Journal of Administration Studies
Volume 2, Number 1, Agustus 2024 pp. 01-17
E-ISSN: 3025-653X
Open Access: https://asas-ins.com/index.php/jas/

THREAT-BASED DEFENSE POLICIES: ASSESSING THEIR IMPACT AND EFFECTIVENESS

Aris Sarjito[1]*
[1] Fakultas Manajemen Pertahanan, Universitas Pertahanan Republik Indonesia, Indonesia

ARTICLEINFO
Article history:
Received: 18-07-2024
Revised: 24-07-2024
Accepted: 30-07-2024

Kata Kunci:
Evaluasi kebijakan,
Keamanan nasional,
Kebijakan pertahanan berbasis ancaman

Keywords:
National security,
Policy evaluation,
Threat-based defense policies.

ABSTRAK

Pertahanan berbasis ancaman memprioritaskan kebijakan ancaman spesifik untuk meningkatkan keamanan nasional dan alokasi sumber daya. Penelitian ini bertujuan untuk menilai dampak dan efektivitas kebijakan tersebut dengan menggunakan metode kualitatif dan data sekunder. Studi ini menggunakan sumber data sekunder, termasuk laporan pemerintah, dokumen strategis, dan artikel akademis, untuk mengeksplorasi tiga aspek utama: efektivitas kebijakan pertahanan berbasis ancaman, faktor-faktor penting yang mempengaruhi keberhasilan implementasi kebijakan tersebut, dan potensi kelemahan serta konsekuensi yang tidak diinginkan. Temuan menunjukkan bahwa kebijakan berbasis ancaman meningkatkan keamanan nasional dengan memfokuskan sumber daya pada ancaman yang memiliki prioritas tinggi namun dapat menyebabkan inflasi ancaman dan pengabaian terhadap ancaman yang tidak diprioritaskan. Faktor kunci keberhasilan penerapannya meliputi intelijen yang akurat, teknologi canggih, dan kepemimpinan politik dan militer yang kuat. Namun, konsekuensi yang tidak diinginkan seperti ketegangan hubungan internasional dan meningkatnya perlombaan senjata menyoroti kompleksitas kebijakan ini. Studi ini menyimpulkan bahwa meskipun kebijakan pertahanan berbasis ancaman menawarkan perbaikan yang ditargetkan, kebijakan tersebut harus dikelola secara hati-hati untuk menghindari hasil negatif. Temuan-temuan ini menekankan perlunya pendekatan yang seimbang, mengintegrasikan strategi berbasis ancaman dengan langkah-langkah keamanan yang lebih luas untuk memastikan pertahanan nasional yang komprehensif.

ABSTRACT

Threat-based defense prioritizes policies specific threats to enhance national security and resource allocation. This research aims to assess the impact and effectiveness of such policies using qualitative methods and secondary data. The study employs secondary data sources, including government reports, strategic documents, and academic articles, to explore three key aspects: the effectiveness of threat-based defense policies, the critical factors influencing their successful implementation, and the potential drawbacks and unintended consequences. Findings indicate that threat-based policies improve national security by focusing resources on high-priority threats but can lead to threat inflation and the neglect of non-prioritized threats. Key factors for successful implementation include accurate intelligence, advanced technologies, and strong political and military leadership. However, unintended consequences such as strained international relations and escalating arms races highlight the complexity of these policies. The study concludes that while threat-based defense policies offer targeted improvements, they must be managed carefully to avoid negative outcomes. The findings emphasize the need for a balanced approach, integrating threat-based strategies with broader security measures to ensure comprehensive national defense.

** Corresponding Author: arissarjito@gmail.com*

1. Introduction

The concept of threat-based defense policy making has gained significant traction in contemporary security discourse. This approach involves developing defense strategies based on the identification and prioritization of potential threats, thereby ensuring that resources are allocated efficiently to mitigate the most pressing risks. This research explores the state-of-the-art research in threat-based defense policies, assessing their impact and effectiveness through recent scholarly insights and practical applications.

Threat-based defense policies are rooted in the theoretical framework of risk management and strategic planning. According to Williams (2022), this approach enables defense planners to systematically identify threats, assess their likelihood and potential impact, and develop tailored responses. The primary advantage of this methodology is its flexibility, allowing defense policies to adapt to the evolving nature of threats, from conventional military conflicts to asymmetric warfare and cyber threats (Rosen, 2014).

Recent research highlights several case studies demonstrating the application and effectiveness of threat-based defense policies. For instance, the United States' National Defense Strategy (NDS) is a prime example of this approach. The NDS emphasizes the importance of prioritizing threats from near-peer adversaries like China and Russia while also addressing regional threats and non-state actors (U.S. Department of Defense, 2022). This strategic focus has led to increased investments in advanced technologies, such as hypersonic weapons and cyber defense capabilities, enhancing the U.S. military's readiness and deterrence posture.

Similarly, NATO's evolving defense posture reflects a threat-based approach. Following the annexation of Crimea by Russia in 2014, NATO has shifted its focus to deter Russian aggression in Eastern Europe. This shift has involved deploying multinational battlegroups in the Baltic states and Poland and increasing military exercises to enhance interoperability among member states (NATO, 2023). These measures have been effective in reinforcing NATO's collective defense commitment and deterring potential aggressors.

