



HYBRID WARFARE AND NON-STATE ACTORS IN THE MIDDLE EAST AND SOUTH ASIA: EMERGING THREATS AND STRATEGIC RESPONSES

<sup>1</sup>Dr. Fawad Ali

<sup>2</sup>Dr. Saima Razzaq Khan

<sup>3</sup>Fareed Ullah

<sup>1</sup>Department of Political Science, Gomal University DI.Khan

<sup>2</sup>Department Of Political Science, Gomal University DI.Khan

<sup>3</sup>Department of Political Science, Qurtuba University Of Science & Information Technology DI.Khan

<sup>1</sup>[fawad.lohani@gu.edu.pk](mailto:fawad.lohani@gu.edu.pk), <sup>2</sup>[dr.saima\\_razzaq@gu.edu.pk](mailto:dr.saima_razzaq@gu.edu.pk), <sup>3</sup>[faridullah.kk@gmail.com](mailto:faridullah.kk@gmail.com)

Abstract

The contemporary security landscape in the Middle East and South Asia has undergone a profound transformation with the rise of hybrid warfare and the increasing influence of non-state actors. Hybrid warfare, characterized by a sophisticated blend of conventional military operations, unconventional tactics, cyber interventions, informational campaigns, and economic coercion, has fundamentally blurred the traditional boundaries between war and peace, and between state and non-state actors. In these regions, hybrid conflicts often manifest through multi-dimensional strategies that combine direct military engagement with asymmetric tactics, proxy warfare, cyber-attacks, propaganda, and resource manipulation, creating highly complex and fluid conflict environments. Non-state actors—including terrorist organizations, insurgent groups, militias, and transnational networks—have become central to these dynamics, exploiting political vacuums, weak governance structures, and globalized technologies to exert influence, disrupt governance, and challenge state sovereignty. Their operations are often enhanced by state sponsorship or external support, further complicating the security calculus and creating environments in which traditional, state-centric models of defense and diplomacy prove inadequate. Addressing these threats requires adaptive, multi-layered strategies that integrate military, cyber, economic, and socio-political tools, along with regional cooperation and international engagement. Policymakers must recognize that hybrid warfare is not solely a military challenge but a deeply political and social one, requiring comprehensive approaches that address underlying vulnerabilities, structural inequalities, and ideological drivers. The evolving interplay between state and non-state actors demonstrates the need for flexible, holistic frameworks that can anticipate hybrid tactics, counter multi-domain threats, and strengthen resilience to ensure stability and security in these volatile regions.

**Keywords:** Hybrid Warfare, Non-State Actors, Cyber Security, Proxy Conflicts, Middle East and South Asia, Strategic Responses

Article Details:

Received on 13 Oct 2025

Accepted on 04 Nov 2025

Published on 06 Nov 2025

Corresponding Authors\*:

## Introduction

### Hybrid Warfare: A Contemporary Paradigm

Hybrid warfare has emerged as a central paradigm in contemporary conflict, representing a significant shift from traditional warfare models. Unlike conventional wars that rely solely on organized military forces and battlefield engagement, hybrid warfare integrates both conventional military operations and unconventional tactics. Azad, T. M., & Haider, M. W. (2021). These unconventional tactics include cyber-attacks that target critical infrastructure, disinformation campaigns designed to manipulate public perception, proxy warfare that enables states to influence conflicts indirectly, economic coercion that leverages trade and financial vulnerabilities, and terrorism as a tool to destabilize societies. Jalil Shah, H., & Ehsan, M. (2023). This combination of strategies creates a multi-dimensional battlefield where the lines between peace and war, state and non-state actors, and military and civilian spheres are increasingly blurred.

### Regional Focus: Middle East and South Asia

The Middle East and South Asia exemplify regions where hybrid threats are pervasive and particularly complex. Kurochkin, A., Lodina, A., & Pankov, G. (2022). These regions are characterized by intricate socio-political landscapes shaped by historical conflicts, sectarian divisions, and colonial legacies. Ideological extremism, often fueled by religious or political motivations, further exacerbates tensions and provides fertile ground for hybrid strategies. Additionally, these regions host powerful non-state actors who are capable of influencing both domestic and regional security dynamics. Matloob, N., Matloob, N., & Ishaq, S. (2023). The combination of historical grievances, geopolitical rivalries, and fragmented governance structures has created an environment in which hybrid warfare can thrive, challenging the effectiveness of traditional security and defense measures.

