International Journal Of Humanities Education And Social Sciences ***(IJHESS)*** *E-ISSN:* **2808-1765**
Volume 5, Number 3, December 2025, *Page. 1646 – 1653*
Email : editorijhess@gmail.com

The Philosophy of Defense Science as a Foundation for Developing National Defense Policies in Addressing Asymmetric Warfare

Khansa Mutiara Syah Putri[1)], Suradi Agung Slamet[2)], Rudianto[3)], Tasdik Mustika Alam[4)]
[1,2,3,4)] Universitas Pertahanan Indonesia

*Corresponding Author
Email: khansa.putri@sp.idu.ac.id

Abstract

This study aims to analyze the role of the philosophy of science in formulating national Defense policies to address asymmetric warfare threats. These threats, such as cyber warfare and digital propaganda, pose significant challenges to traditional Defense strategies. The research employs a qualitative approach with literature review to gain an in-depth understanding of the application of epistemology, ontology, and axiology in modern Defense strategies. The results indicate that the philosophy of science provides an essential conceptual framework for understanding the multidimensional threats of asymmetric warfare. Epistemology ensures that policies are based on valid knowledge through intelligence gathering and strategic data analysis. Ontology aids in defining new threats, such as cyber and disinformation attacks, while axiology ensures ethical policies by integrating humanitarian values. Moreover, national Defense education focusing on digital literacy and cybersecurity is recommended to enhance societal resilience against non-conventional threats. Technologies such as artificial intelligence (AI) and big data are also identified as critical tools for efficiently detecting and responding to threats. In conclusion, the philosophy of science not only aids in formulating responsive policies but also promotes a holistic approach involving social, political, and technological dimensions. Its implementation strengthens the legitimacy of national Defense policies and creates sustainable Defense strategies to address the complexities of asymmetric threats. This study recommends integrating the philosophy of science into education, technology development, and international collaboration to enhance the effectiveness of national Defense policies.

Keywords: Philosophy of Defense Science, National Defense, Asymmetric Warfare.

INTRODUCTION

The philosophy of science is the study of the nature, origins, and limits of knowledge. In the context of national defense, the philosophy of science plays a crucial role in providing a strong conceptual foundation for developing adaptive and visionary defense policies and strategies. The philosophy of science encourages in-depth reflection on the basic assumptions and paradigms used in defense policy, thus establishing a solid theoretical foundation relevant to current challenges (Chalmers, 2013).

The philosophy of science in the context of national defense provides a systematic framework for understanding threats. This includes both conventional and non-conventional threats such as asymmetric warfare and cyberattacks. With the philosophy of science, policymakers can identify and integrate relevant scientific principles, such as understanding how knowledge is acquired and used for defense strategy (Audi, 2015). This provides critical insight into existing strategies, thereby making defense policy more responsive and adaptive to global dynamics.

Furthermore, the philosophy of science can help develop policies based on national values and universal ethics. For example, the development of a national defense policy that prioritizes human rights and justice, grounded in a strong philosophical foundation. With the philosophy of science, policymakers can critically explore these values, thus grounding their policies in morality (Popper, 2002). This approach can enhance defense policy legitimacy and public support.

The philosophy of science also plays a role in facilitating multidisciplinary dialogue between various fields of science relevant to defense, such as technology, economics, and sociology. This combination enriches perspectives in strategic decision-making. For example, in

addressing the threat of terrorism, the philosophy of science helps synergize modern technological approaches with in-depth socio-cultural analysis (Searle, 2010). This, in turn, contributes to more effective and holistic defense policy.

The philosophy of science also plays a crucial role in creating innovation in national defense. Through critical reflection and methodological exploration, the philosophy of science encourages the development of new, more innovative approaches that are relevant to future challenges. This includes the development of artificially based strategies and big data to detect and respond to threats more quickly and accurately (Rescher, 2012). With a strong philosophical foundation, national defense can continue to adapt and develop along with changing times.

Warfare is currently undergoing a significant paradigmatic transformation from conventional to asymmetric forms in line with global technological, social, and geopolitical developments. Conventional warfare, characterized by direct confrontation between states with equal military power, is now shifting toward asymmetric warfare, in which non-state actors are involved and unconventional tactics play a major role. This shift alters perspectives on conflict and national defense strategies. According to Metz & Johnson (2001), asymmetric warfare reflects an imbalance of power, where the weaker party uses innovative strategies to exploit the weaknesses of the stronger party.

