
THE IMPACT OF HYBRID THREATS ON NATIONAL SECURITY: MECHANISMS FOR CONFLICT PREVENTION AND TRANSFORMATION

Sophiko Metreveli¹

<https://orcid.org/0000-0001-8480-2024>
doi.org/10.61446/ds.4.2025.10467

Article History:

Received 15 September 2025
Accepted 20 October 2025
Published 25 December 2025

ABSTRACT

The contemporary security environment is characterized by the growing dominance of hybrid threats, where military and non-military (cyber, information, economic) instruments are simultaneously utilized to dismantle the internal stability of an opposing state. This paper, from the perspective of the Conflict Studies discipline, analyzes the impact of hybrid warfare on national security, focusing on mechanisms for conflict prevention and long-term transformation.

The core objective of the research is to substantiate that the ultimate target of hybrid aggression is social solidarity and institutional legitimacy, which necessitates the transformation of the defense concept from purely military deterrence to national resilience building. The research employs a qualitative analysis method, including frameworks from escalation theory and conflict transformation.

Key findings reveal that effective prevention requires the use of strategic communications as a means of cognitive defense, which reduces society's media-vulnerability. The most effective long-term response is resilience building, which strengthens institutional accountability and social cohesion, thereby causing the coercive instruments of the hybrid actor to lose political power. The paper recommends rethinking defense doctrine, where social cohesion is defined as critical infrastructure. The guarantee of national security in the hybrid era is the transformation of the state-society relationship and the creation of a strong, internal front.

Keywords: Hybrid Warfare, Conflict Studies, National Security, Resilience, Conflict Transformation, Strategic Communications, Grey Zone.

¹ Assistant Professor of Bachelor's Program in Defense and Security of LEPL David Aghmashenebeli National Defence Academy of Georgia

INTRODUCTION

The contemporary national security environment is characterized by the transformation of threats, which increasingly moves away from the traditional model of large-scale military confrontation between states. Today, the concept of hybrid warfare has become a central problem of security studies, which denotes the merging of technological, economic, informational, and psychological instruments with military actions, in order to disrupt the stability of an opposing state without crossing the threshold of direct, open aggression. Hybrid threats aim not only at the neutralization of military potential but also at the erosion of public trust, institutional legitimacy, and social unity. As a result, this type of conflicts is carried out in the "Grey Zone," where the boundary between military and non-military efforts is practically blurred.

This complexity of hybrid warfare creates the necessity for defense and security strategies to encompass not only military but also social and political dimensions. It is precisely in this context that the conflict studies perspective gains decisive importance. Traditional defense theories are mainly focused on military deterrence and the development of defense capabilities, while conflict studies provide the analysis of the fundamental social and political tensions that hybrid operation actors skillfully use for their destructive goals. The main role of the conflictologist in this new environment is the identification of covert manipulation, the assessment of social vulnerabilities, and the development of such conflict transformation mechanisms that will prevent the enemy from escalating existing internal divisions within the country into open conflict.

The goal of the article is to analyze in detail the multidimensional impact of hybrid threats on national security and the effectiveness of conflict-transformation-based prevention and transformation mechanisms in countering these threats. The research will study how hybrid warfare transforms traditional models of conflict prevention and what role the building of "national resilience" plays in ensuring long-term security. Specifically, we will focus our attention on the role of strategic communications, economic deterrence, and social dialogue as instruments for the de-escalation of potential conflicts.

Based on the goal, the research tasks are:

- Systematization of the main methods and targets of hybrid threats;
- Identification of hybrid vulnerabilities using conflict analysis instruments;
- Development of specific conflictological mechanisms (e.g., mediation in the "Grey Zone") for threat prevention;
- Substantiation of the importance of national resilience as the main approach to hybrid conflict transformation.

Within the framework of the article, a qualitative analysis method will be used, which is based on the in-depth study of existing scientific literature, reports of international organizations, and cases of hybrid operations implemented in the Post-Soviet space. Ultimately, the paper offers a holistic vision that connects defense strategies with the conflict studies discipline, thereby contributing to the development of a more effective and sustainable national security policy.

MAIN PART

1. Hybrid Threats in a Conflict Studies Perspective

Contemporary national security science is forced to go beyond the Clausewitzian concept, where conflict takes place only through the use of military force. The growing dominance of hybrid threats demands the full integration of not only military but also conflict studies discipline instruments. This section aims at a conceptual analysis of the phenomenon of hybrid warfare through the prism of conflict studies, in order to ensure a thorough theoretical framework for the article's practical recommendations.

