BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Contemporary Warfare and the Transformation of the Global Military Paradigm

MAJ Cristian-Alexandru SALAC, PhD Candidate*

*Ministry of National Defence
e-mail: salac_cristian@yahoo.com

Abstract

This article analyzes the transformation of the global military paradigm in the context of the technological and strategic developments of the 21st century, using a qualitative approach based on the analysis of specialized literature and the conceptual interpretation of contemporary conflicts. The analysis employs illustrative examples from the Russo-Ukrainian War, the Nagorno-Karabakh conflict, and the field of cyber operations in order to highlight recent transformations of the operational environment. The findings indicate that contemporary warfare is evolving toward a multidimensional model in which the cyber, information, economic, and space domains are becoming as relevant as the traditional military dimension.

The analysis shows that emerging technologies – digitalization, artificial intelligence, drones, and orbital infrastructures – not only support military operations, but also reshape the criteria of strategic superiority, favoring actors capable of coherently integrating information and innovation. Furthermore, the cyber and information dimensions enable the conduct of persistent strategic competition below the threshold of open armed conflict.

The results highlight the need to adapt military structures to a multidomain operational model characterized by interdependence, decision-making speed, and technological integration. This paper contributes to the conceptual clarification of contemporary warfare and emphasizes the strategic implications of ongoing transformations for global security.

Keywords:
Contemporary Warfare; Hybrid Warfare; Cybersecurity; Multi-domain Operations; Emerging Technologies; Information Superiority.

Article info
Received: 29 January 2026; Revised: 19 February 2026; Accepted: 17 March 2026; Available online: 30 June 2026

Citation: Salac, C.A. 2026. "Contemporary Warfare and the Transformation of the Global Military Paradigm." *Bulletin of "Carol I" National Defence University*, 15(2): 257-272. https://doi.org/10.53477/2284-9378-26-27

© „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)

Introduction

The developments in the security environment over recent decades indicate a profound structural transformation in the nature of warfare and in the way military power is conceived, organized, and employed. Contemporary conflicts can no longer be analyzed exclusively through the lens of conventional armed confrontations between states, but must instead be understood as multidimensional processes conducted simultaneously across interconnected domains – physical, information, economic, cyber, and space-related (Freedman 2017, 45-52; Mazarr 2015, 3-7).

Concepts such as hybrid warfare, gray-zone competition, information operations, and cyber conflicts have become essential for understanding the new dynamics of international security. Digital technologies, artificial intelligence, autonomous systems, and orbital infrastructures are no longer merely support tools, but structural factors that influence the distribution of power and the doctrinal architecture of armed forces (Horowitz 2010, 4-8; Johnson 2022, 1397).

The purpose of this research is to analyze the manner in which the technological and strategic transformations of the 21st century contribute to redefining the global military paradigm and shaping a persistent multidimensional conflict model characterized by the simultaneous integration of conventional and non-conventional instruments.

To achieve this purpose, the paper pursues the following research objectives:

identifying the main characteristics of contemporary warfare in relation to the traditional paradigm;

- analyzing the role of emerging technologies in the transformation of modern conflicts;
- examining the impact of the cyber and informational dimensions on security;
- evaluating the implications of these transformations on the organization and functioning of modern armed forces.

In order to provide structure to the analytical approach, the following research questions are formulated:

1. To what extent do current technological transformations alter the nature of armed conflicts?
2. What is the role of the cyber and informational dimensions in redefining power relations?
3. How do these developments influence the organization and functioning of the modern military?

Through this approach, the paper contributes to the conceptual clarification of contemporary warfare and highlights the strategic implications of ongoing transformations for global security and the organization of armed forces, in line

with recent directions emphasized in the literature on security and strategic studies (Manolache 2023, 164).

1. Research Methodology

This paper is based on a qualitative, analytical, and conceptual approach, suitable for studying complex phenomena in the field of international security and the transformation of contemporary conflicts. Given the dynamic and multidimensional nature of modern warfare, the research aims to identify and interpret the main strategic, technological, and doctrinal trends influencing the redefinition of the global military paradigm.

The units of analysis used in this research consist of relevant contemporary conflicts (the Russo-Ukrainian War and the Nagorno-Karabakh conflict), recent doctrinal developments (multi-domain operations), and technological transformations applied to the military environment (drones, cyber capabilities, and artificial intelligence). The analysis seeks to identify the relationships among technological development, changes in the operational environment, and the doctrinal adaptation of military actors.

