Eurasian Science Review ISSN 3006-1164
Volume 2, No 4

HYBRID WARFARE AND THE CHALLENGE TO INTERNATIONAL LAW

Tursyn Alisher[1], Turuntayeva Aigerim[2]

[1] Master student of the Faculty of International Relations, L.N. Gumilyov Eurasian National University, Kazakhstan.
E-mail: alisher.tursyn@gmail.com

[2]Candidate of Historical Sciences, Associate Professor, Faculty of International Relations, L.N. Gumilyov Eurasian National University, Kazakhstan
E-mail: a.turuntaeva@mail.ru

Keywords

Hybrid Warfare
International Law
Cybersecurity
Information Warfare
Strategic Deterrence
Legal Frameworks

Abstract

This article explores the complex landscape of hybrid warfare, a multifaceted conflict strategy blending conventional military tactics with cyberattacks, information warfare, and economic coercion. It examines the challenges hybrid warfare poses to international law, the difficulties in establishing legal definitions, and the strategic responses by major powers including Russia, the United States, and China. The discussion extends to the adaptation of national and international strategies to address the gray zones of conflict that hybrid warfare exploits. Emphasizing the need for innovative legal frameworks and international cooperation, the article highlights hybrid warfare's impact on global security dynamics and the evolving nature of warfare in the digital age.

Introduction.

In a globalized world, where traditional forms of military confrontation give way to new conflict methods, the phenomenon of hybrid warfare takes center stage in discussions on international security and legal order. Hybrid warfare, a complex blend of military and non-military means and actions, openly challenges existing international legal norms and regulatory mechanisms. The difficulty in classifying and regulating hybrid wars stems from their multidimensional nature, which includes not only military operations but also information warfare, cyberattacks, economic pressure, psychological impact, and even cultural influence. This multifaceted approach poses serious challenges to international law, necessitating innovative approaches and a deep understanding of interstate relations dynamics.

Despite the widespread use of the term "hybrid war" in political and academic discourses, its legal definition remains a subject of lively debates and scholarly research. This particularly concerns the legitimacy of using certain methods and means within such conflicts, as well as the possibility of regulating them through existing international agreements and conventions.

It is crucial to emphasize that the international legal regulation of hybrid wars encounters obstacles not only due to their complexity and multifaceted nature but also because of the rapidly changing nature of international relations in the digital and globalization era. Modern hybrid conflicts often include elements beyond the traditional understanding of military actions, such as cyber wars and informational confrontations, complicating the application of existing international treaties and conventions.

Moreover, hybrid wars are often characterized by asymmetry, where one side may use unconventional and non-obvious methods to achieve its goals, while the other side may adhere to more traditional and rule-bound warfare. This asymmetry creates additional difficulties for legal regulation and requires a reassessment of traditional approaches to international law.

2. Russian perspectives on hybrid warfare: multifaceted conflicts and the quest for legal and educational adaptation

In Russia, hybrid wars are considered not only as military conflicts but also as operations that involve a wide range of actions, such as information wars, cyberattacks, economic pressure, and propaganda campaigns. This means that such wars include both forceful and non-forceful elements, making them particularly difficult to analyze and control.

The complexity of hybrid wars in the Russian context also lies in their decentralized nature. This means that actions can be taken by various actors, not necessarily directly linked to state structures, which complicates the identification of threat sources and responsive measures. Moreover, this aspect makes traditional diplomatic and international legal control mechanisms less effective, as they are often oriented towards state structures and traditional forms of conflict.

One of the key characteristics of hybrid wars, according to Russian experts, is their ability to escalate quickly and the difficulty in ceasing them. This is because such wars often include diverse, often unrelated elements, making it difficult to identify them and develop effective control mechanisms and cessation. The issue of hybrid wars in the Russian context is also exacerbated by the lack of clear international legal mechanisms for regulating such conflicts, especially in situations where many actions occur in the "gray zones" of international law.

