BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Aspects of Hybrid Warfare in the Dynamics of Its Manifestation Forms and Action Mechanisms

Mihaela HUŞANU*

*Romanian Parliament – Chamber of Deputies
e-mail: mihaela85husanu@gmail.com
https://orcid.org/0009-0006-1275-3618

Abstract

This article examines hybrid warfare as the dominant form of contemporary conflicts, in the context of profound transformations of the international security environment and the intensification of strategic competition among Great Powers. Starting from the evolution of war generations, from conventional to information confrontation, cyber and societal conflicts, the study highlights how hybrid warfare combines military and non-military instruments so as to produce strategic effects without triggering an open armed conflict. The main forms of manifestation of hybrid warfare at the diplomatic, political, economic, social, information, cultural, cyber, and non-military levels are analyzed, as well as the methods and tools used by hostile entities to render target states vulnerable. Methodologically, the article is based on specialized literature in the military, security studies, and international relations fields, the predominant approach being specific to qualitative study. The research conclusions reveal the need to emphasize the sociological dimension of the perception of hybrid threats among the civilian population. In the case of a hybrid war, strengthening the response capacity does not depend exclusively on military instruments, but on the level of knowledge, security education, and social cohesion, essential elements for the adaptation of states, especially in Eastern Europe, to the new paradigms of modern conflict.

Keywords:
Hybrid Warfare; Fifth Generation Warfare; Hybrid Threats; Impact; Russian Federation; Societal Resilience.

Article info
Received: 28 January 2026; Revised: 6 February 2026; Accepted: 13 March 2026; Available online: 8 April 2026

Citation: Huşanu, M. 2026. "Aspects of Hybrid Warfare in the Dynamics of Its Manifestation Forms and Action Mechanisms." *Bulletin of "Carol I" National Defence University* 15(1): 194-219. https://doi.org/10.53477/2284-9378-26-12

© „Carol I" National Defence University Publishing House
This article is an open access article distribted under the terms and conditions of the Creative Commons Attribution (CC BY-NC-SA)

Motto: "States can potentially lose a war before even knowing that it has already begun." (Cholpon Abdyraeva)

Introduction

The main characteristic of the current international security environment, where antagonistic forces spread and interact, representing state and non-state actors projecting their power, is unpredictability. Considering the accelerated development of new technologies, which influence the world across all aspects, in a direct and still difficult-to-quantify manner, we are witnessing an intensification of strategic competition, in which geopolitical players come to prominence, pursuing opportunities and avoiding risks. From this perspective, the tense relations in the global geopolitical ecosystem develop because of a permanent update of the context of action, of the methods and instruments through which security threats are launched and responded to.

Thus, the physiognomy of conflicts tends to slide, as indicated by the new realities of the security environment, towards a sharp hybridization of the forms of confrontation. The frequent use of the concept of "hybrid war", especially after the invasion of Ukraine by the Russian Federation (2022), marked the moment of its transition from the sphere of military literature and security studies to the spectrum of public, political, and media discourse. Although it contributed substantially to the popularization of the term, this transition generated, at the same time, the risk of diluting its meaning through broad, imprecise, and superficial approaches.

This study aims to outline a relevant and multidimensional analytical framework for understanding the concept of "hybrid warfare" as an instrument capable of determining changes in the balance of power in the contemporary security environment, through the complexity of its forms of manifestation and the variety of specific action mechanisms. This approach is intended to bring more clarity regarding the nature, scope, and intensity of the threats generated by hybrid warfare, especially for decision-makers at the administrative and political level, for whom the ambiguities circumscribed to the topic represent obstacles in the substantiation and development of coherent public policies, adapted to the global context of instability.

At the same time, this analysis proposes a type of structured qualitative research on how the intensification of strategic competition among great powers influences hybrid warfare manifestations and generates an increased need to strengthen societal resilience. Societal resilience can be strengthened by examining not only perceptions, discourses, and institutional and social practices regarding non-military threats (disinformation, economic pressures, cyber-attacks, instrumentalization of social vulnerabilities), but also the mechanisms through which democratic societies can prevent, absorb, and respond effectively to new forms of conflict without eroding

their social cohesion, fundamental values , and public trust. In order to formulate flexible strategic responses, it is necessary, however, to crystallize a definition of hybrid warfare, explore the multiple dimensions at which hybrid threats operate, and understand the subtle phenomenon designed to exploit national vulnerabilities, while remaining below the threshold of detection.

The research objectives aim to clarify the concept of "hybrid warfare", through the comparative analysis of the main approaches in the specialized literature related to the military field, security studies and international relations, identifying the main forms of manifestation and mechanisms of hybrid warfare aggregated in the global environment, examining how the Russian Federation's pattern of action influences the Euro-Atlantic security architecture, as well as assessing the need to integrate and strengthen the role of the "education - societal resilience" binomial in security strategies, given that asymmetric threats constantly test social cohesion.

In order to achieve these objectives, the study is guided by the following research questions: "How has hybrid warfare emerged as the dominant form of contemporary conflicts, in the context of the transformations of the international security environment and the evolution of war generations?" "What are the main characteristics of hybrid warfare, and in what types of associations do these characteristics allow for the achievement of strategic effects without triggering an open armed conflict?" "To what extent do societal resilience and the perception of hybrid threats among the civilian population influence the capacity of states, especially those in Eastern Europe, to respond effectively to hybrid threats?"

Relying largely on secondary data from the specialized literature, on the content analysis of strategic documents, and on findings from comparisons of different theoretical approaches to hybrid warfare, this research is subject to inherent limitations characteristic of predominantly qualitative approaches. The subjectivity involved in the selection of the scientific resources consulted and in the interpretation of the in-depth perspectives of the analyzed authors constitutes a significant threat to the validity of the research. On the other hand, some limitations derive both from the restriction of the analysis to the non-linear warfare strategy of the Russian Federation, with few references to the hybrid warfare models used by other state or non-state actors, and from the complexity and dynamism of the explored phenomenon, which continuously adapts to geopolitical and technological transformations.

The conclusions of this analysis capture a specific stage in the evolution of contemporary conflicts, requiring an update that integrates further conceptual developments or additional theoretical approaches. Despite the limitations, the study provides a useful analytical framework for understanding hybrid warfare and can constitute a starting point for future research, including quantitative research.

Hybrid warfare, the archetype of contemporary war

The shaping of military war strategies has evolved in parallel with the complex transformations of the world, each stage being closely linked to the way in which power, technology, and social organization have been understood and used.
War can be defined, as Bărbulescu (2001) mentioned, as "the most violent form of manifestation of social conflict between large groups of people (states, groups of states, peoples, nations), organized from a military point of view, that use armed struggle to achieve political goals, thereby giving the phenomenon a distinctly destructive character.

The first generations of warfare reflected a world of emerging nation-states and symmetrical conflicts: the first generation, centered on large human mass, aimed at wearing down the opponent through confrontation, while the second generation shifted the emphasis from the power of firearms and artillery to the domination of the battlefield, through industrial superiority and the ability to concentrate "steel on the target". With the acceleration of mobility and complexity of political and economic systems, the third generation of warfare introduced maneuver as a central principle, aiming at the avoidance of the opponent's strengths and generalized collapse. In a world increasingly marked by fragmentation, non-state actors, and prolonged conflicts, the fourth generation of warfare shifted the center of gravity from military force itself to political and social will, through asymmetric and insurgent warfare (Neculcea 2020, 315). Currently, fifth-generation warfare is "dominated by non-kinetic actions, to the detriment of kinetic ones, by high technologies, to the detriment of classical, conventional means" (Popescu 2021), and the objective is no longer the physical destruction of the opponent, but subversion and cognitive manipulation.

Taken together, the fourth and the fifth generations of warfare reveal that, in a deeply interconnected and computerized global environment, forms of conflict tend to take on a predominantly hybrid character, primarily determined by the desire of great powers to avoid direct military confrontation, which involves major risks and high costs (Hoffman, Neumeyer, and Jensen 2024). The result is the transformation of conventional wars into an accumulation of political, economic, information, cyber, and limited military pressures, designed to produce strategic effects without triggering an open conflict. This trend places the international system in a turbulent and dangerous state, characterized by strategic ambiguity, gradual escalation, and the difficulty of clear demarcation between peace and war, a reality that challenges both deterrence mechanisms and the management of long-term security risks.

