et al. (2016)
Strategic Risk Management	- Enables proactive threat identification and preemptive strategies. - Optimizes resource allocation for efficient defense spending. - Supports adaptive planning through real-time feedback. - Facilitates inter-agency coordination and accountability.	Johnson (2021); Abinesh Kamal & Divya (2024); Dieperink et al. (2016); Craparo et al. (2018)); Käihkö (2021)
Challenges of Integration	- Technological limitations, such as outdated systems. - Data silos and lack of inter-agency collaboration. - Cultural resistance to adopting new methodologies. - Budgetary constraints in implementing advanced systems.	Abinesh Kamal & Divya (2024); Dieperink et al. (2016); Craparo et al. (2018); Käihkö (2021)
Enablers of Integration	- Advancements in AI, machine learning, and big data analytics. - Clear policy frameworks like ISO 31000. - International collaboration through alliances (e.g., NATO). - Leadership prioritizing innovation and adaptability. - Training programs to enhance personnel capacity.	Johnson (2021); Abinesh Kamal & Divya (2024); Dieperink et al. (2016); Craparo et al. (2018); Käihkö (2021)

Source: compiled by author based on discussion.

The findings highlight the indispensable role of risk intelligence in modern defense policies by enabling policymakers to navigate complex threat environments proactively. By integrating diverse

data sources, risk intelligence enhances situational awareness, aids in resource optimization, and fosters collaboration across agencies.

Moreover, strategic risk management emerges as a critical tool in improving defense planning through adaptive and transparent decision-making frameworks. It provides a structured approach to managing uncertainty and allocating resources effectively, ensuring resilience against evolving threats.

However, challenges such as technological limitations, cultural resistance, and budgetary constraints hinder the seamless integration of risk intelligence. Addressing these barriers requires leveraging technological advancements, establishing clear frameworks, and fostering international collaborations. The identified enablers, such as leadership and training programs, provide a roadmap for mitigating these challenges and strengthening defense policy frameworks.

These findings emphasize the need for continuous innovation and capacity building to fully harness the potential of risk intelligence in safeguarding national security.

3.2. Discussion

3.2.1. The Role of Risk Intelligence in Modern Defense Policies

Risk intelligence plays a pivotal role in modern defense policies by providing the analytical foundation for proactive threat identification, resource optimization, and informed decision-making. In today's dynamic and interconnected global environment, defense policymakers face an array of complex and hybrid threats, such as cyberattacks, terrorism, and geopolitical instability. Risk intelligence enables policymakers to anticipate these threats and respond effectively, ensuring national security and operational efficiency (Sarjito, 2022).

One of the primary roles of risk intelligence is enhancing situational awareness. It allows defense organizations to gather and analyze data from diverse sources, such as cyber networks, satellite imagery, and human intelligence, to develop a comprehensive understanding of potential threats. For example, Johnson (2021) highlight how risk intelligence systems powered by artificial intelligence have been instrumental in detecting patterns of cyber intrusions, allowing for early intervention before significant damage occurs.

Another critical function of risk intelligence is supporting strategic resource allocation. Defense budgets are often constrained, requiring careful prioritization of spending. Risk intelligence helps

identify the most significant risks and allocate resources efficiently to mitigate those risks. For instance, the United Kingdom's Ministry of Defence has used risk intelligence frameworks to prioritize investments in cyber defense and autonomous systems, thereby enhancing its capabilities to counter emerging threats (Käihkö, 2021).

Risk intelligence also fosters collaboration and integration across defense agencies. By providing a shared platform for data analysis and threat assessment, it ensures that various departments and stakeholders work cohesively. NATO, for example, has leveraged risk intelligence to facilitate joint operations and collective defense strategies, strengthening its response to hybrid threats such as disinformation campaigns and economic coercion (Dieperink et al., 2016).

In conclusion, risk intelligence is integral to modern defense policies as it empowers policymakers with the tools and insights needed to navigate uncertainty and safeguard national interests in an increasingly complex threat landscape.

Risk intelligence is a cornerstone of modern defense policies, offering critical capabilities for managing dynamic and complex threats. It supports defense planners by enabling proactive threat identification, optimal resource allocation, and collaboration across agencies to ensure a unified response to challenges like cyberattacks, terrorism, and geopolitical instability. By leveraging tools like artificial intelligence and shared platforms, risk intelligence enhances situational awareness and operational efficiency.