The comparative analysis was conducted by relating the analyzed cases and developments to three main criteria: the expansion of conflict into non-conventional domains, the integration of emerging technologies, and the transformation of military actors' decision-making and operational processes.
The methodological approach primarily employs a literature review, selecting relevant academic works from the fields of strategic studies, international security, and military technologies. The analyzed sources include articles from indexed journals, monographs, and research reports, which provide both theoretical perspectives and interpretations of recent developments in the security environment. The selection of sources was based on their relevance, timeliness, and contribution to understanding the transformation of contemporary warfare.
In order to increase analytical consistency, the research also uses illustrative examples from recent conflicts to highlight the practical applicability of the analyzed concepts and the manner in which technological transformations influence the conduct of contemporary operations.

The study also employs the comparative analysis method to highlight the differences and continuities between the traditional paradigm of warfare and contemporary forms of conflict, such as hybrid warfare, gray-zone competition, and cyber confrontations. This method enables the identification of novel elements and the determining factors of change, particularly in relation to the development of emerging technologies.
Furthermore, the paper uses conceptual analysis aimed at clarifying and defining key concepts such as "hybrid warfare," "multi-domain operations," "cybersecurity,"

and "persistent strategic competition." This approach contributes to a coherent understanding of the theoretical framework and to the integration of various perspectives existing in the specialized literature.

The data analysis methods are predominantly qualitative, based on critical interpretation, information correlation, and the identification of causal relationships between the analyzed variables (technology, strategy, actors, and operational environments). The research does not employ quantitative methods or statistical instruments, as its primary objective is to explain and understand phenomena rather than measure them.
The limitations of the research derive from the predominantly theoretical nature of the analysis and the absence of extensive empirical studies or quantitative datasets. Nevertheless, the conceptual-analytical approach makes it possible to highlight major trends and formulate relevant conclusions regarding the evolution of contemporary conflicts.
By employing these methods, the research aims to provide an integrated perspective on the transformation of the global military paradigm and to contribute to the development of the conceptual framework necessary for analyzing warfare in the 21st century.

2. The Metamorphosis of Warfare in the 21st Century

The 21st century marks a profound transformation of warfare, not only in technological terms, but also in conceptual and strategic ones. The analysis of recent developments in the security environment highlights the fact that contemporary conflicts can no longer be reduced to conventional military confrontations between states, but must instead be understood as multidimensional phenomena in which the physical, information, economic, and cyber domains interact continuously (Freedman 2017, 48-49).

The analyzed transformations indicate a structural change in the way power is exercised, reflected in the expansion of the battlefield beyond the classical military dimension. This evolution suggests that contemporary warfare is acquiring the characteristics of a continuous process marked by ambiguity, interdependence, and persistent competition below the threshold of open conflict (Mazarr 2015, 6-7). Strategic relevance is no longer determined exclusively by the ability to project force, but by the capability of actors to integrate military and non-military instruments into a coherent framework of influence.

2.1. The Transition from Conventional Conflicts to Hybrid Warfare

Hybrid warfare represents one of the most relevant manifestations of the transformation of conflict in the 21st century. Specialized literature indicates that these forms of conflict are characterized by the integration of conventional military actions with non-traditional tactics, such as cyberattacks, disinformation campaigns,

economic pressure, and the use of proxy actors (Hoffman 2018, 30).
It can be observed that the defining characteristic of hybrid warfare lies in the adaptive synchronization of these instruments, aimed at exploiting the adversary's systemic vulnerabilities. In this sense, the strategic objective is no longer necessarily the immediate control of territory, but rather political and institutional destabilization (Mazarr 2015, 10-11).
Recent conflicts, particularly the war in Ukraine, suggest that hybrid actions may precede and accompany conventional operations, confirming their integrated and flexible nature (Watling 2023, 5-6). Therefore, the hypothesis according to which contemporary warfare is evolving toward a multidimensional model, in which non-conventional instruments become essential, is confirmed.
The Russo-Ukrainian War represents one of the most relevant examples of the convergence between conventional operations and hybrid instruments. Beginning with the annexation of Crimea in 2014 and continuing with the 2022 invasion, the Russian Federation combined classical military operations with cyberattacks, disinformation campaigns, and energy pressure. The synchronized use of these instruments aimed not only at achieving territorial advantages but also at the political and psychological destabilization of the adversary.

