Unraveling Current Trends in Hybrid Warfare 3.0: A Literature Study on Modern Non-Conventional Threats.

Jamal Dani Arifin*

School of Strategic and Global Studies, University of Indonesia, Indonesia
*Correspondence email: wiradharma019@gmail.com

ARTICLE INFO

Article history:
Received : 3 July 2025
Accepted : 21 July 2025
Available : 31 July 2025

Keywords:
Hybrid Warfare, Non-Conventional Threats, Disinformation, Cybersecurity, EU, NATO.

ABSTRACT

Hybrid Warfare 3.0 represents a significant evolution in the global security threat landscape, blending advanced digital technology, disinformation, and non-military geopolitical pressure. This paper presents the findings of a literature review of 12 recent academic journals to identify key trends, manifestations, and responses to non-conventional threats within the context of Hybrid Warfare 3.0. Findings indicate that these threats are characterized by the close integration of technologies such as AI (for deep-fakes and bots), weaponized migration as a geopolitical pressure tool, and offensive cyber operations. The Russia-Ukraine conflict case study clarifies the multifaceted nature of this threat. Institutional responses by the EU and NATO have evolved but still face challenges in adaptation and coordination. This paper concludes that confronting Hybrid Warfare 3.0 requires a holistic approach encompassing strengthened information resilience, closer institutional cooperation, and the development of adaptive technological capabilities.

1. INTRODUCTION

Over the past few decades, the global security landscape has undergone a significant shift from conventional conflicts toward more complex and indirect forms of threats, known as hybrid warfare. This phenomenon combines conventional military and non-military tools, including disinformation, cyber operations, economic intervention, and even manipulation of socio-political issues, creating major challenges for states and international institutions in identifying, understanding, and responding to these threats (Bankov, 2024; Mumford & Carlucci, 2023).

The development of information and communication technology, particularly artificial intelligence (AI), has accelerated the transformation of these threats into what is now called Hybrid Warfare 3.0. At this stage, state and non-state actors fully exploit digital potential to conduct operations that are fast, wide-reaching, and difficult to trace, such as the use of deepfakes, social media bots, and sophisticated disinformation campaigns to influence public opinion and undermine the socio-political stability of target countries (Battista, 2024; GABRIAN & Claudia-Alecsandra, 2024; Steingartner et al., 2024).

Furthermore, the phenomenon of "weaponized migration" or the use of migration as a geopolitical pressure tool, as seen in the Belarus-Poland crisis (Mészáros & Țoca, 2023), demonstrates how non-military threats can be strategically employed to create simultaneous humanitarian and security dilemmas. These threats not only expand the battlefield into civilian domains but also blur the boundaries between war and peace, as well as between internal and external threats (Łubiński, 2022; Stoakes, 2024).

Russia's invasion of Ukraine since 2022 serves as an important case study that clarifies the evolution of hybrid warfare toward stage 3.0. This conflict unfolds not only on the physical battlefield but also in the realms of information, cyber, economic, and even cultural domains, demonstrating the full integration of various non-conventional threat components (Filina, 2023; Fridman et al., 2024; Mecková, 2024).

Amid these developments, significant challenges emerge for international security institutions such as the European Union (EU) and NATO in formulating adaptive and coherent strategies and policies to address evolving hybrid threats (Anagnostakis, 2025; Genini, 2025; ȘTEFAN, 2023). Response to Hybrid Warfare 3.0 requires a holistic approach encompassing information resilience strengthening, critical infrastructure protection, migration crisis management, and enhanced inter-agency and international collaboration (Bertolini et al., 2023; Jasper et al., 2023; Kostarakos, 2023).

Therefore, it is essential to conduct a literature review of current trends in hybrid warfare to provide a more comprehensive understanding of the characteristics, evolution, and manifestations of modern non-conventional threats within the context of contemporary global security. This study is expected to contribute to the development of more effective policy and strategy frameworks in addressing 21st-century security challenges.

2. LITERATURE REVIEW

This section provides a comprehensive review of relevant literature to establish the conceptual and theoretical foundation of this study, with a focus on defining Hybrid Warfare, tracing its conceptual development, and examining the various forms of non-conventional threats associated with it.

2.1 Definition and Evolution of the Hybrid Warfare Concept

The concept of Hybrid Warfare (HW) has undergone considerable debate and evolution since its emergence. (Bankov, 2024) emphasizes that HW often exists in a "conceptual gray zone," and attempts to provide clarity by aligning various perceptions. He demonstrates that HW 3.0 is the result of the evolution from HW 1.0 (focused on the combination of conventional and guerrilla attacks) and HW 2.0 (the emergence of cyber and disinformation threats). HW 3.0 is characterized by the full integration of digital and information technology into all aspects of strategy.