### Role of Non-State Actors

Non-state actors—including terrorist organizations, insurgent groups, militias, and transnational networks—have become central to the execution of hybrid warfare. Unlike conventional state militaries, these actors operate with significant flexibility and adaptability, often exploiting asymmetries in power to achieve strategic objectives. Pandey, M. (2025). In both the Middle East and South Asia, non-state actors capitalize on political vacuums and weak institutional frameworks to extend their influence. They utilize advanced globalized technologies, such as encrypted communications, cyber tools, and social media, to coordinate operations, disseminate propaganda, and mobilize support. By doing so, they are able to disrupt governance, weaken state authority, and challenge the sovereignty of established nations. Yeşiltaş, M., & Kardaş, T. (Eds.). (2017).

### Mechanisms and Tactics of Hybrid Warfare

Hybrid warfare relies on a diverse array of mechanisms to achieve its objectives. Cyber-attacks target critical national infrastructure, including banking systems, energy grids, and communication networks, creating vulnerabilities that states may struggle to mitigate. Disinformation campaigns manipulate public opinion and international narratives, undermining trust in government institutions and shaping policy debates. Felbab-Brown, V. (2024, January 16). Proxy warfare allows states or external actors to project influence indirectly, often by supporting non-state actors with funding, weapons, or strategic guidance. Economic coercion, including sanctions, trade restrictions, or manipulation of critical resources, exerts pressure on adversaries without direct military engagement. Terrorism, in its various forms, not only creates immediate physical threats

but also instills fear, weakens public morale, and diverts state resources from essential governance functions. Abbasi, A. (2020).

### **Interplay Between State and Non-State Actors**

The evolving interplay between state and non-state actors in hybrid warfare creates complex security dynamics. States may leverage non-state actors as instruments of influence, while simultaneously confronting hybrid threats posed by other non-state entities. Azad, T.M., & Haider, M.W. (2021). This dual role complicates conventional defense strategies and challenges traditional frameworks of international law and state sovereignty. In regions like the Middle East and South Asia, state-sponsored militias, proxy groups, and insurgent networks interact dynamically with formal military forces, shaping the operational environment in unpredictable ways. Monaghan, S. (2017). The result is a multifaceted conflict landscape in which conventional and unconventional tactics are closely intertwined, and the distinction between aggressor and defender becomes increasingly ambiguous.

### **Strategic Implications and Security Challenges**

The presence of hybrid threats raises critical questions regarding regional stability, national security, and effective strategic responses. Rauta, V. (2020). Traditional military strategies alone are insufficient to address the multi-dimensional challenges posed by hybrid warfare. States must develop integrated approaches that combine military, cyber, intelligence, economic, and socio-political tools to counter these threats. Jokinen, J., & Normark, M. (2022). The involvement of non-state actors further complicates the security calculus, requiring policies that address root causes such as political marginalization, weak governance, and ideological radicalization. Moreover, the globalized nature of technology and communication networks enables hybrid actors to operate across borders, making international cooperation and intelligence-sharing essential for effective countermeasures.

### **Hybrid Threats**

Hybrid warfare represents a transformative approach to contemporary conflict, particularly in the Middle East and South Asia. By combining conventional and unconventional tactics, it challenges traditional notions of state-centric warfare and introduces a new complexity into global security dynamics. Rauta, V. (2020). Non-state actors play a pivotal role in this paradigm, exploiting vulnerabilities and leveraging technology to influence outcomes. The strategic responses required to counter hybrid warfare must therefore be equally multidimensional, integrating military, economic, cyber, and socio-political measures. Understanding the interplay between state and non-state actors, as well as the regional drivers of conflict, is critical for policymakers and scholars seeking to develop effective strategies for stability, security, and resilience in these volatile regions.

### **Literature Review**

#### **Emergence and Scholarly Attention of Hybrid Warfare**

The concept of hybrid warfare has gained significant scholarly attention in the post-2000 era, particularly following the conflicts in Iraq, Afghanistan, and Syria. Darwich, M. (2021). These conflicts demonstrated that traditional military force alone is often insufficient to achieve strategic objectives in complex environments. Scholars emphasize that hybrid warfare is not confined to conventional military engagement but integrates political, economic, cyber, and informational dimensions, creating a multi-faceted approach to conflict. Qureshi, H.I. (2024). This strategy enables actors to achieve goals without triggering full-scale conventional war escalation, allowing states and non-state entities to exploit vulnerabilities while minimizing direct confrontation. Abbasi, A. (2020). The

effectiveness of hybrid warfare is particularly evident in regions with fragmented political landscapes, weak governance structures, and persistent socio-economic instability, where conventional deterrence mechanisms often fail.

