INTEGRATION OF DEFENSE POLICY AND PUBLIC POLICY FROM A NATIONAL SECURITY PERSPECTIVE IN COUNTERING HYBRID WARFARE THREATS

Rubiyanto P Aji[1]
Universitas Pertahanan, Bogor, Indonesia
aji_rubi@yahoo.co.id

Asep Adang Supriyadi[2]
Universitas Pertahanan, Bogor, Indonesia
aadangsupriyadi@gmail.com

Abstract

The threat of hybrid warfare is now a crucial issue in national security, so the state is required to unite military-based defense policy with public policy. An integrated approach based on national security analysis is key in shaping a resilient national defense system that is ready to face the evolving challenges of hybrid warfare. Literature studies are used to collect, analyze, and synthesize various related studies by identifying, collecting, and analyzing various sources such as journal articles and other relevant data to formulate a framework for the integration of defense policy and public policy in counteracting hybrid warfare threats through a national security perspective that utilizes technology and stakeholder collaboration. This research reveals that hybrid warfare is a complex form of threat that combines physical and non-physical tactics that require states to design adaptive and integrated defense policies and public policies. The national security perspective shows a collaborative approach across sectors, such as economic stability and the use of advanced technology for threat mitigation. Therefore, the integration of defense and public policies is key in building a responsive, flexible, and sustainable national strategy in the face of dynamic and multidimensional hybrid warfare challenges. This research confirms that in facing increasingly hybrid threats, the state needs to adopt an adaptive, integrated, and technology-based national security approach through the formulation of defense and public policies that include strengthening socio-economic resilience, cross-sector collaboration, and the use of artificial intelligence to maintain stability and strengthen national resilience against the dynamics of global threats.

Keywords: Public Policy, Defense Policy, Hybrid Warfare, National Security, Economic

INTRODUCTION

The threat of hybrid warfare has become a national security issue in many countries. It has the potential to occur as increasing reliance on digital technology, social media, and global geopolitical tensions make a country vulnerable to this threat. Hybrid warfare, which combines conventional and unconventional warfare tactics, such as disinformation, cyberattacks, and social manipulation, has the potential to threaten a country's national stability politically, socially, and economically without involving direct combat, requiring the integration of the defense sector and public sector in formulating policies that can respond quickly to this threat (Steingartner & Galinec, 2021; Ide et al., 2023; Razma, 2023). This means that their analysis and impact on national security need to be managed to ensure the accuracy of the state's response to existing and potential threats. The state must respond to these threats through the integration of defense policy with public policy, where defense policy focuses on managing risks and strategies taken from the military and national defense aspects, while public policy focuses on non-military aspects, such as political, economic, social, cultural and so on that affect the life of the nation and state along with the rules that guide its implementation. Therefore, a country facing the increasingly complex threat of hybrid warfare and its impact on national security must integrate the two policies to create a more effective and comprehensive response and follow-up.

Public policy should focus on information management to counter the threat of disinformation, use cognitive warfare and counterintelligence strategies, address social injustice, support reconciliation, and consider the impact of international competition and advances in artificial intelligence in formulating security and defense policies (Daniel & Eberle, 2021; Schmidt, 2022; Bachmann et al., 2023; Putter, 2024; Klein, 2024). This means that public policy must integrate a comprehensive approach to addressing increasingly complex and dynamic security threats, including anticipating disinformation, social injustice, and the impact of international competition and technology. As such, public policy must be designed to regulate aspects of public life comprehensively and adaptively to ensure the security and stability of the state now and in the future.

Public policy should be based on a deep understanding of strategic conditions to formulate effective policies to address hybrid threats, including artificial intelligence regulation, and state resilience, and consider the impact of war and inflation on economic and social stability to sustainably safeguard the interests of the state (Herrera-Cuenca et al., 2021; Henke & Maher, 2021; Banna et al., 2023; Papyshev & Yarime, 2023; Razma, 2023; Heath-Kelly, 2024). This means that public policies must be designed with a range of strategic factors in mind, including technological developments, internal and external threats, and economic impacts, to ensure the country's long-term resilience to evolving threats. As such, public policy must be proactive and adaptive, integrating the various aspects that affect national stability, to create robust resilience against increasingly diverse threats.

Public policy in the face of hybrid warfare threats must manage not only military threats but also consider interrelated aspects that affect national security stability. Hybrid warfare is a threat that combines conventional military attacks, cyber-attacks, and the spread of disinformation to change the political situation without confrontation, by utilizing traditional and non-traditional threats and manipulation of existing social and political values to reduce the state's ability to deal with the threats that occur (Kruck & Weiss, 2023; McWilliams & Legnér, 2024). This means that hybrid warfare utilizes various strategies,

both conventional and unconventional, to weaken the state politically and socially without engaging in direct physical combat, so the state must be prepared to face more complex and hidden threats. Thus, the state needs to develop an adaptive strategy, integrating cyber defense, disinformation monitoring, and military preparedness to deal with increasingly complex and diverse hybrid threats.

An understanding of hybrid warfare with a scope that goes beyond conventional warfare is necessary in analyzing from a national security perspective through the utilization of uncertainty and manipulation outside the military space, as well as evaluating threats from groups that utilize instability, such as natural disasters, to influence state policies (Malone & Hildebrand, 2022; Bergaust & Sellevåg, 2024). This means that analytical approaches from a national security perspective need to take into account hybrid warfare strategies in responding to parties that utilize situations beyond traditional military conflict, including the exploitation of social instability or natural disasters, which can be used to influence state policy. Thus, the scope that needs to be considered from a national security perspective should be broader and deeper, not only military threats but also the potential manipulation of social instability and disasters, to protect the policies made by the state from various types of threats that are not directly visible.

Hybrid warfare often takes advantage of weaknesses in defense policy, exploiting internal instability so that national resources cannot be optimally utilized by the state. The preparation of a thorough security analysis and evaluation of defense policies involving various sectors is necessary to effectively address this threat, including in the face of environmental challenges and domestic policy changes that can reduce the potential for intervention by external parties (Kivimaa & Sivonen, 2021; Räisänen et al., 2021; Qari et al., 2024). This means that to address the threat of hybrid warfare more effectively, the state needs to have a comprehensive defense and security policy, that not only identifies its vulnerabilities, but also involves various sectors, considers various aspects and challenges of a dynamic environment, and creates domestic stability to reduce the risk of intervention from outside parties. Thus, national defense and security policies must be designed thoroughly and involve various parties, both public and private sectors, and consider internal and external factors to ensure the country's resilience to increasingly complex and diffuse threats.