To better understand these roles, the following flow diagram illustrates the key contributions of risk intelligence to defense policies. It highlights its primary functions, including enhancing situational awareness, prioritizing investments, and fostering collaboration across defense agencies. This visual representation simplifies the complex interdependencies and demonstrates how risk intelligence strengthens defense strategies.

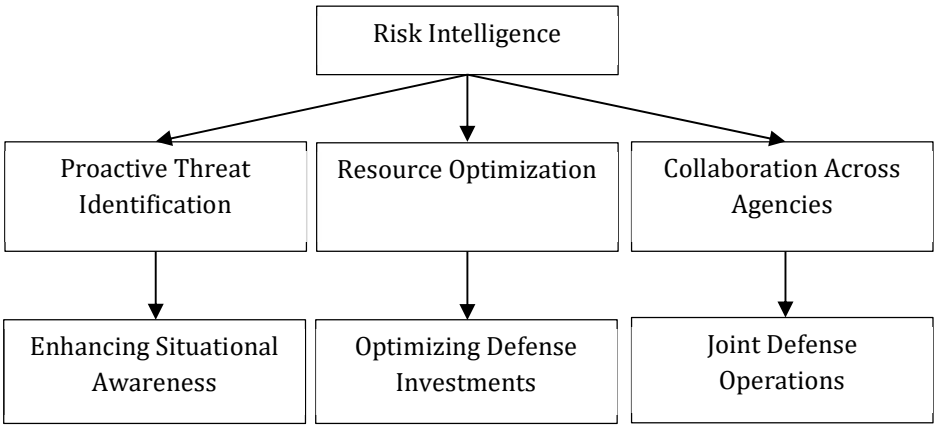

Figure 1. Role of Risk Intelligence in Defense Policies

As illustrated in the diagram, risk intelligence serves as a foundation for effective defense policy. By focusing on proactive threat identification, it allows defense organizations to anticipate risks and take preemptive measures. Strategic resource optimization ensures that constrained budgets are utilized effectively, targeting areas with the greatest impact, such as cyber defense and autonomous systems. Lastly, collaboration across agencies, facilitated by shared data platforms, strengthens the integration of efforts and supports joint operations, as demonstrated by NATO's hybrid threat response strategies.

3.2.2. How Strategic Risk Management Improves Decision-Making in Defense Planning

Strategic risk management (SRM) improves decision-making in defense planning by providing a structured framework for anticipating, prioritizing, and mitigating risks. In an era characterized by hybrid threats and technological advancements, SRM enables policymakers to make informed, proactive decisions that align with long-term defense objectives.

3.2.2.1. Enhancing Proactive Threat Identification

One of the keyways SRM supports decision-making is by enabling proactive threat identification. Through comprehensive risk assessments and scenario analysis, defense planners can foresee potential risks and develop strategies to mitigate them before they escalate. For example, the U.S. Department of Defense employs SRM tools to model potential cyberattacks on critical

infrastructure, allowing for the development of preemptive defense measures (J. Johnson, 2021). This anticipatory approach reduces the likelihood of surprise disruptions and improves readiness.

3.2.2.2. Optimizing Resource Allocation

SRM provides a systematic method for prioritizing risks, ensuring that limited defense resources are allocated where they are most needed. By categorizing risks based on their probability and impact, decision-makers can focus efforts on the most pressing threats. Abinesh Kamal & Divya (2024) notes that the United Kingdom's Ministry of Defence utilized SRM to prioritize investments in advanced surveillance technologies, ensuring operational effectiveness while staying within budget constraints.

3.2.2.3. Supporting Adaptive and Resilient Planning

Defense environments are inherently volatile, requiring adaptive planning to address evolving threats. SRM fosters flexibility by incorporating real-time data and feedback loops into the decision-making process. This allows defense organizations to adjust their strategies dynamically in response to new information. NATO's strategic risk management approach, for instance, integrates continuous monitoring of geopolitical developments, enabling rapid adjustments to joint operations plans (Dieperink et al., 2016).

3.2.2.4. Facilitating Inter-Agency Collaboration

Defense planning often involves coordination among multiple agencies and stakeholders. SRM creates a shared framework for assessing and managing risks, improving communication and alignment. Craparo et al. (2018) highlights how the integration of risk management practices across defense and intelligence agencies in Australia enhanced the country's response to terrorism, ensuring cohesive and timely actions.