### **Political and Economic Dimensions**

Hybrid warfare strategically leverages political and economic tools alongside military operations. Political influence operations aim to manipulate governance processes, exploit societal divisions, and weaken institutional legitimacy. Malik, G. M. (2020). Economic coercion, through sanctions, resource manipulation, or targeted disruption of trade networks, exerts pressure on adversaries without direct armed conflict. These tactics are especially potent in fragile states where institutions are unable to absorb economic shocks or maintain political cohesion. Modern Diplomacy. (2021, January 8). By combining these dimensions with traditional and unconventional military measures, hybrid warfare allows actors to achieve strategic objectives incrementally, shaping the conflict environment over time and limiting opportunities for conventional state retaliation.

### **Cyber and Informational Warfare**

Cyber operations and information warfare constitute critical components of hybrid strategies. Cyber-attacks target infrastructure, communication networks, and financial systems, creating both physical disruption and psychological impact. Fogt, D. (2021). Simultaneously, disinformation campaigns, propaganda, and media manipulation influence public perception, shape international narratives, and undermine confidence in state authorities. The integration of cyber and informational tools allows hybrid actors to operate globally, reach wider audiences, and destabilize opponents without the costs associated with kinetic military engagement. Jokinen, J., & Normark, M. (2022). These capabilities are particularly relevant in the Middle East and South Asia, where connectivity, social media penetration, and political polarization amplify the impact of informational operations.

### **Role of Non-State Actors in Hybrid Conflicts**

Non-state actors have historically shaped conflicts in both the Middle East and South Asia, often serving as the primary agents of hybrid warfare. Qureshi, H. I. (2024). In the Middle East, organizations such as Hezbollah, Hamas, and the Islamic State have employed hybrid tactics to achieve strategic influence. Their operations combine guerrilla warfare, cyber operations, media campaigns, and proxy networks, allowing these actors to exert control over both state institutions and rival non-state groups. Rauta, V. (2025). In South Asia, insurgent groups such as the Taliban, Lashkar-e-Taiba, and other factions have similarly adapted hybrid strategies to pursue political, territorial, and ideological goals. These groups leverage asymmetric advantages, including mobility, local knowledge, and decentralized command structures, to challenge conventional state militaries effectively.

### **External Powers and Proxy Involvement**

Recent scholarship highlights the critical role of external powers in shaping hybrid threats. Proxy wars, foreign funding, arms transfers, and cyber interventions by regional and global actors have exacerbated conflicts in both the Middle East and South Asia. Abbasi, A. (2025). External states often sponsor non-state actors to project influence indirectly, avoid direct confrontation, or achieve geopolitical objectives at low cost. These interventions introduce additional layers of complexity, as hybrid conflicts become arenas where state-sponsored and independent non-state operations intersect. The convergence of these dynamics creates security challenges that traditional military strategies and diplomatic instruments struggle to address, requiring innovative, multi-domain responses from affected states.



## Complex Security Challenges

The convergence of hybrid tactics, non-state actors, and external involvement generates a security environment characterized by unpredictability and volatility. Traditional conflict management frameworks are often inadequate in addressing the multi-dimensional nature of hybrid threats. Rind, S.A. (2021, June 30). Military force alone cannot neutralize decentralized networks that operate across borders, while diplomatic efforts may be undermined by covert operations and external interventions. The interplay between state and non-state actors necessitates adaptive strategies that integrate intelligence, counter-propaganda, cyber-defense, and socio-political resilience measures. Scholars argue that understanding the dynamics of hybrid warfare requires a holistic approach that considers political, economic, technological, and ideological factors simultaneously. Naz, F., & Shamsi, Z.u.-H. (2022). Hybrid warfare represents a transformative paradigm in contemporary conflict, particularly in regions such as the Middle East and South Asia. Its multi-dimensional approach—combining conventional military force with cyber, informational, political, and economic tools—has allowed both state and non-state actors to achieve strategic objectives with reduced risk of direct confrontation. Non-state actors, empowered by technology, ideological networks, and external sponsorship, play a pivotal role in shaping the conflict landscape. Fogt, D. (2021). The involvement of external powers further complicates security challenges, creating a dynamic environment where conventional military and diplomatic instruments are often insufficient. Understanding hybrid warfare in these regions requires an integrated, multi-domain perspective that acknowledges the interplay between state, non-state, and external actors and emphasizes adaptive, comprehensive strategies for conflict mitigation and strategic response.