Introduced in the field of military theory, specialized literature to characterize the complex nature of the conflict between Israel and Hezbollah (2006), the concept of "hybrid warfare" designates the combination of conventional and unconventional

means of confrontation. In this conflict, the Lebanese non-state actor Hezbollah managed to combine conventional and unconventional tactics, modern military means, and guerrilla actions to counter a technologically superior military force. The decentralized organization, the use of autonomous cells, and the exploitation of the urban environment allowed for significant losses and revealed vulnerabilities of the Israel Defense Forces (IDF). The group effectively integrated the military with the political and information dimensions, using advanced weaponry (guided anti-tank missiles, operational and tactical missiles, drones, anti-ship missiles, and radio surveillance equipment) and techniques adapted to densely populated spaces (Potîrniche and Petrescu 2019).

Military history abounds in relevant examples of the use of conflict forms that can be retrospectively classified as hybrid warfare, characterized by the combination of conventional capabilities, subject to classical military rules and norms, with unconventional elements involved in irregular actions. From the Peloponnesian War, fought between the Spartans and Athenians, in the period 431 - 404 BC, the Jewish revolt of 66 AD against the Roman legions of Emperor Vespasian, to the Spanish-Portuguese War of 1807 - 1814 or "Operation Barbarossa" of the invasion of the Soviet Union by the Axis forces, during the Second World War (1941), the advantages of using unconventional actions were exploited together with conventional means of combat and contributed significantly to achieving decisive effects.

Some theorists argue that hybrid warfare, as described in many episodes in history, involves non-standard forces: local auxiliaries, militias, partisans, sabotage, and insurgency tactics. Their use allows a state not only to know better the battlefield, but also to have additional room for maneuvering, especially in expeditionary operations. Anglo-Saxon literature calls this type of warfare "compound warfare", and examples can be found in the French support for the American insurgents (1778 - 1781), the cooperation between Wellington and Spanish guerrillas against Napoleonic troops, and the cooperation between Napoleonic troops and auxiliaries (1809 - 1814).

However, other theorists use the phrase "hybrid warfare" to describe the appropriation, by non-state groups engaged in guerrilla warfare or terrorism, of advanced technologies. These technologies were originally designed for state forces but have been able to offer non-state actors increased firepower, as well as greater freedom of maneuver (portable anti-tank and anti-aircraft missiles, night-vision goggles, and other tools that have allowed the erosion of the comparative advantages of conventional forces).

The specialized literature uses diverse terminology to describe the concept of "hybrid warfare", which reflects an adaptation of the analytical interpretation framework to different strategic and cultural contexts. The Chinese strategic approach, formulated in the theory of "unlimited war", legitimizes the use of any instrument of power as

a means of influence. In the Anglo-Saxon approach, the term "hybrid warfare" has been established as a concept that synthesizes the convergence of a wide spectrum of risks, generated by adversaries who use military and non-military means. In contrast, the Russian approach operates with the term "non-linear warfare", which emphasizes the indirect, progressive, and integrated nature of actions carried out in the political, information, and societal fields, as essential elements of contemporary confrontation. All these concepts are related, emphasizing the plurality of perspectives on the forms of manifestation and mechanisms of action of hybrid wars.

1999 is the year that marked an important change in the way of understanding the conflict, in which the confrontation extends beyond the strict military sphere, with the emergence of the concept of "unlimited war", introduced in the work "War without restrictions", belonging to the officers of the Chinese People's Liberation Army, Qiao Liang and Wang Xiangsui. The authors supported the idea that any instrument at the disposal of a state or non-state actor can be used for conflict purposes, regardless of whether it belongs to the military, political, economic, or cultural domain. From this point of view, diplomatic actions, financial pressures, information manipulation, media influence, or exploitation of technological vulnerabilities were considered as relevant as the use of armed force. Thus, unlimited war is shaped as a continuous, diffuse, and potentially adaptive process, in which strategic competition takes place simultaneously on multiple levels, without respecting pre-established rules and without being conditioned by a formal declaration of war.

In the United States of America, the foundation of the "hybrid warfare" concept was laid by analyst Nathan Freier, one of the authors of the 2005 U.S. National Defense Strategy. The document signaled the transformation of the security environment and the convergence of traditional and unconventional threats (catastrophic and disruptive hi-tech terrorism), the U.S. increased exposure to these new types of threats to international stability, requiring a mandatory adjustment of the security response to hybrid forms of confrontation (Popescu 2014).

In 2007, American journalist and defense scholar Frank Hoffman conceptualized hybrid warfare as a complex form of conflict that combines multiple types of confrontation, from conventional military capabilities to irregular tactics and structures. This form of warfare includes the use of terrorism, with indiscriminate acts of violence and coercion mechanisms, as well as criminal activities designed to cause instability (Wither 2020). Such actions can be simultaneously carried out by both state actors and a diverse range of non-state actors, blurring the traditional boundaries between war, crime, and terrorism.

With the blurring of the boundary between peace and conflict, the security space is transformed into a profoundly unpredictable environment, difficult to manage through traditional means of defense. 5GW marks a paradigm shift because the protagonists of contemporary conflicts are state and non-state actors: "the battlefield is represented

by the entire society of the enemy, and the goal is, rather, the internal collapse of the enemy and not its physical destruction" (Lind 1989, cited in Neculcea 2020).

The hybrid threat was defined in 2009, at the U.S. Joint Forces Command hybrid war conference in Washington, as "any adversary who, adaptively and simultaneously, employs a combination of conventional, irregular, terrorist, and criminal means or activities in the operational environment. This adversary is a combination of state and non-state actors, rather than a single entity" (Potîrniche and Petrescu 2019).

Faced with hybrid warfare rewriting global security, the European Commission proposed a first definition of hybrid threats in 2016, characterizing them as "coercive and subversive activities, using conventional and unconventional methods (e.g. diplomatic, military, economic, technological), that can be used in a coordinated manner by state or non-state actors to achieve specific objectives, but remaining below the threshold of an officially declared state of war. The emphasis is usually on exploiting the vulnerabilities of the intended target and generating ambiguity to hinder decision-making processes. Massive disinformation campaigns, which use social media platforms to control political discourse or to radicalize, recruit and coordinate intermediary actors, can constitute vectors of hybrid threats" (European Commission & High Representative of the Union for Foreign Affairs and Security Policy 2016).

What distinguishes contemporary warfare from previous generations of warfare is that it resides in a form of confrontation which combines conventional with irregular, economic, energetic, cyber, identity, and proxy warfare, in a complex, fluid, and unstable architecture, without limits and without restrictions. Insurgency, terrorism, and information warfare coexist in the same operations theatre because, according to the realist approach of the Italian Renaissance diplomat Niccolò Machiavelli, in war "tous les coups sont permis" (all blows are allowed) and the end justifies the means.

States with major military powers status, such as the USA, the Russian Federation, China, or France, are constantly reorganizing and adapting their military structures, orienting them towards the integration and development of capabilities specific to the conduct of offensive actions in cyber and space environments. This evolution reflects the recognition of the digital and space domains as new dimensions of armed confrontation, characterized by a high degree of interdependence with the land, air, and naval domains, as well as by their potential to generate disproportionate strategic effects.

The attacks on the Pentagon and the World Trade Center (USA, 2001) are examples of operations of unspeakable cruelty, as part of a campaign conducted in accordance with the principles of new generation warfare. They have forever dispelled the idea that contemporary warfare is only "terrorism" or something that happens solely in poverty-stricken third-world countries. 5GW is an unconventional form of warfare in which military force plays a much smaller, although still critical, role

than in previous generations, often in support of political, diplomatic, or economic initiatives. As important as finding and effectively destroying opponents is obtaining and consolidating a base of popular support (which questions the legitimacy of the target state government), which allows combatants to plan and execute their attacks.

Although from a tactical point of view the physiognomy of war has changed and adapted to the characteristics of the historic period in which the conflict took place, it has remained, in its essence, purely Clausewitzian, namely an instrument of politics. The historian and military theorist Carl von Clausewitz (1780 - 1831) spoke of war as "a continuation of politics by different means", and 5GW makes the concrete transition to this reality, with the complete fusion between the two principles, politics and war.