3.2.2.5. Enhancing Accountability and Transparency

Finally, SRM improves accountability by providing clear metrics and documentation for risk management activities. This transparency helps policymakers justify decisions to stakeholders, ensuring trust and support for defense initiatives. For instance, the European Union's risk management guidelines emphasize the importance of documenting risk assessments and decision rationales to foster accountability in defense planning (Käihkö, 2021).

Strategic Risk Management (SRM) is a critical framework for improving decision-making in defense planning. It provides defense organizations with tools to anticipate, prioritize, and mitigate risks effectively. SRM's hierarchical structure allows for clear differentiation between core components and their specific processes, ensuring a comprehensive approach to tackling modern threats.

This approach includes Proactive Threat Identification for anticipating risks, Resource Allocation Optimization to ensure efficient use of limited resources, Adaptive and Resilient Planning to maintain flexibility, Inter-Agency Collaboration for coordinated actions, and Enhanced Accountability to build trust and transparency. The following hierarchical flow diagram visually represents these elements, detailing their interconnections and sub-processes.

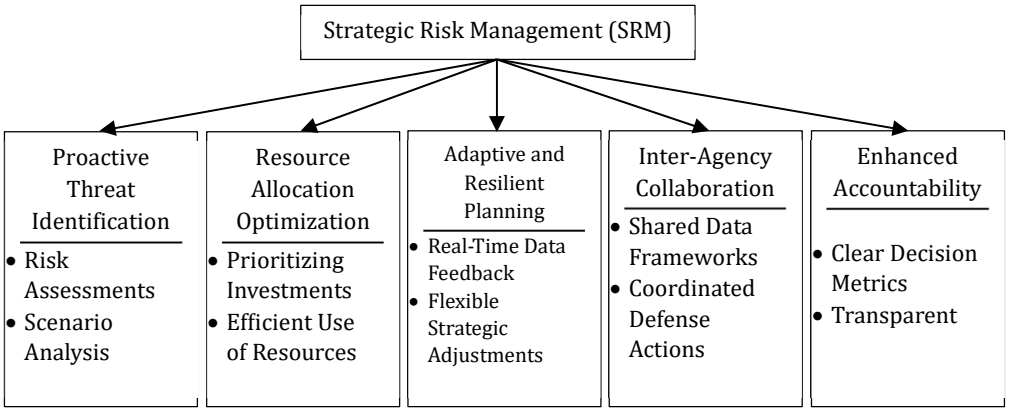

Figure 2. Strategic Risk Management (SRM) in defense planning

As illustrated in the diagram, Strategic Risk Management (SRM) serves as a structured framework that integrates various interconnected components and processes. By implementing Proactive Threat Identification through risk assessments and scenario analysis, defense planners can anticipate and mitigate risks before escalation. Resource Allocation Optimization ensures that defense investments are prioritized, and resources are utilized efficiently.

Furthermore, Adaptive and Resilient Planning supports dynamic adjustments based on real-time feedback, enabling flexible responses to evolving threats. Inter-Agency Collaboration strengthens coordination across defense and intelligence agencies, fostering unified actions. Finally,

Enhanced Accountability ensures clear metrics and transparent documentation, building trust among stakeholders and ensuring informed decision-making.

3.2.3. Key Challenges and Enablers of Integrating Risk Intelligence into Defense Policy

3.2.3.1. Key Challenges

One significant challenge in integrating risk intelligence into defense policy is technological limitations. Despite advancements in artificial intelligence (AI) and data analytics, many defense organizations lack the infrastructure to process and analyze large volumes of data effectively. For instance, outdated legacy systems in several NATO member states have limited their ability to integrate risk intelligence into strategic planning, resulting in gaps in actionable insights (Abinesh Kamal & Divya, 2024; Mandel & Irwin, 2021). This technological gap undermines the potential of advanced tools to enhance decision-making and threat mitigation.

Another critical barrier is the presence of data silos and poor inter-agency coordination. Fragmented data storage across defense and intelligence agencies hinders the seamless sharing and utilization of information, creating a disjointed understanding of threats. Dieperink et al. (2016) highlight that the lack of effective collaboration reduces the efficacy of risk intelligence systems, as organizations fail to build a unified picture of risks. This challenge is particularly detrimental in complex security environments where timely and comprehensive threat assessments are crucial.