Conventional warfare focuses on physical strength and military dominance through open combat. However, in asymmetric warfare, this approach is no longer relevant, as the weaker party adopts guerrilla tactics, sabotage, and non-linear attacks to weaken the opponent's strength. For example, modern conflicts like the war in Afghanistan, where the Taliban used asymmetric tactics to counter NATO forces that were technologically and personnel-superior (Kilcullen, 2009). This shift requires adapting a more flexible and responsive defense strategy.

Asymmetric warfare involves the use of the latest technologies, such as cyberattacks and digital propaganda, with the aim of creating instability without direct involvement. According to Rid (2012), cyberwarfare is a new dimension of asymmetric warfare, allowing non-state actors to attack critical infrastructure without the use of physical weapons. These attacks can cripple an opponent's economy and communications at a lower cost but with high impact, thus changing the way national security is viewed.

Asymmetric warfare is not solely a military phenomenon but is deeply embedded in social, cultural, and political contexts that conventional defense strategies often overlook. Rather than relying on direct confrontation, asymmetric actors exploit societal divisions, public dissatisfaction, and identity-based grievances to mobilize support and undermine state authority. While the concept of *netwar* introduced by Arquilla & Ronfeldt (2001) explains the organizational advantages of decentralized networks, recent empirical studies demonstrate that these dynamics have intensified with digitalization and hybrid conflict environments. Killcullen (2020) shows through comparative case studies that non-state and revisionist actors have increasingly learned to offset conventional military superiority by targeting societal cohesion, information systems, and governance capacity. Empirical analyses further indicate that asymmetric conflicts are most effective when military operations are synchronized with information warfare and social influence campaigns (Hoffman, 2018).

This transformation in the character of warfare compels states to adopt more comprehensive and adaptive defense strategies. Traditional defense policies centered on kinetic superiority and force projection are increasingly insufficient in addressing multidimensional threats. Degaut (2020) empirically demonstrates that contemporary conflicts demand defense approaches integrating military capabilities with political, informational, and societal instruments to prevent strategic surprise and escalation. Similarly, Biddle et al. (2012), through quantitative conflict analysis, show that successful counter-asymmetric strategies depend less on overwhelming force and more on intelligence integration, population security, and institutional coordination.

The implications of asymmetric warfare for national defense policy are therefore profound. Defense planning must shift from a narrow focus on conventional force dominance toward multidimensional frameworks that incorporate intelligence operations, counterterrorism, and community engagement. Empirical research on counterinsurgency and irregular warfare confirms that population-centric approaches significantly reduce the effectiveness of asymmetric actors by limiting recruitment and legitimacy (Killcullen, 2020). This shift reflects a broader transition from coercive military responses toward preventive and resilience-based defense policies.

Moreover, asymmetric warfare increasingly manifests in non-physical domains, particularly cyber and information warfare. Empirical studies on cyber conflict indicate that cyber operations enable asymmetric actors to disrupt critical infrastructure and influence political decision-making without crossing traditional thresholds of armed conflict (Smeets, 2021; Brantly, 2021). Rid (2020) further demonstrates that disinformation and covert influence operations have become central tools of asymmetric strategy, blurring the distinction between war and peace and complicating deterrence frameworks. Consequently, national defense policies must incorporate cyber resilience, public–private cooperation, and strategic communication as core components of national security.

Beyond technological and military dimensions, asymmetric warfare exerts significant social impacts that directly influence national stability. Empirical research on disinformation campaigns reveals that asymmetric actors deliberately target public trust in state institutions to generate political paralysis and social fragmentation (Kavanagh et al., 2020; Lanoszka, 2019). These findings underscore the necessity for defense policies that address information security, narrative control, and societal resilience alongside physical defense measures.

Given the transnational nature of asymmetric threats, international cooperation and defense diplomacy have become indispensable. Empirical assessments of hybrid and cyber threats show that unilateral defense measures are insufficient, as asymmetric operations frequently transcend national borders and exploit regulatory gaps between states (Hoffman, 2018; United Nations Development Programme (UNDP), 2021). Accordingly, states must align domestic defense policies with regional and international security frameworks to effectively counter evolving asymmetric challenges.

Based on this context, this study aims to analyze the role of the philosophy of defense science in shaping national defense policy and to examine how contemporary philosophical perspectives can inform strategic responses to asymmetric warfare in an increasingly complex security environment.

