FRI-2B.312-1-NS-02

HYBRID WARFARE AS A FORM OF CONTEMPORARY ARMED CONFLICTS

Kremena Rayanova
"Angel Kanchev" University of Ruse
Tel: +359 82 888 729
E-mail: krayanova@uni-ruse.bg

Abstract: *The phenomenon of hybrid warfare has emerged as a distinctive form of modern armed conflict, combining conventional military operations with a wide range of non-military instruments such as cyberattacks, disinformation campaigns, economic pressure, and political destabilization. Building on the theoretical foundations proposed by scholars such as Frank Hoffman, Thomas Hammes, and Valery Gerasimov, hybrid warfare is understood as an integrated strategy that blurs the boundaries between war and peace, as well as between military and civilian domains. The study highlights the multidimensional nature of hybrid warfare, emphasizing the decisive role of information operations, the disruptive potential of cyber activities, and the strategic impact of economic and political measures. Empirical examples such as the conflict in Ukraine after 2014 and the activities of non-state actors in the Middle East illustrate the hybrid model in practice. The analysis concludes that hybrid warfare represents not only an evolution of traditional conflict but also a systemic challenge to global security in the twenty-first century. Effective responses require interdisciplinary approaches that integrate military, diplomatic, technological, and societal instruments in order to enhance resilience and protect state sovereignty.*

INTRODUCTION

In the context of globalization and rapidly developing technologies, armed conflicts of the twenty-first century are undergoing significant transformations that alter both their nature and the strategic environment in which they unfold. The classical understanding of war, based on the direct use of armed forces and a clear distinction between the battlefield and civilian space, no longer fully reflects the specific characteristics of contemporary confrontations. In its place, new forms of conflict are emerging that combine military and non-military means, state and non-state actors, as well as overt and covert strategies.

One of the most significant and widely discussed concepts in this field is so-called hybrid warfare. According to Frank Hoffman (2007), it can be defined as a form of conflict in which conventional military means, irregular actions, terrorist practices, and criminal structures are combined in an integrated campaign. In this way, hybrid warfare transcends the boundaries of classical military theory and poses new challenges to state security and stability. The purpose of this study is to examine hybrid warfare as a form of contemporary armed conflict, focusing on its characteristics, instruments, and strategic consequences.

The essence of hybrid warfare lies precisely in the layering of influences, their coordinated use, and the pursuit of strategic objectives without formally transitioning to open, conventional war. For this reason, it proves to be highly effective in contemporary conditions: it erodes societies not through a single powerful blow, but through a series of small yet constant impacts aimed at the most vulnerable points of the state—public trust, economic resilience, the information environment, political stability, and social cohesion.

The theoretical foundations of hybrid warfare are developed by authors such as Thomas Hammes (2004), who views modern conflict as a phenomenon in which the boundaries between civilian and military objects, between state and non-state actors, and between the battlefield and the information sphere are completely blurred. Hammes defines this as "fourth-generation warfare," in which victory is achieved not by destroying the enemy's army, but by undermining its society.

A significant contribution is also made by Frank Hoffman (2007), according to whom hybrid warfare represents a "blending of different forms of warfare"—from conventional operations to terrorism, guerrilla actions, criminal networks, propaganda, and cyberattacks. According to Hoffman, the uniqueness of this type of warfare lies precisely in the combination of these elements rather than in the individual means themselves. Hybrid strategy employs all these instruments simultaneously, in a way that confuses the adversary and renders its response ineffective.

The Russian school has also developed a specific approach to contemporary conflicts. Valery Gerasimov (2013) emphasizes that in modern wars, non-military instruments—such as information operations, cognitive influence, diplomatic and economic means—can be more decisive than traditional military actions. He notes that the share of non-military means may reach up to 80 percent, clearly indicating a reconceptualization of warfare as a multidimensional phenomenon. Although the so-called "Gerasimov Doctrine" is often misinterpreted, it undoubtedly reflects an important stage in understanding hybrid threats.