The threat of hybrid warfare encourages the state to build and develop a more complex defense system, not only relying on physical strength. The state must develop a comprehensive defense strategy, covering protection against threats from various dimensions, including physical, cyber and social threats. In addition, the defense policy must be able to maintain political and economic stability so that the country remains resilient in the face of increasingly diverse threats. Defense policy and public policy must be integrated with national security considerations to deal with more hidden hybrid warfare threats, to maintain national stability and security. Based on the literature review discussed earlier, it is necessary to integrate defense policy with public policy through an approach based on a national security perspective in dealing with hybrid warfare threats.

REVIEW OF LITERATURE

States need to understand the process of hybrid warfare threats, both in conventional and unconventional warfare. A comprehensive analytical approach from a national security perspective can provide a picture of how to address these threats through a more predictive

analytical approach based on data and information technology so that the state can develop policies that are more responsive and adaptive to these threats (Legrand & Stone, 2021; Wróblewski & Wiśniewski, 2024). This means that defense policy needs to ensure that the defense system can face threats, both conventional, non-conventional and hybrid warfare to maintain national security. Strategic integration between physical defense and cyber defense in national defense is important to overcome the risk of occurrence and the impact of the emergence of increasingly complex hybrid warfare, while defense policy also needs to consider public sector conditions, such as global economic and political changes and be able to adapt to evolving global risks, which will affect the future direction of defense policy (Steingartner & Galinec, 2021; Ide et al., 2023; Bocquillon et al., 2024). This means that national defense policy needs to be more responsive to changes in the strategic environment and changing threats to protect the country from various risks that are increasingly complex in the future. Thus, defense policies must be designed and the strategies chosen can be implemented flexibly and adaptively, by integrating aspects of social life and considering global dynamics to maintain national security.

Defense policy should include strategies to address new hybrid threats such as disinformation and economic warfare, by adjusting international political economy policies combining military, diplomatic and economic responses, and taking into account public expectations for maintaining national security in an unstable global context, including cyber defense (Legrand & Stone, 2021; Bocquillon et al., 2024; Qari et al., 2024). This means that defense policy must be more comprehensive and integrated, covering various aspects such as responses to non-conventional threats, the risk of global economic and political changes, and public interests, with a special emphasis on cyber defense as an important part of maintaining state security amid increasingly complex challenges. Thus, defense policy must be designed comprehensively and adaptively, combining various approaches, including military, diplomatic and economic, to address hybrid threats and ensure effective protection of national security in the face of changing global dynamics.

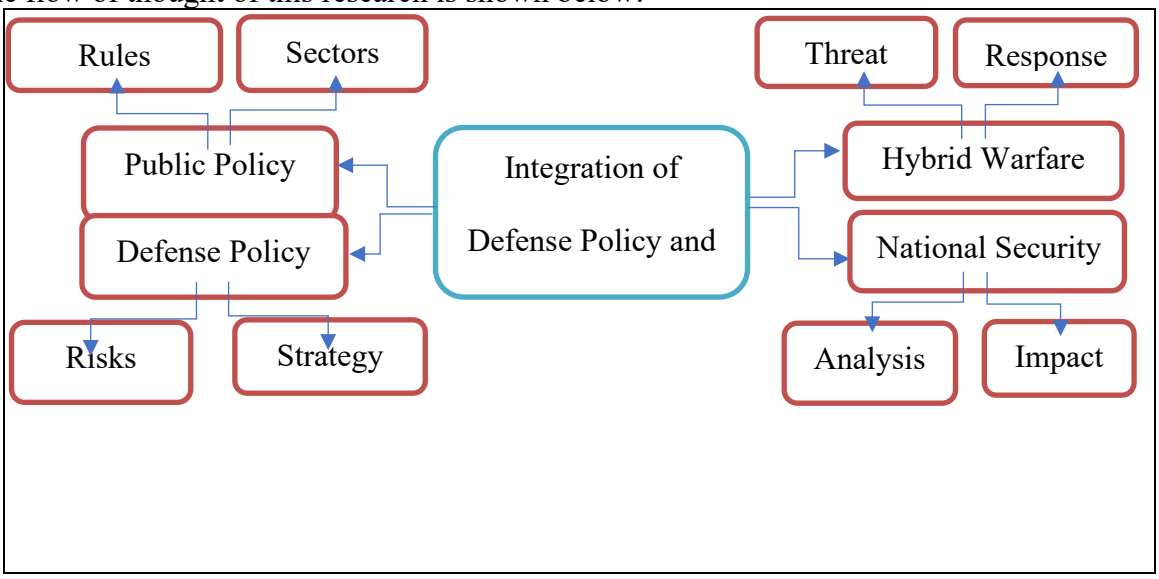
In addition to defense policy, public policy is needed to address the threat of hybrid warfare. Public policy is the state's effort to regulate the public sphere and strengthen its political influence, to maintain social, economic, national integrity and cultural stability, including energy policies that can influence defense policy, especially in the face of hybrid threats that include physical and non-physical attacks (Andrews, 2022; Kruck & Weiss, 2023; McWilliams & Legnér, 2024; Zenz, 2025). This means that in facing the threat of hybrid warfare, the state does not only rely on military defense policies but also needs to strengthen public policies that involve various other sectors, such as the economy, energy and culture. Energy policy, for example, must be formulated with national security in mind, given the threats that can come both physically, such as attacks on energy infrastructure and non-physically, such as economic sabotage or information warfare. Thus, the state must formulate integrated and comprehensive policies, where sectors such as defense, energy, economy and culture work together to create stronger national resilience.

RESEARCH METHOD

The research method in this essay uses a literature study, where which is done by identifying and analyzing related literature as the bibliography in this study. The literature study was conducted to obtain theories and results of previous research on the integration of

defense policy and public policy in counteracting the threat of hybrid warfare: a national security analysis approach. This step aims to formulate and explain the framework for the integration of defense policy and public policy in countering the threat of hybrid warfare: a national security analysis approach that utilizes technology and cooperation from stakeholders. The literature reviewed includes journal articles and data from government agencies relevant to this topic. The literature search used keywords such as public policy, defense policy, hybrid warfare, national security, and economic to ensure the relevance of the research. The literature obtained is then determined as support material in describing or providing an overview of the conditions and opportunities for implementation or adoption of the research problem, namely the integration of defense policy and public policy in counteracting hybrid warfare threats: a national security analysis approach.