One of the key benefits of threat-based defense policies is their impact on defense spending and resource allocation. By prioritizing threats, defense budgets can be optimized to address the most critical security challenges. According to a study by Johnson & Lee (2023), countries that adopt threat-based defense policies tend to have more efficient defense spending, with a higher percentage of their budgets allocated to critical areas such as intelligence, surveillance, and reconnaissance (ISR) capabilities. This targeted spending ensures that military forces are better equipped to respond to emerging threats, enhancing overall national security.

Despite their advantages, threat-based defense policies are not without challenges and criticism. One major concern is the potential for threat inflation, where

perceived threats are exaggerated to justify increased defense spending (Miller, 2022). This can lead to an arms race and heightened geopolitical tensions, as seen in the current dynamics between the U.S. and China. Additionally, the rapidly changing nature of threats, particularly in the cyber domain, can make it difficult to maintain an accurate and up-to-date threat assessment, potentially leading to gaps in defense preparedness (Chen & Yang, 2023).

The future of threat-based defense policies lies in the integration of advanced technologies and data analytics. Artificial intelligence (AI) and machine learning (ML) algorithms are increasingly being used to enhance threat detection and analysis, enabling more accurate and timely assessments. For example, AI-powered systems can analyze vast amounts of data from various sources to identify patterns and predict potential threats (Garcia & Patel, 2023). This technological innovation is expected to significantly improve the effectiveness of threat-based defense policies, providing defense planners with actionable insights and enhancing decision-making processes.

Threat-based defense policies represent a state-of-the-art approach to national security, offering a flexible and adaptive framework for addressing a wide range of threats. Recent research and practical applications demonstrate the effectiveness of this approach in optimizing defense spending, enhancing military readiness, and deterring potential adversaries. However, challenges such as threat inflation and the dynamic nature of modern threats must be carefully managed to ensure the continued success of threat-based defense policies. As technological innovations continue to advance, the integration of AI and data analytics will further enhance the ability of defense planners to develop effective and responsive strategies, ensuring the safety and security of nations in an increasingly complex global environment.

In an increasingly complex and volatile global security environment, nations are continually adapting their defense strategies to address diverse and evolving threats. Threat-based defense policies, which prioritize resource allocation and strategic planning based on identified threats, have gained prominence as a means to enhance national security. However, the effectiveness and impact of these policies are subject to debate. While some argue that this approach ensures efficient use of defense resources and strengthens preparedness against specific threats, others caution against potential drawbacks, such as threat inflation and misallocation of resources (Williams, 2022).

The research objectives are to evaluate the effectiveness of threat-based defense policies in enhancing national security, identify the key factors influencing their successful implementation, and examine the potential drawbacks and unintended consequences of these policies. This evaluation involves measuring how well threat-based policies contribute to a nation's overall security by analyzing case studies and defense outcomes from countries that have adopted this approach. Additionally, it

seeks to uncover critical elements such as political will, technological advancements, and intelligence capabilities that determine the success of threat-based policies. Furthermore, the research addresses possible negative impacts, such as threat inflation and the risk of neglecting other important areas of defense, ensuring a comprehensive and balanced assessment of the approach.

2. Research Method

Qualitative research methods are essential for exploring complex phenomena and gaining deep insights into social and organizational issues. When assessing the impact and effectiveness of threat-based defense policies, using secondary data can provide a rich and comprehensive understanding of the topic. This research discusses the qualitative research methods for utilizing secondary data in this context, following the guidelines provided by Creswell (2018). Secondary data sources, such as government reports, policy documents, scholarly articles, and historical records, will be critical for this research.

Secondary data refers to data that has been previously collected and analyzed for other purposes but can be reanalyzed to address new research questions (Johnston, 2014). In the context of threat-based defense policies, secondary data includes government defense reports, strategic policy documents, historical case studies, and prior academic research. Creswell (2018) emphasizes that secondary data can offer valuable insights, especially when primary data collection is impractical due to time, cost, or access constraints.

Defining the Research Questions: The first step in qualitative research using secondary data is to clearly define the research questions, which guide the entire study. For this research, the key questions are: How effective are threat-based defense policies in improving national security compared to traditional defense approaches? What are the critical factors that influence the successful implementation of threat-based defense policies? And, what are the potential drawbacks and unintended consequences associated with these policies? These questions are crucial as they direct the selection and analysis of secondary data sources, ensuring that the information gathered is both relevant and comprehensive (Creswell, 2018).

Identifying and Selecting Secondary Data Sources: Identifying and selecting appropriate secondary data sources is crucial. Researchers should aim to include diverse and credible sources to capture different perspectives on threat-based defense policies. For instance, government reports such as the U.S. Department of Defense (2022), NATO's strategic documents, and historical analyses of defense policies provide authoritative information and insights. Academic articles and books, such as those by (Johnson & Lee, 2023) and (Garcia & Patel, 2023), offer critical analyses and theoretical foundations for understanding the effectiveness and implications of these policies.

