PUBLICNESS
Journal of Public Administration Studies
https://publicness.ppj.unp.ac.id - Volume 3 | Nomor 1 | Tahun 2024

ISSN 2830-1714 (Cetak)
ISSN 2830-0963 (Online)

COUNTERING HYBRID THREATS: CHALLENGES AND THE ROLE OF DEFENSE SCIENCE

Aris Sarjito[1(a)]

[1]*Fakultas Manajemen Pertahanan, Universitas Pertahanan Republik Indonesia*
[a)]*arissarjito@gmail.com*

INFORMASI ARTIKEL

Article History:
Dikirim:
01-04-2024
Diterbitkan Online:
30-04-2024

Kata Kunci:
Ancaman Hibrida, Ilmu Pertahanan, Keamanan Nasional, Keamanan Siber, Perang Informasi

ABSTRAK

Studi ini mengkaji evolusi ancaman hibrida, implikasi keamanan nasional, dan peran ilmu pertahanan dalam melawan dan memperkuat kemampuan pertahanan menggunakan analisis data sekunder. Penelitian ini bertujuan untuk mengidentifikasi tren dan strategi utama untuk melawan ancaman hibrida secara efektif, dengan fokus pada peran ilmu pertahanan dalam meningkatkan kemampuan pertahanan nasional. Metode penelitian kualitatif digunakan untuk menganalisis literatur dan studi kasus yang ada mengenai ancaman hibrida dan kontribusi ilmu pertahanan. Temuan menunjukkan bahwa ancaman hibrida telah berkembang secara signifikan dalam lanskap keamanan kontemporer, sehingga memerlukan strategi pertahanan yang adaptif dan inovatif. Ilmu pertahanan memainkan peran penting dalam mengembangkan teknologi dan metodologi canggih untuk melawan ancaman hibrida, termasuk langkah-langkah keamanan siber, taktik perang informasi, dan strategi komunikasi strategis. Rekomendasi diberikan kepada para pembuat kebijakan dan praktisi pertahanan untuk memperkuat kemampuan pertahanan dan memitigasi tantangan perang hibrida, dengan menekankan pentingnya kolaborasi interdisipliner, kerja sama internasional, dan pengembangan sumber daya manusia. Sebagai kesimpulan, studi ini menggarisbawahi pentingnya mengintegrasikan wawasan dari ilmu pertahanan ke dalam upaya perencanaan dan kesiapsiagaan pertahanan untuk secara efektif melawan ancaman hibrida dan menjaga keamanan nasional.

Keywords:
Cybersecurity, Defense Science, Hybrid Threats, Information Warfare, National Security

Corresponding Author:
arissarjito@gmail.com

ABSTRACT

This study examines hybrid threats' evolution, national security implications, and defense science's role in countering and strengthening defense capabilities using secondary data analysis. The research aims to identify key trends and strategies for countering hybrid threats effectively, with a focus on the role of defense science in enhancing national defense capabilities. Qualitative research methods are employed to analyze existing literature and case studies on hybrid threats and defense science contributions. Findings suggest that hybrid threats have evolved significantly in the contemporary security landscape, necessitating adaptive and innovative defense strategies. Defense science plays a critical role in developing advanced technologies and methodologies to counter hybrid threats, including cybersecurity measures, information warfare tactics, and strategic communication strategies. Recommendations are provided for policymakers and defense practitioners to strengthen defense capabilities and mitigate the challenges of hybrid warfare, emphasizing the importance of interdisciplinary collaboration, international cooperation, and human capital development. In conclusion, the study underscores the importance of integrating insights from defense science into defense planning and preparedness efforts to effectively counter hybrid threats and safeguard national security.

DOI:
https://doi.org/10.24036/publicness.v3i1.188

INTRODUCTION

In today's complex security landscape, traditional notions of warfare have evolved, giving rise to hybrid threats that blend conventional military tactics with unconventional methods such as cyberattacks, disinformation campaigns, and proxy warfare. Hybrid threats pose significant challenges to national security, requiring innovative approaches for effective countering. This essay explores the state-of-the-art research on countering hybrid threats, focusing on the role of defense science in addressing these challenges.