An additional complexity involves the control and influence over informal groups and networks, which often play a key role in hybrid wars. This goes beyond the traditional understanding of diplomacy and international relations, where states are the main actors. Thus, the Russian approach to hybrid wars emphasizes the need to develop new, more flexible and adaptive political and legal regulatory tools to effectively respond to such complex and dynamic threats.

In Russian higher education institutions, there is a trend towards increasing and systematizing educational programs dedicated to hybrid wars and information conflicts. In 2022, the Russian Ministry of Education approved the introduction of a course on hybrid wars, developed by the Russian Social State University, and its integration into the educational programs of most universities. This course covers "elements of theory and practice" of hybrid wars, emphasizing their reality in the 21st century as conflicts that occur not only on the battlefield but also in the economy, media, and people's consciousness.

Additionally, proposals for increasing the training of specialists in hybrid wars are being discussed in Russia, supported by high-ranking officials and presented as a response to information wars waged against the Russian Federation. This includes the creation of specialized faculties in military universities and educational

programs in civilian educational institutions. Lomonosov Moscow State University stands out as a venue for developing and implementing the program "Information and Hybrid Wars," becoming the first university in Russia where training of specialists to counteract information and hybrid warfare operations at a high level began.

3. US perspectives on hybrid warfare: strategic deterrence and national defense in the gray zone

In the United States, the concept of hybrid warfare is considered a reality requiring the readiness of military forces to counter and deter. Hybrid warfare, also known as "gray zone" conflict or low-intensity conflict, encompasses diverse activities such as information operations, troop movements, disinformation campaigns, cyberattacks, and the actual use of force. Examples of hybrid warfare include China's actions in the South China Sea and Russia's operations in Georgia and Ukraine. A key feature of hybrid warfare is its ability to achieve strategic goals without the use of significant force.

In 2022, the National Defense Strategy of the USA highlights integrated deterrence as a key component aimed at countering hybrid and "gray zone" military strategies. The definition of gray zone methods includes "coercive approaches that may not reach perceived thresholds of USmilitary actions and cover areas of responsibility across various parts of the US government." This strategy recognizes that strategic competitors are increasingly engaging in battles outside the physical battlefield, using unconventional and non-military means to undermine US security and that of their allies. A vital element of integrated deterrence is the US's ability to articulate its "red lines"—actions by adversaries that would trigger a US military response—in order to effectively shape behavior that supports US interests and those of its allies.

Lieutenant General Karen H. Gibson, the Deputy Director of National Intelligence for National Security Partnerships, provided profound insights on the concept and challenges of hybrid warfare at a Defense News conference in Arlington, Virginia. Her remarks highlighted the evolving nature of conflicts in the modern world and the necessity for US military readiness to counter and deter these threats. She defined hybrid warfare as an attempt to achieve strategic objectives without the use of significant force, including tactics such as information operations, troop movements, disinformation campaigns, cyberattacks, and sometimes the actual use of force, exemplified by Russia's actions in Ukraine. Lieutenant General Gibson cited China's actions in the South China Sea and Russian operations in Georgia and Ukraine as examples of hybrid warfare. She also noted the ongoing efforts of Russia and China to influence and undermine alliances in Europe and the Pacific region, respectively.

A significant change in modern warfare is the expanded capability to use information as a tool of war, facilitated by global IT systems. This includes disseminating information and targeting specific audiences with greater precision than ever before. Identifying and publicly explaining the actions of adversaries in the realm of hybrid warfare presents a complex challenge. It involves balancing the need to protect intelligence sources and methods with the need to ensure accuracy and timeliness. Hybrid warfare is attractive to adversaries because it carries a low level of risk, is low-cost, and allows for obfuscated accountability.