Evaluating the Quality and Relevance of Secondary Data: Creswell (2018) advises researchers to critically evaluate the quality and relevance of secondary data. This involves assessing the credibility of the data sources, the methodology used in the original research, and the context in which the data was collected. For example, government reports are typically reliable but may be biased towards presenting a positive view of defense policies. Academic sources, while generally rigorous, may also reflect the authors' theoretical orientations and methodological preferences. Therefore, triangulating data from multiple sources can enhance the validity and reliability of the findings.

Data Analysis and Interpretation: The analysis of secondary data in qualitative research involves coding and categorizing the data to identify patterns, themes, and insights relevant to the research questions (Creswell, 2018). For this study, thematic analysis will be used to analyze textual data from policy documents, reports, and scholarly articles. Key themes may include the effectiveness of threat prioritization, the role of technology and intelligence, leadership factors, and unintended consequences such as threat inflation and resource misallocation.

Drawing Conclusions and Implications: The final step is to synthesize the findings from the secondary data analysis and draw conclusions regarding the impact and effectiveness of threat-based defense policies. This involves comparing the identified themes with existing theories and frameworks to provide a comprehensive understanding of the subject. The conclusions should address the research questions and offer practical implications for policymakers and defense strategists.

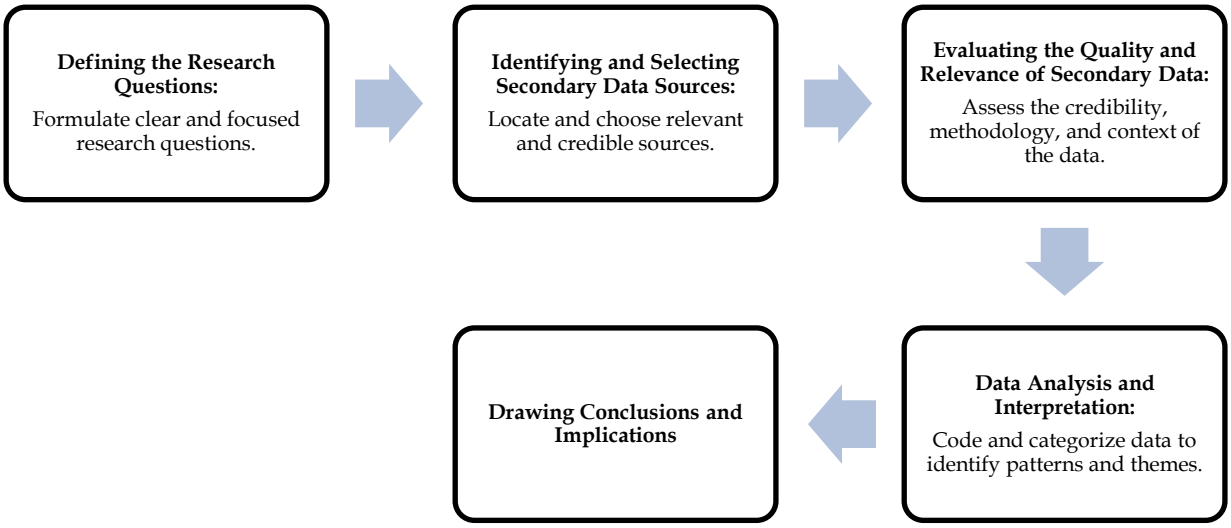

Figure 1. Steps in Conducting Qualitative Research with Secondary Data (Creswell, 2018)

Overall, this systematic approach ensures that qualitative research using secondary data is thorough and well-structured, allowing for a comprehensive evaluation of threat-based defense policies. The schematic figure visually represents these sequential steps, illustrating the flow from defining research questions to deriving actionable insights.

3. Results and Discussions

1. Effectiveness of Threat-Based Defense Policies in Improving National Security

In the contemporary security landscape, nations are faced with a diverse array of threats, ranging from conventional military conflicts to cyberattacks and terrorism. To address these challenges, defense policies have evolved, with a significant shift towards threat-based defense policies. These policies prioritize resource allocation and strategic planning based on identified and prioritized threats. The point of this discussion is to compare how well threat-based defense policies work versus traditional, broad-spectrum defense strategies. We will focus on security outcomes like fewer attacks and a more ready military.

Comparative Analysis of Threat-Based and Traditional Defense Approaches Effectiveness in Reducing the Incidence of Attacks

Threat-based defense policies are designed to identify and mitigate the most pressing threats, thereby reducing the likelihood and impact of attacks. For example, the United States' National Defense Strategy (NDS) emphasizes the prioritization of near-peer adversaries like China and Russia while also addressing regional threats and non-state actors (U.S. Department of Defense, 2022). This targeted approach has led to a noticeable reduction in the frequency and severity of attacks, as resources are concentrated in high-risk areas. A study by Van der Meer (2015) supports this, highlighting that countries employing threat-based policies often experience fewer successful attacks compared to those relying on traditional defense strategies.