Mumford & Carlucci, (2023) add that the core characteristic of HW 3.0 is its ambiguity ("continuation of ambiguity by other means"). They argue that this ambiguity is not new, but rather a strategic choice that enables actors to achieve political objectives without engaging in open conflict. This ambiguity makes attribution (identifying perpetrators) and clear responses extremely difficult.

2.2 Non-Conventional Threats in Hybrid Warfare 3.0

Threats in HW 3.0 are primarily non-conventional and exploit various domains. Several major forms identified in the literature include:

a. Technology-Based Disinformation: Battista, (2024) emphasizes how disinformation in the digital era has become a primary tool for global destabilization. The use of AI to create deepfakes and social media bots enables the spread of false information on a large scale and at high speed. (Waltzman, 2017) provides the theoretical foundation with the concept of "weaponization of information," emphasizing the need for "cognitive security" to protect societies from information manipulation that exploits mass psychological understanding.

b. Weaponized Migration: Mészáros & Țoca, (2023) and CIEKANOWSKI et al. (2025) specifically analyze the phenomenon of weaponized migration. They demonstrate how states can deliberately facilitate migrant flows to neighboring countries to create humanitarian crises and pressure foreign policy, as occurred during the 2021-2022 Belarus-Poland crisis. Mészáros & Țoca (2023) discuss how this is considered a hybrid attack and how the EU attempts to build resilience to address it.

c. Cyber Operations and Infrastructure Security: (Ormrod et al., 2023) analyze offensive cyber operations as an integral part of hybrid warfare strategies, particularly in the context of the Russia-Ukraine conflict, including the use of specific malware. (GABRIAN & Claudia-Alecsandra, 2024) emphasizes the ransomware threat in the AI era, which is becoming increasingly sophisticated and difficult to trace, as well as how AI can be used by both criminal actors and for cyber defense.

2.3. Case Study and Institutional Response

The Russia-Ukraine conflict case study is crucial for understanding the real-world application of HW 3.0. (Ormrod et al., 2023) and (Mumford & Carlucci, 2023) and demonstrate that this conflict unfolds not only on the physical battlefield but also through information, cyber, and psychological warfare.

Institutional responses to HW 3.0 have evolved. Anagnostakis (2025) analyzes the EU-NATO relationship in addressing this threat, emphasizing the importance of coordination from "functional overlap" toward "functional cooperation." Genini (2025) discusses how NATO must adapt post-Ukraine war based on official documents and case studies. Ștefan (2023) analyzes EU policies in developing capabilities to address hybrid threats.

3. METHODS

This research employs a systematic literature review approach to analyze and examine current trends in Hybrid Warfare 3.0, particularly regarding modern non-conventional threats. This method was chosen because it enables researchers to comprehensively identify, evaluate, and synthesize available knowledge in academic literature related to complex phenomena such as Hybrid Warfare 3.0.

The research methodology steps are as follows:

a. Scope Determination and Research Questions: The research focus was established on Hybrid Warfare 3.0 and non-conventional threats such as AI-based disinformation, weaponized migration, and cyber operations.

b. Literature Source Selection: Based on initial bibliography and document availability, 12 primary sources were selected consisting of peer-reviewed academic journals published between 2017-2025 and directly relevant to the research theme. These sources are: Bankov (2024), Battista (2024), Ciekanowski et al. (2025), Mészáros & Țoca (2023), Ormrod et al. (2023), Mumford & Carlucci (2022), Anagnostakis (2025), Genini (2025), Gabrian (2024), Stefan (2023), Waltzman (2017), and Steingartner et al. (2024).

c. Quality and Relevance Evaluation: Each selected source was evaluated based on author credibility, institutional affiliation, and direct relevance to the research theme.

d. Data Extraction and Collection: Data were extracted from each source based on the initial analytical framework, covering: definition and concept of Hybrid Warfare 3.0, types and examples of non-conventional threats, case studies or examples of real-world implementation, and institutional responses (EU, NATO).

e. Data Analysis and Synthesis: The extracted data were analyzed using a thematic analysis approach. Major themes sought and examined include: Conceptual Evolution, Threat Components, Case Studies, and Institutional Responses.

f. Report/Proceedings Compilation: Findings from the analysis are systematically compiled in the form of this proceedings.