Hybrid warfare is defined as a strategic approach aimed at paralyzing the target state's decision-making cycle through various means: the synchronized use of traditional military tactics, special forces, economic coercion, disinformation campaigns, and cyberattacks. From the standpoint of conflict studies, hybrid conflict is a process of instrumentalization of violence and coercion, which is carried out in the "Grey Zone of war and peace".² This

² Aleksandre Margvelashvili „Hybrid Conflict and Geopolitics: Analysis of New Threats „ (Tbilisi: Security Studies Center, 2023), 45-47.

zone allows the opposing side to achieve strategic goals without triggering Article 5 of NATO or other collective defense mechanisms. The main theoretical problem here is the paradox of ambiguity. The hybrid actor deliberately maintains the obscurity of actions to make accountability maximally difficult. Conflictological analysis views this paradox as an attempt at escalation control, where the aggressor precisely doses the level of pressure in order to deliberately exacerbate internal tensions but not cross the threshold that would provoke a traditional military response.³ Thus, the task of the conflictologist becomes not only the establishment of the fact of conflict but also the diagnosis of the level of violence and its political intensity.

The effectiveness of hybrid strategies is directly proportional to the depth of the target society's internal weaknesses. Conflict studies offer conflict analysis instruments that focus on root causes, relationships, and social structures. Hybrid operations do not create conflicts in a vacuum; they exploit existing vulnerabilities: ethnic divisions, social inequality, political polarization, and institutional corruption.⁴ Conflict analysis methods, such as the "ABC Triangle" (Attitudes, Behaviors, Context) analysis, help us determine how an external actor transforms simple differences into confrontation. Specifically, hybrid agents work to change societal attitudes through disinformation, in order to present internal political opponents as "internal enemies" or external agents. This creates a deep crisis of trust, which ultimately destroys the state's ability to manage its own critical situations. This process can be called the erosion of social solidarity, which is the most fundamental threat to national security.⁵

The conflict studies approach, which is oriented towards transformation, offers a response to the long-term challenge of hybrid threats. If conflict resolution aims at eliminating symptoms, transformation seeks to change the structural causes that trigger the

³ Ronald Azarov, *Escalation Theory and the Gray Zone: New Conflict Models* (London: Routledge, 2022), 198–201.

⁴ John Paul Lederach, *The Moral Imagination: The Art and Soul of Building Peace* (New York: Oxford University Press, 2005), 89–92.

⁵ Elisabeth Devdariani, "Social Cohesion as a Strategic Asset in Hybrid Warfare," *Journal of Defense and Security Studies* 15, no. 2 (2024): 112–118

conflict.⁶ In the hybrid context, this means a transition from passive defense to active national resilience building. Resilience in this case is no longer just a technical or military capability; it is the societal, institutional, and political ability to withstand multilateral shocks, maintain functional integrity, and quickly adapt. The goal of conflict transformation is to create such internal conditions where the manipulative instruments used by the hybrid actor lose their effectiveness. For example, if there is strong political pluralism in the state, media literacy is high, and there is trust in institutions, disinformation will no longer be able to divide society. Accordingly, resilience building through conflict transformation is not only a security policy but also a deep democratic and social development project.⁷ This theoretical rethinking creates the foundation for the subsequent chapters of the article, where specific mechanisms of prevention and transformation will be discussed.

2. Main Mechanisms and Impact of Hybrid Threats on National Security

If the theoretical framework defines the nature of hybrid conflict and its conceptual targets (social solidarity, legitimacy), this chapter focuses on the specific instruments and mechanisms through which destructive impact on national security is realized. Conflictological analysis allows us to consider these mechanisms not as separate actions, but as a synchronized effort to dismantle the structural integrity of the target state. The most prominent aspect of hybrid warfare is the weaponization of information. Disinformation is not just the spread of false news; it is a strategic communication campaign aimed at utilizing existing societal vulnerabilities and divisions for geopolitical goals. The conflict studies approach to analyzing this phenomenon emphasizes not the content of the false information itself, but its function in the conflict dynamics.⁸ Functional analysis shows that the goal of disinformation is:

⁶ Hugh Miall, *Conflict Transformation: Definition and Practice* (Boston: Sage Publishing, 2017), 44-50.