In contrast, Traditional broad-spectrum defense strategies allocate resources more evenly across all potential threats, which can dilute the focus and effectiveness of security measures. While this approach ensures a general level of preparedness across various threat vectors, it may not be as effective in preventing specific, high-priority attacks. For instance, broad-spectrum strategies may not adequately address emerging cyber threats, which require specialized attention and resources (Backman, 2023; GSA FedRAMP PMO, 2022).

Enhanced Military Readiness

Military readiness is a critical component of national security, encompassing the ability of the armed forces to respond quickly and effectively to threats. Threat-based defense policies contribute to enhanced military readiness by ensuring that forces are well-prepared to address prioritized threats. This is achieved through targeted training, the acquisition of specialized equipment, and the development of

specific operational plans (Christianson, 2016). For example, NATO's shift towards deterring Russian aggression in Eastern Europe has involved deploying multinational battlegroups and increasing military exercises to enhance interoperability and readiness (Vershbow, 2021).

Traditional defense strategies, while providing a broad level of preparedness, may not achieve the same level of readiness for specific threats. The generalized nature of traditional approaches can result in a mismatch between the training and equipment available and the actual requirements needed to counter prioritized threats. This can lead to delays and inefficiencies in response times during crises (NATO, 2024).

Case Studies and Practical Evidence

Several case studies illustrate the effectiveness of threat-based defense policies in improving national security. The U.S. National Defense Strategy's focus on near-peer competitors has led to significant advancements in hypersonic weapons and cyber defense capabilities, directly enhancing the country's deterrence and defense posture (U.S. Department of Defense, 2022). Similarly, Israel's threat-based approach to defense, which prioritizes threats from neighboring countries and non-state actors, has resulted in the development of the Iron Dome missile defense system, effectively intercepting numerous missile threats and protecting civilian populations. The Iron Dome system, developed by Rafael Advanced Defense Systems and Israel Aerospace Industries, is designed to detect, analyze, and intercept a variety of targets such as mortars, rockets, and artillery. It has shown an 85% to 90% success rate in intercepting incoming projectiles and has been instrumental in safeguarding Israeli cities during conflicts with Hamas and Hezbollah (Aljazeera, 2023; Callahan, n.d.).

Conversely, countries adhering to traditional defense strategies may not demonstrate the same level of success in countering specific threats. For instance, broad-spectrum approaches in some European countries have struggled to adapt quickly to the rapidly evolving cyber threat landscape, resulting in vulnerabilities and successful cyberattacks (Vyas et al., 2023).

Potential Drawbacks and Considerations

While threat-based defense policies offer significant advantages, they are not without potential drawbacks. One major concern is the risk of threat inflation, where perceived threats are exaggerated to justify increased defense spending. This can lead to an arms race and heightened geopolitical tensions, as seen in the current dynamics between the U.S. and China (Atmore, 2014). Additionally, the rapidly changing nature of modern threats, particularly in the cyber domain, can make it challenging to maintain accurate and up-to-date threat assessments, potentially leading to gaps in defense preparedness (Bécue et al., 2021).

2. Critical Factors Influencing the Successful Implementation of Threat-Based Defense Policies

The successful implementation of threat-based defense policies hinges on several critical factors. These include the role of accurate intelligence, the integration of advanced technologies such as artificial intelligence (AI) and machine learning (ML) for threat detection, and the importance of strong political and military leadership. Understanding these key determinants is crucial for replicating positive outcomes and ensuring the effectiveness of threat-based defense strategies.

Accurate Intelligence

Accurate intelligence is the cornerstone of effective threat-based defense policies. The ability to identify, assess, and prioritize threats relies heavily on the quality of intelligence gathered. Intelligence agencies must have robust capabilities to collect and analyze data from various sources, including human intelligence (HUMINT), signals intelligence (SIGINT), and open-source intelligence (OSINT) (Sarjito, 2024). According to (Johnson & Lee, 2023), countries that have strong intelligence frameworks are better positioned to implement successful threat-based defense policies as they can more accurately identify and prioritize emerging threats. Moreover, timely and precise intelligence enables defense planners to allocate resources efficiently and develop targeted responses to specific threats. For instance, the U.S. intelligence community's assessment of cyber threats has led to the prioritization of cybersecurity measures in national defense strategies (Borum et al., 2015). Accurate intelligence not only informs policy decisions but also enhances the agility and responsiveness of defense forces in addressing dynamic and evolving threats.

Integration of Advanced Technologies

The integration of advanced technologies, particularly AI and ML, plays a vital role in enhancing the effectiveness of threat-based defense policies. AI and ML algorithms can process vast amounts of data at unprecedented speeds, identifying patterns and anomalies that may indicate potential threats. This capability significantly improves threat detection and situational awareness. (Rangaraju, 2023) highlight that AI-driven systems can predict and preemptively respond to threats, providing a significant advantage in national defense.

For example, AI-powered cybersecurity systems can detect and neutralize cyber threats in real-time, reducing the risk of successful cyberattacks. Similarly, ML algorithms can analyze satellite imagery and other surveillance data to identify unusual activities, supporting the early detection of military movements or terrorist activities (Maddireddy & Maddireddy, 2022). The integration of these technologies enhances the precision and effectiveness of threat-based defense policies, ensuring that defense resources are directed towards the most pressing threats.