The role of advanced technologies in achieving victory in fifth-generation wars is decisive, as eloquently illustrated by the second Nagorno-Karabakh war, fought in the fall of 2020, between Azerbaijan and Armenia. The conflict demonstrated that military superiority is no longer determined exclusively by the size of conventional forces or classical territorial control, but by the coherent integration of advanced technological systems into the operational architecture, which acts as a force multiplier. The extensive use of reconnaissance and attack drones, loitering munitions, real-time surveillance systems, and electronic warfare capabilities allowed Azerbaijan to gain a significant information and operational advantage (Popescu 2021). This war also highlighted the importance of information integration, decision speed, and synchronized action in physical, information, and cognitive spaces, defining features of fifth-generation warfare.

Hybrid Warfare, a Component of the Russian Federation's Power Strategy

The "hybrid" dimension of war, a topic that has been intensely debated by the defense and security community, is not an absolute novelty. Over time, weaker adversaries have tried to identify and exploit to the maximum the vulnerabilities of stronger opponents and have done so countless times without considering rules, norms, or morality. "Victory can be created," said Sun Tzu, half a millennium BC, in his work "The Art of War". For this, the number of combatants and their strength are not enough, but skill, ability, capacity for analysis and synthesis, and the creative initiative that allows finding solutions to counter the adversary´s superiority in situations of asymmetry.

The concept of "hybrid warfare" gained increased theoretical relevance in the specialized literature since the middle of the last decade, especially because of the actions taken by the Russian Federation in Crimea, resulting in the annexation of the peninsula in 2014, as well as the military intervention in Syria, initiated in 2015.

As a particular form of non-linear conflict, hybrid warfare is associated with the Russian Federation's strategy of challenging the Euro-Atlantic security architecture and reconfiguring the spheres of influence in its strategic proximity, with reference to the historic spaces of Tsarist and Soviet domination. In this context, the Kremlin has developed and adapted a set of multidimensional strategies aimed at ensuring the expansion of its control capacity over the global geopolitical environment, including maritime, information, and strategic spaces, with the objective of asserting a hegemonic position in the international system.

The annexation of Crimea (2014) and the Russian invasion of Ukraine (2022) have validated the darkest fears, namely the return to a conflictual, anachronistic, 19th-century nature of warfare, while the means of waging war acquire extremely versatile valences: "vast geopolitical spaces are about to succumb to the flames of sectarian and religious conflicts, while supremacy for resources and economic influence pits the most prominent centers of power on the front line" (Bălăşoiu 2017, cited in Hornea 2017).

Revealing for understanding the Russian strategy and for deepening the risks associated with hybrid warfare are the directions indicated in 2013 by General Valery Gerasimov, Chief of the General Staff of the Russian Federation, strategic directions that substantiated what would later be the "Gerasimov doctrine". The rules of war themselves have changed, Valery Gerasimov specified, arguing that the role of non-military means in achieving political and strategic objectives has increased and, in many cases, these means are more effective than the power of arms. The methods applied in a conflict are more focused on bringing the target state to collapse through internal revolution and will emphasize "the integrated, large-scale application of political, economic, diplomatic, information, humanitarian and other non-military measures, in full correlation with the potential for revolt and protest of the population" (Eremia 2018).

The typology of the "Russian New-Generation War" described by Gerasimov integrates the armed forces with all other instruments of national power, using both conventional and unconventional forces, all equipped with cutting-edge technologies, the result being "total war". His strategic hypothesis starts with the idea that, in the 21st century, at a global level, there is a permanent state of conflict, with a tendency to blur the demarcations between war and peace. Moreover, the way wars are conducted has changed; wars are no longer formally declared, and after they are triggered, developments become unpredictable. The unprecedented rate of change characterizes the contemporary operational environment, and the rapid transition of some states from relative stability to violent confrontations and civil war is not an abnormality.

Other essential aspects concern: prevalence of the use of non-military means to achieve political-military objectives, clandestine application of the military

instrument, involvement of military capabilities being officially assumed in the final phase of the conflict, after the achievement of the decisive conditions for definitive success, reduction of the adversary's potential for action, even if it is superior in terms of conventional capabilities, by affecting cognitive capacity and exploiting identified vulnerabilities.

In the version adopted by the Russian Federation, hybrid warfare is presented as a form of adaptation to the political - economic - military reality, an attempt to overcome the technological gap and the differences in the quantity and quality of conventional military capabilities between the North Atlantic Treaty Organization (NATO) and Russia. This approach involves the revitalization of Soviet concepts, such as reflexive control and deep operation (Kasapoglu 2015).

Reflexive control, a concept developed since the 1960s, refers to the act of providing a partner or adversary with especially prepared information that leads them to voluntarily make a decision that benefits the initiator of the action. In this way, the targeted entity is influenced to adopt a course of action that is advantageous to the opposing party, without being aware of it.

As for the deep operation (battle), this concept was developed by a group of officers led by Marshal Mikhail Tukhachevsky during 1920-1930. In the context of hybrid warfare, the implementation of the deep strike principle involves paralyzing the adversary´s vital institutions and systems. Thus, necessary conditions are created for unrestricted action in which elements will execute shaping or decisive interventions during various phases of the operation itself.

The theoretical dimensions of the concept of "hybrid warfare" are in a permanent dynamic, ensuring an epistemological reflection on the practical aspect of applying multidimensional strategies and tactics that have changed the paradigm of conducting contemporary warfare (Ioniță 2014). The concept was also mobilized by NATO to explain the Russian strategy, highlighting its option to employ forces without uniforms and badges that allow identification ("little green men"), the engagement of local allies ("proxy war"), the use of propaganda promoted by social networks or the reinterpretation of agreements or treaties (giving rise to the concept of "lawfare").

Russia, however, does not have a monopoly on this type of war. U.S. permanently uses mercenaries, the famous "private military contractors", a fact which allows for economies of scale and gives the Pentagon greater maneuverability (in Iraq, Afghanistan). Beijing sometimes uses maritime militias ("little blue men"), interpretations and reinterpretations of maritime law, including by appropriating islands under commercial pretexts, but by creating infrastructure that could be suitable for military installations.

There is also a very close connection between asymmetric actions such as terrorism, organized crime, drug and human trafficking, and actions taken to undermine the legitimacy of the government or local authorities and generate or amplify a crisis. Opium production in Afghanistan or organized crime groups in the Americas (especially in Mexico) are disruptive factors that support this theory, advocated by Frank G. Hoffman (2009).

The combination of standard and non-standard or conventional and unconventional tactics makes it possible to carry out large-scale land operations, but sometimes also naval (for example, those carried out by the "Tamil Tigers" in Sri Lanka, the most dangerous terrorist organization in the world by the number of victims, or by Al-Qaeda in the Arabian Peninsula), air and ballistic ("Tamil Tigers", Hezbollah), information. The process of professionalization of non-standard fighters allows them to carry out combined operations, including all the mentioned components. In this sense, hybrid warfare is not just a tactical bricolage but rises to the level of an operational maneuver (Briot 2020).