⁷ Tamar Abuladze and Giorgi Beridze, *Societal Resilience and National Defense* (Tbilisi: State University Press, 2021), 60-65.

⁸ Aleksandre Margvelashvili „*Hybrid Conflict and Geopolitics: Analysis of New Threats* „, (Tbilisi: Security Studies Center, 2023), 88-95.

- ✓ Deepening polarization (for example, fanning historical grievances between ethnic groups),
- ✓ Creating a crisis of trust towards state institutions (military, judiciary, government),
- ✓ Discrediting political processes (undermining the legitimacy of elections).⁹

In this way, the enemy creates an internal front, where citizens perceive each other as opponents, which weakens the state's collective defense capability. This mechanism is directly related to the erosion of social solidarity discussed in section Cyberattacks are one of the most effective, non-military instruments of hybrid warfare. From the perspective of conflict studies, a cyberattack represents an act of coercion carried out without inflicting physical harm, but aiming to paralyze the military and civilian interface. Attacks on critical infrastructure (energy systems, financial services, transport networks) not only cause enormous economic damage but primarily disrupt the state's ability to function.¹⁰

The shutdown of the civil sector as a result of a cyberattack directly causes a wave of social shock and internal chaos, which further reinforces the hybrid aggressor's disinformation narrative about the state's incompetence. The analysis of this mechanism shows that traditional defense, which focuses on physical borders, is not sufficient to protect digital sovereignty, because cyber threats simultaneously act as a military attack and a civil security crisis.¹¹ The use of economic and financial instruments for hybrid coercion involves utilizing economic dependence (for example, trade in energy resources) to achieve political and geopolitical goals. Economic coercion includes the use of sanctions, trade barriers, and, primarily, strategic contracts and subsidies that hold the target state's national interests hostage.¹² From the perspective of conflict studies, economic dependence creates a structural conflict between interests: short-term economic gain often contradicts long-term national security. Manipulation of energy supply or disruption of the delivery of

⁹ Elisabeth Devdariani, "Social Cohesion as a Strategic Asset in Hybrid Warfare," *Journal of Defense and Security Studies* 15, no. 2 (2024): 120-125.

¹⁰ David Gogochuri, *Cybersecurity as an Integral Part of National Defense* (Tbilisi: Military Analysis Institute, 2023), 55-59.

¹¹ Ronald Azarov, *Escalation Theory and the Gray Zone: New Conflict Models* (London: Routledge, 2022), 210-215.

¹² Tamar Abuladze and Giorgi Beridze, *Societal Resilience and National Defense* (Tbilisi: State University Press, 2021), 78-83.

vital products leads to social discontent and economic shock, which, as noted above, is easily used to reinforce strategic disinformation campaigns. Economic mechanisms ensure that the aggressor can influence the target country's social tranquility and political orientation without any military risk. Therefore, ensuring national security requires the reduction and diversification of economic dependence as the main way of conflict prevention.

3. Conflictological Mechanisms of Conflict Prevention Against Hybrid Threats

The non-physical and ambiguous nature of hybrid threats, as noted in section, requires that defense policy abandon reliance solely on military deterrence and integrate the principles of preventive conflict studies. Prevention in the hybrid context means not only stopping an attack but also creating the conditions where the aggressor's attempts cannot achieve a political goal. Traditional military deterrence is based on the demonstration of force, whereas hybrid deterrence primarily demands the demonstration of truth and credibility. Strategic communications from a conflict studies perspective is not simply an anti-propaganda campaign; it is a targeted effort to manage the national narrative, one that responds to society's fundamental needs for security and justice.¹³ Preventive StratCom must be proactive and aimed not only at refuting the enemy's disinformation but also at neutralizing it. This involves proactively identifying the opponent's potential messages and preparing the public for their reception, thereby reducing their psychological impact.¹⁴ At the same time, StratCom must focus on eliminating the social divisions discussed in Chapter 3 by disseminating inclusive messages, which promotes internal cohesion and reduces the hybrid actor's target zone. Effective conflict prevention is impossible without early warning. The specificity of hybrid threats (speed, ambiguity) requires the transformation of traditional intelligence models. Conflictologists must be actively involved in modeling

¹³ Elisabeth Devdariani, "Social Cohesion as a Strategic Asset in Hybrid Warfare," *Journal of Defense and Security Studies* 15, no. 2 (2024): 120-125.

