ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

PANTEION UNIVERSITY OF SOCIAL AND POLITICAL SCIENCES

ΣΧΟΛΗ ΔΙΕΘΝΩΝ ΣΠΟΥΔΩΝ, ΕΠΙΚΟΙΝΩΝΙΑΣ ΚΑΙ ΠΟΛΙΤΙΣΜΟΥ

ΤΜΗΜΑ ΔΙΕΘΝΩΝ, ΕΥΡΩΠΑΪΚΩΝ ΚΑΙ ΠΕΡΙΦΕΡΕΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ «ΔΙΕΘΝΕΙΣ ΣΧΕΣΕΙΣ ΚΑΙ ΣΤΡΑΤΗΓΙΚΕΣ ΣΠΟΥΔΕΣ»

Hybrid Threats: Expanding Domains - Cross Domain Effects

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αικατερίνη Βακάκη

Αθήνα, 2022

Τριμελής Επιτροπή

Κωνσταντίνος Αρβανιτόπουλος, Καθηγητής Παντείου Πανεπιστημίου (Επιβλέπων)
Χαράλαμπος Παπασωτηρίου, Καθηγητής Παντείου Πανεπιστημίου
Κωνσταντίνος Κολιόπουλος, Καθηγητής Παντείου Πανεπιστημίου

Δήλωση περί μη λογοκλοπής

Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις, που προβλέπονται από τις διατάξεις της παρ. 6 του άρθρου 22 του Ν.1599/1986, δηλώνω ότι:

Η εργασία που παραδίδω είναι αποτέλεσμα πρωτότυπης έρευνας και δεν χρησιμοποιεί πνευματική ιδιοκτησία τρίτων χωρίς αναφορές. Αναλαμβάνω όλες τις νομικές και διοικητικές συνέπειες σε περίπτωση που αποδειχθεί ότι η εργασία μου αποτελεί προϊόν λογοκλοπής ή προϊόν τρίτων.

Αθήνα, 20.12.2022
Αικατερίνη Βακάκη

Table of Contents

Περίληψη

Τον εικοστό πρώτο αιώνα, η έννοια των υβριδικών απειλών έχει γίνει ιδιαιτέρως δημοφιλής και έχει κυριαρχήσει στις ανησυχίες για την ασφάλεια των κρατών, δεδομένου ότι οι υβριδικές απειλές θολώνουν τις διαχωριστικές γραμμές μεταξύ πολέμου και ειρήνης. Το φαινόμενο χαρακτηρίζεται από τον συνδυασμό καλυμμένων και απροκάλυπτων, συμβατικών και ανορθόδοξων, στρατιωτικών και μη στρατιωτικών μεθόδων και πραγματοποιείται με συντονισμένο τρόπο σε πολλαπλούς τομείς. Η έννοια των "υβριδικών απειλών" στο πλαίσιο αυτής της εργασίας βασίζεται στην έννοια του "υβριδικού πολέμου" που έχει αναλυθεί εκτενώς στην ακαδημαϊκή βιβλιογραφία. Ο όρος "υβριδικές απειλές" θα χρησιμοποιηθεί ως όρος-ομπρέλα που περιλαμβάνει απειλές που κυμαίνονται από οργανωμένες ενέργειες κάτω από το όριο της επίσημης κήρυξης πολέμου με σκοπό την εκμετάλλευση συστημικών αδυναμιών των κρατών για την επίτευξη πολιτικών σκοπών, έως συνδυασμένες ενέργειες οι οποίες διεξάγονται σε εμπόλεμη κατάσταση και δεν περιορίζονται στο φυσικό πεδίο της μάχης. Σε αυτό το πλαίσιο, τίθεται το ερώτημα ποια είναι ακριβώς η έννοια των υβριδικών απειλών και σε ποιους τομείς εμφανίζονται οι υβριδικές απειλές στο σύγχρονο πολιτικό και στρατηγικό περιβάλλον.