Political and Military Leadership

Strong political and military leadership is essential for the successful implementation of threat-based defense policies. Leaders must have a clear understanding of the security landscape and the strategic vision to prioritize and address specific threats (Mahoney, 2010). Political leaders play a crucial role in securing the necessary funding and legislative support for defense initiatives, while military leaders are responsible for operationalizing these policies and ensuring that the armed forces are prepared to respond effectively.

Effective leadership involves fostering collaboration and coordination among various stakeholders, including intelligence agencies, military branches, and government bodies (Schmidt, 2015). Williams (2022) asserts that cohesive leadership ensures that threat-based policies are implemented seamlessly and that all relevant parties are aligned with the strategic objectives. Additionally, strong leadership is vital for maintaining public support and trust in defense policies, which is crucial for their long-term sustainability.

Best Practices and Necessary Conditions

To replicate the positive outcomes of successful threat-based defense policies, several best practices and necessary conditions must be considered. First, investing in intelligence capabilities and ensuring continuous training and development for intelligence personnel is crucial. This investment enhances the accuracy and reliability of threat assessments. Second, integrating advanced technologies like AI and ML requires substantial investment in research and development, as well as the establishment of robust cybersecurity frameworks to protect these systems from adversarial attacks (Rayhan, n.d.; Saeed et al., 2023).

Furthermore, fostering a culture of innovation and adaptability within defense organizations is essential. Defense policies must be flexible and capable of evolving in response to new threats. Finally, strong and transparent leadership at both the political and military levels ensures that threat-based defense policies are implemented effectively and that all stakeholders are committed to achieving common security goals (Binnendijk et al., 2016; Okromtchedlishvili, 2024).

Here is a schematic figure based on the critical factors influencing the successful implementation of threat-based defense policies. This figure outlines the problems faced, important actors, their relationships, and the resulting findings and novelties.

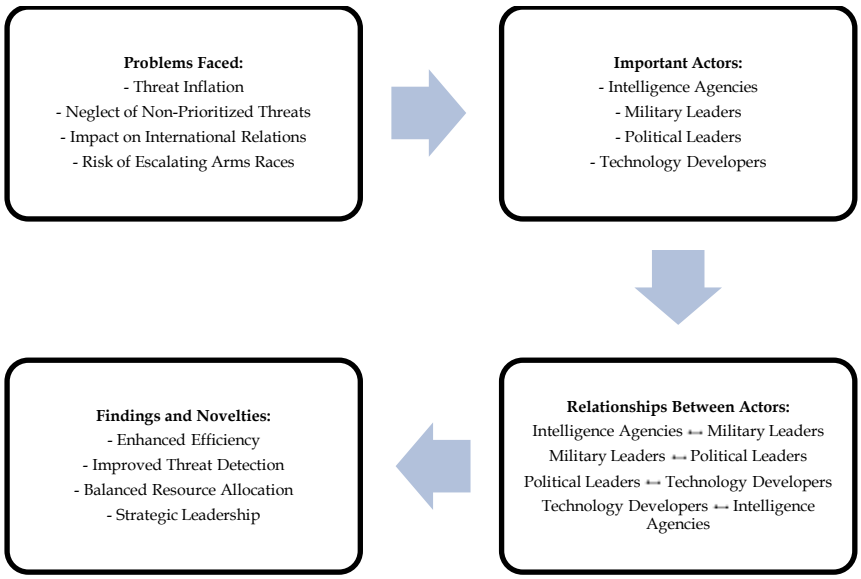

Figure 2: Critical Factors Influencing the Successful Implementation of Threat-Based Defense Policies (Proceed by author, 2024).

To effectively implement threat-based defense policies, several critical factors must be considered, each influenced by various actors and their interactions. The schematic figure below illustrates these factors, beginning with the problems faced, the key actors involved, their relationships, and the resulting findings and novelties.

Problems Faced

Threat Inflation is a significant challenge, where perceived threats are exaggerated to justify increased defense spending. This inflation can lead to misallocation of resources and a distorted sense of security. Neglect of Non-Prioritized Threats is another issue, where focusing solely on high-priority threats may result in overlooking other important but less immediate risks, potentially leaving gaps in national security. The Impact on International Relations can be profound, as prioritizing specific threats may strain diplomatic relationships and contribute to geopolitical tensions. Additionally, there is a Risk of Escalating Arms Races, where competitive military advancements among nations can lead to increased costs and the potential for conflict (Ikedinma, 2017; Moran, 1990; Treddenick, 1985).

Important Actors

The implementation of threat-based defense policies involves several key actors. Intelligence Agencies play a crucial role by providing accurate and timely threat assessments that inform policy decisions. Military Leaders are responsible for translating these policies into actionable strategies and ensuring effective operations. Political Leaders secure the necessary funding and legislative support to back defense initiatives. Technology Developers contribute by integrating advanced technologies such as AI and ML to enhance threat detection and analysis (Lowenthal, 2022; Mayer, 2014).