Cultural resistance to change poses additional obstacles to adopting risk intelligence systems. Integrating these systems often requires significant organizational changes, which can face resistance from personnel accustomed to traditional decision-making processes. Craparo et al. (2018) notes that this inertia can slow the adoption of innovative practices, creating barriers to modernizing defense policies. Addressing this resistance requires leadership and organizational alignment to foster a culture that embraces technological and procedural advancements.

Finally, budgetary constraints remain a persistent challenge, particularly for developing nations. Implementing advanced risk intelligence systems demands substantial investment in technology, training, and infrastructure. Käihkö (2021) emphasizes that limited defense budgets can hinder widespread adoption, leaving organizations unable to leverage the full potential of risk intelligence. These financial limitations necessitate prioritization and strategic planning to ensure that available resources are used efficiently.

By addressing these challenges, technological limitations, fragmented data, cultural resistance, and budget constraints, defense organizations can create a more cohesive and effective framework for integrating risk intelligence into policy and operations.

3.2.3.2. Key Enablers

One of the most significant enablers for integrating risk intelligence into defense policy is advancements in technology. Innovations in artificial intelligence (AI), machine learning, and big data analytics have transformed the capabilities of risk intelligence systems. These technologies enable real-time threat detection, predictive analytics, and automated decision-making, making them indispensable in modern defense strategies. For instance, AI-powered tools can analyze massive data streams to identify patterns, providing defense organizations with actionable insights for addressing emerging threats (J. Johnson, 2021).

The implementation of policy frameworks and standards has also been instrumental in guiding defense organizations toward effective risk intelligence integration. Standards such as ISO 31000 for risk management provide structured methodologies for assessing and mitigating risks. These frameworks bridge the gap between theoretical concepts and practical applications, ensuring that risk intelligence systems are implemented systematically and consistently across organizations. Abinesh Kamal & Divya (2024) highlights how adopting such standards has improved alignment between risk management practices and broader defense objectives.

International collaboration further enhances the feasibility of integrating risk intelligence systems. Alliances like NATO have demonstrated the value of joint initiatives in cybersecurity and intelligence sharing. By pooling resources and expertise, nations can collectively strengthen their defense capabilities. (Dieperink et al., 2016) emphasize that international partnerships not only reduce the cost of developing advanced systems but also promote interoperability among member states, making risk intelligence integration more robust and comprehensive.

The role of leadership and vision cannot be overstated in driving organizational change and fostering a culture that supports innovation. Effective leaders prioritize adaptability and champion the adoption of new technologies and methodologies. Craparo et al. (2018) highlights that strong leadership inspires confidence and creates an environment where stakeholders are more likely to embrace the transformational changes required for integrating risk intelligence into defense policies.

Finally, training and capacity building play a crucial role in ensuring that defense personnel can effectively use risk intelligence tools. Continuous professional development programs, such as simulation-based training, enhance the operational readiness of defense agencies. Käihkö (2021) notes that such initiatives not only improve the technical competencies of personnel but also foster a deeper understanding of how risk intelligence can be leveraged to inform strategic decisions. This investment in human capital is essential for realizing the full potential of risk intelligence systems.

These five enablers, technological advancements, policy frameworks, international collaboration, visionary leadership, and targeted training, create a comprehensive foundation for successfully integrating risk intelligence into defense policies. By addressing these areas, defense organizations can enhance their preparedness and adaptability in an increasingly complex threat environment.

Integrating risk intelligence into defense policy is essential for modern security strategies, yet it faces numerous challenges and relies on key enablers to succeed. The challenges include technological limitations, fragmented data systems, cultural resistance, and budgetary constraints, all of which hinder the seamless adoption of risk intelligence frameworks. Conversely, advancements in technology, clear policy standards, international collaboration, strong leadership, and training initiatives serve as critical enablers, driving the successful implementation of these systems.

To provide a clearer understanding, the following hierarchical flow diagram visualizes these challenges and enablers, categorizing them into distinct branches under the overarching theme of integrating risk intelligence into defense policy.