4. RESULTS AND DISCUSSION

Based on the analysis of 12 relevant journals (attached analysis table), several key themes emerged that offer a comprehensive understanding of Hybrid Warfare 3.0 and modern non-conventional threats. These themes focus on four main aspects: (1) Hybrid Warfare Concept Evolution, (2) Non-Conventional Threat Manifestations (including AI-based disinformation, weaponized migration, and cyber operations), (3) Case Studies and Practical Implementation, and (4) Institutional Responses (especially from the EU and NATO).

4.1 Evolution of Hybrid Warfare Concept: Towards the 3.0 Era

Analysis of several journals indicates that understanding of hybrid warfare continues to evolve. Bankov (2024) provides a current definition of Hybrid Warfare (HW), emphasizing that HW 3.0 is the result of evolution from conventional and cyber-centric approaches (HW 1.0 and 2.0) into a highly integrated form with digital and information technology. Mumford & Carlucci (2023) add that the main characteristic of HW 3.0 is its ambiguity, which makes clear attribution and response difficult. They state that this is not a "new" war, but rather a strategic choice made by major powers to achieve political objectives in a specific era.

Wróblewski et al. (2025) refers to this phenomenon as a "Battle of Buzzwords," indicating that overly broad definitions sometimes create confusion, but its essence lies in

4.2. Manifestation of Non-Conventional Threats in Hybrid Warfare 3.0

Non-conventional threats in HW 3.0 primarily manifest in three main forms based on analysis of selected journals:

a. AI and Digital Technology-Based Disinformation: Battista (2024) explicitly emphasizes how disinformation in the digital era has become a primary tool for global destabilization. The use of technologies such as deepfakes and AI bots enables the spread of false information on a large scale and at high speed. Steingartner et al. (2024) discuss disinformation campaigns and how resilience models can be developed to address them, including the use of software to combat fake news (as implemented by Lithuania). Waltzman (2017) provides the theoretical foundation with the concept of "weaponization of information" and the need for "cognitive security" to protect societies from information manipulation.

b. Weaponized Migration: CIEKANOWSKI et al. (2025) analyze how migration crises are used as a geopolitical pressure tool at the European Union's borders, particularly between Belarus and Poland, with statistical data showing surges in migrants from specific countries. Mészáros & Țoca (2023) provide a specific case study of the 2021 Belarus-Poland situation, demonstrating how state actors can deliberately facilitate migrant flows to create crises and pressure the foreign policies of other countries. They discuss the policy dilemmas faced by the EU in managing these hybrid threats.

c. Cyber Operations and Infrastructure Security: Ormrod et al. (2023) analyze offensive cyber operations as an integral part of hybrid warfare strategies, particularly in the context of the Russia-Ukraine conflict. They provide examples of malware usage such as CredoMap and Cobalt Strike by APT28 (Fancy Bear) groups associated with Russia. GABRIAN & Claudia-Alecsandra (2024) emphasizes the ransomware threat in the AI era, which is becoming increasingly sophisticated and difficult to trace, as well as how AI can be used by both criminal actors and for cyber defense.

4.3. Case Study: The Ukraine War as a Manifestation of Hybrid Warfare 3.0

The Russia-Ukraine war since 2022 represents a crucial case study for understanding HW 3.0. Analysis from various journals, including Ormrod et al.

(2023), demonstrates that this conflict extends beyond the physical battlefield to encompass Information Warfare (Ormrod et al., 2023), Cyber Warfare involving ransomware attacks (GABRIAN & Claudia-Alecsandra, 2024; Ormrod et al., 2023), and Psychological Warfare through disinformation campaigns (Battista, 2024; Waltzman, 2017).

4.4. Institutional Response: The Role of the EU and NATO in Addressing Hybrid Warfare 3.0

Institutional responses to HW 3.0 have evolved:

a. EU-NATO Cooperation: Anagnostakis (2025) emphasizes the importance of coordination between the EU and NATO to avoid functional overlap and enhance effectiveness, moving toward "functional cooperation."

b. Resilience Strengthening: Mészáros & Țoca (2023) and Steingartner et al. (2024) suggest a holistic approach that encompasses information resilience.

c. Policy Development and Capabilities: Ștefan (2023) analyzes EU policies, while Genini (2025) emphasizes that NATO must continue to adapt post-Ukraine war.

5. CONCLUSION

Based on the analysis of 12 major journals, it can be concluded that Hybrid Warfare 3.0 represents a significant evolution from previous forms of warfare, characterized by the full integration of digital and information technology in threat strategies. Non-conventional threats such as AI-based disinformation, weaponized migration, and cyber operations have become the main pillars of this strategy. Institutional responses by the EU and NATO have evolved, but still face challenges in adaptation and coordination. The Ukraine war case study provides important lessons about the complexity and multifaceted nature of these threats. Effectively addressing these challenges requires an integrated and adaptive approach from all stakeholders.