This approach enables a thorough understanding of the integration of defense policy and public policy in countering the threat of hybrid warfare: a national security analysis approach. The flow of thought of this research is shown below:



RESULTS AND DISCUSSION

Hybrid warfare threats involve a combination of physical and non-physical tactics, which include identity manipulation to destabilize states, incorporating elements such as cyber warfare, disinformation, and conventional military strategies (Freedman et al., 2021; Gunneriusson, 2021). Hybrid warfare can undermine state stability through propaganda to divide societies and control social media to influence public opinion so states must execute defense strategies to detect and mitigate potential future damage (Jackson, 2021; Lekunze, 2023; Wither, 2023). This means that states need to design more flexible and adaptive defense strategies, given the threat of hybrid warfare that combines various tactics and elements that are difficult to predict, including the manipulation of information and third parties. Thus, the state needs to develop a comprehensive and responsive defense policy in the face of threats that are increasingly complex and involve various unconventional tactics.

Countries involved in hybrid warfare need to adjust their defense strategies so that they can face threats and reduce their impact. Some examples of hybrid warfare cases include Ukraine facing the threat of cyber-attacks that not only damage infrastructure but also

undermine public trust in the government; disinformation and cyber-attacks by outside actors to disrupt social and political stability in Sweden, illegal immigration to create crises at European borders, separatist conflicts in Cameroon (Nizovtsev et al., 2022; Meszaros & Țoca, 2023; Lekunze, 2023; Ljungkvist, 2024). As such, states must develop a more holistic and adaptive approach to defense, encompassing both physical and non-physical aspects to anticipate and address threats that are more difficult to detect and address. This requires collaboration between the government, society and the private sector to strengthen information security and maintain national stability amidst more complex challenges.

Defense policy and public policy are tools used by the state to maintain national security stability and the sustainability of a country, especially in the face of threats, such as hybrid warfare. Public policy plays a role in regulating aspects of community life for the benefit of the state as a whole and national resilience (Henke & Maher, 2021; Kruck & Weiss, 2023), including the protection of social, economic and cultural aspects. Meanwhile, defense policy plays a role in formulating strategies in responding to multi-dimensional risks and threats, both physical and non-physical, including cyber threats. Hybrid warfare combines various approaches, including military force, information manipulation, and cyber combat as well as the threat of economic warfare that can destabilize a country's resilience (Freedman et al., 2021; Gunneriusson, 2021; Iuga & Socol, 2023). This means that hybrid warfare relies on various strategies that combine cyber, economic, and military tactics to weaken states. Thus, states need to develop more comprehensive and adaptive policies and strategies, integrating military, information, and economic aspects to deal with hybrid warfare threats.

Public trust in defense policies and public policies formulated by the Government is necessary for the public to actively participate in supporting national security. This is supported by transparency, accountability and effective communication from the Government regarding defense policies and public policies in maintaining national security. In facing the threat of hybrid warfare through sharpening the early detection system and timely response and adaptation to unexpected threats (Derleth & Pickler, 2022; Alshammari, 2023), it is necessary to seek the integration of defense policy with public policy through an analytical approach from a national security perspective, which can be explained as follows:

3.1. Defense Policy

Defense policy aims to resolve existing injustices and anticipate possible future threats through measures taken by the state to strengthen control and form a more uniform identity (Klein, 2024; Zenz, 2025). Defense policy relies on the state's ability to immediately address evolving threats, including physical and non-physical attacks on state sovereignty (Kruck & Weiss, 2023; McWilliams & Legnér, 2024). This means that defense policy must be able to deal with various types of threats, both physical and non-physical, and be designed with the flexibility to anticipate changes in the situation and maintain uniformity and control of national identity. Thus, defense policy must be prepared with an adaptive and comprehensive approach, so that the state can maximize its defense capabilities in responding to threats quickly.

Defense policy is affected by competition between major countries that utilize artificial intelligence to gain a strategic advantage, so regulations and strategies related to artificial intelligence are needed to deal with threats that arise from the use of these technologies (Schmidt, 2022; Papyshev & Yarime, 2023). Defense strategy must be based

on factual understanding in responding to evolving threats, including hybrid warfare, through a smarter and data-driven approach in formulating defense policy. (Razma, 2023; Putter, 2024). This means that defense policy should include proactive measures to deal with current and future threats, taking into account technological advances such as artificial intelligence, as well as ensuring the regulations and strategies implemented can face global challenges and maintain national security. Thus, defense policy must be structured to mitigate risks and anticipate threats that arise along with technological developments and global dynamics, with a focus on strengthening national security through appropriate regulations and adaptive response strategies.

To maintain national security, the state develops defense policies to deal with hybrid warfare threats through identification, detection, and rapid response, as well as adaptation to unforeseen threats, which include identity manipulation, cyber-attacks, disinformation, and conventional military tactics, so that the policies implemented must be flexible and comprehensive (Gunneriusson, 2021; Freedman et al., 2021; Derleth & Pickler, 2022; Alshammari, 2023). This means that defense policy must be able to identify and respond to complex and diverse threats, including unexpected ones, and adapt to evolving global risks, in the form of unconventional security threats (Ide et al., 2023; Qari et al., 2024). As such, defense policy needs to be designed to address increasingly complex and diverse threats through the ability to adapt quickly to changing and interconnected forms of attack.

Defense policy must take into account psychological and tactical factors that influence decisions in dealing with threats (Mattingsdal et al., 2024; Zenz, 2025). This means designing strategies that can address non-military threats without engaging in armed conflict, by integrating military and civilian elements to deal with hybrid threats and taking into account local emergency policies influenced by political dynamics (Malone & Hildebrand, 2022; Bergaust & Sellevåg, 2024; Ljungkvist, 2024). Defense policy must be designed with a multifaceted approach, including psychological, tactical and non-military, to anticipate threats that are increasingly diverse and difficult to predict. This includes adjustments to the defense strategy implemented to be able to respond to threats, and political and social changes. Thus, defense policy needs to be designed to address various threats as a whole, combining military and civilian strategies, and considering psychological, tactical and political factors in facing increasingly complex challenges.