Hybrid threats encompass a spectrum of tactics employed by state and non-state actors to achieve strategic objectives while avoiding confrontation. According to NATO's definition of hybrid threats, they frequently take advantage of weaknesses in the political, economic, and information domains by combining conventional, irregular, and asymmetric methods (NATO, 2010). These threats blur the lines between war and peace, making deterrence and defense strategies more difficult to formulate and implement.

Countering hybrid threats requires a comprehensive understanding of the multifaceted nature of contemporary warfare. One of the primary challenges lies in identifying and attributing attacks conducted through unconventional means, such as cyber operations and disinformation campaigns. The lack of clear-cut definitions and boundaries exacerbates this challenge, hindering effective response mechanisms (Rid & Buchanan, 2015).

Additionally, hybrid threats exploit the interconnectedness of modern societies, leveraging global communication networks and economic dependencies to undermine stability and sow discord. Traditional military capabilities alone are insufficient to address these complex threats, necessitating a holistic approach that incorporates diplomatic, economic, and technological measures (Hoffman, 2007).

Defense science plays a crucial role in developing innovative solutions to counter hybrid threats effectively. By leveraging advances in technology and interdisciplinary research, defense scientists can enhance capabilities in areas such as cybersecurity, information warfare, and strategic communication.

In the realm of cybersecurity, defense science focuses on developing robust defensive mechanisms to protect critical infrastructure and networks from cyberattacks launched by hybrid adversaries. This includes the development of advanced encryption protocols, intrusion detection systems, and threat intelligence platforms (Schneier, 2015).

Furthermore, defense science contributes to the field of information warfare by studying the psychology of influence and designing counter-narratives to combat disinformation campaigns. By understanding the tactics employed by hybrid actors to manipulate public opinion and undermine trust in democratic institutions, defense scientists can develop effective strategies to counter these efforts (Wardle & Derakhshan, 2017).

Moreover, defense science plays a vital role in enhancing situational awareness and decision-making capabilities through the use of advanced data analytics and artificial intelligence. By aggregating and analyzing vast amounts of heterogeneous data sources, defense scientists can provide policymakers and military commanders with timely and accurate assessments of hybrid threats, enabling proactive response measures (Cummings, 2017).

Countering hybrid threats requires a concerted effort that integrates military, diplomatic, economic, and technological measures. Defense science plays a pivotal role in this endeavor by developing innovative solutions to address the multifaceted challenges posed by hybrid warfare. By leveraging interdisciplinary research and advanced technologies, defense scientists can enhance the resilience and effectiveness of national defense capabilities against evolving security threats.

Problem Statement

In recent years, the emergence of hybrid threats has presented a formidable challenge to national security, blending conventional military tactics with unconventional methods such as cyber warfare, disinformation campaigns, and proxy conflicts. These hybrid tactics exploit vulnerabilities in political, economic, and societal domains, posing significant challenges to traditional defense mechanisms. Addressing these challenges requires a nuanced understanding of hybrid threats and innovative strategies to counter them effectively, highlighting the crucial role of defense science in bolstering national defense capabilities.

The research aims to analyze the evolving nature of hybrid threats and their impact on national security, including cyber-attacks, information warfare, and proxy conflicts. It also evaluates the role of defense science in developing strategies and technologies to counter hybrid threats effectively, focusing on advanced technologies like artificial intelligence, data analytics, and encryption protocols. The objective also proposes recommendations for enhancing defense capabilities in response to hybrid threats, translating research findings into actionable recommendations for policymakers and practitioners. These recommendations aim to support decision-making processes and enhance national defense preparedness by synthesizing insights from the analysis of hybrid threats and defense science contributions.

Research Questions

1. How have hybrid threats evolved in the contemporary security landscape, and what are their implications for national security? This question seeks to explore the various forms of hybrid threats, including cyber attacks, information manipulation, and irregular warfare, and their impact on national security. By examining the changing nature of hybrid threats, researchers can identify emerging trends and anticipate future challenges in defense planning and preparedness.
2. What contributions does defense science make in countering hybrid threats, particularly in areas such as cybersecurity, information warfare, and strategic communication? This question focuses on evaluating the role of defense science in developing innovative strategies and technologies to counter hybrid threats effectively. It involves assessing the effectiveness of existing defense technologies and methodologies in addressing the challenges posed by hybrid warfare and identifying areas for further research and development.
3. What recommendations can be formulated to strengthen defense capabilities and mitigate the challenges posed by hybrid warfare effectively? This question aims to translate research findings into actionable recommendations for policymakers and defense practitioners. It involves synthesizing insights from the analysis of hybrid threats and the evaluation of defense science contributions to develop comprehensive strategies for countering hybrid warfare. By providing practical recommendations, this question seeks to enhance national defense preparedness and resilience against hybrid threats.