2.2. State and Non-State Actors in the New Conflict Dynamics

The interaction between state and non-state actors constitutes a defining element of contemporary conflicts. Non-state actors no longer represent merely peripheral entities, but rather relevant actors capable of influencing strategic dynamics at both the regional and global levels (Salehyan 2009, 16-17).
Through the use of transnational networks, the information environment, and infrastructural vulnerabilities, these actors are capable of generating strategic effects disproportionate to the resources they possess. This evolution confirms the growing asymmetry of conflicts, in which the advantage no longer belongs exclusively to actors with conventional military superiority (IISS 2024, 15-16).
The interdependence between state and non-state actors contributes to increasing the complexity of conflicts, requiring the development of integrated strategies that combine military, political, and information instruments. In this context, international cooperation and collective security mechanisms become essential for managing emerging risks.

2.3. The Gray Zone and Competition Below the Threshold of Direct Confrontation

The concept of the "gray zone" describes a spectrum of strategic competition situated between peace and war, in which actors seek to obtain advantages through ambiguous, gradual, and difficult-to-attribute actions. Conceptual analysis highlights that this form of competition represents a defining characteristic of the contemporary security environment (Mazarr 2015, 6-7).
Operations conducted within the gray zone, including cyberattacks, information influence campaigns, and economic pressure, enable the gradual erosion of an adversary's security without triggering open conflict. This approach reduces the risk

of direct escalation and complicates deterrence processes and strategic responses (NATO 2022, 5-7).

Recent NATO strategic documents emphasize that hybrid threats and persistent competition below the threshold of armed conflict represent one of the principal challenges to Euro-Atlantic security, as they combine military and non-military instruments in a manner that is difficult to attribute and counter (NATO 2022, 5-7).

Gray-zone competition confirms the transformation of warfare into a continuous process characterized by persistent and multidimensional pressure and strongly demonstrates the hypothesis that the traditional distinction between peace and war is becoming increasingly blurred, being replaced by a continuum of strategic confrontation.

3. Technology as a Transformative Force in Contemporary Warfare

Technology represents one of the principal factors driving the profound transformation of contemporary warfare, influencing not only tactical capabilities but also the way military power is conceived and employed at the strategic level. The analysis of specialized literature highlights that the integration of emerging technologies alters the distribution of power and the competitive advantage among actors, favoring those capable of rapidly adopting and integrating innovation (Horowitz 2010, 4–8).

Military superiority is no longer determined exclusively by material resources or the size of armed forces, but by the ability to integrate technology into coherent operational structures and to exploit informational advantages (Horowitz 2010, 15; Biddle 2022, 32).

3.1. The Digital Revolution and Its Impact on Military Tactics

The digital revolution constitutes one of the main structural factors behind the transformation of contemporary warfare, simultaneously influencing the tactical, operational, and strategic levels. The integration of information technologies into military structures has generated an operational environment characterized by extensive connectivity and continuous data flows. This process enables the real-time analysis and utilization of data originating from multiple sources. Recent literature highlights that digitalization redefines the manner in which military power is generated and employed, surpassing the traditional paradigm based on material superiority (Jensen, Valeriano, and Maness 2019, 212–214).

The results of the analysis indicate that information becomes an essential force multiplier, while operational success increasingly depends on the ability to collect, integrate, and exploit data at a faster pace than the adversary. The integration of digital technologies leads to the compression of the decision-making cycle and to the growing relevance of information superiority, which enables actors to obtain strategic advantages even under conditions of material inferiority (Biddle 2022, 35).

At the tactical level, digitalization facilitates the coordination of dispersed units and the integration of weapon systems into common networks, contributing to increased

operational flexibility. At the same time, this dependence on digital infrastructures generates significant vulnerabilities, as information systems become targets for cyberattacks capable of producing disproportionate strategic effects (Kello 2013, 18-21). Therefore, the hypothesis according to which the digital revolution fundamentally transforms the logic of military action, shifting the emphasis from quantitative superiority to informational superiority, is confirmed.