RESEARCH METHODS

The research methodology used combines a qualitative approach with a literature review to gain a more comprehensive understanding of the research problem. This qualitative approach focuses on empirical research experience, which is crucial for a deeper understanding of the philosophy of defense science, which serves as the foundation for developing national defense policies in the face of asymmetric warfare (Sugiyono, 2010).

In data collection, a literature review was used to gather valid data from various sources, such as books, journals, and relevant previous articles. This was used to help identify knowledge gaps, develop new ideas, and strengthen the theoretical basis of the research.

In addition, the use of data analysis techniques in secondary data from previous studies to gain more insight into the problems being studied and support research findings (Petersen et al, 2015).

RESULT AND DISCUSSION

a. Philosophy of Defense Science as the Basis for National Defense Policy

The philosophy of science is an in-depth study of the foundations of knowledge, methods, and validity of science. In the defense context, the philosophy of science provides a conceptual and normative foundation that guides the development of state policies in response to various security threats. The philosophy of science is used by policymakers to understand the complex realities of war, including conventional and asymmetric threats, through a systematic framework. This thinking applies because defense policy addresses not only military strategy but also political, social, economic, and cultural dimensions (Nagel, 2021).

The current era of asymmetric warfare has led the philosophy of defense science to sharpen its analysis of the nature of conflict, threat identification, and necessary responses. Thus, the philosophy of defense science serves not only as a guideline for developing security theories but also as a practical guide for governments in designing adaptive and effective policies (Huntington, 2020).

The philosophy of science also provides an inherent theoretical framework for understanding the nature of national defense. For example, ontology is a key aspect related to the nature of threats. Threats to the state no longer consist of military aggression, but also encompass non-conventional threats such as cyberwarfare, terrorism, climate change, and pandemics. The ontology of the philosophy of science also aids policymaking in identifying threats comprehensively (Gutting, 2020).

In epistemology, the philosophy of science plays a crucial role in studying how to acquire knowledge. In the context of defense policy, epistemology ensures that information used in decision-making comes from valid and reliable sources. For example, in asymmetric warfare, understanding enemy tactics requires data-driven intelligence gathering and in-depth analysis. The philosophy of science also ensures that this process is not based on mere assumptions but on verifiable empirical knowledge (Nagel, 2021).

Axiology, or the study of values, helps formulate defense policies that are not only effective but also ethical. As in asymmetric warfare, defense strategies often face moral dilemmas such as the protection of civilians and the proportional use of force. The philosophy of defense science integrates these ethical values into policy to ensure that state actions remain consistent with humanitarian principles and international law (Rawls, 2020).

Asymmetric warfare currently poses a significant challenge to defense policy due to the involvement of non-state actors and unconventional tactics. For example, the actions of terrorist groups, transnational criminal organizations, and cyberattacks pose asymmetric threats that are difficult to address with conventional approaches. Therefore, the philosophy of science requires states to develop responsive and adaptive policies.

A comprehensive approach involving political, social, economic, and technological dimensions is needed because military power alone is insufficient. The philosophy of science helps identify the multidimensional nature of asymmetric warfare. For example, counterterrorism strategies require not only military operations but also deradicalization programs, strengthening state ideology, and digital literacy to counter extremist propaganda (Cronin, 2020).

The philosophy of science also provides a framework for understanding the importance of technological innovation in countering asymmetric warfare. Cyberattacks require a high-tech response and the development of advanced cyber capabilities. With a philosophical approach, countries can prioritize research and development (R&D) in cybersecurity as part of their national defense policy (Clarke & Knake, 2021).

Furthermore, the philosophy of science also helps states formulate policies that strengthen societal resilience. In asymmetric warfare, communities are often the target of both physical and

psychological attacks. With an axiological approach, defense policies can be designed to directly involve communities in defense efforts through national defense education and increased threat awareness (Huntington, 2020).

In the modern era of uncertainty, philosophy remains relevant for designing defense policies. The philosophy of science sharpens the ability to analyze and predict future threats. With a philosophical approach, policymakers can also identify global trends such as technological advancements and geopolitical changes that have the potential to impact national security (Nagel, 2021).

The philosophy of science also ensures that defense policies are not merely reactive but also proactive. For example, in the face of cyber threats, the philosophy of science helps countries design policies that not only protect existing infrastructure but also help prevent attacks by strengthening regulations and international cooperation (Clarke & Knake, 2021).