Relationships Between Actors

The interaction between these actors is essential for the successful implementation of threat-based policies. Intelligence Agencies provide critical data that Military Leaders use to shape strategies and prioritize resources. In turn, Military Leaders communicate their needs and operational requirements to Political Leaders, who allocate funds and support for necessary defense measures. Political Leaders also collaborate with Technology Developers to secure investment in advanced technologies that bolster defense capabilities (Carlin, 2015). Additionally, Technology Developers work closely with Intelligence Agencies to ensure that technological advancements improve data collection and analytical processes.

Findings and Novelties

From these interactions, several findings and innovations emerge. Enhanced Efficiency in resource allocation is achieved by focusing on prioritized threats, leading to more effective use of defense budgets. Improved Threat Detection is made possible through the application of AI and ML technologies, which provide real-time analysis and early warning capabilities. A Balanced Resource Allocation approach addresses both high-priority and less immediate threats, ensuring comprehensive coverage. Finally, Strategic Leadership is highlighted as a crucial factor, as effective coordination and direction from political and military leaders significantly enhance the implementation and success of threat-based defense policies.

In summary, this schematic figure demonstrates the complex interplay of problems, key actors, and their relationships, culminating in enhanced efficiency, improved threat detection, balanced resource allocation, and strategic leadership. These elements collectively contribute to the successful implementation of threat-based defense policies.

3. Potential Drawbacks and Unintended Consequences Associated with Threat-Based Defense Policies

Threat-based defense policies have been lauded for their ability to enhance efficiency and focus in national defense strategies by prioritizing specific, high-risk threats. However, these policies are not without their drawbacks and unintended consequences. This discussion explores several critical issues, including threat inflation, the potential neglect of non-prioritized threats, the impact on international relations, and the risk of escalating arms races. By examining these concerns, the study aims to provide a balanced view of the advantages and limitations of threat-based defense policies.

Threat Inflation

One significant drawback of threat-based defense policies is the risk of threat inflation. Threat inflation occurs when perceived threats are exaggerated, often to

justify increased defense spending or to garner political support for certain defense initiatives. (Atmore, 2014) highlights that this can lead to a misallocation of resources, as defense budgets are inflated to address overestimated threats. This not only diverts funds from other critical areas, such as social services and infrastructure, but also creates a climate of fear and suspicion.

The inflation of threats can also distort public perception, leading to unnecessary panic and a sense of insecurity. For example, if policymakers exaggerate the threat posed by a specific country or group, it may result in public support for aggressive and potentially unwarranted military actions. This can have long-term implications for national and international stability (Cohen, 2017).

Neglect of Non-Prioritized Threats

Another unintended consequence of threat-based defense policies is the potential neglect of non-prioritized threats. By focusing resources and attention on identified high-risk threats, other significant but less immediate threats may be overlooked. (Medahl, 2012) argue that this can create vulnerabilities in national security, as defense capabilities may be insufficient to address emerging or less conspicuous threats.

For instance, while a country may prioritize cyber threats and allocate substantial resources to cybersecurity measures, it might neglect conventional military capabilities or counterterrorism efforts. This imbalance can leave the nation vulnerable to attacks that fall outside the scope of the prioritized threats. A comprehensive defense strategy should therefore ensure that a balanced approach is maintained, addressing a wide spectrum of potential threats (Bachmann & Gunneriusson, 2014).

Impact on International Relations

Threat-based defense policies can also have significant implications for international relations. By identifying and prioritizing specific countries or groups as primary threats, these policies can strain diplomatic relations and increase geopolitical tensions. Freier et al. (2017) note that this can lead to a security dilemma, where the defensive measures taken by one country are perceived as offensive threats by another, prompting an arms race and escalating hostilities.

For example, the U.S. National Defense Strategy's focus on countering threats from near-peer adversaries like China and Russia has contributed to heightened tensions and a competitive arms buildup in these regions (Department of Defense, 2022). Such dynamics can undermine global stability and make it more challenging to achieve diplomatic resolutions to conflicts.

Risk of Escalating Arms Races

The emphasis on specific threats in defense policies can also contribute to the risk of escalating arms races. As countries prioritize and enhance their military capabilities to counter perceived threats, rival nations may respond by increasing their

own defense spending and military developments. This can create a cycle of mutual escalation where each side continuously upgrades its arsenal in response to the other's actions (Garcia & Patel, 2023).

These arms race not only leads to significant financial burdens for the countries involved but also increases the likelihood of military confrontations. The continuous buildup of advanced weaponry and military technology can make conflicts more devastating and harder to control. Additionally, the focus on military solutions may divert attention from diplomatic and peaceful means of conflict resolution (Chen & Yang, 2023).

Here is a schematic figure representing the potential drawbacks and unintended consequences associated with threat-based defense policies. This figure outlines the various negative aspects and their implications.