3.2. Drones and the Reduction of Technological Monopoly

The proliferation of unmanned aerial vehicles (UAVs) represents one of the most significant technological developments in contemporary warfare, contributing to changes in the balance of power and reducing barriers to access to aerial capabilities. Specialized literature shows that drones enable both states and non-state actors to conduct surveillance, reconnaissance, and precision-strike operations at relatively low costs (Boyle 2015, 4).

These systems contribute to the reduction of technological monopoly, redistributing strategic advantage and favoring the emergence of asymmetric forms of conflict. Recent conflicts, particularly the war in Ukraine, demonstrate the central role of drones in transforming combat tactics and increasing the importance of remote operations, where precision and adaptability become decisive factors (Watling 2023, 5-6).

The Nagorno-Karabakh conflict (2020) highlighted the major impact of drones on the balance of power at the tactical and operational levels. Azerbaijan employed Bayraktar TB2 drones and loitering munitions to neutralize Armenian air defense systems and armored equipment, demonstrating the capacity of relatively accessible systems to produce significant strategic effects. Subsequently, the war in Ukraine confirmed this trend through the large-scale use of FPV drones for the identification and engagement of targets in real time.

These developments suggest that the accessibility of autonomous technologies reduces the exclusive advantage of traditional military actors and encourages the emergence of asymmetric forms of competition based on flexibility and rapid adaptation.

Analyses conducted by the Royal United Services Institute show that the use of tactical drones in Ukraine contributed to reducing the time between target identification and strike execution, significantly increasing the effectiveness of artillery and reconnaissance operations (Watling 2023, 18-19).

Therefore, drones represent not merely a technological instrument, but a factor that directly influences the conduct of conflicts and the distribution of power among actors.

3.3. Artificial Intelligence, Autonomous Systems, and the Automation of the Battlefield

The integration of artificial intelligence and autonomous systems into the military domain marks a significant stage in the transformation of contemporary warfare. These technologies enable the rapid analysis of data, pattern identification, and the optimization of operational decisions under conditions of high uncertainty (Scharre 2018, 37-38).

The results of the analysis indicate that artificial intelligence contributes to accelerating the decision-making cycle and increasing operational efficiency, becoming an information-based force multiplier. Recent literature emphasizes that the use of autonomous systems raises significant ethical and strategic challenges, particularly regarding decision-making responsibility and human control over the use of force (Johnson 2022, 1397-1399).

Recent studies on the integration of artificial intelligence into the military domain suggest that the automation of analytical and decision-support processes may fundamentally alter the pace and logic of contemporary conflicts (Payne 2021, 76–77). Moreover, recent analyses concerning the integration of artificial intelligence into military affairs suggest that autonomous systems will significantly influence decision-making speed and the architecture of future operations (Konaev 2023, 15-16).

Therefore, the analysis highlights that the integration of artificial intelligence transforms not only military capabilities but also the very nature of decision-making in warfare.

3.4. The Militarization of Space and Orbital Infrastructures

Outer space has become an essential operational domain for the conduct of modern military operations, providing decisive strategic advantages in communications, navigation, and surveillance. Recent analyses in the field of strategic studies indicate that orbital infrastructures are directly integrated into the architecture of multidomain operations (Manolache 2023, 163).

Dependence on these infrastructures generates critical vulnerabilities, since the disruption or destruction of space systems may affect command-and-control capabilities. In addition, the development of anti-satellite capabilities and cyberattacks against orbital systems amplifies the risks associated with space security. Thus, the trend toward the expansion of conflict into new domains, including outer space, is confirmed, reinforcing the multidimensional character of contemporary warfare.

4. The Cyber Dimension of Conflict: A Vector in Contemporary Warfare

The cyber dimension has become a central component of contemporary conflicts, redefining the manner in which power is exercised in international relations. Unlike the traditional domains of confrontation, cyberspace enables the conduct of operations with significant strategic impact without the mobilization of conventional military force, altering the relationship among cost, attribution, and strategic effect in contemporary competition (Kello 2013, 7; Schmitt 2017, 3).

Specialized literature emphasizes the fact that cyber operations can influence political, economic, and social processes, affecting the stability of states without necessarily generating a direct military response (Kello 2013, 8). The difficulty of attributing attacks, combined with the relatively low costs of conducting them, encourages the use of cyber instruments as part of persistent strategic competition.

In this context, control over digital infrastructures and information flows becomes an essential element of power.