The definition of hybrid warfare presented in the North Atlantic Treaty Organization Summit Declaration (September 2014, Wales) refers to "a wide range of military, paramilitary and civilian actions, conducted overtly or covertly in a highly integrated manner". The definition reveals the quintessence of the phenomenon, specifying that hybrid threats are represented by adversaries (states, irregular non-state groups - insurgents, terrorists, guerrillas, and members of organized crime; hybrid groups

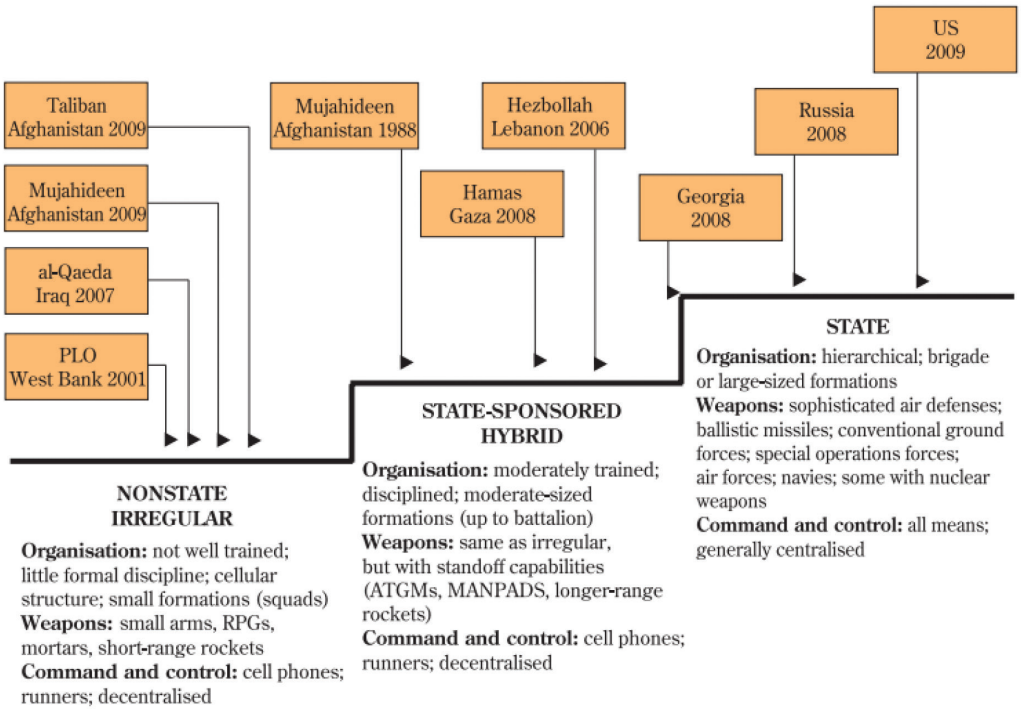


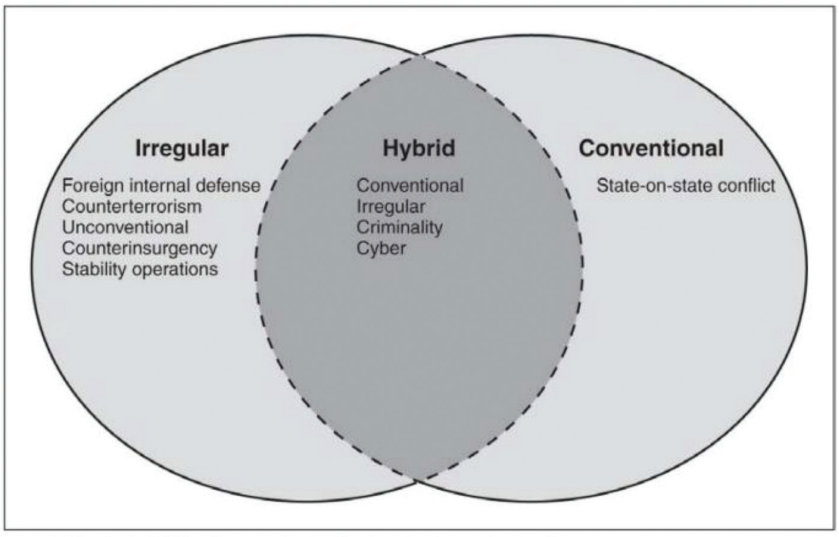
Figure 1 The Evolution of Hybrid Threats
Source: David Johnson 2009, RAND OP295-1

supported by states - Figure no. 1) who can simultaneously use conventional and unconventional means in order to achieve objectives.

Specific forms of manifestation and mechanisms of action

Certainly, in hybrid warfare, there are no longer separate threats with fundamentally different approaches. One can observe a convergence of irregular threats in which adversaries have a comprehensive, integrated approach to achieve their objectives. Hybrid threats target and influence a wide range of ways of waging war, combining conventional forces and capabilities with unconventional tactics and formations, subversive and terrorist acts that include generalized violence and coercion, destabilization of public order, and cyber-attacks.

Multimodal actions can be executed by separate structures, or even by the same unit, but are directed and coordinated in the operational space, at the operational and tactical levels, to obtain synergistic effects in the physical and psychological dimensions of the conflict. Consequently, the effects can be obtained at all levels of war: conventional, irregular, criminal, and cyber (according to Figure no. 2, which highlights the generic model of hybrid war).



Source: GAO analysis of DOD military concept and briefing documents and academic writings.

Figure 2 The Hybrid Warfare Concept

The diversity of forms in which hybrid warfare manifests itself is given by the multitude of areas in which asymmetric threats interfere: politics, diplomacy, culture, society, the rule of law, military and defense, outer space, administration, infrastructure, economy, intelligence, information, and cyber. These areas have been identified by the European Commission (EC) and the European Center of Excellence for Countering Hybrid Threats (Hybrid CoE) and are presented in the figure No. 3 (Source: https://euhybnet.eu).

Figure 3 The areas in which hybrid warfare operates

Clarifying the hybrid threat orchestration pattern are the methods used by the Kremlin to control the Great Planetary Ocean and ensure its global hegemony. These methods involve both military and non-military means, which will have repercussions in diplomatic, political, economic, information, cultural, cyber, and non-military terms, as Simileanu (2018a, 2018b) explains.

Hybrid warfare includes a distinct diplomatic dimension, in which the classical instruments of foreign policy are used primarily to undermine the existing international order and to advance the interests of the aggressor state without direct recourse to military force. From this perspective, diplomatic actions are oriented towards discrediting strategic competitors and reconfiguring international agendas in forums such as the United Nations or the Security Council, so that the attention of the international community is diverted from its own violations of international law. Relevant examples are the efforts to relativize or justify the annexation of the Crimean Peninsula by the Russian Federation and the constant diplomatic support granted to regimes under sanctions, such as the Syrian one, by blocking or diluting unfavorable international resolutions.

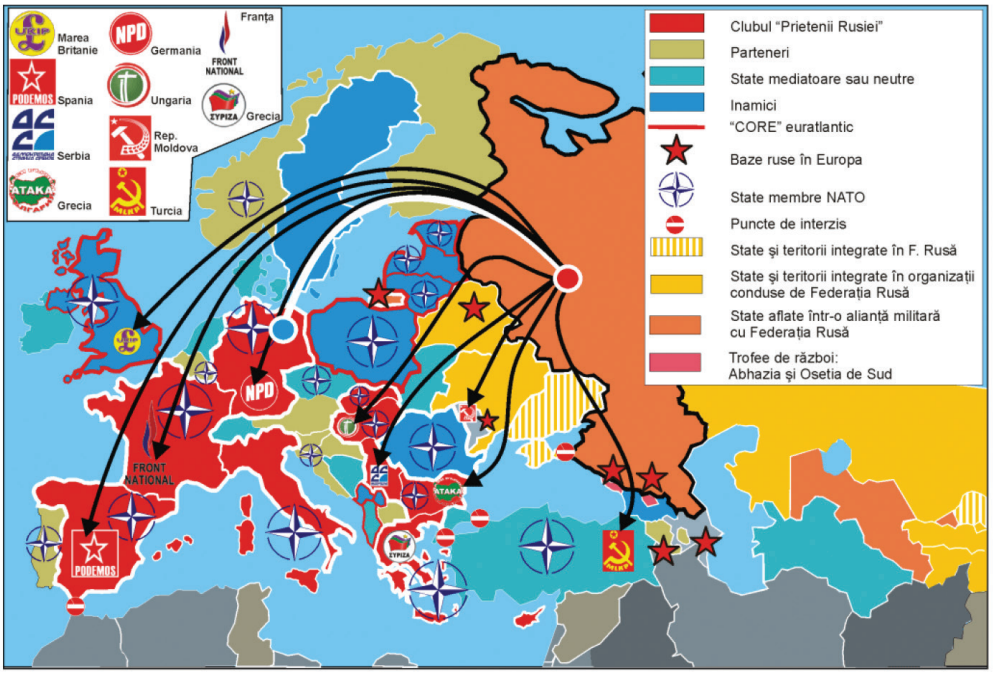
Russia's constant "reflexive control" campaigns demonstrate the Kremlin's concern to create narratives which seek to reinforce the perception – among Western countries and the Russian population – that it is an attacked state, responding in self-defense. Thus, alleged attempts to assassinate Russian President Vladimir Putin by the Ukrainian army are frequently invoked, and recently these practices have aimed to compromise diplomatic relations between Kiev and Washington, amid

negotiations to end the war in Ukraine. The Russian Ministry of Defense published on Telegram, in January 2026, a video showing the moment when the Chief of the Main Directorate of the General Staff of the Russian Armed Forces, Admiral Igor Kostyukov, hands an American attaché the control mechanism of a drone that he claimed was found among the fragments shot down at President Putin's residence in the Novgorod region (Saghin 2026). After Russia claimed that the residence had been targeted by an attack with 91 long-range drones, U.S. President Donald Trump initially took a favorable stance towards the Russian Federation, showing himself "very angry" about the alleged incident, and later qualified his position, sharing on social platforms an editorial from the "New York Post" that attributed responsibility to Russia for obstructing the peace process in Ukraine. Kiev denied that it carried out an attack targeting President Vladimir Putin, but the U.S. leader's reaction shows that the Russian tactic of shaping opponents through rhetoric and disinformation operations can produce temporary advantages for the Russian Federation by destabilizing Western decision-makers.