## Data Analysis

### Hybrid Warfare in the Middle East

The Middle East has become a testing ground for hybrid warfare, given the region's long-standing political instability, sectarian divides, and strategic importance. Hybrid strategies employed in the region often include a combination of the following:

- **Proxy Engagements:** Regional powers such as Iran and Saudi Arabia engage in proxy conflicts through non-state actors to expand influence while minimizing direct confrontation. For example, Iran's support for Hezbollah and Shia militias in Iraq exemplifies a sophisticated hybrid approach combining military, economic, and political leverage.
- **Cyber and Information Operations:** Non-state actors in the Middle East have increasingly exploited cyber capabilities and media channels to propagate propaganda, recruit members, and manipulate public opinion. Social media campaigns by the Islamic State have demonstrated the efficacy of information warfare in mobilizing global support.
- **Economic and Political Coercion:** Hybrid warfare in the Middle East often integrates sanctions, blockades, and economic manipulation to weaken adversaries indirectly. Non-state actors benefit from these dynamics by capitalizing on the resulting governance vacuums.

The Middle East's hybrid conflicts are further complicated by overlapping identities, sectarian divides, and intervention by extra-regional powers, which collectively create a multi-layered battlefield where non-state actors are empowered.

### Hybrid Warfare in South Asia

- South Asia exhibits similar patterns of hybrid warfare, but with region-specific dynamics shaped by historical conflicts, territorial disputes, and socio-political

fragmentation. Non-state actors have leveraged hybrid tactics to pursue political, ideological, and territorial objectives, often under the shadow of state complicity or tacit support.

➤ **Insurgency and Guerrilla Operations:** Groups like the Taliban in Afghanistan employ hybrid strategies by combining conventional insurgency with asymmetric attacks, governance challenges, and negotiation tactics to achieve strategic influence.

➤ **Cyber and Technological Exploitation:** While less technologically advanced than Middle Eastern counterparts, South Asian non-state actors have increasingly employed cyber tools for propaganda, recruitment, and financial networks.

➤ **Cross-Border Networks and State Sponsorship:** Hybrid warfare in South Asia often involves cross-border movements and support networks. Non-state actors benefit from porous borders, local sympathizers, and regional power rivalries, thereby challenging traditional state control mechanisms.

Hybrid warfare in South Asia is complicated by longstanding territorial disputes, insurgency dynamics, and the interplay of domestic and international politics, making conventional military solutions insufficient.

## Strategic Responses

States in both regions have attempted a range of strategic responses to counter hybrid warfare and non-state actor threats:

➤ **Integrated Security Frameworks:** Modern security strategies increasingly combine military, intelligence, cyber, and diplomatic tools. For example, Pakistan and India have developed counter-insurgency and counter-terrorism mechanisms that integrate local policing, military operations, and intelligence sharing.

➤ **Regional Cooperation and Alliances:** States seek collaborative approaches, such as intelligence-sharing mechanisms and joint counter-terrorism operations. Middle Eastern states have leveraged coalitions to counter extremist non-state actors, although regional rivalries often limit effectiveness.

➤ **Counter-Information and Cyber Operations:** Combating propaganda, misinformation, and cyber threats has become central to strategic responses. Nations invest in digital surveillance, media monitoring, and cyber-security infrastructure to mitigate hybrid threats.

➤ **Political and Socio-Economic Measures:** Recognizing that hybrid warfare exploits governance vacuums, states adopt measures to improve political inclusivity, economic development, and social resilience to reduce non-state actor influence.

Despite these responses, challenges remain due to the adaptability of hybrid tactics, the resilience of non-state actors, and the involvement of external powers that often complicate conflict resolution.