4.1. Cyberattacks and the Vulnerability of Critical Infrastructures

Cyberattacks against critical infrastructures highlight the vulnerabilities generated by the extensive digitalization of modern societies. Energy, financial, communication, and transportation systems are deeply interconnected, and this interdependence creates the conditions for cascading effects, in which the disruption of one element may affect the entire system.

A relevant example is the cyberattack against Ukraine's energy infrastructure in 2015, which caused power outages affecting approximately 230,000 people. The operation demonstrated that cyberattacks can generate significant strategic effects without the use of conventional armed force, highlighting the vulnerability of digitally integrated critical infrastructures.

Analyses in the specialized literature show that such attacks can produce major dysfunctions without the use of armed force, affecting the functioning of essential services and generating economic and social instability (Kello 2013, 18-19). Recent examples, including cyber operations associated with the conflict in Ukraine, highlight the ability of these actions to amplify the effects of confrontation through the disruption of critical infrastructures.

The asymmetric character of cyberattacks enables actors with limited resources to generate disproportionate strategic effects. This reality alters the traditional logic of conflict, in which material superiority no longer guarantees security. Consequently, the protection of critical infrastructures becomes a strategic priority, while cybersecurity is increasingly integrated into national defense policies.

4.2. Information Warfare: Disinformation and Strategic Manipulation

Information warfare constitutes an essential dimension of contemporary conflicts, in which influencing perceptions becomes a strategic objective in itself. The development of digital platforms and social networks has facilitated the conduct of disinformation campaigns capable of affecting social cohesion and decision-making processes at both the national and international levels.

Recent studies highlight that informational manipulation can erode trust in institutions, amplify social polarization, and influence electoral behavior, thereby contributing to the internal destabilization of states (Jensen, Valeriano, and Maness 2019, 219). Unlike traditional propaganda, these operations employ algorithms and digital amplification mechanisms that enable the rapid and widespread dissemination of content.

This dynamic reflects a significant change in the way power is exercised, in which control over narratives becomes as important as military superiority. In this context, the distinction between truthful information and disinformation becomes increasingly difficult, complicating response and counteraction processes.

4.3. Cyber Defense and the Development of National Resilience

The growing complexity of cyber threats has led to a paradigm shift in the approach to security, moving from the strictly technical protection of systems toward the development of resilience. This involves not only preventing attacks, but also the ability to absorb their impact and rapidly restore the functioning of affected systems. Specialized literature points out that cyber resilience requires the integration of institutional mechanisms, coherent public policies, and cooperation between the public and private sectors. The interdependence of critical infrastructures means that security can no longer be ensured exclusively at the national level, making international coordination necessary.

In this context, the capacity of states to manage cyber risks becomes an essential indicator of security. Continuous adaptation to the evolution of threats and the development of rapid-response mechanisms are fundamental elements for maintaining stability in the digital environment.

4.4. The Integration of Cyber Capabilities into Military and Geopolitical Strategies

The cyber dimension has progressively been integrated into military and geopolitical strategies, becoming an instrument for the projection of power and strategic influence. States are developing offensive cyber capabilities that enable them to conduct espionage, disruption, and influence operations without crossing the threshold of open armed conflict.

This evolution extends the logic of gray-zone competition, in which strategic pressure is exerted through non-conventional instruments, exploiting ambiguity and the difficulty of attribution (Mazarr 2015, 3-7). Within this framework, conflict is no longer limited to discrete episodes of confrontation, but acquires the character of a continuous process.

The integration of the cyber dimension into state strategies influences the global balance of power, as digital capabilities become an essential element of strategic competitiveness. This reality requires the development of adapted doctrinal and legal frameworks, as well as the strengthening of international cooperation for managing associated risks.

Recent literature in the field of international law applicable to cyberspace highlights the difficulties in defining the threshold between cyber operations and acts of aggression, as well as the problems related to attribution and state responsibility (Schmitt 2017, 11-12).

5. The Transformation of the Modern Military

The transformation of the modern military reflects the adaptation of military structures to a security environment characterized by complexity, interdependence, and the accelerated pace of technological change. Armed forces can no longer be analyzed exclusively through the lens of troop size or conventional capabilities, but rather as integrated systems capable of operating simultaneously across multiple domains and exploiting the advantages provided by emerging technologies.