A central component of hybrid warfare is the use of regional conflicts and "peacekeeping" formats as levers of geopolitical influence. Involvement in frozen conflicts, such as those in Transnistria, South Ossetia, or the Donbas region, has allowed the aggressor state to simultaneously present itself as an interested party and an indispensable mediator, maintaining indirect control over the evolution of these files. In parallel, active participation in alternative or complementary multilateral formats to Western ones, such as BRICS, G20, G8 or the Shanghai Cooperation Organization, contributes to the consolidation of political and diplomatic support networks, often described as "clubs of friends" - according to the map in Figure No. 4 (Source: Anatoly Karlin), which can be mobilized to legitimize or defend controversial actions on the international stage - the "Club of Friends of Russia".

Last but not least, diplomatic hybrid warfare is also manifested through strategic involvement in negotiations and processes to resolve major international crises, to gain influence and control of dialogue channels. This is visible both in the role assumed in negotiations on regional conflicts, such as the one in Syria or attempts to position itself as a negotiator in the Ukrainian file, and in the involvement in sensitive discussions between other states, for example the negotiations between the United States of America and Iran or the support given to problematic nuclear programs, such as the North Korean one. Through such actions, the aggressor state not only consolidates its status as an indispensable actor but also manages to fragment collective efforts to combat global threats, from the proliferation of weapons of mass destruction to terrorism, drug trafficking, and organized crime, weakening the cohesion and efficiency of the international response.

At the political level, the Russian Federation's hybrid warfare is focused on practices through which it can maintain its dominant influence in the post-Soviet space, especially within the Commonwealth of Independent States, and extend this



Sursa: Anatoly Karlin blog, unzcloud.com/upload/2013/01/europe-future.gif
www.rusbg.com/s-kego-sche-druzi-i-vrazhduva-russia.html

Figure 4 The "Club of Friends of Russia"

influence on Western states. In this sense, Russia capitalizes on the vulnerabilities already existing in Western societies. Social, economic, or identity problems are amplified and reinterpreted until they come to be perceived as major internal crises, capable of generating polarization and political instability. Nationalist rhetoric and patriotic discourse play an essential role in this process, being used to camouflage anti-Western messages and to undermine the legitimacy of the values and institutions that were the basis of European and Euro-Atlantic stability in the post-war period.

Another important component of this hybrid political strategy consists of exerting pressure on the European Union through strategic blackmail instruments, especially in the energy sector, and through capital controlled by oligarchic groups close to the Kremlin. In parallel, formal channels of dialogue with partners and allies are deliberately reduced or interrupted, while informal networks of influence, some built years ago, are reactivated and put to good use. These networks have also been used by involving top political actors from Western states, which has contributed to the erosion of internal consensus and the weakening of the cohesion of Euro-Atlantic alliances.

This type of hostile action aims to internally destabilize the target states. By heightening social tensions, cultivating collective fears, and deliberately stimulating feelings of hatred, radical political currents and extremist formations are encouraged, and they openly challenge alliances, treaties, and international institutions essential for the functioning of Western democracies. The support given to leaders of populist or far-right parties in Europe (for example, "Golden Dawn", "Jobik", "Syriza", "Patria", "Podemos", "National Front", "Ataka" or "Yukip), the use of former military

personnel or pensioners from the ex-Soviet space (Republic of Moldova, Latvia, Lithuania and Estonia) and the instrumentalization of sensitive areas, such as the Republic of Moldova, Ukraine or Crimea, as means of lateral pressure on Romania, Ukraine, Poland and Turkey, show this strategy´s methodical nature. Overall, the objective is not negotiation or cooperation, but induction of a climate of uncertainty and political chaos, intended to diminish the capacity of target states to coherently react to external influence and constraints.

The orchestration of hybrid warfare to have an impact at the societal level is based on recurrent discourses that call for the increased role of the social factor in the context of armed conflicts and local wars fueled by the Russian Federation. In fact, the policy of Russian President Vladimir Putin interferes with internal social strategies and creates development gaps compared to Euro-Atlantic states. Through Stalinist and neo-Soviet-style discourses, Putin has managed to "reanimate" the social sacrifice imposed by the arming of a non-existent enemy, permanently demonized. The result also consists of inducing insecure, national-defensive behavior at home, but also in diplomatic and international relations. Particularly important is the method of bringing the target state to collapse through internal revolution, a method that emphasizes the large-scale application of political, economic, diplomatic, information, humanitarian, and other non-military measures, in full correlation with the population´s potential for revolt and protest. Such operations have the potential to transform a stable political and social situation in a target state into a general state of chaos, bordering on the outbreak of civil war, which creates the premises for external intervention.

The economic dimension of hybrid warfare relies on the deliberate use of economic interdependencies as an instrument of influence and coercion. One of the constant objectives of the Russian Federation is to deepen the dependence of European states on Russian energy resources, especially gas, by expanding the transport infrastructure to Western markets and, simultaneously, by obstructing or delegitimizing alternative energy diversification projects. This strategy is supported by investments in key areas of the economy (banking, hospitality, professional sports, or information technology), which allow both secure access to capital and the exercise of indirect influence on economic and political decisions. Against the background of the economic pressure exerted, strategic advantages are obtained, and dependent states have limited room for maneuver.

To maintain energy dependence, Russia often resorts to explicit forms of coercion, illustrated by repeated episodes of interruption or conditioning of energy supplies in relations with Ukraine and Georgia. The practices known as "energy coercion" have direct effects on the targeted state's economic and political stability. In parallel, the hybrid war with economic implications includes the financing of anti-state structures (anti-Ukrainian in Crimea and the Donetsk-Lugansk area), pro-Russian NGOs in the ex-Soviet and ex-communist space, with main targets such as Poland,

Romania, and Turkey, and pro-Russian networks in regions such as Crimea, Donbas, Ukraine, the Republic of Moldova, or Georgia. These financial flows have the role of supporting the challenge to the state's authority, fueling internal tensions and creating economic dependencies that can later be exploited for political purposes.

Another pillar of the Russian strategy for implementing hybrid warfare is represented by cross-border money laundering networks, involving politicians, members of security structures, actors in the judicial system, banking institutions, and criminal groups, a strategy that has been documented both in the European Union and in the former Soviet states. Such practices have been complemented by the promotion of the Eurasian Customs Union, transformed into the Eurasian Economic Union as of January 1, 2015. Far from being just an economic integration project, this framework has functioned as an instrument for forcibly anchoring the participating states in an economic space dominated by the Russian Federation, reducing their decision-making autonomy and external strategic options.

At the cultural level, the hybrid warfare practiced by the Russian Federation is based on the use of identity, religion, and historic memory as tools of geopolitical influence, through "cognitive hacking" (Chifu 2018). A central element of this strategy is the promotion of a messianic discourse, which reinterprets older ideological traditions, such as pan-Orthodoxy and pan-Slavism, to legitimize contemporary geopolitical ambitions. These currents are reactivated as mechanisms of symbolic mobilization, intended to justify Russia's self-proclaimed role as "protector" of the Orthodox and Slavic world. In this context, references to the occupation of Constantinople and the control of the maritime constriction points of the Bosphorus and the Dardanelles acquire a clear geopolitical significance, being integrated into a discourse that combines religious, historic, and strategic elements to support objectives of regional influence (Figure No. 5).