A key element of hybrid warfare is the information space. Never in history has information had such importance and such large-scale influence. In the modern world, media and social networks have become an arena in which battles for public consciousness are fought. Disinformation, fake news, targeted campaigns to discredit leaders, manipulated images and videos, so-called "deepfakes"—all of these create a parallel reality in which societies often lose the ability to distinguish truth from falsehood. Information attacks not only influence public opinion but can also undermine political stability by fostering distrust, fear, and polarization.

This has been observed particularly clearly in Europe and the United States after 2014, when numerous influence campaigns unfolded on social media. Cases such as interference in electoral processes, deliberate amplification of social divisions, and support for far-left or far-right groups all represent hybrid methods for weakening democratic systems.

Cyberspace is another decisive domain for hybrid operations. Cyberattacks may target critical infrastructure—power grids, banks, government systems, healthcare facilities, and transportation networks. One example is the cyberattack against Estonia in 2007, which paralyzed the state for several days. In Ukraine, in 2015 and 2016, cyberattacks led to power outages affecting hundreds of thousands of people. Each such attack creates chaos, panic, and mistrust, and when conducted as part of a sustained campaign, it can weaken a state to the point of systemic collapse.

The economic dimension of hybrid warfare includes manipulation of energy supplies, the imposition of targeted trade restrictions, the creation of dependencies, corruption, and financial influence. Through such methods, significant geopolitical pressure can be exerted. An example is the role of gas supplies in relations between Russia and several European states. In addition, economic instruments may include support for criminal networks, smuggling, money laundering, and other practices that undermine state control.

Of course, military force remains part of the hybrid strategy, but it is used in a manner distinct from traditional warfare. Instead of large armies and massive operations, hybrid warfare favors small, mobile groups, often disguised as volunteers or local paramilitary forces. These formations can create hotspots of instability that are later used as justification for political or military interventions. This was precisely the case with the annexation of Crimea in 2014—through a carefully coordinated combination of military actions, propaganda, political influence, and diplomatic maneuvers that presented the international community with a fait accompli.

Another striking example is Hezbollah, which represents a model hybrid organization—simultaneously a political party, a social service provider, an armed group, and a regional actor. It manages schools, hospitals, and social programs while also possessing well-armed units capable of conducting high-intensity conflict. This makes it difficult to neutralize, as its activities are deeply embedded within society.

In Asia, China also employs hybrid methods, particularly in the South China Sea. Rather than relying on overt force, it uses a combination of economic pressure, paramilitary maritime formations, diplomatic coercion, legal arguments, and information campaigns through which it gradually expands its influence.

CONCLUSION

Hybrid warfare represents a qualitatively new form of contemporary armed conflict, combining classical military actions with unconventional methods such as cyberattacks, disinformation campaigns, and economic pressure. It has been extensively examined in the works of Frank Hoffman, Thomas Hammes, Valery Gerasimov, and many other authors, who emphasize its complexity and strategic significance.

The essence of hybrid warfare lies in the integrated impact on various spheres of society, in which the boundary between war and peace becomes increasingly blurred. This necessitates the development of new security concepts, the construction of resilient institutions, and the formulation of interdisciplinary counterstrategies.

Therefore, hybrid warfare is not merely an episodic trend, but a structural characteristic of the international environment in the twenty-first century. It will continue to shape the ways in which states and non-state actors interact, compete, and confront one another in a globalized world.

REFERENCES

Berti, B. (2016). *Hezbollah and Hybrid Warfare: Lessons from Lebanon*. Washington, DC: Carnegie Middle East Center.

Coffman, M. & Clowen, A. (2016). "Economic Instruments in Hybrid Conflicts." *Journal of Strategic Studies*, 39(4), pp. 455–472.

Gerasimov, V. (2013). "The Value of Science in Prediction." *Military-Industrial Courier*, 27 February.

Velchev, A. (2025). Media Battlefields: Hybrid Threats and Communication Strategies in Contemporary Warfare. Public Trust, Sofia, pp. 21–24.