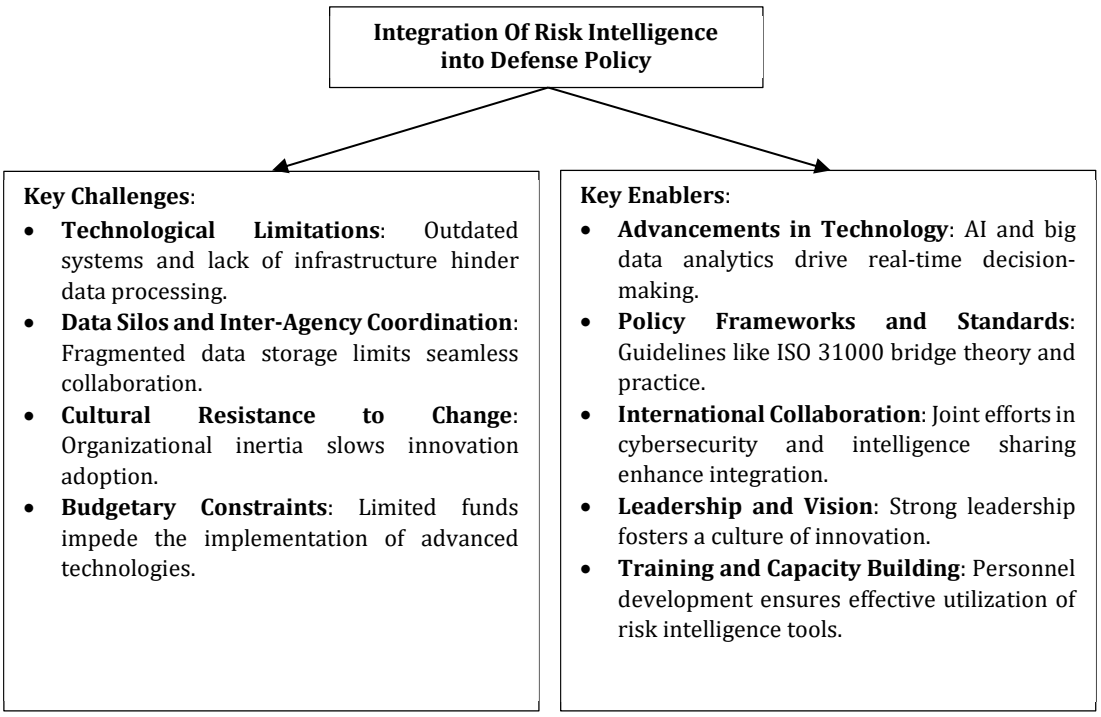

Figure 3. Challenges and Enablers of Integrating Risk Intelligence

The diagram illustrates the dual dimensions influencing the integration of risk intelligence into defense policies:

Key Challenges: These include systemic barriers such as outdated technologies and fragmented data silos, along with organizational hurdles like resistance to change and financial limitations. Addressing these obstacles is critical for advancing risk intelligence frameworks.

Key Enablers: Innovations in AI, robust policy frameworks, and global partnerships act as catalysts for integration. Additionally, strong leadership and targeted capacity-building efforts ensure the workforce is equipped to implement and utilize risk intelligence tools effectively.

This visualization underscores the need to strategically address challenges while leveraging enablers to build resilient and adaptable defense policies. By focusing on these areas, policymakers can ensure that risk intelligence becomes an integral component of national security strategies.

4. CONCLUSION

The integration of risk intelligence into defense policy is not only critical but also highly beneficial in addressing the complexities of modern security challenges. It enhances situational awareness, optimizes resource allocation, and supports proactive decision-making, ensuring that defense strategies remain adaptive and resilient in the face of evolving threats. However, successful implementation requires addressing key challenges, including technological gaps, data silos, and resistance to change. Key consianalytics tools andstering inter-agency coordination, adopting advanced analytics tools, and embedding risk intelligence into the broader strategic framework of defense operations.

4.1. Policy Recommendations

Establishing Dedicated Risk Intelligence Units within Defense Ministries: These units should be tasked with collecting, analyzing, and disseminating risk intelligence to support informed decision-making at all levels of defense operations. Their mandate should include collaboration across governmental and international agencies to ensure a unified approach to risk management.

Investing in Technology and Training for Defense Personnel: Governments should allocate resources to acquire advanced data analytics tools, AI-driven platforms, and cybersecurity technologies. Additionally, tailored training programs for defense personnel should be developed to enhance their capacity to utilize these tools effectively.

Promoting International Collaboration for Shared Risk Intelligence: Partnerships among nations, particularly through alliances like NATO and regional defense agreements, can facilitate the sharing of critical intelligence and best practices. Such collaborations will strengthen collective resilience and reduce resource duplication.