Defense policy needs to integrate environmental protection with national defense strategy, especially for countries facing both traditional and non-traditional threats, including natural resource-related conflicts, by designing a robust policy framework to address complex threats (Kivimaa & Sivonen, 2021; Steingartner & Galinec, 2021). This means defense policy should include important elements, such as environmental protection, as well as strategies to deal with contemporary threats such as cyberattacks and the spread of disinformation. With this comprehensive approach, states can be better prepared to deal with evolving and increasingly complex threats through the integration of foreign and defense policies, including controlling production and regulation beyond their borders (Ide et al., 2023; Farrand, et.al, 2024). As such, defense policy should be comprehensively designed to encompass both traditional and non-traditional strategies and be able to adapt to new risks involving technology and information to ensure more effective national security.

3.2. Public Policy

Public policy is the state's effort to organize public space to control various aspects of life, including in dealing with hybrid threats (Kruck & Weiss, 2023; Zenz, 2025). Furthermore, public policy needs to strengthen political power, maintain social and economic stability, protect cultural heritage and protect national integrity from external threats, including playing a role in shaping energy policy that affects defense policy (Andrews, 2022; McWilliams & Legnér, 2024). This means that public policy needs to pay attention to a variety of factors, ranging from strengthening political to cultural aspects to ensure national stability is maintained. This is done to deal with increasingly complex threats, which combine physical and non-physical threats. Thus, public policies need to be designed thoroughly to integrate political, social, economic and cultural aspects to ensure effective national protection in the face of diverse threats.

Public policies need to be formulated with a deep understanding of the current strategic situation to formulate effective actions in the face of hybrid threats. This includes the impact of war and inflation, which have the potential to destabilize the economy and society to ensure that decisions are made that prioritize the interests of the state (Banna et al., 2023; Henke & Maher, 2021). In addition, the state needs to strengthen its resilience to both internal and external threats, including in the face of terrorism and radicalization, and pay attention to regulations governing the development of artificial intelligence (Heath-Kelly, 2024; Papyshev & Yarime, 2023). This means that public policies must be formulated taking into account various strategic factors, technologies, and global challenges and ensuring sustainable economic, social, and political stability. Thus, public policies need to be designed thoroughly to address complex threats and ensure the country's resilience in the face of domestic and global challenges, while maintaining sustainable economic and social stability.

Public policies to address hybrid threats should expand their scope from just military threats, but also other aspects, such as the environment and socio-economics, taking into account factors such as economic sanctions, disruption of energy supply, as well as the utilization of artificial intelligence in detecting threats, while paying attention to ethical issues, privacy, and the impact of natural disasters, not just the physical damage (Jonek-Kowalska, 2022; Kharazishvili & Kwilinski, 2022; Bond & Mortensen, 2023; Bergaust & Sellevåg, 2024). This means that public policy should adopt a more comprehensive and integrated approach, taking into account non-military domains such as the economy, environment, technology, and social impacts in the face of new and diverse hybrid threats (Wróblewski & Wiśniewski, 2024; Bocquillon et al., 2024). Thus, public policies need to be designed to deal with more complex and multi-dimensional threats covering various aspects that affect national security stability, such as economic, technological, environmental and social.

Public policies should be proactive and decisive in addressing security risks in society, including strengthening cyber defenses to deal with threats related to digital technology (Steingartner & Galinec, 2021; Carvalho & Lima, 2023). Moreover, in implementing its public policies, the state needs to balance between national resilience and global economic strategies through the use of predictive methodologies in public policies that can provide more effective insights in responding to hybrid threats (Legrand & Stone, 2021; Wróblewski & Wiśniewski, 2024). This means that public policies must be designed thoroughly and flexibly to address the threats that develop as the dynamics of problems that develop in society. Thus, public policies need to be formulated proactively to overcome

increasingly complex threats, taking into account various factors that affect national and international stability, and ensuring readiness to face challenges that arise from various sectors in the life of the state.

3.3. *Hybrid Warfare* Threat

Hybrid warfare is a modern form of conflict that combines physical and non-physical threats to damage and change a country's political system without involving direct combat, but its impact can shake economic and social stability, and attack vital sectors, such as energy and finance, as well as manipulate public opinion and create divisions in society (Banna et al., 2023; Razma, 2023; Heath-Kelly, 2024). This means that hybrid warfare relies on a variety of tactics that not only focus on the military sector but also on economic, social and political aspects, which requires the state to develop a comprehensive and adaptive strategy to maintain its security stability. Thus, states need to design comprehensive and flexible policies, given the threats that arise from various sectors, including economic, social and political in the face of hybrid warfare.

Hybrid warfare combines military strategies and more covert non-physical attacks, such as the manipulation of public opinion through social media and other threats such as disruption of energy supplies and cyber-attacks on vital infrastructure that can destabilize economies and worsen state resilience in the face of natural disasters or sabotage (Jonek-Kowalska, 2022; Kuhn et al., 2022; Kharazishvili & Kwilinski, 2022; Bond & Mortensen, 2023; Bergaust & Sellevåg, 2024). This means hybrid warfare encompasses various forms of threats that combine military and non-military tactics, influence state policies, and add complexity to maintaining economic stability and resilience to natural and man-made disasters. Thus, the state needs to develop an integrated strategy to deal with threats that come from various sectors, both military, economic and social to maintain national stability and resilience in the face of hybrid warfare.

Hybrid warfare also involves a variety of tactics, both physical and non-physical, designed to destabilize states and undermine international relations, with information as the primary tool to influence public opinion and foster distrust of governments, which can lead to dynamic changes in domestic politics and create more destructive conflict in society (Bachmann et al., 2023; Klein, 2024; Putter, 2024). This means that hybrid warfare utilizes various strategies that combine physical and non-physical forces, especially through information, to undermine state stability and international relations, which can lead to significant domestic political changes and create more destructive conflict impacts in society. As such, hybrid warfare requires states to develop more complex and adaptive strategies to protect internal stability and maintain international relations, focusing on information management and resilience to threats that are not only physical but also psychological and political.

The threat of hybrid warfare is increasingly complex with advances in technology, which allows cyberattacks and information manipulation or disinformation to alter reality (Freedman et al., 2021; Gunneriusson, 2021) and influence countries' strategic decisions, so countries must design defense policies that can deal with physical, informational and psychological threats, difficult to recognize because they involve various forms of aggression, both obvious and hidden (Henke & Maher, 2021; Herrera-Cuenca et al., 2021; Papyshev & Yarime, 2023). This means that states need to develop more comprehensive and

adaptive defense policies, not only focusing on physical threats but also being able to address informational and psychological attacks that can undermine stability and strategic decisions. Thus, the state must design a more comprehensive defense strategy to identify and address threats that come in various forms, including cyberattacks, disinformation, and social manipulation.