Furthermore, the philosophy of science also provides a moral and ethical foundation for defense policy. In asymmetric warfare, decision-making often has significant consequences for civilians. By considering the axiological dimension, the philosophy of science ensures that defense policy remains compliant with humanitarian values and justice (Rawls, 2020).

b. Implementation of the Philosophy of Science in Facing Asymmetric Warfare

Asymmetric warfare poses a strategic threat to state sovereignty and stability in the modern era. Unlike conventional warfare, asymmetric warfare relies on indirect tactics such as terrorism, cyber warfare, and propaganda, often exploiting weaknesses in a nation's social, economic, and political systems. Therefore, the philosophy of science plays a crucial role in developing a holistic approach based on rationality and scientific methodology to understand, analyze, and develop adaptive strategies to address this threat.

As is well known, the philosophy of science prioritizes an epistemological approach in examining how knowledge is generated and applied in specific contexts. In the face of asymmetric threats, this approach encourages analysis that encompasses various disciplines, such as information technology, psychology, and sociology.

Asymmetric threats tend to be non-conventional and not bound by traditional rules of war. These include cyberattacks that paralyze critical infrastructure, such as banking and communications systems. According to a report from Center for Strategic and International Studies (2022), cyber attacks have increased significantly in recent decades and have a global economic impact reaching billions of dollars.

This threat also involves information warfare and disinformation that have the aim of creating social instability. Jean Baudrillard in Simulacra and Simulation highlights the existence of a reality that can be manipulated through the media and used as a tool of war to shape public opinion (Baudrillard, 1994). Therefore, an understanding of the philosophy of science helps develop policies that focus not only on physical defense, but also on the information and psychological security of society.

In the face of asymmetric threats, national defense policies must be dynamic and adaptive. This includes integrating advanced technological approaches and utilizing trained human resources. For example, the policy cyber defense designed by Estonia after a major cyberattack in 2007 became a global model for digital infrastructure protection (NATO CCDCOE, 2020).

The philosophy of science informs the development of this policy through an evidence-based approach and critical analysis of the successes and failures of similar policies in other countries. This approach also emphasizes the importance of technology-based national defense education, including digital skills training and strengthening media literacy to counter propaganda and disinformation.

National defense education is a crucial component in addressing asymmetric threats. According to Pierre Bourdieu, cultural capital, in the form of individual knowledge and skills, is key to building community resilience (Bourdieu, 1986). Therefore, the national defense

curriculum must include a thorough understanding of asymmetric threats and how to address them.

For example, Finland's national defense education program, which includes practical training in cybersecurity and media literacy, demonstrates increased societal resilience to disinformation (European Commission, 2021). The implementation of the philosophy of science in national defense education emphasizes the importance of an interdisciplinary approach in developing the adaptive capacity of communities.

In addition to education, the development of technology and infrastructure is crucial to national defense policy. By utilizing artificial intelligence (AI) in analyzing threat data, as well as developing sophisticated cybersecurity systems, are strategic steps in facing asymmetric warfare. According to a McKinsey & Company (2022), integration AI in national security strategy can increase the efficiency of threat detection and response by 70%.

However, this policy must be based on strong ethical principles to prevent the misuse of technology. This aligns with Immanuel Kant's view of the importance of morality in the application of science for just and beneficial purposes for humanity (Kant, 1997).

Implementing national defense policies in the face of asymmetric threats faces various challenges, including cultural resistance, lack of resources, and the complexity of inter-agency coordination. Therefore, a philosophy-based approach that emphasizes a deep understanding of the socio-political context is key to success. As Thomas Kuhn put it in The Structure of Scientific Revolutions, paradigm shifts require critical and innovative thinking in overcoming existing obstacles (Kuhn, 1962).

With an evidence-based, adaptive, and interdisciplinary approach, national defense policies can be developed with the aid of the philosophy of science to protect national sovereignty and stability in the modern era. Implementing national defense education, developing technology, and adapting strategies are crucial elements in addressing this challenge.

CONCLUSION

Asymmetric warfare is transforming the traditional paradigm of national defense, presenting new challenges, such as cyberattacks, digital propaganda, and other unconventional threats. To address these threats, the philosophy of science provides an essential conceptual framework through epistemological, ontological, and axiological approaches. This approach allows for adaptive national defense policies to be designed, evidence-based, and grounded in universal ethical values. With the integration of these disciplines, defense strategies become more comprehensive, encompassing technological, social, and political aspects in addressing ever-changing global dynamics.