Furthermore, overall these journals provide a comprehensive overview that Hybrid Warfare 3.0 is a complex and multifaceted threat that requires a holistic and well-coordinated approach in terms of conceptual understanding, threat identification, and institutional responses.

6. REFERENCES

Anagnostakis, D. (2025). “Taming the Storm” of Hybridity: The EU-NATO

Relationship on Countering Hybrid Threats–From Functional Overlap to Functional Cooperation. *Defence Studies*, *00*(00), 1–25. https://doi.org/10.1080/14702436.2025.2464636

Bankov, B. (2024). Hybrid Warfare: How to Escape the Conceptual Gray-Zone. *Journal of Strategic Security*, *17*(1), 1–23. https://doi.org/10.5038/1944-0472.17.1.2118

Battista, D. (2024). The Hybrid Warfare of the Digital Age: How Disinformation Destabilizes the World. *HAPSc Policy Briefs Series*, *5*(2), 65–70. https://doi.org/10.12681/hapscpbs.40782

Bertolini, M., Minicozzi, R., & Sweijs, T. (2023). *Ten guidelines for dealing with hybrid threats: A policy response framework*. Hague Centre for Strategic Studies (HCSS).

CIEKANOWSKI, H. A. B. Z., ŻURAWSKI, S., & OSKIERKO, M. (2025). The migration crisis as a tool of hybrid warfare–Analysis of selected cases at the borders of the European Union. *L'europe/United Europe*, *22*(march), 20–29.

Filina, A. (2023). *Gibridnaya Voyna in Light of the War in Ukraine: Analysing Changes in Russian Interpretations and the Use of Hybrid Warfare Concept.*

Fridman, O., Daukšas, V., Venclauskienė, L., & Urbanavičiūtė, K. (2024). *War on All Fronts: How the Kremlin's Media Ecosystem Broadcasts the War in Ukraine*. NATO Strategic Communicaitons Centre of Excellence.

GABRIAN, & Claudia-Alecsandra. (2024). Claudia-Alecsandra GABRIAN RANSOMWARE IN THE AGE OF AI : NAVIGATING CYBERSECURITY CHALLENGES. *Studia Securitatis*, *18*, 151–163.

Genini, D. (2025). Countering hybrid threats: How NATO must adapt (again) after the war in Ukraine. *New Perspectives*, *33*(2), 122–149. https://doi.org/10.1177/2336825X251322719

Jasper, S., Vijayakumar, D., Stalin, B., Rajesh, S., & Ida, S. J. (2023). Experimental investigation of a multilayer nitride coating deposited on austenitic coating steel. *Materials Today: Proceedings*, *74*, 117–121.

Kostarakos, M. (2023). European Union and NATO Cooperation in Hybrid Threats. In *Handbook for Management of Threats: Security and Defense, Resilience and Optimal Strategies* (pp. 405–423). Springer.

Łubiński, P. (2022). Hybrid warfare or hybrid threat–the weaponization of migration as an example of the use of lawfare–case study of Poland. *Polish Political Science Yearbook*, *51*(1), 43–55.

Mecková, S. (2024). *Faces of Truth: Analyzing Russian Hybrid Warfare Narratives in newsfront.*

Mészáros, E. L., & Ţoca, C. V. (2023). The EU's resilience and the management of hybrid threats coming from the Eastern neighbourhood: Belarus and the deliberate facilitation of irregular immigration. *Eastern Journal of European Studies*, *14*(1).

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

Ormrod, A., Ormrod, D., & Slay, J. (2023). Cyber Offensive Operations in Hybrid Warfare: Observations from the Russo-Ukrainian Conflict. *Journal of Information Warfare*, *22*(1), 76–87. https://www.jinfowar.com/sites/default/files/Cyber Offensive Operations in Hybrid Warfare_0.pdf

ȘTEFAN, M. (2023). EU Policies for Developing Capabilities to Counter Hybrid Threats. *Romanian Military Thinking*, *2023*(1), 168–181. https://doi.org/10.55535/rmt.2023.1.9

Steingartner, W., Galinec, D., Vaľko, D., & Ádám, N. (2024). Disinformation Campaigns: Battling Misinformation for Resilience in Hybrid Threats Model. *Acta Polytechnica Hungarica*, *21*(10), 517–532. https://doi.org/10.12700/aph.21.10.2024.10.31

Stoakes, E. (2024). *Toward a self-defence model for media in small democracies: responding to weaponised information in the 'new cold war'environment*.