To deal with increasingly complex hybrid warfare threats, countries need to implement data-driven policies and analysis that enable rapid response (Kharazishvili & Kwilinski, 2022; Ide et al., 2023). Moreover, to deal with the widespread threat of hybrid warfare, states need to conduct predictive analysis to mitigate risks, strengthen cyber defenses and effectively combat disinformation (Rauta & Monaghan, 2021; Steingartner & Galinec, 2021; Wróblewski & Wiśniewski, 2024). This means that states need to adopt a smarter, data-driven approach to identify and respond efficiently to hybrid warfare threats, in addition to improving cyber defenses and addressing disinformation that can undermine national stability. Thus, to deal with increasingly complex hybrid warfare threats, the state needs to adopt data-driven policies. This approach makes it possible to quickly identify, analyze and respond to a wide range of threats, both military and non-military.

3.4. National Security Approach in the Face of Hybrid Threats

To deal with hybrid threats, a national security approach should involve evaluating the role of non-military sectors through economic, social, and technological channels, as well as examining the relationship between defense policy and public policy, as their incongruence can increase its vulnerability to external threats, in addition to proactively assessing physical and non-physical threats, adapting to technological developments (Räisänen et al., 2021; Qari et al., 2024; Bocquillon et al., 2024). This also includes analyzing and evaluating hard-to-detect threats such as information manipulation and cyberattacks (Steingartner & Galinec, 2021; Rauta & Monaghan, 2021). This means that in dealing with hybrid threats, the state must develop a comprehensive approach that does not only consider physical threats, but also non-physical threats such as cyberattacks and disinformation, and ensure that defense and public policies are aligned. Thus, the state needs to formulate a comprehensive and responsive policy towards hybrid threats, by strengthening collaboration between sectors and ensuring alignment between defense and public policies to maintain stability and reduce its vulnerability to external and internal threats.

National security approach must also consider the integration of economic stability and national defense, as both play an important role in addressing hybrid threats that can undermine state resilience, including threats from separatist groups that apply hybrid tactics in combat. (Jackson, 2021; Iuga & Socol, 2023; Lekunze, 2023). This means that economic stability and national defense must be viewed as interrelated elements in maintaining national security, with a focus on hybrid threats such as the efforts of separatist groups that seek to undermine state resilience. Thus, the state needs to integrate economic and defense aspects in the national security strategy to effectively address hybrid threats, including preventing and overcoming the actions of separatist groups in maintaining state resilience.

To implement comprehensive national security, states need to understand the mechanisms of disinformation and other unconventional strategies in defense policy as they are key factors in addressing threats, in addition to identifying potential dangers from sectors such as cyber and media that often appear in hybrid warfare (Gunneriusson, 2021; Freedman et al., 2021; Derleth & Pickler, 2022). This means defense policy must be constantly updated

to capture and augment new threats, and ensure the conditions of various sectors, such as cyber and media, are taken into account to effectively counter hybrid warfare. Thus, the country needs to develop a more adaptive and comprehensive defense policy, which not only focuses on traditional threats but also includes non-conventional threats such as disinformation and cyberattacks in the face of hybrid warfare.

National security also needs to mitigate the impact of hybrid threats by engaging communities and militaries in dealing with asymmetric challenges, and assessing the role of military and police actors in decision-making related to these threats (Ljungkvist, 2024; Mattingsdal et al., 2024). In addition, national security needs to include an assessment of potential threats from groups that could capitalize on instability resulting from natural disasters and hybrid threats, including damage to energy infrastructure vital to the stability of the country (Mara et al., 2022; Malone & Hildebrand, 2022). This means that the national defense approach must involve collaboration between society, the military and the police to deal with hybrid threats while taking into account the potential risks from natural disasters and threats to critical infrastructure such as energy, to maintain the overall stability and security of the country. As such, the state must develop a defense strategy that involves multiple sectors and actors, to effectively respond to hybrid threats, including the potential misuse of natural disasters and threats to vital infrastructure.

3.5. Integration of Defense Policy and Public Policy in Countering Hybrid Warfare Threats

The threat of hybrid warfare requires a defense policy to be able to prevent hidden threats. Policies that rely solely on military power are insufficient to deal with non-physical threats, such as cyberattacks or information warfare, so conventional defense strategies are no longer adequate. This requires defense policies that combine military power and digital and social resilience to be more effective in dealing with threats. Thus, a coordinated approach between defense policy and public policy is needed in addressing hybrid warfare threats. With the development of technology and the growing dependence on the digital world, both policies need to support each other to build resilient digital resilience, given the evolving cyber threats.

National defense policies that include energy security must consider their vulnerability to hybrid threats, including cyberattacks and energy supply disruptions, while hybrid warfare can also involve environmental threats that exacerbate regional tensions, making it necessary to integrate environmental issues in defense and public policies (Kivimaa & Sivonen, 2021; Räisänen et al., 2021). In addition, the increased need for common defense policies may change the public view of defense strategies that focus on the durability of defense systems in the face of conventional and hybrid warfare threats (Fernández et al., 2023; Bocquillon et al., 2024). This means that public and defense policies must be designed in an integrated manner to address complex threats, including climate change, hybrid warfare and other new challenges. Thus, public and defense policies need to support each other to deal with increasingly diverse and complex threats, focusing on the balance between sustainable development, protection against unconventional threats, and maintaining national stability.

Public policy in the face of hybrid warfare needs to be based on a deep understanding of the internal and external dynamics that affect the state, and must be innovative, sustainable and flexible to be able to respond to rapidly evolving threats. The hybrid warfare threat combines conventional and unconventional tactics so that the state must manage defense and

public policies simultaneously to create an adaptive and responsive strategy. This can be done through effective civil society and intelligence collaboration to strengthen public and defense policy in the face of complex hybrid warfare threats that require cross-policy coordination (Njoku, 2022; Nte et al., 2022). This includes efforts to increase awareness and implementation of state defense in public programs and activities with the support of appropriate budget allocations for character building, mental resilience, and mental health. Defense policies also need to be synergized with public needs in the economic, social and cultural fields to build comprehensive national resilience to encourage active community participation in maintaining national sovereignty. For example, proper budget prioritization can strengthen a country's economic system and ensure the social stability needed to deal with both domestic and international threats (Böller & Wenzelburger, 2024; Iuga & Socol, 2023). This means that the right budget can support various sectors of the economy through judicious allocations, such as for economic growth, inflation control, or ensuring national security is maintained in forming a strong and stable economy (Mumford & Carlucci, 2023; Böller & Wenzelburger, 2024).