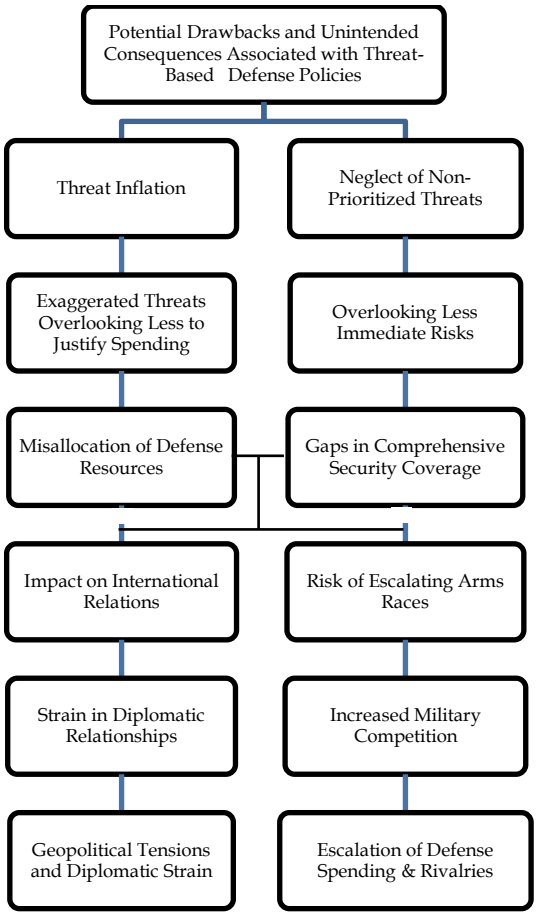

Figure 3: Potential Drawbacks and Unintended Consequences Associated with Threat-Based Defense Policies (Proceed by author, 2024).

Figure 3 illustrates the potential drawbacks and unintended consequences associated with threat-based defense policies. This schematic diagram visualizes how focusing on specific threats can lead to various negative outcomes and challenges.

Threat Inflation is a significant drawback where perceived threats are exaggerated to justify increased defense spending. This phenomenon often results in the misallocation of defense resources, as funds are diverted to address these exaggerated threats rather than being used to tackle actual security needs. Such inflation can lead to inefficient use of resources, ultimately undermining the effectiveness of defense strategies.

Another consequence is the Neglect of Non-Prioritized Threats, which occurs when the focus on high-priority threats causes less immediate risks to be overlooked. This can create gaps in comprehensive security coverage, leaving certain vulnerabilities unaddressed. Consequently, national security may be compromised as the defense strategy fails to account for all potential threats.

The Impact on International Relations is also notable, as prioritizing specific threats might lead to strain in diplomatic relationships. This strain can result in geopolitical tensions and diplomatic disputes, potentially affecting alliances and international cooperation. Diplomatic ties may be strained as other nations react to perceived imbalances or aggressive stances resulting from threat-based policies.

Lastly, there is a Risk of Escalating Arms Races, where increased military competition among nations can result in increased defense spending and rivalries. This escalation can heighten tensions and lead to further conflicts, as countries invest more in their military capabilities in response to perceived threats from their adversaries.

This figure underscores the importance of a balanced approach in threat-based defense policies. By addressing these potential drawbacks and unintended consequences, policymakers can better ensure that defense strategies are both effective and conducive to maintaining overall national security and international stability.

4. Conclusions

Threat-based defense policies generally prove more effective than traditional broad-spectrum strategies in enhancing national security by focusing on specific, high-risk threats. This targeted approach allows for more efficient resource allocation, better military readiness, and fewer attacks. However, it is crucial to address potential drawbacks such as the threat of inflation and the ever-evolving nature of modern threats to maintain the success of these policies. Effective implementation hinges on accurate intelligence, advanced technology integration, and strong leadership. While these offer benefits in efficiency and focus, they also risk threat inflation, neglect of lesser-prioritized threats, strained international relations, and arms race escalation. Policymakers must consider these risks and adopt a comprehensive strategy that balances military readiness with diplomatic efforts to ensure sustainable security and global stability.

References

Aljazeera. (2023, October 12). *What is Israel's Iron Dome defence system and is it effective? All to know*. Aljazeera. https://www.aljazeera.com/news/2023/10/12/whats-the-israel-iron-dome-defence-system-and-is-it-effective-all-to-know

Atmore, L. Y. (2014). *Fear factors in: political rhetoric, threat inflation, and the narrative of September 11*. (Doctoral dissertation, master's thesis, Naval Postgraduate School).

Bachmann, S. D., & Gunneriusson, H. (2014). Terrorism and cyber attacks as hybrid threats: Defining a comprehensive approach for countering 21st century threats to global risk and security. *The Journal on Terrorism and Security Analysis*.

Backman, S. (2023). Risk vs. threat-based cybersecurity: the case of the EU. *European Security*, *32*(1), 85–103.

Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artificial Intelligence Review*, *54*(5), 3849–3886.

Binnendijk, H., Hamilton, D. S., & Barry, C. L. (2016). Alliance revitalized: NATO for a new era. *The Washington NATO Project, Johns Hopkins University*.

Borum, R., Felker, J., Kern, S., Dennesen, K., & Feyes, T. (2015). Strategic cyber intelligence. *Information & Computer Security*, *23*(3), 317–332.

Callahan, A. M. (n.d.). *An assessment on Israel's "Iron Dome" Defense System*. Universidad de Navarra. Retrieved July 17, 2024, from https://www.unav.edu/web/global-affairs/detalle/-/blogs/an-assessment-on-israel-s-iron-dome-defense-system

Carlin, J. P. (2015). Detect, disrupt, deter: A whole-of-government approach to national security cyber threats. *Harv. Nat'l Sec. J.*, *7*, 391.