RESEARCH METHODS

Qualitative research methods, particularly those utilizing secondary data, offer valuable insights into complex phenomena such as hybrid threats and the role of defense science in addressing them. In the context of countering hybrid threats, qualitative research methods allow researchers to explore the multifaceted nature of these challenges and assess the effectiveness of defense strategies. This essay will discuss qualitative research methods using secondary data according to Creswell's framework, focusing on their application to the study of hybrid threats and defense science.

Creswell (2014) outlines several key steps in conducting qualitative research using secondary data, including identifying a research problem, determining the purpose of the study, selecting appropriate data sources, analyzing the data, and interpreting the findings. In the case of researching hybrid threats and defense science, the first step involves clearly defining the research problem, such as understanding the evolving nature of hybrid threats and evaluating the contributions of defense science in countering them.

Once the research problem is identified, researchers must determine the purpose of the study, which may include exploring trends in hybrid warfare, examining case studies of successful defense strategies, or assessing the impact of technological advancements on defense capabilities. With a clear purpose in mind, researchers can then select appropriate data sources, including academic journals, government reports, policy documents, and case studies (Creswell, 2014).

The next step in qualitative research using secondary data is data analysis. This involves systematically reviewing and synthesizing existing literature and other relevant sources to identify key themes, patterns, and insights related to hybrid threats and defense science. Researchers may employ various analytical techniques, such as thematic analysis or content analysis, to organize and interpret the data effectively (Creswell, 2014).

Finally, researchers must interpret the findings of their analysis, drawing conclusions and implications for theory, practice, and policy. This may involve identifying gaps in the existing literature, proposing theoretical frameworks for understanding hybrid threats or recommending strategies for enhancing defense capabilities. Through rigorous analysis and interpretation, qualitative research using secondary data contributes to a deeper understanding of hybrid threats and informs evidence-based policymaking and defense planning (Creswell, 2014).

In summary, qualitative research methods using secondary data offer valuable insights into the complex challenges posed by hybrid threats and the role of defense science in addressing them. By following Creswell's framework, researchers can systematically explore and analyze existing literature and other sources to uncover key insights and inform effective strategies for countering hybrid threats.

Theoretical Frameworks for Analyzing Research Questions:

Evolution of Hybrid Threats and Implications for National Security:

To analyze the evolution of hybrid threats and their implications for national security, researchers can draw upon several theoretical frameworks:

a) Complex Systems Theory: This theory posits that hybrid threats emerge from the interaction of various interconnected systems, including political, economic, technological, and social domains (Mitchell, 2009). Researchers can examine how hybrid threats change over time as a result of dynamic interactions between various actors and factors in the current security landscape by applying complex systems theory.

b) Strategic Culture Theory: Strategic culture theory emphasizes the influence of historical experiences, values, and norms on the behavior of states and non-state actors in security matters (Krause & Williams, 1996). By examining the strategic cultures of hybrid adversaries, researchers can gain insights into their motivations, tactics, and objectives, thereby elucidating the evolution of hybrid threats and their implications for national security.

Contributions of Defense Science to Countering Hybrid Threats:

To analyze the contributions of defense science to countering hybrid threats, researchers can utilize the following theoretical frameworks:

a) Innovation Diffusion Theory: Innovation diffusion theory explores how new technologies and methodologies spread and are adopted within organizations and societies (Rogers et al., 2014). Researchers can use this theory to look at how new ideas in defense science are spread and used in areas like cybersecurity, information warfare, and strategic communication. This lets them see how well these new ideas help fight hybrid threats.

b) Deterrence Theory: Deterrence theory examines strategies for dissuading adversaries from engaging in hostile actions through the credible threat of retaliation (Gray, 1979). Researchers can evaluate how defense science contributes to deterrence capabilities against hybrid threats, such as through the development of advanced cyber defense systems or the use of strategic communication to shape adversary perceptions and behavior.