Specialized literature highlights that this transformation has a dual dimension: on the one hand, technological, through the integration of digital systems and artificial intelligence, and on the other hand, organizational, through the adaptation of doctrines and decision-making processes (Manolache 2023, 169-170). The accelerated pace of change requires the development of flexible structures capable of responding rapidly to developments in the operational environment.

5.1. The Concept of Multi-Domain Operations (MDO)

The concept of Multi-Domain Operations (MDO) reflects the evolution of military thinking toward the simultaneous integration of effects across the land, air, naval, cyber, and space domains. This approach goes beyond the traditional logic of combined operations, emphasizing rapid coordination and the synchronization of capabilities in complex operational environments.

Recent doctrinal strategies developed by the U.S. Department of Defense emphasize the necessity of integrating capabilities from all operational domains into a common command-and-control architecture based on rapid data exchange and real-time coordination (U.S. Department of Defense 2022, 11-13).

The Multi-Domain Operations concept is reflected in recent U.S. Army doctrine, which aims to integrate effects generated across the land, air, naval, cyber, and space domains into a unified command-and-control system. The conflict in Ukraine demonstrates the applicability of this model through the integration of satellite imagery, tactical drones, and precision artillery into an accelerated decision-making cycle.

Recent analyses emphasize that operational success depends on the ability to integrate information originating from multiple domains and to generate convergent effects against the adversary (Manolache 2023, 165-166). System interconnectivity and data-processing speed become determining factors of military effectiveness, while superiority is no longer associated with control over a single domain, but rather with the capacity to act coherently across all domains.

This evolution implies significant doctrinal and organizational adaptations, including the development of command structures capable of managing the complexity of multidomain operations.

5.2. The Digitalization of Logistics and the Optimization of Supply Chains

Military logistics has undergone an accelerated process of transformation driven by the integration of digital technologies and the increasing complexity of the operational environment. Modern systems enable the real-time monitoring of resources, the anticipation of logistical requirements, and rapid adaptation to changes on the battlefield.

Studies in the field show that the digitalization of logistics contributes to increased operational efficiency by reducing uncertainty and optimizing resource distribution. Supply chains become more transparent and flexible, enabling the sustainment of operations in contested or unstable environments.

This transformation changes the role of logistics, which is no longer merely a support function but a strategic element capable of directly influencing operational

outcomes. The ability to ensure continuity of supply and manage disruptions becomes an essential factor of military success.

5.3. Interoperability and the Modernization of Allied Forces

Interoperability represents a fundamental condition for the effective functioning of contemporary military alliances. The technological compatibility of systems, the harmonization of doctrines, and the standardization of procedures enable the conduct of joint operations and reduce operational friction.

Specialized literature highlights that interoperability is not limited to technical aspects, but also includes organizational and cultural dimensions. Multinational exercises and information sharing contribute to strengthening collective response capabilities and increasing operational cohesion.

The modernization of allied forces is closely linked to the integration of emerging technologies and the development of common command-and-control systems. This evolution strengthens the ability of alliances to respond rapidly and effectively to contemporary threats.

5.4. The Role of Emerging Technologies in the Transformation of Military Mindset

Emerging technologies influence not only the technical capabilities of armed forces but also the manner in which military thinking is conceived. The integration of artificial intelligence and autonomous systems drives the transition from linear planning to adaptive decision-making processes based on the continuous analysis of data.

Recent studies highlight that this transformation involves a redefinition of the role of the human factor, which must manage interaction with automated systems and understand their limitations (Johnson 2019, 1417-1418). Military decision-making becomes the result of collaboration between humans and technology, raising challenges related to responsibility and control.

This evolution requires the development of an organizational culture oriented toward innovation, continuous learning, and adaptability. Armed forces capable of integrating these technologies into flexible structures may obtain significant advantages in a strategic environment characterized by uncertainty and persistent competition.

The analysis suggests that the future of global conflicts will be dominated by persistent forms of multidomain competition, in which information, cyber, and economic instruments will become as relevant as the direct use of military force. This trend indicates the emergence of a conflict model characterized by permanent strategic competition and the simultaneous integration of pressure across multiple operational domains.