Public policy has a role to play in creating national stability that supports defense policy. The state needs to strengthen public policies that not only focus on economic and political welfare but are also able to identify and respond to external threats, including energy availability for hybrid defense. Policies that respond quickly to cyber threats, such as media literacy training and strengthening cyber regulations, are important for national resilience. Cyberattacks and threats to energy security as a defense resource point to the need for synergy between defense and public policies to protect national stability, given that hybrid warfare involve not only physical attacks but also damaging critical infrastructure that sustains the economy and politics (Matzkin, et.al, 2024). This means proactive and intergative public policies can address hybrid threats arising from social and economic tensions, by integrating defense policies that cover social, economic and environmental issues to ensure strong stability.

3.6. Challenges in Integrating Defense Policy and Public Policy

Changes in foreign and security policy present challenges in integrating defense and public policy, especially in responding to hybrid warfare threats that require an adaptive and comprehensive approach, covering both military and non-military aspects (Böller & Wenzelburger, 2024; Mumford & Carlucci, 2023). The integration of defense policy and public policy faces challenges at the political, economic and social levels. In many cases, the defense sector tends to develop policies focused on military capabilities, while public policy may be more oriented toward solving long-term social or political problems. However, in the face of hybrid threats, these two policies must work together. Public and defense policies should be detailed and prepared for threats emanating from multiple sectors, with special attention to protecting vulnerable energy infrastructure and balancing sustainable development with mitigating unconventional threats such as climate change that can trigger tension and conflict (Kivimaa & Sivonen, 2021; Bond & Mortensen, 2023). Public and defense policies need to be comprehensive and flexible, focusing on the protection of vital infrastructure and preparedness for environmental challenges and unconventional threats that can disrupt national and international stability. Integration between defense and public policy faces major challenges due to social and political diversity. In addition, community

participation is critical to addressing threats such as radicalization and disinformation. However, social and political tensions and resource constraints can hinder countering hybrid warfare threats, requiring resource optimization as well as collaboration with the private, international and energy security sectors to maintain economic and political stability.

Based on the literature review, it can be concluded that to deal with the threat of hybrid warfare, the state needs to effectively integrate defense and public policies and ensure that these two policies support each other to maintain national stability and address increasingly serious threats to global security. Thus, efforts to integrate defense policy and public policy in countering the threat of hybrid warfare include:

1. Develop a defense policy that is integrated with public policy, which can be exemplified through the provision of a budget for the defense sector and safe and reliable energy security to meet public needs, support military operations and socio-economic stability, and strengthen the country's resilience in the face of hybrid warfare threats.
2. Strengthening cyber defense and information security capacity through collaboration between government agencies and communities, as well as education involving training in dealing with cyber threats, disinformation and unconventional tactics to prepare communities and other stakeholders to effectively respond to these challenges.
3. The application of predictive analytics and increased international collaboration in cybersecurity and disinformation management will strengthen states' capabilities in the face of hybrid warfare, enabling faster identification and mitigation of increasingly complex digital threats.
4. Improving collaboration between government agencies, including the military, police, intelligence and civilian sectors, is critical to effectively addressing hybrid warfare threats, by establishing information networks and unified command systems to ensure rapid, appropriate and mutually supportive responses.

CONCLUSION

Increasingly diverse hybrid warfare threats have the potential to threaten national security stability. These threats not only involve direct traditional military attacks against a country but also include cyber-attacks, disinformation and social disruption that can disrupt a country's social, political and economic life. Therefore, the state needs to respond to this threat through a more adaptive, thorough, and comprehensive approach from a national security perspective to design defense and public policies that can address the threat of hybrid warfare.

The state needs to design defense policies that include preparedness and follow-up strategies against cyber threats, disinformation management, and strengthening the country's social, economic and political resilience. An effective way to strengthen the response to this threat is through strengthening synergies between government agencies in accelerating strategic decision-making and increasing efficiency in dealing with the impact of rapidly evolving threats. In addition, continuous training for state apparatus and the community can strengthen the country's preparedness against hybrid threats. For example, efforts to increase awareness of state defense must be supported by programs, budget allocations for character building and mental health, as well as defense policies that are integrated with economic, social and cultural aspects to strengthen national resilience and community participation in maintaining national sovereignty. This also includes utilizing state resources and budget

priorities to maintain stability and drive the economy in support of national security. With this coordinated and comprehensive approach, the state will be better equipped to protect its national security stability.

The state must ensure that the policies implemented can cover all sectors, including social, political, economic, and technological sectors. In addition, the fulfillment and adequacy of budget allocations that support energy security and strategic infrastructure must also be considered, so that the state can ensure that the military and civilian sectors run synergistically. This is because the sustainability of military operations and the country's socio-economic stability are highly dependent on safe and reliable energy management. Thus, the state needs to ensure the availability of energy resources that not only meet military needs but also support public needs in maintaining the stability of the economic sector to strengthen national security.

While growing digital threats, strengthening the capacity of cyber defense and information security is a top priority that needs to be implemented. Cyber threats continue to grow, and the state must have the ability to protect vital information infrastructure and ward off cyber-attacks that can disrupt government systems and society. International cooperation in cybersecurity and disinformation management is also needed to strengthen state resilience. Countries need to cooperate with other countries to share information, technologies and strategies that can strengthen cyber defense and combat disinformation globally.

Future defense policies must be more flexible, and adaptive to technological developments and geopolitical dynamics that continue to change and become new threats. Data-based technology and artificial intelligence (AI) can be utilized to predict threats more quickly and strengthen preparedness for cyber-attacks, and disinformation, as well as responses to complex hybrid threats. Thus, systematic and sustainable efforts are needed to integrate defense policy with public policy from a national security perspective in the face of hybrid warfare threats. Collaboration across sectors, including the government, private sector and society is needed to strengthen the country's resilience. By increasing public awareness of existing threats and strengthening training and education on how to deal with hybrid threats, the state can build social resilience and reduce its vulnerability to potential threats. With a coordinated, integrated and technology-driven approach, the state can respond more effectively to hybrid threats, maintain national stability and enhance the country's resilience in the face of increasingly complex and dynamic global challenges.