Formulating Recommendations to Strengthen Defense Capabilities:

To formulate recommendations for strengthening defense capabilities and mitigating the challenges posed by hybrid warfare, researchers can draw upon the following theoretical frameworks:

a) Resilience Theory: Resilience theory focuses on enhancing the ability of systems and organizations to withstand and recover from disruptions and adversities (Holling, 1973). By applying resilience theory, researchers can develop recommendations for building adaptive and resilient defense capabilities capable of responding effectively to hybrid threats, including investments in redundancy, diversity, and flexibility.

b) Network Theory: Network theory examines the structure and dynamics of interconnected systems and organizations

(Barabási, 2013). Researchers can look at defense partnerships and networks, both in the United States and other countries, to find ways that people can work together and coordinate their efforts to fight hybrid threats. This helps them come up with suggestions for how to improve defenses by using network-centric approaches.

RESULT AND DISCUSSION

Evolution of Hybrid Threats and Implications for National Security

In the contemporary security landscape, hybrid threats have evolved into a formidable challenge, blending conventional military tactics with asymmetric methods such as cyber-attacks, information manipulation, and irregular warfare. These hybrid tactics exploit vulnerabilities across various domains, including political, economic, technological, and social, posing significant implications for national security (NATO, 2010).

Complex Systems Theory provides a valuable framework for understanding the evolution of hybrid threats. According to Mitchell (2009), hybrid threats emerge from the dynamic interactions between interconnected systems, wherein changes in one domain can have ripple effects across others. By applying this theory, researchers can analyze how hybrid threats evolve as a result of complex interactions between various actors and factors in the contemporary security landscape.

Strategic Culture Theory offers insights into the motivations and objectives of hybrid adversaries. According to Krause & Williams (1996), strategic culture shapes how states and non-state actors behave in security-related situations, influencing their perceptions of threats and responses. By examining the strategic cultures of hybrid adversaries, researchers can gain valuable insights into their tactics, strategies, and decision-making processes, thereby elucidating the evolution of hybrid threats and their implications for national security.

The evolution of hybrid threats has significant implications for national security, necessitating a holistic approach to defense planning and preparedness. Cyber-attacks targeting critical infrastructure, disinformation campaigns undermining trust in democratic institutions, and irregular warfare tactics exploiting societal vulnerabilities all underscore the complexity of the contemporary security landscape (Rid & Buchanan, 2015).

As hybrid threats continue to evolve, policymakers and defense practitioners need to anticipate emerging trends and challenges in defense planning and preparedness. By drawing upon theoretical frameworks such as Complex Systems Theory and Strategic Culture Theory, researchers can deepen their understanding of hybrid threats and develop effective strategies for countering them (Hoffman, 2007).

Hybrid Threats Evolution and National Security Implications: A Defense Science Perspective

In the contemporary security landscape, hybrid threats have undergone a significant evolution, presenting formidable challenges to national security. These threats, characterized by their blend of conventional military tactics with asymmetric methods such as cyber-attacks, information manipulation, and irregular warfare, have profound implications for defense planning and preparedness (Hickman et al., 2018).

Hybrid threats have evolved in response to advancements in technology and changes in geopolitical dynamics. Cyberattacks, for example, have become increasingly sophisticated, targeting critical infrastructure, government agencies, and private sector organizations (Treverton et al., 2018). Information manipulation campaigns, facilitated by social media platforms, seek to sow discord, undermine trust in democratic institutions, and influence public opinion (Morgan, 2018). Irregular warfare tactics, including the use of proxy forces and unconventional tactics, exploit societal vulnerabilities and challenge traditional defense paradigms (Lindsay, 2013).

The implications of hybrid threats for national security are profound and multifaceted. Cyberattacks targeting critical infrastructure pose significant risks to economic stability, public safety, and national defense capabilities (Lewis, 2019). Information manipulation campaigns undermine democratic processes, erode public trust, and exacerbate social divisions, posing threats to political stability and societal resilience (Sanchez, 2021). Irregular warfare tactics, such as proxy conflicts and unconventional warfare, challenge traditional notions of deterrence and defense, requiring adaptive and innovative responses from defense practitioners (Mumford, 2013).