6. Perspectives on the Future of Global Conflicts

The evolution of global conflicts indicates a structural transformation in the way strategic competition is conducted, marking a transition from high-intensity

conventional confrontations toward persistent forms of multidimensional competition. Economic interdependence, accelerated digitalization, and the development of emerging technologies contribute to shaping a security environment in which strategic pressure can be exercised continuously without crossing the threshold of open armed conflict (Mazarr 2015, 3-7; NATO 2022, 5-7).
This evolution reflects a change in the logic of conflict, in which the gradual accumulation of effects on infrastructures, perceptions, and decision-making processes becomes more relevant than achieving decisive victories on the battlefield. Recent studies emphasize that state actors increasingly prefer the use of indirect instruments capable of generating strategic advantages without direct military escalation (Jensen, Valeriano, and Maness 2019, 212–214).

A central element of future conflicts is the deep integration of the cyber dimension into geopolitical strategies. Cyberspace offers opportunities for conducting influence operations, sabotage, and intelligence gathering, all characterized by difficulties of attribution and low operational costs. This reality encourages the development of strategies based on continuous pressure, in which cyber, information, and economic instruments are used in an integrated manner to alter the balance of power.

At the operational level, future conflicts will be characterized by the acceleration of the decision-making cycle and the integration of autonomous systems into combat processes. The ability to rapidly correlate information from multiple sources and generate coordinated effects across several domains becomes a determining factor of military effectiveness. Specialized literature highlights that superiority is no longer associated exclusively with the mass of forces, but with the capacity to integrate technology, information, and organizational structures into a coherent system (Manolache 2023, 168-170).

Another defining element is the growing role of non-state actors and asymmetric conflicts. These actors are capable of exploiting infrastructure and information vulnerabilities of states, generating strategic effects without possessing comparable conventional military capabilities. This trend contributes to the complexity of the security environment and to the difficulty of conflict management.
In the long term, international stability will depend on the ability of actors to manage the balance between technological innovation and regulatory mechanisms. The accelerated development of artificial intelligence, autonomous systems, and cyber capabilities raises issues related to control, responsibility, and predictability. The absence of clear normative frameworks may amplify risks and increase systemic instability.
The future of global conflicts will be defined by persistent competition, in which the distinction between peace and war becomes increasingly difficult to delineate. The ability of states to integrate technology, develop resilience, and manage the complexity of the security environment will represent a decisive factor in maintaining strategic advantage.

Conclusions

The analysis confirms that contemporary warfare has undergone a structural transformation, evolving from the paradigm of conventional confrontations toward a multidimensional model in which the cyber, informational, economic, and space domains acquire an importance comparable to the traditional military dimension. This evolution supports the hypothesis that the nature of conflict in the 21st century is defined by interdependence, ambiguity, and persistent competition below the threshold of direct confrontation.

The examination of the role of emerging technologies highlights that digitalization, artificial intelligence, and autonomous systems represent not merely instruments of operational efficiency, but factors that reconfigure power relations and the conduct of conflicts. The ability to integrate and exploit information becomes a central determining element of strategic advantage, confirming the hypothesis regarding the transformation of the criteria of military superiority.
The analyzed examples, such as the Russo-Ukrainian War, the use of drones in the Nagorno-Karabakh conflict, and cyber operations against critical infrastructures, demonstrate that strategic advantage is increasingly determined by the capacity for multidomain integration and the rapid exploitation of information.
The cyber and information dimensions demonstrate that the disruption of critical infrastructures and the exploitation of digital vulnerabilities enable the exercise of continuous strategic pressure without direct military escalation.

From a methodological perspective, the use of a qualitative, analytical, and conceptual approach, based on the analysis of specialized literature and the comparison between traditional and contemporary forms of conflict, made it possible to identify coherent trends and causal relationships among technology, strategy, and the transformation of the military paradigm. This approach provides a relevant interpretative framework for understanding the evolution of conflicts in the 21st century.
The theoretical contribution of the paper consists of integrating the concepts of hybrid warfare, multidomain operations, and gray-zone competition into a unified interpretative model of contemporary conflict. The analysis supports the idea that modern warfare is evolving toward a persistent form of multidimensional strategic competition, in which the distinction between peace and conflict becomes increasingly difficult to establish.