Σκοπός αυτής της εργασίας είναι να εξετάσει, να κατανοήσει και να αναλύσει τις υβριδικές απειλές και να παρουσιάσει τους τομείς στους οποίους ενεργούν οι υβριδικοί δρώντες για να επιτύχουν τους πολιτικούς και στρατηγικούς τους στόχους. Συγκεκριμένα, στο Μέρος Ι, η πρώτη ενότητα αναλύει τις υβριδικές απειλές ως γενική έννοια, περιγράφοντας το θεωρητικό πλαίσιο που εξηγεί την χρήση των υβριδικών απειλών στο πλαίσιο των διεθνών σχέσεων, τον ορισμό των υβριδικών απειλών και την πιθανή κλιμάκωση των ενεργειών σε υβριδικό πόλεμο. Η επόμενη ενότητα αυτού του μέρους εξετάζει την προέλευση και την εξέλιξη, τον ορισμό και τις διαστάσεις του υβριδικού πολέμου ως τη θεμελιώδη έννοια που αναλύεται στη βιβλιογραφία. Στο Μέρος ΙΙ της εργασίας γίνεται εκτενής αναφορά στους τομείς που εμφανίζονται και αλληλοεπιδρούν οι υβριδικές απειλές. Συγκεκριμένα, οι υβριδικές απειλές αφορούν τη χρήση συμβατικών και αντισυμβατικών μέσων στο επίπεδο του πολέμου και τρομοκρατίας και εγκληματικής συμπεριφοράς καθώς και την εφαρμογή διαφορετικών μέσων και μεθόδων στον πολιτικό και διπλωματικό, οικονομικό τομέα, στον τομέα πληροφοριών και μέσων ενημέρωσης, στον κοινωνικό τομέα, στον τομέα πληροφορικής, στον επιστημονικό και τεχνολογικό τομέα και τέλος στον νομικό τομέα. Το τελευταίο τμήμα αυτού του μέρους

αναφέρεται στην θεωρία της αποτροπής ως θεμελιώδη στρατηγική για την αντιμετώπιση υβριδικών απειλών.

Abstract

In the twenty-first century, the concept of hybrid threats has become very popular and it has dominated the security concerns of States as hybrid threats blur the lines between war and peace. The multiplicity of domains and the cross-domain effects of modern hybrid threats add a level of complexity to the portfolio of strategic options, namely the means by which strategic efforts can be achieved. The concept of "hybrid threats" in the context of this dissertation builds on the concept of "hybrid warfare" a phenomenon that has been analyzed extensively in academic literature, and the term is used as an umbrella term that encompasses activities ranging from interference to warfare. In this context, the question arises as to what the concept of hybrid threats is and how they are perceived and realized in postmodern politics and strategy.

The purpose of this dissertation is to examine, understand, and analyze hybrid threats and to present the domains, both in the physical and conceptual dimension, that hybrid actors employ their actions to achieve their political and strategic goals. Specifically, Part I analyzes hybrid threats as an overarching concept by first delineating the theoretical framework that explains the use of hybrid threats in the context of international relations and the definition of hybrid threats as well as the potential escalation of hybrid threat actions to hybrid warfare. The next section of this Part examines the origins and evolution, definition, and characteristics of hybrid warfare as the foundational concept analyzed in the literature. Part II of the dissertation provides a comprehensive analysis of the domains that hybrid threat activity concerns, namely; in the physical dimension, hybrid threats employ conventional/regular and unconventional/irregular means of warfare, terrorism and criminal behavior, and in the conceptual dimension, hybrid threats target the political and diplomatic, economic, information and media, social, information technology, scientific and technological, and legal domains. The final section of this Part relates to deterrence theory and, in particular, cross-domain deterrence as a fundamental strategy for countering hybrid threats.