Waltzman, R. (2017). The Weaponization of Information: The Need for Cognitive Security. *The Weaponization of Information: The Need for Cognitive Security*. https://doi.org/10.7249/ct473

Wróblewski, W., Wiśniewski, M., & Bieniasz, J. (2025). *Civil Protection and Domestic Security in Contemporary Hybrid Warfare*. Routledge.

Appendix: Literature Analysis Table

No.	Title and author (years)	Main Focus	Theme approach/ methodology	Key Finding/ main contributions	Relevance to Research theme
1	Bankov, B. (2024). Hybrid Warfare.	Definition & Conceptual Mapping of Hybrid Warfare	Conceptual Analysis & Mapping	Identifying various definitions of HW and proposing an initial concept mapping based on hybridity to reduce conceptual ambiguity.	Very High - Provides conceptual foundation for understanding HW 3.0.
2	Battista, D. (2024). The Hybrid Warfare of the Digital Age: How Disinformation Destabilizes the World.	Disinformation & Destabilization in the Digital Era	Policy & Technology Analysis	Emphasizes how disinformation in the digital era has become a primary tool for destroying global stability	Very High - Core of technology-based non-conventional threats in HW 3.0.
3	Ciekanowski et al. (2025). Migration Crisis as a Tool...	Weaponized Migration & Border Data Analysis	Statistical Data Analysis & Case Study	Analyzes migration crises as a geopolitical pressure tool through detailed border data between Poland and Belarus.	Very High - Concrete case study of weaponized migration with supporting data.
4	Mészáros, E. L., & Ţoca, C. V. (2023). The EU's resilience and the management of hybrid threats...	Weaponized Migration & EU Response	Case Study (Belarus-Poland) & Policy Analysis	Case study of Belarus-Poland 2021, discussing EU policy dilemmas and challenges in building resilience.	Very High - Specific case study and EU institutional response.
5	Ormrod, A., Ormrod, D., & Slay, J. (2023). Cyber Offensive Operations in Hybrid Warfare...	Cyber Operations & Ukraine Conflict	Cyber Data Analysis & Case Study	Analyzes offensive cyber operations in Russia/Ukraine, including the use of specific malware (APT28, Sandworm, etc.) in HW.	Very High - Important technology component in HW 3.0 with real-world examples.
6	Mumford, A., & Carlucci, P. (2022). Hybrid warfare: The continuation of ambiguity by other means.	Ambiguity in Hybrid Warfare	Theoretical & Conceptual Analysis	Emphasizes that ambiguity is the core characteristic of HW, not a new phenomenon, making attribution and response difficult.	High - Supports understanding of the fundamental nature of HW 3.0.

7	Anagnostakis, D. (2025). "Taming the Storm" of Hybridity: The EU-NATO Relationship...	Institutional Response (EU-NATO)	Policy Analysis & Cooperation	Discusses the evolution of EU-NATO relations in addressing HW, from "functional overlap" to "functional cooperation".	High - Core of institutional response to HW 3.0.
8	Genini, D. (2025). Countering hybrid threats: How NATO must adapt...	NATO's Adaptation to HW	Official Document Analysis & Adaptation Study	Analyzes how NATO must adapt post-Ukraine war based on official documents and case studies.	High - Focus on the evolution of NATO's institutional response.
9	Gabrian, C. A. (2024). Ransomware In the Age of AI...	Ransomware & AI in Cyber Security	Technology Analysis & Threat Assessment	Explains how ransomware evolves with AI and the cybersecurity challenges in the context of HW.	High - Specific technology aspect in HW 3.0 cyber threats.
10	Stefan, M. (2023). EU Policies for Developing Capabilities to Counter Hybrid Threats.	EU Policy & Capability Development	EU Policy Document Analysis	Analyzes EU policies and initiatives (such as Council Conclusions) in developing capabilities to address hybrid threats.	High - Focus on EU policy approach and capability development.
11	Waltzman, R. (2017). The weaponization of information...	Weaponisasi Informasi & Cognitive Security	Early Theoretical Concept	Provides the basic concept of information weaponization and the need for "cognitive security" to protect society.	High - Theoretical foundation for understanding psychological/information threats in HW.
12	Steingartner et al. (2024). Disinformation campaigns...	Disinformation Campaigns & Resilience Model	Case Study (Lithuania) & Technology Analysis	Discusses disinformation campaigns and how resilience models (including software usage such as in Lithuania) can be developed.	High - Supports technology analysis and response models against disinformation.