The philosophy of defense science also emphasizes the importance of national defense education oriented toward strengthening digital literacy, cybersecurity, and social resilience. Adaptive policy implementation with the support of modern technologies such as artificial intelligence (AI) can increase the effectiveness of responses to asymmetric threats. In the long term, a philosophy-based approach can create innovative defense strategies, encourage collaboration between sectors, and ensure policy legitimacy in the public eye. Thus, the philosophy of science serves not only as an analytical tool but also as a foundation for developing a more visionary and sustainable national defense policy.

REFERENCES

Arquilla, J., & Ronfeldt, D. (2001). *Networks and Netwars: The Future of Terror, Crime, and Militancy*.

Audi, R. (2015). *Epistemology: A Contemporary Introduction to the Theory of Knowledge* (3rd ed.). Routledge.

Baudrillard, J. (1994). *Simulacra and Simulation*. University of Michigan Press.

Biddle, S., Friedman, J. A., & Shapiro, J. N. (2012). Testing the Surge: Why Did Violence Decline in Iraq in 2007? *International Security*, *37*(1), 7–40. http://www.jstor.org/stable/23280403

Bourdieu, P. (1986). The Forms of Capital. In J. Richardson (Ed.), *in Handbook of Theory and Research for the Sociology of Education* (pp. 241–258). Greenwood Press.

Brantly, A. F. (2021). *The decision to attack: Military and intelligence cyber decision-making*. University of Georgia Press.

Center for Strategic and International Studies (CSIS). (2022). *Significant Cyber Incidents*. https://www.csis.org

Chalmers, A. F. (2013). *What Is This Thing Called Science?* Hackett Publishing.

Clarke, R. A., & Knake, R. K. (2021). *Cyber War: The Next Threat to National Security and What to Do About It*. HarperCollins.

Cronin, A. K. (2020). *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns*. Princeton University Press.

Degaut, M. (2020). Do the new forms of warfare require new forms of defense? *Comparative Strategy*, *3*(2), 97–118. https://doi.org/10.1080/01495933.2020.1737371

European Commission. (2021). *Digital Education Action Plan 2021-2027*.

Gutting, G. (2020). *What Philosophers Know: Case Studies in Recent Analytic Philosophy*. Cambridge University Press.

Hoffman, F. G. (2018). Examining complex forms of conflict. *PRISM*, *7*(4), 30–47.

Huntington, S. P. (2020). *The Soldier and the State: The Theory and Politics of Civil-Military Relations*. Harvard University Press.

Kant, I. (1997). *Groundwork of the Metaphysics of Morals*. Cambridge University Press.

Kavanagh, J., Marcellino, W., Blake, J. S., Smith, S. G., Davenport, S., & Triezenberg, B. (2020). *False information as a weapon: Understanding and countering disinformation*. RAND Corporation.

Kilcullen, D. (2009). *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One*. Oxford University Press.

Kuhn, T. S. (1962). *The Structure of Scientific Revolutions*. University of Chicago Press.

Lanoszka, A. (2019). Disinformation in international politics. *European Journal of International Security*, *4*(2), 227–248. https://doi.org/10.1017/eis.2019.6

McKinsey & Company. (2022). *The Future of National Security: AI and Data*. https://www.mckinsey.com

Metz, S., & Johnson, D. V. (2001). *Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts*. Strategic Studies Institute.

Nagel, T. (2021). *The View from Nowhere*. Oxford University Press.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (2020). *Cyber Security Strategy of Estonia*. https://ccdcoe.org

Popper, K. (2002). *The Logic of Scientific Discovery*. Routledge.

Rawls, J. (2020). *A Theory of Justice*. Harvard University Press.

Rescher, N. (2012). *Philosophical Inquiries: An Introduction to Problems of Philosophy*. University of Pittsburgh Press.

Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.

Searle, J. R. (2010). *Making the Social World: The Structure of Human Civilization*. Oxford University Press.

Smeets, M. (2021). Cyber deterrence and escalation. *Journal of Strategic Studies*, *44*(4), 527–553. https://doi.org/10.1080/01402390.2020.1734506

United Nations Development Programme (UNDP). (2021). *Human security handbook*. UNDP.