The analysis also emphasizes that strategic advantage is no longer determined exclusively by material resources, but by the capacity to integrate technology, information, and decision-making processes into a coherent and adaptable system. This conclusion has direct implications for the manner in which states shape their defense strategies and develop their military capabilities.
The paper provides an analytical perspective on the transformation of contemporary warfare and contributes to clarifying the relationship between technology, strategy,

and security, highlighting the main directions of evolution of global conflicts.
Based on the analysis conducted, the paper proposes the interpretation of contemporary warfare through the concept of "persistent multidimensional conflict," defined as a form of strategic competition conducted simultaneously across the military, cyber, information, economic, and space domains, characterized by continuity, strategic ambiguity, and technological integration. Unlike the classical paradigm of conventional confrontation, this model highlights that strategic advantage is determined primarily by the ability of actors to integrate information, technology, and simultaneously applied pressure across multiple domains into a coherent mechanism of influence and operational adaptation.

However, the present research has certain limitations generated by its predominantly conceptual character and the absence of quantitative empirical analyses or in-depth case studies. Although the adopted approach enables the identification of major trends and the formulation of relevant conclusions, the integration of empirical data could strengthen the validity of the results.
Future research could focus on the comparative analysis of recent conflicts, the use of mixed methods (qualitative and quantitative), and the evaluation of the impact of emerging technologies on different categories of actors. Furthermore, exploring the relationship between artificial intelligence, decision-making autonomy, and strategic stability represents a relevant direction for the further development of the field.

References

Biddle, Stephen. 2022. "Back in the Trenches: Why Attrition Still Dominates the Battlefield." International Security 46(4): 32-35. https://direct.mit.edu/isec/article/46/4/7/109111/Back-in-the-Trenches-Why-Attrition-Still.

Boyle, Michael J. 2015. "The Legal and Ethical Implications of Drone Warfare." International Journal of Human Rights 19(2): 4. https://doi.org/10.1080/13642987.2014.991210.

Freedman, Lawrence. 2017. The Future of War: A History. New York: Public Affairs.

Hoffman, Frank G. 2018. "Examining Complex Forms of Conflict: Gray Zone and Hybrid Warfare." PRISM 7(4): 30-47. https://ndupress.ndu.edu/Media/News/Article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/.

Horowitz, Michael C. 2010. The Diffusion of Military Power: Causes and Consequences for International Politics. Princeton, NJ: Princeton University Press.

International Institute for Strategic Studies (IISS). 2024. "The Military Balance 2024." The Military Balance 124(1): 15-16. London: Routledge. https://doi.org/10.4324/9781003485834.

Jensen, Benjamin M., Brandon Valeriano, and Ryan C. Maness. 2019. "Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist." Journal of Strategic Studies 42(2): 212-219. https://doi.org/10.1080/01402390.2018.1559152.

Johnson, James. 2019. "Artificial Intelligence & Future Warfare: Implications for International Security." International Affairs 95(6): 1397-1418. https://doi.org/10.1093/ia/iiz125.

Manolache, Ionela Cătălina. 2023. "The Role of Multi-Domain Operations in Modern Warfare." Land Forces Academy Review 28(3): 163-170. https://doi.org/10.2478/raft-2023-0020.

Kello, Lucas. 2013. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." International Security 38(2): 7-21. https://doi.org/10.1162/ISEC_a_00138.

Konaev, Margarita. 2023. The Future of Conflict: Autonomous Systems and Artificial Intelligence. Washington, DC: Center for Security and Emerging Technology (CSET).

Mazarr, Michael J. 2015. Mastering the Gray Zone: Understanding a Changing Era of Conflict. Santa Monica, CA: RAND Corporation. https://doi.org/10.7249/RR1003.

NATO. 2022. NATO Strategic Concept. Brussels: North Atlantic Treaty Organization. https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf.

Payne, Kenneth. 2021. I, Warbot: The Dawn of Artificially Intelligent Conflict. London: Hurst Publishers.

Salehyan, Idean. 2009. Rebels without Borders: Transnational Insurgencies in World Politics. Ithaca, NY: Cornell University Press. https://www.degruyterbrill.com/document/doi/10.7591/9780801459214/html.

Scharre, Paul. 2018. Army of None: Autonomous Weapons and the Future of War. New York: W. W. Norton & Company.

Schmitt, Michael N. 2017. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316822524.

U.S. Department of Defense. 2022. Joint All-Domain Command and Control (JADC2) Strategy. Washington, DC: U.S. Department of Defense. https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.pdf.

Watling, Jack. 2023. The War in Ukraine and the Evolution of Modern Warfare. London: Royal United Services Institute (RUSI).