## Discussion

The emergence of hybrid warfare and empowered non-state actors has fundamentally reshaped the security calculus in the Middle East and South Asia, creating a paradigm in which traditional state-centric models of warfare and diplomacy are no longer sufficient. Unlike conventional conflicts, hybrid threats integrate multiple domains—military, cyber, economic, informational, and ideological—creating complex challenges that transcend borders and conventional strategies. Non-state actors, including terrorist organizations, insurgent groups, militias, and transnational networks, operate with agility, exploiting weaknesses in state institutions and leveraging globalized technologies to pursue strategic objectives. The interplay between these non-state actors and state sponsors further

complicates the operational environment, blurring the lines between aggression, defense, and governance. Proxy involvement, external funding, and cross-border coordination amplify these dynamics, making conflicts highly unpredictable and multidimensional. For regional and global actors, addressing these hybrid threats requires an adaptive, multi-layered approach that combines hard power measures, such as military deterrence and intelligence operations, with soft power tools, including diplomacy, development assistance, and strategic communication. The integration of technology and cyber capabilities is crucial, as non-state actors increasingly exploit digital networks for propaganda, recruitment, and operational coordination. Socio-economic resilience is equally important, as hybrid warfare often targets marginalized communities and fragile states to gain influence. International cooperation, intelligence sharing, and multilateral engagement are essential to counter cross-border threats effectively and to manage the spillover effects of hybrid conflicts. Policymakers must also recognize that hybrid warfare is not solely a military challenge but a deeply political and social one, requiring comprehensive solutions that address the root causes of instability, including governance deficits, economic deprivation, and ideological radicalization. Failure to engage these structural vulnerabilities allows non-state actors to exploit systemic weaknesses, prolonging conflicts and undermining regional stability. Adaptive strategies must therefore focus on both short-term mitigation and long-term structural resilience, balancing military operations with socio-political initiatives that reduce the appeal and operational space of hybrid actors. Ultimately, understanding hybrid warfare in these regions demands a holistic approach that acknowledges the fluid interactions between state and non-state actors, the multi-dimensional nature of modern conflict, and the necessity of combining technological, economic, social, and diplomatic tools to secure lasting peace and stability. The reshaped security landscape underscores the importance of dynamic policy frameworks that can respond flexibly to evolving threats while strengthening institutional capacity, promoting regional cooperation, and addressing the socio-political drivers of hybrid conflict.

## Conclusion

Hybrid warfare and the increasing influence of non-state actors in the Middle East and South Asia represent a transformative challenge to both regional and global security, fundamentally reshaping the way conflicts are understood and managed. Unlike traditional warfare, hybrid conflict blends conventional military operations with unconventional tactics, including cyber-attacks, disinformation campaigns, economic coercion, and proxy engagements, creating multi-domain threats that are difficult to predict or contain. Both state and non-state actors exploit these strategies, blurring the traditional lines of conflict, governance, and authority, and challenging the assumptions of state-centric security frameworks. Non-state actors, such as insurgent groups, terrorist organizations, and transnational networks, are increasingly empowered by technology, social media, and globalized resources, enabling them to operate across borders and exert influence in ways that were previously unimaginable. Addressing these threats requires comprehensive strategic responses that integrate military capabilities, cyber defense, economic policy, and socio-political measures, ensuring that states can respond to both immediate threats and long-term structural vulnerabilities. Regional cooperation and international engagement are essential to manage the transnational nature of hybrid threats, as non-state actors often exploit gaps in coordination, jurisdiction, and intelligence sharing to advance their objectives. Understanding hybrid warfare in these regions is

therefore critical for scholars and policymakers alike, as it provides key insights into the evolving nature of modern conflict, the adaptability and resilience of non-state actors, and the limitations of conventional security approaches. Effective responses depend on the ability of states to anticipate and preempt hybrid tactics, strengthen multi-domain defenses, and build socio-political resilience that reduces the operational space and influence of non-state actors. Cyber capabilities, strategic communication, economic incentives, and targeted governance reforms must be integrated into a holistic security framework to counter the complex and dynamic threats posed by hybrid actors. Furthermore, policy strategies must account for the interplay between local grievances, ideological motivations, and external sponsorship that enable non-state actors to thrive. By adopting adaptive, multi-layered approaches, states can mitigate the risks associated with hybrid conflict, strengthen regional stability, and enhance global security. Ultimately, hybrid warfare underscores the need to rethink traditional assumptions of sovereignty, military power, and conflict resolution, emphasizing the importance of comprehensive strategies that address the political, social, technological, and economic dimensions of contemporary security challenges. The evolving landscape in the Middle East and South Asia demonstrates that hybrid threats are not temporary anomalies but persistent features of modern conflict, requiring sustained, coordinated, and innovative responses from both regional and international actors. Recognizing the transformative impact of non-state actors and hybrid tactics is essential for crafting policies that ensure resilience, protect governance structures, and prevent the escalation of multifaceted conflicts.