Defense science plays a critical role in addressing the challenges posed by hybrid threats and enhancing national security preparedness. By leveraging advancements in technology and interdisciplinary research, defense scientists develop innovative strategies and technologies to counter hybrid threats effectively (Efthymiopoulos, 2019). Cyber defense systems, artificial intelligence algorithms, and advanced data analytics enable the detection and mitigation of cyber-attacks in real-time (Radanliev et al., 2020). Additionally, strategic communication methodologies and counter-narrative strategies help to counter disinformation campaigns and propaganda efforts (Colley, 2019).

Contributions of Defense Science to Countering Hybrid Threats

Defense science plays a crucial role in countering hybrid threats, particularly in areas such as cybersecurity, information warfare, and strategic communication. By leveraging innovative strategies and technologies, defense science contributes to enhancing national defense capabilities and resilience against evolving security challenges.

Innovation Diffusion Theory offers valuable insights into the spread and adoption of new ideas and technologies within defense organizations and societies (Rogers et al., 2014). Researchers can use this theory to examine how defense science innovations are disseminated and utilized in areas such as cybersecurity, information warfare, and strategic communication. By studying the diffusion of new ideas, researchers can assess their effectiveness in addressing the challenges posed by hybrid threats and identify opportunities for further research and development.

Defense science innovations in cybersecurity play a critical role in protecting critical infrastructure and networks from cyber attacks launched by hybrid adversaries (Sarjito, 2022). Advanced encryption protocols, intrusion detection systems, and threat intelligence platforms developed through defense science contribute to enhancing cyber defense capabilities and resilience against evolving cyber threats (Schneier, 2015).

Similarly, defense science contributes to countering hybrid threats in the realm of information warfare. By leveraging insights from psychology and communication studies, defense scientists develop strategies to counter disinformation campaigns and propaganda efforts aimed at manipulating public opinion (Wardle & Derakhshan, 2017). Through the use of advanced data analytics and artificial intelligence, defense science enables the identification and mitigation of malicious information operations, thereby safeguarding democratic institutions and societal resilience.

Deterrence Theory offers another theoretical lens through which to evaluate the contributions of defense science in countering hybrid threats. According to (Morgan, 2018), deterrence strategies seek to dissuade adversaries from engaging in hostile actions through the credible threat of retaliation. In the context of hybrid warfare, defense science contributes to deterrence capabilities through the development of advanced cyber defense systems, offensive cyber capabilities, and the use of strategic communication to shape adversary perceptions and behavior.

The Role of Defense Science in Countering Hybrid Threats

In the contemporary security landscape, characterized by the emergence of hybrid threats, defense science plays a crucial role in developing innovative strategies and technologies to counter these multifaceted challenges effectively. Particularly in areas such as cybersecurity, information warfare, and strategic communication, defense science contributes significantly to enhancing national defense capabilities and resilience against hybrid threats (Sarjito, 2024).

One of the primary contributions of defense science to countering hybrid threats lies in the field of cybersecurity. As cyber-attacks become increasingly sophisticated and prevalent, defense scientists develop advanced technologies and methodologies to protect critical infrastructure, government networks, and private sector organizations from cyber threats (Tabansky, 2011). From developing robust encryption protocols to designing intrusion detection systems and threat intelligence platforms, defense science enables the detection, prevention, and mitigation of cyber-attacks in real time.

Furthermore, defense science plays a vital role in addressing the challenges of information warfare. In an era where disinformation campaigns and propaganda efforts pose significant threats to democratic institutions and societal stability, defense scientists develop strategic communication strategies and counter-narrative methodologies to combat misinformation and propaganda (Archetti, 2018). By leveraging insights from psychology, communication studies, and data analytics, defense science enables the identification and mitigation of malicious information operations, safeguarding public discourse and democratic processes.

Strategic communication is another area where defense science makes significant contributions in countering hybrid threats. By developing innovative communication strategies and technologies, defense scientists enhance the effectiveness of government messaging and public diplomacy efforts in shaping perceptions, countering propaganda, and building societal resilience against hybrid threats (Wigell et al., 2021). From utilizing social media analytics to crafting tailored messaging campaigns, defense science enables governments to communicate effectively in an increasingly complex and interconnected information environment.