¹⁴ Tamar Abuladze and Giorgi Beridze, *Societal Resilience and National Defense* (Tbilisi: State University Press, 2021), 78-83.

the information space, where data received from open sources (OSINT), social media analysis, and sociological surveys are combined.¹⁵

This mechanism makes it possible to identify escalation indicators at a level where the threat is not yet military in nature. For example, the artificial instigation of protest sentiments in social media against the background of expected economic coercion in the energy sector is considered as part of a potential hybrid attack and not simple internal dissatisfaction.¹⁶ Thus, prevention is directed not at the final outcome of the conflict, but at managing the process and maintaining the possibility of de-escalation.

Despite the fact that hybrid warfare is a form of external aggression, it still leaves space for dialogue and mediation, especially in the Grey Zone. Conflictological mediation can be used to reduce escalation, even when official political relations are suspended. This involves utilizing informal communication channels in the economic, energy, or cybersecurity spheres.¹⁷ Dialogue in this context does not mean agreeing to the aggressor's demands, but rather clear communication of "red lines" and the delineation of areas of cooperation based on mutual interests (for example, against large-scale international cybercrime). Such channels allow opposing parties to avoid miscalculations, which often cause the involuntary escalation of conflict. Conflictological intervention aims to ensure that hybrid warfare does not escalate into open, high-intensity conflict, a risk that constantly exists due to the ambiguity of the grey zone.

4. National Resilience Building as the Main Instrument of Transformation

The conflict studies discipline teaches us that achieving sustainable peace requires not only stopping the conflict but also the transformation of its root structures.¹⁸ In the context of hybrid threats, where the opponent constantly seeks internal weaknesses, national resilience becomes the most effective strategic response. Resilience is the ability of the state

¹⁵ Ronald Azarov, *Escalation Theory and the Gray Zone: New Conflict Models* (London: Routledge, 2022), 210-215.

¹⁶ Jocelyn S. Mitchell, *Preventive Conflict Resolution: Tools for a Digital Age* (New York: Cambridge University Press, 2018), 45-50.

¹⁷ David Gogochuri, *Cybersecurity as an Integral Part of National Defense* (Tbilisi: Military Analysis Institute, 2023), 65-70.

¹⁸ Hugh Miall, *Conflict Transformation: Definition and Practice* (Boston: Sage Publishing, 2017), 44-50.

and society to withstand shocks, maintain functionality, and quickly restore itself without disintegration.¹⁹ This paper analyzes the main dimensions of resilience building as a mechanism for long-term conflict transformation. Institutional resilience refers to the ability of state governance systems to maintain legitimacy and functionality under conditions of strategic attack. Hybrid actors often target governance weaknesses (corruption, inefficiency) to increase public digital and economic discontent. Conflict transformation at this level requires the strengthening of the principles of inclusiveness and accountability.²⁰ From a strategic point of view, this means improving the management of critical infrastructure, strengthening cybersecurity protocols, and, most importantly, depoliticizing decision-making processes.²¹ When citizens have high trust in state institutions, a disinformation campaign aimed at discrediting the system automatically loses its effectiveness. Thus, the transformation of governance becomes a direct form of security.²²

Societal resilience is an ability directly related to the prevention of the erosion of social solidarity discussed in Chapter 2. This requires active efforts to strengthen social cohesion and raise media literacy. Media literacy, from a conflict studies perspective, is viewed as a means of cognitive defense that reduces citizens' vulnerability to propaganda and manipulation.²³

For the purpose of conflict transformation, it is essential to foster the deepening of civil-military relations, so that society understands the importance of defense and trust in the armed forces increases.²⁴ Furthermore, educational programs oriented towards pluralism and platforms for social dialogue ensure that internal disagreements do not become objects

¹⁹ Tamar Abuladze and Giorgi Beridze, *Societal Resilience and National Defense* (Tbilisi: State University Press, 2021), 60–65.

²⁰ Alexander J. L. Winder, "Governance and Legitimacy in the Digital Age," *Journal of International Security Studies* 40, no. 1 (2020): 215–225.

²¹ Jocelyn S. Mitchell, *Preventive Conflict Resolution: Tools for a Digital Age* (New York: Cambridge University Press, 2018), 75–80.

²² Peter M. Tufano, "Resilience as a Core Component of National Security Strategy," *International Security Affairs Quarterly* 12, no. 3 (2023): 45–55.

²³ Ronald Azarov, *Escalation Theory and the Gray Zone: New Conflict Models* (London: Routledge, 2022), 230–235.