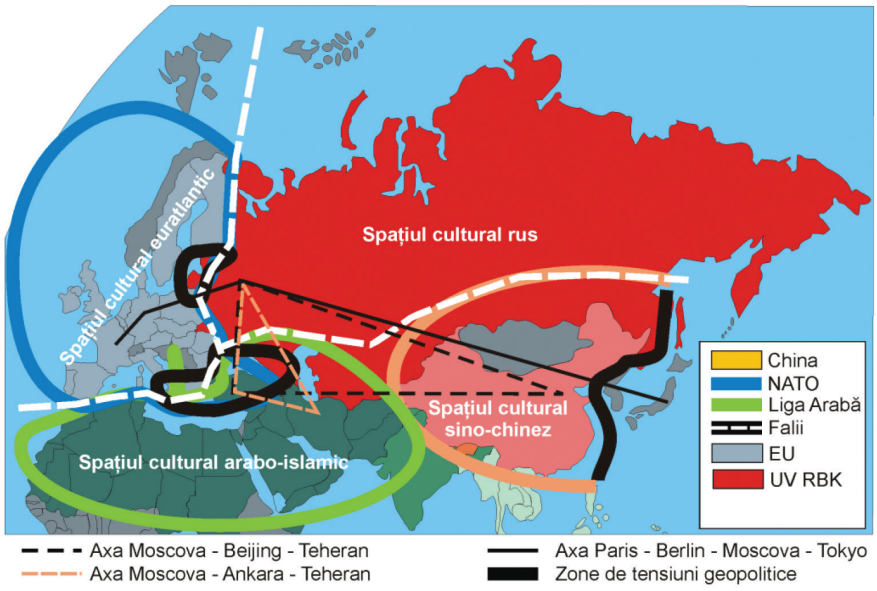


Figure 5 Russian cultural space (GeoPolitica 2018)

In addition, this cultural strategy includes forms of symbolic aggression and the instrumentalization of existing identity tensions. By organizing cultural and academic events in the Euro-Atlantic space, which promote narratives favorable to Moscow, Russia aims to normalize alternative interpretations of political and economic realities in the context of major internal difficulties of the Russian Federation. At the same time, one can observe a tendency to resuscitate and exploit ethnic and religious conflicts by emphasizing identity differences and fueling historical resentments. These practices allow social cohesion fragmentation in the targeted states and favorable terrain for external influence, in which cultural identity becomes a vector of political pressure and long-term destabilization.

At the information level, hybrid warfare mainly acts in the online environment, especially on social media platforms, which provide a favorable framework for the use of asymmetric instruments of influence. The information space allows for low-cost, high-impact operations aimed at eroding social cohesion, diminishing trust in institutions, and weakening the response capacity of the targeted states. New digital technologies facilitate strategic influence operations, through which public perceptions are shaped with certain goals that serve the aggressor, and the potential for mobilization of the adversary is reduced without resorting to direct military confrontation. In this context, traditional press has also become a target, but differences in regulation, transparency of financing, and mechanisms for editorial accountability clearly delimit it from the opaque ecosystem of social networks.

A defining element of the mechanisms aggregated by hybrid warfare is the use of information manipulation techniques, which, from the perspective of the psychological impact pursued, show many similarities to the methods encountered in terrorist threats. Practices such as selection and truncation of information, biased framing of statements by political leaders, or presentation of opinions as indisputable facts are frequently used to build narratives favorable to the hostile entity. Media platforms affiliated with Russia ("Russia Today" or "Sputnik") are often associated with such strategies, complemented by the limitation of the right to reply in the domestic information space. Intentional overlap of factual statements and opinions, generalization of specific events, or selective omission of relevant international developments also contribute to distorting reality and inducing confusion among the public.

At the same time, the manifestations of information warfare are amplified by certain characteristics of social media platforms, where the lack of rigorous control over the identity of users and the dynamics of algorithms favors the proliferation of fake accounts, troll networks, and coordinated disinformation operations. Techniques such as the spread of fake news, imagological attacks on political leaders and international organizations, or the symbolic use of public shaming gestures have the role of undermining the morale of the targeted societies and eroding confidence in the prospects of success or stability. All these actions, carried out both through media

channels loyal to Moscow and through global digital platforms, configure a toxic information ecosystem in which disinformation, propaganda, and manipulation are central tools of contemporary hybrid warfare.

Beyond the classical military dimension, hybrid warfare is increasingly manifested through a set of non-military actions that target the vulnerabilities of modern societies. A central role is played by cyber-attacks, directed both against states and international organizations, as well as against financial and banking institutions or individual actors considered inconvenient (journalists, analysts, groups active in the online environment). These attacks do not exclusively aim to cause technical damage, but have as their main objective the intimidation, collection of information, and discrediting of independent sources of analysis. In parallel, ideological propaganda is strategically integrated into diplomatic and academic contexts or in high-visibility international events, where messages are calibrated to influence political and opinion elites.

Another level of these non-military manifestations is represented by the expansion of influence networks and the attraction of supporters through unconventional methods. Intelligence structures, digital social networks, and informal communities, including groups associated with ultras phenomena or online subcultures, are used to create loyalties and mobilization channels. Alternative financial instruments, such as cryptocurrencies, as well as global trading platforms, are exploited to facilitate discreet financing and coordination of actions. At the same time, sustained efforts are observed to co-opt or influence media trusts from the Western space, to legitimize certain narratives and amplify messages favorable to Russian interests within democratic societies.

At the same time, non-military hybrid warfare includes actions of symbolic denigration and discrediting. Cultural values in the historical territories of states that belonged to the former Soviet Union are frequently the target of delegitimization campaigns, designed to weaken national identity and social cohesion. Attacks on political leaders, often focused on their personal lives, are used to diminish public credibility and induce distrust (for example, the pro-Kremlin press constantly portrays Ukrainian President Volodymyr Zelensky as a "drug-addicted leader with worsening mental health problems") (Gherman 2025). These practices are complemented by campaigns to destroy the country's image and the use of extortion or non-transparent financing to support pro-Russian groups and influential individuals. Overall, these non-military instruments outline a broad strategy of pressure and destabilization, which aims to obtain political and strategic advantages without direct recourse to armed force.

At the cyber level, hybrid warfare exploits states' vulnerabilities with potential consequences both on national security and on the integrity of physical, digital, and financial assets. The aim is to gradually erode the functioning of essential public services and diminish the population's trust in the ability of state institutions to

ensure the protection of fundamental interests. Cyber interventions can take various forms, from the interruption of vital services and identity theft to the manipulation of control systems used in the management of critical transport infrastructures, with a direct impact on road, rail, or air traffic. In addition, there are attacks on IT security mechanisms and cyber espionage campaigns aimed at civilian and military servers of EU and NATO member states, as well as cybercrime activities aimed at obtaining financial benefits through illegal theft and exploitation of information.

The accelerated development of new technologies and the expansion of digital space have multiplied the tools available for hostile actions in the online environment. The Internet is used not only for propaganda and psychological warfare, but also for recruitment, mobilization, fundraising, and information collection through advanced data analysis techniques. Encrypted communication, coordinated cyber-attacks, and distribution of extremist content through mobile applications complete this spectrum of threats. In addition, advances in the field of artificial intelligence allow the generation of extremely realistic fake content, from the real-time manipulation of facial expressions and voices to the creation of synthetic images and audio-video materials or press articles built on data sets (polls, election results, financial reports) that can mislead public opinion.

All these developments highlight the fact that modern warfare is characterized by the simultaneous integration of several types of capabilities and instruments of influence. Cyber operations are correlated with information warfare actions, economic pressures, political and diplomatic approaches, as well as, in certain situations, with the use of special operations forces acting in connection with internal opposition groups in the target state. Depending on developments on the ground and the reactions of the actors involved, these actions are adjusted, coordinated, and permanently recalibrated, with the aim of maximizing efficiency and achieving the established strategic objectives, without exceeding the threshold of a direct conventional military confrontation.