While defense science has made significant strides in countering hybrid threats in areas such as cybersecurity, information warfare, and strategic communication, there is still room for further research and development. As hybrid threats continue to evolve and adapt, defense scientists must remain agile and innovative in their approach to developing defense technologies and methodologies (Otaiku, 2018). Investing in interdisciplinary research, collaboration with academia and industry, and continuous assessment and adaptation of defense strategies are essential for staying ahead of emerging hybrid threats.

Strengthening Defense Capabilities to Mitigate the Challenges of Hybrid Warfare

Hybrid warfare presents a multifaceted challenge to national security, requiring comprehensive strategies to strengthen defense capabilities and mitigate its impact effectively. By synthesizing insights from resilience theory and network theory, policymakers, and defense practitioners can formulate actionable recommendations to enhance national defense preparedness and resilience against hybrid threats.

Resilience Theory offers valuable guidance for building adaptive and resilient defense capabilities capable of withstanding and recovering from disruptions and adversities (Holling, 1973). One key recommendation stemming from this theory is to invest in redundancy, diversity, and flexibility within defense systems. By diversifying defense capabilities and infrastructure, such as critical infrastructure protection and communication networks, policymakers can reduce vulnerabilities and enhance resilience against hybrid threats. Additionally, fostering a culture of flexibility and adaptability within defense organizations enables rapid response and adaptation to evolving threat landscapes.

Network theory provides insights into the structure and dynamics of interconnected systems and organizations, offering opportunities for collaboration and coordination in countering hybrid threats (Barabási, 2013). By leveraging defense partnerships and networks, both domestically and internationally, policymakers can enhance information sharing, resource allocation, and joint operational planning. Strengthening interagency and international cooperation enables the pooling of expertise and resources to address shared security challenges effectively. Moreover, adopting network-centric approaches to defense planning and operations facilitates agile decision-making and response mechanisms, enhancing the effectiveness of defense efforts against hybrid threats (Jonas, 2005).

In addition to resilience theory and network theory, policymakers and defense practitioners should prioritize investments in research and development to stay ahead of emerging hybrid threats (Kalniete & Pildegovičs, 2021). By leveraging advancements in technology, such as artificial intelligence, quantum computing, and biotechnology, defense organizations can enhance their capabilities in areas such as cybersecurity, information warfare, and strategic communication. Furthermore, investing in human capital development, including training and education programs, ensures a skilled workforce capable of understanding and responding to the evolving nature of hybrid threats.

Furthermore, enhancing public-private partnerships and engaging with civil society stakeholders are essential components of comprehensive defense strategies against hybrid threats. By leveraging the expertise and resources of the private sector and civil society organizations, policymakers can augment defense capabilities and resilience against hybrid threats. Additionally, fostering transparency and accountability in defense decision-making processes strengthens public trust and confidence in national defense efforts, contributing to a more resilient society (Musilová, 2022).

Strengthening Defense Capabilities Against Hybrid Warfare: A Defense Science Perspective

Hybrid warfare, characterized by its blend of conventional military tactics with asymmetric methods such as cyber-attacks, information manipulation, and irregular warfare, presents complex challenges to national security (Weissmann et al., 2021). To effectively counter these threats, policymakers and defense practitioners must implement comprehensive strategies informed by insights from defense science research. Here are several actionable recommendations to strengthen defense capabilities and mitigate the challenges posed by hybrid warfare effectively.

Invest in Advanced Cyber Defense Technologies: Cyber-attacks are a prominent feature of hybrid warfare, targeting critical infrastructure, government networks, and private sector organizations. Investing in advanced cyber defense technologies, such as artificial intelligence (AI)-powered threat detection systems and blockchain-based encryption protocols, is essential (Dhayanidhi, 2022). These technologies enhance the resilience of cyberinfrastructure and enable proactive threat detection and response, thereby mitigating the impact of cyberattacks on national security.

Foster Interdisciplinary Collaboration: Hybrid warfare requires a multidisciplinary approach that combines insights from cybersecurity, information warfare, strategic communication, and the social sciences. Policymakers should prioritize fostering interdisciplinary collaboration between defense scientists, academics, industry experts, and government agencies (Vaseashta, 2022). By leveraging diverse expertise and perspectives, defense practitioners can develop holistic strategies for countering hybrid threats effectively.