Introduction

Hybrid threats are a phenomenon as old as conflicts and wars, but one that is being amplified by the changing dynamics of the security environment, new tools and technologies that target vulnerabilities in different areas, with the aim of undermining democratic institutions, deepening polarization, and even challenging the meaning of democracy. Hybrid threats challenge the laws, the order, and the fundamental values in democratic societies by attempting to circumvent and undermine the norms that regulate aggression in both domestic and international contexts. They attempt to expand the scope for aggressive action and transform Clausewitz's famous dictum that "war is a continuation of politics by other means" into hybrid threats that are the continuation of war by other unrestricted means, toward a "creative weaponization of everything"[1]. The multiplicity of means and the cross-domain character of contemporary hybrid threats adds another layer of complexity to the portfolio of strategic options, namely the multiplicity of means by which strategic efforts can be achieved. Historically, the concept of hybridity was used to describe the simultaneous use of regular and irregular means and tactics in the context of warfare. Gradually, however, the meaning of the concept evolved to describe hybrid threats that denote a spectrum of nonviolent to violent activities in both the military and nonmilitary domains. For this reason, hybrid threats are considered as an overarching term, an umbrella concept, that includes activities ranging from interference to warfare.

The history of mankind is a history of battles, and throughout history there have been several attempts to define and characterize the phenomenon of war, which has been the subject of constant study in international relations and military schools. In the postmodern world, as technologies develop, new methods of warfare are introduced. Hybrid warfare is not a brand new phenomenon. There is an impression that we are dealing with a completely new, unprecedented war event or a special novelty of warfare that is difficult to deal with. Hybrid warfare, however, is no different from the war that Sun Tzu described in his work or from the wars that philosophers, sociologists, political scientists, historians, strategists, soldiers, and other thinkers have tried to understand throughout history. But as the world and humanity evolve, so does warfare. What is new about the idea of hybrid warfare is the growing ability of

[1] Hybrid CoE, "Deterring hybrid threats: Towards a fifth wave of deterrence theory and practice", Paper 12, 2022, p. 13; referring to Mark Galeotti, *The Weaponisation of Everything, A field Guide to the New Way of War*, Yale University Press, 2002.

international actors to use all the means at their disposal to exercise power, as technological advances have made it easier to conduct global initiatives in a coordinated manner and achieve synergistic effects in the physical and non physical dimensions of conflict.

The purpose of this dissertation is to examine, understand, and analyze hybrid threats and to present the domains, both physical and conceptual, in which hybrid actors employ their activities to achieve political and strategic goals. Specifically, Part I analyzes hybrid threats as an overarching concept by first describing in Section A the theoretical framework that explains the use of hybrid threats in the context of international relations. The realist paradigm offers the most insightful perspective on explaining the use of threats as an instrument of the State to maximize its power. This section also examines the definition of hybrid threats as a concept and the dynamic spectrum of potential escalation of hybrid threat action to hybrid warfare. Section B of this Part examines the origins and evolution of hybrid warfare taking into consideration that the techniques of hybrid warfare cannot really be called new, as the military thinking associated with it has its roots in history. The basic concept of mixing conventional and irregular tactics to achieve a political goal is consistent with earlier forms of conflict, although the methods by which State and non-State actors wage hybrid war have changed. This section of the dissertation also examines the definition of hybrid warfare as a concept, looking at both the Western and Russian concepts of achieving political and strategic goals in the twenty-first century through hybrid action. Despite the diversity of terms in the academic literature, in all cases it is described as a threat with similar characteristics. The last section of this Part refers to the four characteristics of hybrid warfare: simultaneity, convergence, multimodality, and catastrophic.