Hybrid warfare and societal resilience

Through the complexity of integrated dimensions, as well as through the variety of tools and methods used, hybrid warfare involves society at large, subjecting it to a permanent test of cohesion while faced with asymmetric threats. Since the adversary acts at the limit of detection (in the "gray area"), and the methods of confrontation are marked by ambiguity and the lack of clear demarcations, the process of identifying risks and formulating responses becomes sinuous, favoring the amplification of vulnerabilities and their transformation into systemic crises.

The concept of "societal resilience" refers to "the capacity of communities to flexibly absorb major disruptions and to rapidly recover from the inevitable decline in basic functionality" (Elran 2017, cited in Lesenciuc 2024). The term implies the state´s

ability to protect its sensitive points, which may be perceived by hybrid actors as strategic opportunities, as well as to consolidate, rebuild, and adapt its critical infrastructure (made up of both tangible and intangible components) after the manifestation of a hybrid action.

Managing a hybrid war and all the effects that arise from its impact on society does not solely lie in the state´s power, with its entire network of administrative institutions. Countering hybrid threats also depends on citizens´ resilience, which is built over time, and its foundation is education in the spirit of defending national values and the nation itself. The effort must be conscious and convergent, with each citizen's reactions being guided by the feeling of strong identity, but also by the deep component of patriotism that animates society. In this sense, recognizing the education - societal resilience nexus is essential for any security strategy.

The hybrid war mechanism (according to Figure 6) acts on the territory of a state, defense forces, leaders and population predominantly with informational attack forces, so that societal resilience must be built in the sense of blocking the action of media and other instruments of influence on the psychology of the masses and "opaquing" distorted perception, through the bombardment with fake news and images regarding the events in progress.

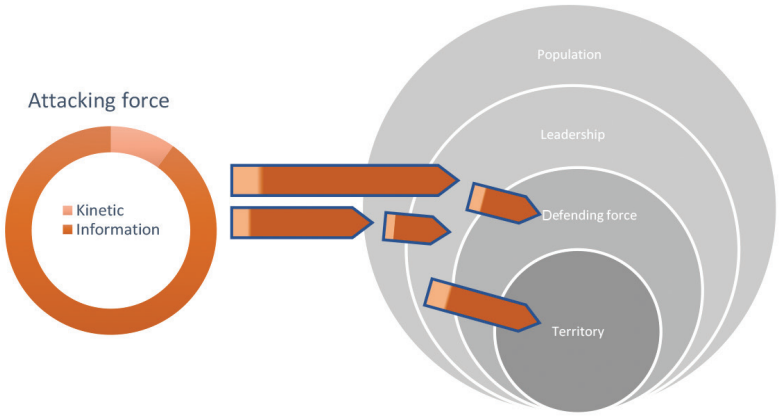


Figure 6 The mechanism of hybrid warfare
Source: Mînzărari 2020

In fact, public perception must be based on the image dimension of the state, the leadership, the political decision-maker, and the regime. Trust in these elements is mandatory, because on trust are built the ideas of national representation and the perspective of the development of the state and society, respectively the credibility of the leader and the state force, which induces a high level of hope at the individual and societal level.

One of the characteristics of asymmetric warfare is the continuous interaction, within the same confrontation, between the elements of hard and soft power, which are enhanced in strategic combinations adapted to the context, thus resulting in smart

power. While hard power represents the use of military force or the coercive capacity of a state, soft power cultivates compliance through a variety of policies, qualities, and actions, indirectly and through non-coercive measures. Hybrid warfare allows actors to operate in the shadow, at the border between war and peace, with both hard coercive instruments and soft instruments (e.g., propaganda and disinformation campaigns aimed at psychosocial destabilization), as a complex interface located at the meeting point between conventional and unconventional threats (Figure no. 7).

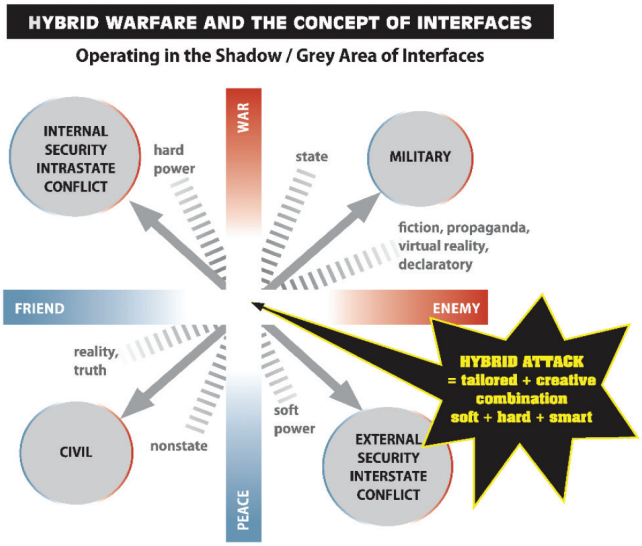


Figure 7 Hybrid warfare and the interface concept (NATO StratCom COE)

"A more resilient Europe, fully equipped to face today's complex and dynamic security threats" is also the aspiration of the European Union leaders, who are working to develop resilience and counter hybrid threats. In this regard, the European Commission is monitoring the overall implementation of the Joint Framework on Countering Hybrid Threats. The EU proposals aim, among others, at various means to develop capabilities and counter cyber threats, such as a mandate to strengthen and modernize the European Union Agency for Cybersecurity, a "blueprint" for cooperation between Member States and EU agencies in the event of an attack, and the cyber diplomacy toolbox. Moreover, "if 2025 was the year of recognition of Russia's hybrid threats, 2026 must be the year of response" (Bowser 2025).
On the other hand, the NATO 2030 Strategy mentions that, in the event of a hybrid war, the North Atlantic Council could decide to invoke Article V of the Washington Treaty, as in the case of an armed attack.

Conclusions

Hybrid warfare can be understood as the result of an evolutionary process of armed conflicts, generated by the dynamics of social, technological, and political transformations that characterize the contemporary international environment. Against the background of this evolution, the paradigm of conventional

confrontation, centered almost exclusively on the use of military force, has been progressively complemented by flexible forms of action, in which state and non-state actors simultaneously resort to military and non-military instruments. This expansion of the spectrum of means has contributed to a substantial redefinition of the concept of security, demonstrating that traditional military advantage no longer constitutes a guarantee of strategic success. The potential to correlate political, economic, information, and cyber pressures becomes, in this context, a determining factor of strategic efficiency.

The ongoing hybrid war of the Russian Federation constitutes a reference point in the analytical consolidation of this type of conflict, requiring a reassessment of the prevention and response tools used at the international level. The ambiguity of the actions of the Russian Federation, the coordination of military means (in Ukraine) with non-military ones, and the conduct of operations in several areas have significantly complicated the early identification of aggression and the articulation of a coherent response. Thus, the need to orient research on hybrid warfare towards institutional, sociological, and operational perspectives, capable of capturing the interdependence and complexity of this phenomenon that represents the main threat to the security of states in the 21st century, becomes imperative.

Strengthening societal resilience emerges as a central dimension of countering hybrid threats. Security requires not only the accumulation of military capabilities, but also an integrated approach, which includes security education, increasing public awareness, strengthening social cohesion, and adapting institutions to new risk patterns.

For Romania and for the Eastern European states, located in the vicinity of areas marked by instability, the development of flexible and multidimensional response mechanisms is a strategic necessity. Only through a coherent approach, which articulates the military with the societal and institutional dimensions, can contemporary hybrid conflicts be effectively managed, as expressions of the way in which the world is configured, interpreted, and contested.

References

Bărbulescu, I. 2001. "War and armed struggle. The content and general physiognomy of armed struggle." *Land Forces Academy Review* 2. https://www.armyacademy.ro/reviste/2_2001/c3.html.

Bârgăoanu, A., and E. Negrea-Busuioc. 2024. "Hybrid warfare is less than warfare: A dangerous illusion." *IW Perspectives* No. 19. https://irregularwarfarecenter.org/wp-content/uploads/P_19_Hybrid_Warfare_is_Less_Than_Warfare.pdf.

Bowser, D. 2025. "Russian organized crime and its links to hybrid warfare in Europe." GLOBSEC Report. https://www.globsec.org/sites/default/files/2025-12/Russian%20Organised%20Crime%20and%20Links%20to%20Hybrid%20War%20in%20Europe%20ver3%20web%20spreads.pdf.