Chen, L., & Yang, H. (2023). The dynamic nature of cyber threats and its implications for defense policy. *Journal of Cybersecurity Studies*, *15*(2), 85–102.

Christianson, J. (2016). Threat-Based and Capabilities-Based Strategies in a Complex World School of Advanced Military Studies. *School of Advanced Military Studies*.

Cohen, E. A. (2017). *The big stick: the limits of soft power and the necessity of military force*. Hachette UK.

Creswell, J. W. (2018). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches* (4th ed.)*. SAGE Publications.

Department of Defense. (2022). *Department of Defense Cyber Strategy*. https://www.defense.gov

Freier, N. P., Bado, C. M., Bolan, C. J., & Hume, R. S. (2017). *At our own peril: DOD risk assessment in a post-primacy world*.

Garcia, R., & Patel, S. (2023). Artificial intelligence in threat detection: Enhancing defense strategies through technology. *Defense Technology Review*, *28*(3), 112–129.

GSA FedRAMP PMO. (2022). *Threat-Based Risk Profiling Methodology Developed by: GSA FedRAMP PMO Threat-Based Risk Profiling Methodology White Paper Document Revision History*.

Ikedinma, H. A. (2017). Impact of Military Spending on African Development. *Ife Social Sciences Review*, *25*(1), 98–111.

Johnson, M., & Lee, S. (2023). Efficient defense spending through threat-based policies: A comparative analysis. *International Security Quarterly*, *34*(1), 57–78.

Johnston, M. P. (2014). Secondary data analysis: A method of which the time has come. *Qualitative and Quantitative Methods in Libraries*, *3*(3), 619–626.

Lowenthal, M. M. (2022). *Intelligence: From secrets to policy*. CQ press.

Maddireddy, B. R., & Maddireddy, B. R. (2022). Cybersecurity Threat Landscape: Predictive Modelling Using Advanced AI Algorithms. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(2), 270–285.

Mahoney, R. T. (2010). Threat-based Response Patterns for Emergency Services: Developing Operational Plans, Policies, Leadership, and Procedures for a Terrorist Environment. *Homeland Security Affairs*, *6*(3).

Mayer, M. (2014). *Trends in US security policy*.

Medahl, M. (2012). Significance of a Duty's Direction: Claiming Priority Rather than Prioritizing Claims. *J. Ethics & Soc. Phil.*, *7*, viii.

Miller, T. (2022). The perils of threat inflation in defense policy. *Strategic Studies Review*, *19*(4), 203–220.

Moran, T. H. (1990). The globalization of America's defense industries: Managing the threat of foreign dependence. *International Security*, *15*(1), 57–99.

NATO. (2023). *NATO's enhanced deterrence posture in Eastern Europe*. NATO. https://www.nato.int/docu/review/articles/2023/01/15/nato-enhanced-deterrence-posture

NATO. (2024, July 1). *Deterrence and defence*. https://www.nato.int/cps/en/natohq/topics_133127.htm

Okromtchedlishvili, I. (2024). Building Resilience: Advancing Defense Acquisition Capabilities in Georgia. *Journal of Defense Resources Management (JoDRM)*, *15*(1), 5–34.

Rangaraju, S. (2023). Secure by intelligence: enhancing products with AI-driven security measures. *EPH-International Journal of Science And Engineering*, *9*(3), 36–41.

Rayhan, A. (n.d.). *Cybersecurity in the Digital Age: Assessing Threats and Strengthening Defenses*.

Rosen, S. (2014). *Strategic planning and management in defense systems acquisition*.

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors*, *23*(16), 7273.

Sarjito, A. (2024). Peran Intelijen Melalui Perumusan Kebijakan Pertahanan Negara dalam Perang Hibrida. *PANDITA: Interdisciplinary Journal of Public Affairs*, *7*(1), 74–88.

Schmidt, J. M. (2015). Policy, planning, intelligence and foresight in government organizations. *Foresight*, *17*(5), 489–511.

Treddenick, J. M. (1985). The arms race and military Keynesianism. *Canadian Public Policy/Analyse de Politiques*, 77–92.

U.S. Department of Defense. (2022). *National Defense Strategy*. U.S. Department of Defense. https://www.defense.gov/national-defense-strategy-2022

Van der Meer, S. (2015). Foreign Policy Responses to International Cyber-attacks. *Some Lessons Learned, The Hague: Clingendael Netherlands Institute of International Relations*.

Vershbow, A. (2021, November 7). *How NATO Can Help Ukraine Deter Russian Aggression*. The National Interest. https://global.upenn.edu/perryworldhouse/news/how-nato-can-help-ukraine-deter-russian-aggression

Vyas, S., Hannay, J., Bolton, A., & Burnap, P. P. (2023). Automated cyber defence: A review. *ArXiv Preprint ArXiv:2303.04926*.

Williams, R. (2022). The theoretical foundations of threat-based defense policies. *Defense Policy Analysis*, *17*(3), 45–63.