4.2. Future Research Directions

Examining the Role of Artificial Intelligence in Enhancing Risk Intelligence: Future studies should explore how AI technologies, including machine learning and natural language processing, can further augment the capabilities of risk intelligence systems, particularly in predictive analysis and real-time decision-making.

Exploring Case Studies of Risk Intelligence Applications in Other Sectors: Comparative research into how sectors like finance, healthcare, and energy leverage risk intelligence can provide

valuable insights and transferable lessons for defense policy. This cross-sectoral perspective may highlight innovative approaches and technologies that can be adapted for national security purposes.

By addressing the identified challenges and implementing the recommended strategies, defense policymakers can ensure that risk intelligence becomes a cornerstone of national security planning. This integration will not only strengthen operational readiness but also enhance the agility and resilience of defense systems in an increasingly complex global environment.

REFERENCES

Abinesh Kamal, K. U., & Divya, S. V. (2024). Integrated threat intelligence platform for security operations in organizations. *Automatika*, *65*(2), 401–409. https://doi.org/10.1080/00051144.2023.2295146

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

Craparo, G., Magnano, P., Paolillo, A., & Costantino, V. (2018). The Subjective Risk Intelligence scale. The development of a new scale to measure a new construct. *Current Psychology*, *37*(4), 966–981.

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE Publications. https://cumming.ucalgary.ca/sites/default/files/teams/82/communications/Creswell%202003%20-%20Research%20Design%20-%20Qualitative%2C%20Quantitative%20and%20Mixed%20Methods.pdf

Dhlamini, J. (2022). Strategic risk management: A systematic review from 2001 to 2020. *Journal of Contemporary Management*, *19*(2), 212–237. https://doi.org/10.35683/jcm22008.165

Dieperink, C., Hegger, D. L. T., Bakker, M. H. N., Kundzewicz, Z. W., Green, C., & Driessen, P. P. J. (2016). Recurrent governance challenges in the implementation and alignment of flood risk management strategies: a review. *Water Resources Management*, *30*, 4467–4481.

Dorn, N. (2007). European strategic intelligence: How far integration. *Erasmus L. Rev.*, *1*, 163.

Evans, D. (2015). *Risk intelligence: How to live with uncertainty*. Simon and Schuster.

Ige, A. B., Kupa, E., & Ilori, O. (2024). Analyzing defense strategies against cyber risks in the energy sector: Enhancing the security of renewable energy sources. *International Journal of Science and Research Archive*, *12*(1), 2978–2995.

Johnson, J. (2021). 'Catalytic nuclear war'in the age of artificial intelligence & autonomy: Emerging military technology and escalation risk between nuclear-armed states. *Journal of Strategic Studies*, 1–41.

Johnson, T. (2021). Bureaucratic Inefficiencies in Defense Policy: Challenges and Solutions. *Defense Policy Review*.

Käihkö, I. (2021). The evolution of hybrid war: Implications for strategy and the military profession. *Parameters*, *51*(3), 115–128. https://doi.org/10.55540/0031-1723.3084

KOUKAKIS, L. T. C. G. (2024). *National Security, Foreign Policy, Intelligence, Cybersecurity, National Defense, Maritime Security, Risk Analysis and Foresight Strategic Documents Issued by Regional and International Actors in 2023.*

Mandel, D. R., & Irwin, D. (2021). Uncertainty, intelligence, and national security decisionmaking. *International Journal of Intelligence and CounterIntelligence*, *34*(3), 558–582.

MBN. (n.d.). *What is Risk Intelligence? Definition and Examples*. MBN. Retrieved December 4, 2024, from https://marketbusinessnews.com/financial-glossary/what-is-risk-intelligence-definition-and-examples/#:~:text=Risk%20intelligence%20involves%20gathering%20risk%20data%2C%20understanding%20potential,making%20informed%20decisions%2C%20and%20continuously%20improving%20your%20approach.

Metricstream. (2024). *Your Ultimate Guide to Risk Intelligence in 2024*. Metricstream. https://www.metricstream.com/learn/risk-intelligence.html

Mızrak, F. (2023). Integrating cybersecurity risk management into strategic management: a comprehensive literature review. *Research Journal of Business and Management*, *10*(3), 98–108.

Sarjito, A. (2022). Perang Hibrida: Perang Generasi Keempat. *Manajemen Pertahanan: Jurnal Pemikiran Dan Penelitian Manajemen Pertahanan*, *8*(1).