In a new preface to his work, Ofer Fridman emphasizes that in the context of often exaggerated claims by both Russia and the West about hybrid warfare, which began with Russia's annexation of Crimea in 2014, the events of 2022 led to a real military conflict. He points out the importance of words and their impact on reality. Fridman discusses the politicization of the concept of hybrid warfare, particularly in the context of attempts by Russia and the West, including NATO and the US, to understand each other's motives. Both sides accuse each other of employing hybrid warfare methods, including actions in the "gray zone." Interestingly, the concept of hybrid warfare did not originate in Russia but in the US, thanks to the work of military theorist Frank Hoffman, who in the 2000s described a "new tactical-operational environment" that included a combination of regular and irregular forces and methods.

Hoffman emphasized that hybrid warfare involves actual military actions, which Fridman also points out. However, when Russia adapted the concept of hybrid warfare, it took on a different meaning, describing primarily an information war aimed at intensifying internal disagreements within the opponent's society. These methods, as perceived in the West, are actively used by Russia to spread disinformation through social networks, influence elections, and support Russian narratives in the West. Meanwhile, in Russia, hybrid warfare is understood to mean actions by the US, primarily against Russia, more closely describing Hoffman's definition of hybrid warfare.

In developing the concept of hybrid warfare, several thinkers and theorists have

developed variations on ideas about how states undermine their enemies from within and undermine their will to fight. Some of these, such as post-war theorist Yevgeny Messner with his concept of "subversive war" and contemporary "Eurasian" ideologist Alexander Dugin with "net-centric warfare," have influenced how Russians think about information warfare. For many Russians, the dissolution of the Soviet Union without a single shot being fired was the direct result of an information war led by the US. Supposedly a complex, well-planned, and flawlessly implemented recipe for defeating the USSR, proposed by the Western world, is something that contemporary Russians are very eager to master and use against their adversaries. Fridman says that the West should strive to understand Russia better and not succumb to fear of Russian hybrid warfare, as the previous generation of the Cold War feared "reds under every bed.

4. China's hybrid warfare: strategic integration of tradition and technology

The Chinese understanding and implementation of hybrid warfare is a unique blend of traditional military strategies and modern technologies aimed at achieving strategic goals without the direct use of significant force. This approach is grounded in ancient military thinking, tailored to modern conditions where digital technologies and information space play a crucial role.

At the core of modern Chinese hybrid warfare strategy is the work of Chinese military theorists Qiao Liang and Wang Xiangsui. In their 1999 publication "Unrestricted Warfare," they explored the nature of contemporary warfare and defined the future battlefield as an "expanded domain." In this domain, the focus is not on lethal actions but on the ability to "paralyze and undermine the enemy" using tools such as cyber attacks, financial operations, and media as instruments of warfare.

Over time, China's strategy has evolved, adapting to new technological realities and the global political climate. Throughout the tenures of Hu Jintao and Xi Jinping, China has actively developed its military, cybernetic, and informational capabilities, aiming for the "intellectualization" of military actions and strengthening its position as a global superpower capable of competing with the USA for spheres of influence.

In the context of global hybrid warfare, China employs tools such as psychological warfare, propaganda, and legal manipulation to advance its territorial claims without needing to resort to open conflict. This demonstrates the deep integration of military strategy, information operations, and legal maneuvering, aimed at strengthening China's positions both regionally and globally.

The United Kingdom acknowledges the severity of hybrid threats and is actively developing strategies to counter them. The "Countering Hybrid Warfare" (CHW) initiative, spearheaded by the UK Ministry of Defence, aims to understand the nature and characteristics of modern hybrid threats. This multinational project emphasizes the need for collaboration and the development of conceptual guidelines for countering hybrid warfare, based on a series of informational notes covering key ideas and concepts related to hybrid warfare.

An important aspect of the UK's efforts in this area is the development and updating of policies to counter hybrid threats, as reflected in publications on the official government website. These documents provide a fundamental assessment and understanding of hybrid warfare, including containment strategies, methods to counter hybrid attacks, and the role of corruption as an element of hybrid warfare.