REFERENCES

Adrian Zenz (2025) Innovating Repression: Policy Experimentation and the Evolution of Beijing's Re-Education Campaign in Xinjiang, Journal of Contemporary China, 34:152, 328-349, https://doi.org/10.1080/10670564.2024.2302484.

Alshammari, A. (2023). A Novel Security Framework to Mitigate and Avoid Unexpected Security Threats in Saudi Arabia. Engineering, Technology & Applied Science Research, 13(4), 11445–11450. https://doi.org/10.48084/etasr.6091.

Andreas Kruck & Moritz Weiss (2023) The regulatory security state in Europe, Journal of European Public Policy, 30:7, 1205-1229, https://doi.org/10.1080/13501763.2023.2172061.

Andrews, P.-S. (2022). How May National Culture Shape Public Policy? The Case of Energy Policy in China. *The Energy Journal*, *43*(3), 257-273. https://doi.org/10.5547/01956574.43.3.pand.

Anna McWilliams & Mattias Legnér (2024) Threat assessments and heritage in the age of hybrid warfare, International Journal of Heritage Studies, 30:12, 1379-1392, https://doi.org/10.1080/13527258.2024.2393610.

Benjamin Farrand, Helena Carrapico, Aleksei Turobov, The new geopolitics of EU cybersecurity: security, economy and sovereignty, *International Affairs*, Volume 100, Issue 6, November 2024, Pages 2379–2397, https://doi.org/10.1093/ia/iiae231.

Böller, F., & Wenzelburger, G. (2024). Grasping Foreign and Security Policy Change: Patterns and Conditions of Change Among Liberal Democracies. *Politics and Governance, 12*, Article 7172. https://doi.org/10.17645/pag.7172.

Daniel, J., & Eberle, J. (2021). Speaking of hybrid warfare: Multiple narratives and differing expertise in the 'hybrid warfare' debate in Czechia. *Cooperation and Conflict*, *56*(4), 432-453. https://doi.org/10.1177/00108367211000799.

Derleth, J., & Pickler J. (2022). Twenty-first Century Threats Require Twenty-first Century Deterrence. Connections: The Quarterly Journal. 21(2), 11-23., https://doi.org/10.11610/Connections.21.2.01.

Dov Bachmann, S.-D., Putter, D. & Duczynski, G. (2023) Hybrid warfare and disinformation: A Ukraine war perspective. *Global Policy*, 14, 858–869. Available from: https://doi.org/10.1111/1758-5899.13257.

Dries Putter (15 Dec 2024): Navigating the interplay of cognitive warfare and counterintelligence in African security strategies: insights and case studies, Journal of Policing, Intelligence and Counter Terrorism, https://doi.org/10.1080/18335330.2024.2440873.

Elise Klein (2024) Reparative public policy, Critical Policy Studies, 18:4, 600-619, https://doi.org/10.1080/19460171.2023.2288666.

Eric Schmidt; AI, Great Power Competition & National Security. *Daedalus* 2022; 151 (2): 288–298. https://doi.org/10.1162/daed_a_01916.

Freedman, J., Hoogensen Gjørv, G. & Razakamaharavo, V. (2021). Identity, stability, Hybrid Threats and Disinformation, Icono 14, 19(1), 38-69. https://doi.org/10.7195/ri14.v19i1.1618.

Gintautas Razma (2023) Strategic Facts as a Comprehensive Model for Defence Analysis, Defence Studies, 23:2, 254-273, https://doi.org/10.1080/14702436.2022.2113516.

Gleb Papyshev & Masaru Yarime (2023) The state's role in governing artificial intelligence: development, control, and promotion through national strategies, Policy Design and Practice, 6:1, 79-102, https://doi.org/10.1080/25741292.2022.2162252.

Gunneriusson, H. (2021). Hybrid warfare: Development, historical context, challenges and interpretations, Icono 14, 19(1), 15-37. https://doi.org/10.7195/ri14.v19i1.1608.

Hasanul Banna, Ashraful Alam, Xihui Haviour Chen, Ahmed W. Alam, Energy security and economic stability: The role of inflation and war, Energy Economics, Volume 126, 2023, 106949, https://doi.org/10.1016/j.eneco.2023.106949.

Heath-Kelly, C. (2024). 'Social defence' and the resilience of the domestic war on terror: A genealogy of social security, national security, and defence. European Journal of International Security, 1–18. https://doi.org/10.1017/eis.2024.33.

Henke, M., & Maher, R. (2021). The populist challenge to European defense. Journal of European Public Policy, 28(3), 389–406. https://doi.org/10.1080/13501763.2021.1881587.

Herrera-Cuenca M, Landaeta Jimenez M and Sifontes Y (2021) Challenges in Food Security, Nutritional, and Social Public Policies for Venezuela: Rethinking the Future. Front. Sustain. Food Syst. 5:635981. https://doi.org/10.3389/fsufs.2021.635981.

Isabelle Bond & James Mortensen (2023) The changing value of Antarctica to Australia's security policy, Australian Journal of International Affairs, 77:3, 299-316, https://doi.org/10.1080/10357718.2023.2216139.

Iuga, I.-C., & Socol, A. (2023). Defending the nation, securing the economy. E&M Economics and Management, 26(4), 17–37. https://doi.org/10.15240/tul/001/2023-4-002.

Jackson, N. J. (2021). The Canadian government's response to foreign disinformation: Rhetoric, stated policy intentions, and practices. International Journal, 76(4), 544-563. https://doi.org/10.1177/00207020221076402.

Jonek-Kowalska, I. (2022). Assessing the energy security of European countries in the resource and economic context. Oeconomia Copernicana, 13(2), 301–334. https://doi.org/10.24136/oc.2022.009.

Julie Celine Bergaust & Stig Rune Sellevåg (2024) Improved conceptualising of hybrid interference below the threshold of armed conflict, European Security, 33:2, 169-195, https://doi.org/10.1080/09662839.2023.2267478.

Kharazishvili, Y., & Kwilinski, A. (2022). Methodology for Determining the Limit Values of National Security Indicators Using Artificial Intelligence Methods. Virtual Economics, 5(4), 7-26. https://doi.org/10.34021/ve.2022.05.04(1).

Kuhn, C.E., Reis, F.A., Oliveira, V.G., Cabral, V.C., Gabelini, B.M., & Veloso, V.Q. (2022). Evolution of public policies on natural disasters in brazil and worldwide. *Anais da Academia Brasileira de Ciencias, 94 suppl 4*, e20210869. https://doi.org/10.1590/0001-3765202220210869.