Briot, T. 2020. *Hybrid warfare, the new nature of global conflicts.* https://truestoryproject.ro/razboi-hibrid-natura-conflictelor-mondiale/.

Chifu, I. 2016. *Hybrid war, "lawfare," information warfare. Wars of the future.* https://adevarul.ro/blogurile-adevarul/razboi-hibrid-lawfare-razboi-informational-1696690.html.

___. Chifu, I. 2018. "Hybrid warfare and societal resilience. Planning hybrid defense." *Infosfera. Journal of Security and Defense Intelligence Studies* Nr. 1: 28-30.

___. 2022. *Reconfiguring security and international relations in the 21st century.* Vol. 2: Threats and conflicts in the 21st century. Bucharest: RAO Publishing House.

___. 2025. "Conceptualization and epistemological assessment: Cognitive warfare." *Infosfera. Journal of Security and Defense Intelligence Studies* Nr. 2: 5-18. https://www.mapn.ro/publicatii_militare/arhiva_infosfera/documente/2025/2_2025.pdf.

Eremia, C. 2018. „Innovative Russian approaches to modern warfare." *Monitorul Apărării și Securității.* https://monitorulapararii.ro/abordari-inovative-ale-rusiei-privind-razboiul-modern-1-4718.

European Commission & High Representative of the Union for Foreign Affairs and Security Policy. 2016. "Joint framework on countering hybrid threats: A European Union response." JOIN(2016) 18 final. https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52016JC0018.

European Commission. 2020. "Communication on the EU Security Union Strategy." Bruxelles, pp. 14–20. https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52020DC0605.

Frunzeti, T., and C. Bărbulescu. 2018. *National resilience to hybrid threats and security culture: An analytical framework.* https://www.aosr.ro/wp-content/uploads/2019/03/Anexa-1_Articol-Impact-Strategic-2018.pdf.

Gherman, M. 2025. *War propaganda: Zelensky is using drugs and is mentally unstable.* https://www.veridica.ro/fake-news-dezinformare-propaganda/propaganda-de-razboi-zelenski-se-drogheaza-si-e-instabil-psihic.

Hoffman, F. 2009. "Hybrid vs. compound war." *Armed Forces Journal.* http://www.armedforcesjournal.com/hybrid-vs-compound-war/.

Hoffman, F., M. Neumeyer, and B. Jensen. 2024. "The future of hybrid warfare." *Center for Strategic & International Studies.* https://www.csis.org/analysis/future-hybrid-warfare.

Hornea, I. 2017. "Hybrid warfare, a transitional stage toward the conflict of the 21st century." *Military Sciences Review* 4 (49): 77-93. https://aos.ro/wp-content/anale/R-S-M-Vol-17-Nr4Full.pdf.

Ioniță, C.C. 2014. „Is hybrid warfare something new?" *Impact Strategic* 4 (53): 64-76. https://cssas.unap.ro/ro/pdf_publicatii/is53.pdf.

Kasapoglu, C. 2015. „Russia's renewed military thinking: Non-linear warfare and reflexive control ." NATO Defense College Research Paper No. 121. https://www.ndc.nato.int/download/russias-renewed-military-thinking-non-linear-warfare-and-reflexive-control/?wpdmdl=7278.

Lesenciuc, A. 2024. "Societal resilience as intangible critical infrastructure." *Gândirea Militară Românească* Nr. 2: 94-109. https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2024/2/LESENCIUC.pdf.

Libiseller, C. 2023. "„Hybrid warfare" as an academic fashion." *Journal of Strategic Studies* 46 (4): 858–880. https://doi.org/10.1080/01402390.2023.2177987.

Lupulescu, G.D. 2023. "Hybrid, defining the concept of war, operations, and threats of the 21st century." *Bulletin of "Carol I" National Defence University* 12 (2): 56-68. https://revista.unap.ro/index.php/revista/article/view/1713.

Marcuzzi, S. 2018. "Hybrid warfare in historical perspective ." [Paper presentation, Max Weber International Workshop, NATO Defense College Foundation]. https://www.natofoundation.org/wp-content/uploads/2018/06/NDCF_StefanoMarcuzzi_Paper.pdf.

Mînzărari, D. 2020. "Understanding 'hybrid warfare': A conceptual approach." *Institute for European Policies and Reforms*. https://ipre.md/wp-content/uploads/2020/12/Policy-Paper_Understanding-hybrid-war_Dumitru-Minzarari.pdf.

Neculcea, C. 2020. "Generations of warfare, conventional and unconventional in the evolution of wars." In *Proceedings of the International Scientific Conference „Gândirea Militară Românească"*, 310-317. https://gmr.mapn.ro/webroot/fileslib/upload/files/conferinta%202020/proceedings/neculcea.pdf.

Popescu, A.I.C. 2014. "Observations on the relevance of hybrid warfare. Case study: Ukraine." *Impact strategic* 4 (53): 124-148. https://cssas.unap.ro/ro/pdf_publicatii/is53.pdf.

___. 2021. "Observations on fifth-generation warfare and the Second Nagorno-Karabakh War." *Bulletin of "Carol I" National Defence University* 10 (4): 39-45. https://revista.unap.ro/index.php/revista/article/view/1297.

Potîrniche, M.T., and D. Petrescu. 2019. *Countering hybrid threats to state security: Specialized study.* București: "Carol I" National Defence University Publishing House. https://cssas.unap.ro/ro/pdf_studii/modalitati_de_contracarare_a_amenintarii_hibride.pdf.

Presidency of Romania. 2021. *NATO Brussels Summit communiqué.* https://www.presidency.ro/ro/media/comunicate-de-presa/comunicatul-summitului-nato-de-la-bruxelles-14-iunie-2021.

___. 2025. *National Defence Strategy of Romania for 2025–2030. Independence and solidarity, Romania's vision for a changing world.* https://www.presidency.ro/ro/media/csat/strategia-nationala-de-aparare-a-tarii-pentru-perioada-2025-2030.

Răpan, F. 2019. "Symmetry and asymmetry in current military conflicts." *International Scientific Conference „Gândirea Militară Românească.* Ministry of National Defence Publishing House. pp. 266–281. https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2019%20gmr/2019/Conferinta%20GMR%202019/GMR_CONF%20ro_Rapan.pdf.

Saeed, A. 2024. "Fifth-generation warfare." *Defence Journal.* https://defencejournal.com/2024/04/08/the-5th-generation-warfare/.

Saghin, S. 2026. *Russia handed the U.S. evidence of an alleged Ukrainian attempt to attack Putin. Ukraine's response.* https://stirileprotv.ro/stiri/international/rusia-a-inmanat-sua-dovezi-despre-presupusa-tentativa-de-atac-ucrainean-asupra-lui-putin-cum-raspunde-ucraina.html.

Sciutto, J. 2025. *The return of great powers: Russia, China, and the next world war.* Bucharest: Corint Istorie Publishing House.

Simileanu, V. 2018a. "From frozen conflicts to hybrid warfare I." *GeoPolitica* Anul XVI (Nr. 73 (1)).

___. 2018b. "Hybrid warfare, conceptual approach." *Relații Internaționale. Plus* (Institute of International Relations of Moldova) (nr. 1): 32-43. https://ibn.idsi.md/sites/default/files/imag_file/32-43.pdf.

___. 2019. "The impact of hybrid threats on regional security." *GeoPolitica* Nr. 7.

Stancu, M.C. 2019. "Hybrid warfare and its forms of manifestation in the Ukraine crisis." *Gândirea Militară Românească* Nr. 2: 5-26. https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2019%20gmr/2019/2%202019%20gmr/stancu.pdf.

Tzu, S. 2019. *The art of war.* Bucharest: Cartex Publishing House.

Wither, J.K. 2020. "Defining hybrid warfare." *per Concordiam: Journal of European Security and Defense Issues* (George C. Marshall European Center for Security Studies) 10 (1): 7–9. https://www.marshallcenter.org/sites/default/files/files/2020-05/pC_V10N1_en_Wither.pdf.

Wójtowicz, T. 2021. "Chinese concept of unrestricted warfare: Characteristic and contemporary use." *Humanities and Social Sciences.* https://doi.org/10.7862/RZ.2021.HSS.39.