## References

- Abbasi, A. (2020). Hybrid war threats and essence of perception management. *IPRI Journal*, XX(II).
- Abbasi, A. (2020). *Hybrid warfare – The historical preview*. *IPRI Journal*, XX(2), 1- 24.
- Abbasi, A. (2025). Hybrid war threats and essence of perception management: Challenges for Pakistan. *IPRI Journal*, XX(II). Islamabad, Pakistan: Institute of Policy Studies.
- Azad, T. M., & Haider, M. W. (2021). *Cyber warfare as an instrument of hybrid warfare: A case study of Pakistan*. *South Asian Studies*, 36(2), 383-398.
- Azad, T. M., & Haider, M. W. (2021). *Cyber warfare as an instrument of hybrid warfare: A case study of Pakistan*. *South Asian Studies*, 36(2), 383-398
- Darwich, M. (2021). Foreign policy analysis and armed non-state actors in world politics: Lessons from the Middle East. *Foreign Policy Analysis*, 17(4), .
- Felbab- Brown, V. (2024, January 16). Non-state armed actors in 2024: The Middle East and Africa. *Brookings Institution*.
- Fogt, D. (2021). Legal challenges or “gaps” in countering hybrid warfare – Building legal resilience. *Southwestern Law Review*, 49(2-3).
- Fogt, D. (2021). Legal challenges or “gaps” in countering hybrid warfare – Building legal resilience. *Southwestern Law Review*, 49(2-3).
- Jalil Shah, H., & Ehsan, M. (2023). Hybrid warfare: Emerging challenges for Pakistan. *Journal of Contemporary Studies*, 11(2), 69-85.
- Jokinen, J., & Normark, M. (2022). *Hybrid threats from non-state actors: A taxonomy* (Hybrid CoE Research Report 6). Helsinki, Finland: European Centre of Excellence for Countering Hybrid Threats.
- Jokinen, J., & Normark, M. (2022). *Hybrid threats from non-state actors: A taxonomy* (Hybrid CoE Research Report 6). European Centre of Excellence for Countering Hybrid Threats.



- Kurochkin, A., Lodina, A., & Pankov, G. (2022). Hybrid warfare in the Middle East. *Sovremennaya Politika: Global'naya Studiya i Problemy Upravleniya*, (1-2), Article 10.
- Malik, G. M. (2020). Weaponization of all elements of national power by India: Hybrid warfare against Pakistan. *The Dialogue*, 15(2).
- Matloob, N., Matloob, N., & Ishaq, S. (2023). Hybrid warfare: Strategies and counterstrategies in the India-Pakistan rivalry. *Journal of Peace and Diplomacy*, 4(1), 78-99.
- Modern Diplomacy. (2021, January 8). Hybrid threats & warfare in South Asia. *Modern Diplomacy*.
- Monaghan, S. (2017). *Countering Hybrid Warfare: So what for the future joint force?* PRISM: A Journal of the United States Navy.
- Naz, F., & Shamsi, Z. u.-H. (2022). Hybrid warfare and its nuances: A case study from South Asia. *IPRI Journal*, XXII(1).
- Pandey, M. (2025). The role of non-state actors in modern warfare: Case studies from the Middle East. *European Economic Letters (EEL)*, 15(1), 3640-3645.
- Qureshi, H. I. (2024). Hybrid warfare in the 21st century: Implications for Pakistan. *Journal of Defence & Strategic Studies*.
- Qureshi, H. I. (2024). Hybrid warfare in the 21st century: Implications for Pakistan. *Journal of Defence & Strategic Studies*, (Winter).
- Rauta, V. (2020). *Towards a typology of non-state actors in 'hybrid warfare': Proxy, auxiliary, surrogate and affiliated forces*. *Cambridge Review of International Affairs*, 33(6), 868-887.
- Rauta, V. (2020). *Towards a typology of non-state actors in 'hybrid warfare': Proxy, auxiliary, surrogate and affiliated forces*. *Cambridge Review of International Affairs*, 33(6), 868-887.
- Rauta, V. (2025). *Towards a typology of non-state actors in 'hybrid warfare': Proxy, auxiliary, surrogate and affiliated forces*. *Cambridge Review of International Affairs*, 33(6), 868-887.
- Rind, S. A. (2021, June 30). Hybrid warfare challenges. *SouthAsia Magazine*.
- Yeşiltaş, M., & Kardaş, T. (Eds.). (2017). *Non-state armed actors in the Middle East: Geopolitics, ideology, and strategy*. Palgrave Macmillan.