Leal Filho, W.; Fedoruk, M.; Paulino Pires Eustachio, J.H.; Barbir, J.; Lisovska, T.; Lingos, A.; Baars, C. How the War in Ukraine Affects Food Security. Foods 2023, 12, 3996. https://doi.org/10.3390/foods12213996.

Ljungkvist, K. (2024). The military-strategic rationality of hybrid warfare: Everyday total defence under strategic non-peace in the case of Sweden. European Journal of International Security, 9(4), 533–552. https://doi.org/10.1017/eis.2024.18.

Malone, M.A., Hildebrand, S. Is there coercion in local emergency management policy implementation?. Natural Hazards 113, 1663–1674 (2022). https://doi.org/10.1007/s11069-022-05362-3.

Manu Lekunze (2023) Insurgency and national security: a perspective from Cameroon's separatist conflict, Third World Quarterly, 44:6, 1155-1173, https://doi.org/10.1080/01436597.2023.2177149.

Mara, D.; Nate, S.; Stavytskyy, A.; Kharlamova, G. The Place of Energy Security in the National Security Framework: An Assessment Approach. Energies 2022, 15, 658. https://doi.org/10.3390/en15020658.

Mattingsdal, J., Espevik, R., Johnsen, B. H., & Hystad, S. (2024). Exploring Why Police and Military Commanders Do What They Do: An Empirical Analysis of Decision-Making

in Hybrid Warfare. *Armed Forces & Society*, *50*(4), 1218-1244. https://doi.org/10.1177/0095327X231160711.

Matzkin, S., Shandler, R., & Canetti, D. (2024). The limits of cyberattacks in eroding political trust: A tripartite survey experiment. *The British Journal of Politics and International Relations*, *26*(4), 1033-1054. https://doi.org/10.1177/13691481231210383.

Meszaros, Edina & Constantin - Vasile, Țoca. (2023). The EU's resilience and the management of hybrid threats coming from the Eastern neighbourhood: Belarus and the deliberate facilitation of irregular immigration. 14. 5-30. https://doi.org/10.47743/ejes-2023-0101.

Mumford, A., & Carlucci, P. (2023). Hybrid warfare: The continuation of ambiguity by other means. European Journal of International Security, 8(2), 192–206. https://doi.org/10.1017/eis.2022.19.

Nizovtsev, Y. Y., Lyseiuk, A. M., & Kelman, M. (2022). From self-affirmation to national security threat: analyzing the Ukraine's foreign experience in countering cyberattacks. Revista Científica General José María Córdova, 20(38), 355-370. https://dx.doi.org/10.21830/19006586.905.

Njoku, E. T. (2022). The State and the Securitization of Civil Society Organizations in Nigeria. *Nonprofit and Voluntary Sector Quarterly*, *51*(1), 190-215. https://doi.org/10.1177/08997640211003256.

Nte, Ngboawaji Daniel, Vigo Augustine Teru, and Nadiyah Meyliana Putri. "Intelligence Education for National Security and Public Safety Policy: A Comparative Analysis of Nigeria, South Africa, and Indonesia". Lex Scientia Law Review 6, No. 1 (2022): 187-218. https://doi.org/10.15294/lesrev.v6i1.54431.

Óscar Fernández, Marie Vandendriessche, Angel Saz-Carranza, Núria Agell & Javier Franco (2023) The impact of Russia's 2022 invasion of Ukraine on public perceptions of EU security and defence integration: a big data analysis, Journal of European Integration, 45:3, 463-485, https://doi.org/10.1080/07036337.2023.2183392.

Paula Kivimaa, Marja H. Sivonen, Interplay between low-carbon energy transitions and national security: An analysis of policy integration and coherence in Estonia, Finland and Scotland, Energy Research & Social Science, Volume 75, 2021, 102024, https://doi.org/10.1016/j.erss.2021.102024.

Pierre Bocquillon, Suzanne Doyle, Toby S. James, Ra Mason, Soul Park & Matilde Rosina (2024) The effects of wars: lessons from the war in Ukraine, Policy Studies, 45:3-4, 261-281, https://doi.org/10.1080/01442872.2024.2334458.

Räisänen, H., Hakala, E., Eronen, J., Hukkinen, J., & Virtanen, M. (2021). Comprehensive Security: The Opportunities and Challenges of Incorporating Environmental Threats in Security Policy. Politics and Governance, 9(4), 91-101. https://doi.org/10.17645/pag.v9i4.4389.

Salmai Qari, Tobias Börger, Tim Lohse, Jürgen Meyerhoff, The value of national defense: Assessing public preferences for defense policy options, European Journal of Political Economy, Volume 85, 2024, 102595, https://doi.org/10.1016/j.ejpoleco.2024.102595.

Steingartner, W., & Galinec, D. (2021). Cyber Threats and Cyber Deception in Hybrid Warfare. *Acta Polytechnica Hungarica*. https://doi.org/10.12700/APH.18.3.2021.3.2.

Tim Legrand & Diane Stone (2021) Governing global policy: what IPE can learn from public policy?, Policy and Society, 40:4, 484-501, https://doi.org/10.1080/14494035.2021.1975218.

Tobias Ide, McKenzie F. Johnson, Jon Barnett, Florian Krampe, Philippe Le Billon, Lucile Maertens, Nina von Uexkull & Irene Vélez-Torres (2023) The Future of Environmental Peace and Conflict Research, Environmental Politics, 32:6, 1077-1103, https://doi.org/10.1080/09644016.2022.2156174.

Vinicius Mariano de Carvalho & Raphael C. Lima (2023) The development, security, and defence nexus in Brazil, Conflict, Security & Development, 23:2, 93-103, https://doi.org/10.1080/14678802.2023.2225350.

Vladimir Rauta & Sean Monaghan (2021) Global Britain in the grey zone: Between stagecraft and statecraft, Contemporary Security Policy, 42:4, 475-497, https://doi.org/10.1080/13523260.2021.1980984.

Wither, J. K. (2023). Hybrid Warfare Revisited: A Battle of 'Buzzwords'. Connections: The Quarterly Journal. 22(1), 7-28. https://doi.org/10.11610/Connections.22.1.02.

Wróblewski, W. & Wiśniewski, M. The Concept of a Method for Predicting the Cascade Effect Under Conditions of Hybrid Warfare. Foundations of Management, 2024, Sciendo, vol. 16 no. 1, pp. 233-246. https://doi.org/10.2478/fman-2024-0014.