Enhance Strategic Communication and Counter-Disinformation Efforts: Information manipulation and propaganda are key components of hybrid warfare, aimed at undermining trust in democratic institutions and shaping public opinion. Enhancing strategic communication capabilities and implementing robust counter-disinformation efforts is critical (Svetoka, 2016). This includes developing tailored messaging campaigns, leveraging data analytics to identify and counter malicious content, and collaborating with social media platforms to combat disinformation.

Strengthen International Cooperation and Information Sharing: Hybrid threats often transcend national borders, necessitating coordinated responses from the international community. Policymakers should prioritize strengthening international cooperation and information-sharing mechanisms to facilitate the exchange of threat intelligence and best practices ((ODNI), 2019). This includes participating in joint exercises, sharing threat assessments, and fostering partnerships with allied nations and international organizations.

Invest in Human Capital Development: A skilled and knowledgeable workforce is essential for effectively countering hybrid threats. Policymakers should invest in human capital development initiatives, including cybersecurity training programs, information warfare courses, and strategic communication workshops (AlDaajeh et al., 2022). By equipping personnel with the necessary skills and expertise, defense organizations can enhance their ability to respond to evolving hybrid threats effectively.

CONCLUSSION

The evolution of hybrid threats in the security landscape has significant implications for national security. Researchers can analyze these threats using theoretical frameworks like Complex Systems Theory and Strategic Culture Theory and develop strategies to mitigate their impact. This requires adaptive responses from defense practitioners and leveraging defense science insights to develop comprehensive strategies to effectively mitigate the risks posed by hybrid warfare.

Defense practitioners and policymakers can effectively counter hybrid threats by integrating innovation diffusion theory and deterrence theory. Defense science, particularly in cybersecurity, information warfare, and strategic communication, contributes to enhancing national defense capabilities and resilience against these threats. However, ongoing research and development efforts are necessary to effectively address the evolving nature of hybrid threats. Defense science's investment in research and development in these areas is crucial for a more robust defense response.

To combat hybrid warfare, a comprehensive strategy involving resilience theory and network theory is needed. This involves investing in redundancy, diversity, and flexibility within defense systems and leveraging defense partnerships and networks. This approach can enhance national defense preparedness and resilience against hybrid threats, safeguarding society's security and stability. This multifaceted approach, based on defense science research, is crucial for addressing the challenges posed by hybrid warfare.

The analysis of hybrid threats suggests several recommendations to strengthen defense capabilities and mitigate their challenges. These include integrating theoretical frameworks like Complex Systems Theory and Strategic Culture Theory into defense planning, leveraging insights from Innovation Diffusion Theory and Deterrence Theory, investing in research and development in key areas like cybersecurity, information warfare, and strategic communication, developing comprehensive defense strategies involving resilience theory and network theory, and prioritizing a multifaceted approach based on defense science research. These strategies can enhance national defense preparedness and resilience against hybrid threats, safeguarding society's security and stability in an increasingly complex security landscape.

REFERENCES

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K.-K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, *119*, 102754.

Archetti, C. (2018). The unbearable thinness of strategic communication. In *Countering Online Propaganda and Extremism* (pp. 81–95). Routledge.

Barabási, A.-L. (2013). Network science. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *371*(1987), 20120375.

Colley, T. (2019). Strategic narratives and war propaganda. *The SAGE Handbook of Propaganda*, 38–54.

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE Publications.

Cummings, M. (2017). *Artificial intelligence and the future of warfare*. Chatham House for the Royal Institute of International Affairs London.

Dhayanidhi, G. (2022). *Research on IoT threats & implementation of AI/ML to address emerging cybersecurity issues in IoT with cloud computing*.

Efthymiopoulos, M. P. (2019). A cyber-security framework for development, defense and innovation at NATO. *Journal of Innovation and Entrepreneurship*, *8*(1), 12.

Gray, R. C. (1979). *Deterrence: A Conceptual Analysis*. JSTOR.

Hickman, K., Weissmann, M., Nilsson, N., Bachman, S.-D., Gunneriusson, H., & Thunholm, P. (2018). Hybrid Threats and Asymmetric Warfare: what to do? *Hybrid Threats and Asymmetric Warfare: What to Do? Stockholm 14-15 November, 2017, the Swedish Defence University, Stockholm, Sweden*.

Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies Arlington, VA.

Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*, *4*(1), 1–23.