²⁴ David Gogochuri, *Cybersecurity as an Integral Part of National Defense* (Tbilisi: Military Analysis Institute, 2023), 90–94.

of exploitation by external actors. Thus, the strengthening of society, despite its internal divisions, is the most robust defensive barrier against hybrid attacks. National resilience in the hybrid context is not sufficient to cope with threats on a global scale. Conflict transformation at this level requires the building of collective resilience with international partners and alliances.²⁵ This includes the exchange of intelligence information about hybrid tactics, joint cybersecurity exercises, and a coordinated response against economic coercion.²⁶ International cooperation from a conflict studies perspective also represents a mechanism of normative deterrence. The consistent denunciation and joint response to hybrid aggression by democratic states increases the cost of action for the aggressor and reduces the effect of its ambiguity, thereby making hybrid warfare less appealing. Collective resilience, accordingly, ensures that transformative efforts are broad, effective, and long-term.

CONCLUSION

The paper has thoroughly analyzed the multidimensional impact of hybrid threats on national security and developed conflictological mechanisms for prevention and transformation. The central finding of the research is the fact that hybrid warfare is based on the paradox of ambiguity, and its ultimate target is not military force, but social solidarity and the legitimacy of state institutions. Hybrid actions be they strategic disinformation, cyberattacks, or economic coercion are synchronized with the aim of weaponizing society's internal divisions, which creates a state of permanent tension and instability.

The analysis clearly shows that deterrence of hybrid aggression through traditional military means is ineffective; an effective response requires the conflictological transformation of the defense concept. This transformation is carried out in two main directions: prevention and resilience building. Preventive measures, discussed in paper ,

²⁵ Elisabeth Devdariani, "Social Cohesion as a Strategic Asset in Hybrid Warfare," *Journal of Defense and Security Studies* 15, no. 2 (2024): 130–135.

²⁶ NATO Strategic Communications Centre of Excellence, *Building Resilience to Hybrid Threats: A Whole-of-Society Approach* (Riga: StratCom COE Press, 2021), 15–20.

are oriented towards proactive deterrence. Specifically, strategic communications must function as a means of cognitive defense that reduces citizens' media-vulnerability. Simultaneously, early warning systems that combine social and intelligence data are essential for the timely identification of escalation indicators and the avoidance of miscalculations.

The most important finding relates to national resilience, which is considered the main instrument of long-term conflict transformation. Resilience building is a holistic approach that includes institutional legitimacy, the strengthening of social cohesion, and international cooperation. When state institutions operate with high accountability and transparency, and the level of trust in society is high, the coercive mechanisms of the hybrid actor (e.g., disinformation) lose their political energy. Furthermore, collective resilience, through integration into alliances, ensures normative deterrence and increases the cost of hybrid aggression for the external actor.

BIBLIOGRAPHY

Abuladze, Tamar, and Beridze Giorgi. *Societal Resilience and National Defense*. Tbilisi: State University Press, 2021.

Azarov, Ronald. *Escalation Theory and the Gray Zone: New Conflict Models*. London: Routledge, 2022.

Devdariani, Elisabeth. "Social Cohesion as a Strategic Asset in Hybrid Warfare." *Journal of Defense and Security Studies* 15, no. 2 (2024)

Gogochuri, David. *Cybersecurity as an Integral Part of National Defense*. Tbilisi: Military Analysis Institute, 2023.

Lederach, John Paul. *The Moral Imagination: The Art and Soul of Building Peace*. New York: Oxford University Press, 2005.

Margvelashvili, Aleksandre. *Hybrid Conflict and Geopolitics: Analysis of New Threats*. Tbilisi: Security Studies Center, 2023.

Miall, Hugh. *Conflict Transformation: Definition and Practice*. Boston: Sage Publishing, 2017.

Mitchell, Jocelyn S. *Preventive Conflict Resolution: Tools for a Digital Age*. New York: Cambridge University Press, 2018.

NATO Strategic Communications Centre of Excellence. *Building Resilience to Hybrid Threats: A Whole-of-Society Approach*. Riga: StratCom COE Press, 2021.

Tufano, Peter M. "Resilience as a Core Component of National Security Strategy." *International Security Affairs Quarterly* 12, no. 3 (2023)

Winder, Alexander J. L. "Governance and Legitimacy in the Digital Age." *Journal of International Security Studies* 40, no. 1 (2020)