In the context of broader analysis on hybrid wars, the UK's approach demonstrates a comprehensive view of the issue, including understanding how hybrid threats can be countered and what political and military strategies can be effective in combating these threats. The UK is committed to international cooperation and knowledge exchange as part of its efforts to counter hybrid threats, emphasizing the importance of collective actions and joint strategy development.The approaches to hybrid warfare differ significantly between Russia, China, and the Western countries. Russia utilizes hybrid strategies, including informational wars, cyberattacks, and economic pressure, exemplified by the 2014 annexation of Crimea which combined military and non-military tactics to achieve political goals without large-scale armed conflict. China focuses on leveraging cyberspace and technological innovations for hybrid warfare, utilizing strategies like the "Three Warfares" — psychological, media, and legal warfare — to shape public opinion and justify actions strategically.

Western nations, including the USA and EU countries, adopt a comprehensive approach to hybrid threats, emphasizing cyber security, countering misinformation, and strengthening international legal order. The USA's National Security Strategy underscores the importance of fortifying cyberspace and information environments to guard against hybrid threats. The EU is actively developing initiatives to combat misinformation and promote media literacy.

The principal differences in these

approaches lie in the objectives, preferred tools, and methods of conflict. Russia and China use hybrid strategies to extend their influence and achieve national interests through a mix of military force and non-military means. In contrast, Western countries focus on protecting their societies and infrastructures from such threats, prioritizing international cooperation and legal framework strengthening.

Hybrid wars serve as a multifunctional tool for states aiming to advance their interests on the international stage, necessitating the development of coordinated strategies and mechanisms by the global community to effectively counter hybrid threats and maintain international peace and stability.

Conclusion

There is no unified definition of hybrid warfare within the United Nations due to the ambiguity and multifaceted nature of the phenomenon. Hybrid warfare combines traditional military actions and non-military methods such as cyberattacks, economic pressure, information campaigns, and psychological effects. This complexity makes it difficult to develop a universally acceptable definition that accommodates the diverse legal traditions and security interests of UN member states. Furthermore, the international community faces challenges in adapting existing international norms and agreements to new forms of conflict. The absence of a clear definition complicates the identification and attribution of responsibility for hybrid attacks, thereby hindering the implementation of targeted countermeasures at the international level. This creates gaps in the legal framework that can be exploited by states and non-state actors to carry out destabilizing actions under a veil of uncertainty. For example, the International Committee of the Red Cross has highlighted the need to adapt international humanitarian law to new challenges posed by the blurred lines between military and civilian spheres in hybrid conflicts.One of the key documents in this context is NATO's "Strategy on Hybrid Threats," developed in response to the increasing complexity and diversity of security challenges faced by member states. The strategy outlines that hybrid threats can encompass a wide range of military and non-military measures, including cyberattacks, propaganda, political pressure, and economic impact. These actions are often conducted in a manner that makes identifying and attributing the aggressor difficult, complicating decision-making processes within NATO and national governments. In response, NATO has devised a comprehensive approach that includes enhancing the alliance's intelligence capabilities to better identify hybrid threats, developing cyber defense measures, and strategies for information security. Additionally, NATO actively works on strengthening the resilience and defense capabilities of its members through intelligence sharing, joint exercises, and the development of recommendations for improving national security systems.

Reference

1. Atlantic Council. (n.d.). The National Defense Strategy shows the Pentagon's increased focus on the gray zone. Here's what that means. Retrieved from www.atlanticcouncil.org
2. Defense.gov. (2019). Military Must Be Ready to Confront Hybrid Threats, Intel Official Says. Retrieved from https://www.defense.gov/News/News-Stories/Article/Article/1952023/military-must-be-ready-to-confront-hybrid-threats-intel-official-says/
3. European Commission. (2018). Action Plan Against Disinformation.
4. Fridman, O. (2022). Russian "Hybrid Warfare": Resurgence and Politicization. Oxford University Press. Retrieved from https://www.cia.gov/static/8-Review-Russian-Hybrid-Warfare.pdf
5. Hoffman, F. G. (2009). Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies.
6. International Committee of the Red Cross (ICRC). (2015).
7. Kodaneva, K., et al. (n.d.). "Hybrid threats" to Russia's security: Identification and counteraction. Contours of Global Transformations: Politics, Economics, Law. Retrieved from www.ogt-journal.com
8. Kluver, J. (2016). Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present. Cambridge University Press.
9. Ministry of Defence. (2018). Countering hybrid warfare: Information notes. Retrieved from https://www.gov.uk/government/publications/countering-hybrid-warfare-information-notes
10. National Defense Strategy 2022. (n.d.). Retrieved from media.defense.gov
11. National Security Strategy of the