Jonas, K. W. (2005). Network-centric operations: European capabilities. *Report A1899. Assembly of the Western European Union (WEU), Inter-Parliamentary European Security and Defense Assembly. Http://Www. Assembly-Weu.*

Org/En/Documents/Sessions_ordinaires/Rpt/2005/1899. Php.

Kalniete, S., & Pildegovičs, T. (2021). Strengthening the EU's resilience to hybrid threats. *European View*, *20*(1), 23–33.

Krause, K., & Williams, M. C. (1996). Broadening the agenda of security studies: Politics and methods. *Mershon International Studies Review*, *40*(Supplement_2), 229–254.

Lewis, T. G. (2019). *Critical infrastructure protection in homeland security: defending a networked nation*. John Wiley & Sons.

Lindsay, J. R. (2013). Proxy wars: Control problems in irregular warfare and cyber operations. *International Studies Association Anual Meeting, San Francisco,(April 2013). Http://Www. Jonrlindsay. Com/Papers*.

Mitchell, M. (2009). *Complexity: A guided tour*. Oxford university press.

Morgan, S. (2018). Fake news, disinformation, manipulation and online tactics to undermine democracy. *Journal of Cyber Policy*, *3*(1), 39–43.

Mumford, A. (2013). *Proxy warfare*. John Wiley & Sons.

Musilová, K. (2022). *Countering Hybrid Threats: Public-Private Cooperation in Norway and the Czech republic*.

NATO. (2010). *Allied Joint Doctrine for Hybrid Warfare*. https://www.act.nato.int/images/stories/media/doclibrary/Allied_Joint_Doctrine_for_Hybrid_Warfare_-_AJD_H-4_Edition_A.pdf

(ODNI), O. of the D. of N. I. (2019). The National Intelligence Strategy Of The United States Of America 2019. *Office of the Director of National Intelligence*.

Otaiku, A. A. (2018). A framework for hybrid warfare: Threats, challenges and solutions. *J Def Manag*, *8*(178), 374–2167.

Radanliev, P., De Roure, D., Page, K., Van Kleek, M., Santos, O., Maddox, L., Burnap, P., Anthi, E., & Maple, C. (2020). Design of a dynamic and self-adapting system, supported with artificial intelligence, machine learning and real-time intelligence for predictive cyber risk analytics in extreme environments–cyber risk in the colonisation of Mars. *Safety in Extreme Environments*, *2*, 219–230.

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, *38*(1–2), 4–37.

Rogers, E. M., Singhal, A., & Quinlan, M. M. (2014). Diffusion of innovations. In *An integrated approach to communication theory and research* (pp. 432–448). Routledge.

Sanchez, L. (2021). Bolstering the Democratic Resilience of the Alliance Against Disinformation and Propaganda. *NATO Parliamentary Assembly. Https://Www. Nato-Pa. Int/Document/013-Cds-21-Edemocratic-Resilience-against-Disinformation-and-Propaganda-Report-Sanchez*.

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

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

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. WW Norton & Company.

Svetoka, S. (2016). *Social media as a tool of hybrid warfare*. NATO Strategic Communications Centre of Excellence.

Tabansky, L. (2011). Critical Infrastructure Protection against cyber threats. *Military and Strategic Affairs*, *3*(2), 2.

Treverton, G. F., Thvedt, A., Chen, A. R., Lee, K., & McCue, M. (2018). *Addressing hybrid threats*. Försvarshögskolan (FHS).

Vaseashta, A. (2022). Applying Resilience to Hybrid Threats in Infrastructure, Digital, and Social Domains Using Multisectoral, Multidisciplinary, and Whole-of-Government Approach. In *Building Cyber Resilience against Hybrid Threats* (pp. 42–59). IOS Press.

Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policymaking* (Vol. 27). Council of Europe Strasbourg.

Weissmann, M., Nilsson, N., Palmertz, B., & Thunholm, P. (2021). *Hybrid warfare: Security and asymmetric conflict in international relations*. Bloomsbury Academic.

Wigell, M., Mikkola, H., & Juntunen, T. (2021). Best practices in the whole-of-society approach in countering hybrid threats. *European Parliament Coordinator: Policy Department for External Relations Directorate General for External Policies of the Union. Doi*, *10*, 379.