United States of America. (2017).
12. Rodachin, V. M. (2019). Hybrid wars and national security of Russia. Humanities Sciences. Vestnik of the Financial University, 9(4), 93-99. https://doi.org/10.26794/2226-7867-2019-9-4-93-99
13. Sazonova, K. L. (2017). "Hybrid war": International legal dimension. Law. Journal of the Higher School of Economics, (4), 177-187. Retrieved from www.law-journal.hse.ru
14. Scowcroft Center for Strategy and Security's Forward Defense. (n.d.). Gray Zone Task Force. Retrieved from www.atlanticcouncil.org
15. Snyder, T. (2015). The Road to Unfreedom: Russia, Europe, America. Tim Duggan Books.
16. The State Council Information Office of the People's Republic of China. (2015). China's Military Strategy.
17. Topychkanov, P. (n.d.). Hybrid war and the hybrid world. Russian Council on International Affairs. Retrieved from russiancouncil.ru
18. Acero, J., Bustos, E., & Quesada, D. (1982). Introducción a la filosofía del lenguaje. Cátedra.
19. Collins, J., Hall, N., & Paul, A. (Eds.). (2004). Causation and Counterfactuals. The MIT Press.
20. Horkheimer, M., & Adorno, T. W. (1972). Dialectic of Enlightenment. Herder and Herder.
21. Husserl, E. (1950). Cartesianische Meditationen und Pariser Vorträge. Nijhoff, Den Haag. https://ophen.org/pub-109001
22. Kar, E. (2019). Universality and Particularity of Aristotelian Substances. [Doctoral thesis]. The University of Bristol. https://research-information.bris.ac.uk/ws/portalfiles/portal/204326248/Final_Copy_2019_06_25_Kar_E_PhD.pdf
23. Kitsantonis, N. (2016, May 26). Greek Archaeologist Says He Has Found Aristotle's Tomb. The New York Times. https://www.nytimes.com/2016/05/27/world/europe/greece-aristotle-tomb.html
24. Kripke, S. (1980). Naming and Necessity. Harvard University Press.
25. Mullett, M. (2021, April 20). Performance Issues in the Christos Paschon. [Video]. GKA HUMAN 2021 - 10th International Conference on Humanities.https://events.gkacademics.com/dashboard/videos/105
26. Quine, W. O. (1951). Two Dogmas of Empiricism, The Philosophical Review, 60, 20–43.
27. Quine, W. O. (1960). Word and Object. MIT Press.
28. Ruhe, P. (2001, February 5). Pair of Recitals Show Musicians' Contrasting Styles. The Atlanta Journal and Constitution, p. 5 D.
29. Rutherford, D. (1994). Philosophy and language in Leibniz. In N. Jolley (Ed.), The Cambridge Companion to Leibniz (pp. 224-269). Cambridge University Press.https://doi.org/10.1017/CCOL0521365880.008
30. Searle, J. (1968) Austin on locutionary and illocutionary acts. The Philosophical Review, 77(4), 405–424. https://doi.org/10.2307/2183008.
31. Stone, S. (Director). (2021). The Dig. [Film]. BBC Films & Netflix.
32. Waldstein, P. (2016, October 6). Peter Kalkavage on Hegel's Anti-Aristotelian Account of Desire. Sancrucensis. https://sancrucensis.wordpress.com/2016/10/06/peter-kalkavage-on-hegels-anti-aristotelian-account-of-desire/