Part II of the dissertation provides a comprehensive analysis of the domains which hybrid threats concern. In the physical domain hybrid threats employ conventional/regular and unconventional/irregular means of warfare, terrorism and criminal behavior. In the conceptual domain, the means used cannot usually be considered acts of aggression, so they do not reach the level of war and thus remain in “grey areas”. Such hybrid threats are considered one of the greatest security threats in democratic societies today. The idea behind hybrid threats as a means of “undeclared war” is that they are designed in such a way that they cannot be identified as clear violations of international law in order to exploit the weaknesses of the adversary and blur the lines between war and peace. In the conceptual realm, hybrid threats concern the means employed in the political and diplomatic, economic, information and media, social, information

technology, scientific and technological, and the legal domain. The final Section of this Part addresses the deterrence theory and, in particular, cross-domain deterrence as a concept applicable to hybrid threats and as the fundamental strategy for countering hybrid threats.

PART I. Hybrid threats as an umbrella concept

In an effort to describe the complexity of modern threats in the security environment, which encompass a variety of domains and blur the conventional lines between war and peace, hybrid threats have emerged as the most commonly used term. States aim to achieve their strategic and political goals by combining conventional and non-conventional means into a hybrid strategy. Hybrid can be defined as something heterogeneous that is formed by combining two or more things[2]. Hybrid threats should be examined as the overarching concept that includes a spectrum of activities ranging from interference to war and for this reason the term "hybrid threat" is considered as an umbrella term and hence non-military means become as important as military means of intervention. In this context, hybrid warfare has been referred to by different terms by different organizations, and despite the variety of terms, in all cases it seemed to be one and the same thing, a threat with the same, or almost the same characteristics and at the same time without specific features[3].

Hybrid threats generally have to do with the combination or convergence of different hybrid means, while hybrid conflicts and wars are distinct phenomena in which opposing parties use hybrid threats through specific tactics to achieve their goals and when a situation escalates it can evolve from a hybrid conflict to a hybrid war[4]. Besides, hybrid warfare concerns active hybrid actions by one actor against another, while hybrid threats need not be active actions but can also be passive, i.e., real or perceived threats to possible future actions[5]. Analysts have emphasized that hybrid tactics may often remain below the threshold of war in order to wear down the adversary while avoiding a major confrontation and the risk of mutual destruction, as might be the case in a conflict between nuclear powers[6].

[2] The Britannica Dictionary, "Hybrid", available at: https://www.britannica.com/dictionary/hybrid (last accessed 20.12.2022)
[3] Toumpani Margarita Georgia, *supra* note 3, p. 10.
[4] *Ibid*, pp. 14-15.
[5] Mikael Weissmann, "Conceptualizing and countering hybrid threats and hybrid warfare", in Mikael Weissmann, Niklas Nilsson, Björn Palmertz, Per Thunholm (eds.), *Hybrid Warfare Security and Asymmetric Conflict in International Relations*, I.B. Tauris, 2021, p. 63.
[6] Ofer Fridman, *Russian "Hybrid Warfare": Resurgence and Politicisation,* Hurst & Company, 2018, pp. 157-160.

A. Hybrid threats

1. Hybrid threats in the context of the realist paradigm

The theory of realism provides the most insightful perspective on the explanation behind the use of hybrid threats placing hybrid warfare in the context of power politics. After World War II, classical realism was established as the dominant theory in international relations, dating back to its founding fathers Thucydides, Machiavelli, and Hobbes. The basic propositions of realism are that States are the main actors in an international system that is anarchic and in which they pursue only their own national interests, while the main concern of all States is power and security.

Under the realist paradigm, the State is sovereign and guided by a national interest defined in terms of power[7]. Hans Morgenthau stated that "International politics is a struggle for power. Whatever the ultimate aims of international politics, power is always the immediate aim"[8]. Among the elements of national powers are the material; geography, natural resources, the industrial capacity, military preparedness as well as human factors in quantitative components the size of the population and qualitative as the national character, the national morale and the quality of diplomacy[9]. However, the primary source of power for realists is reliance on military capabilities associated with "hard power" as the main tool for ensuring survival which may be used for improving their position in the international system. Armed strength is considered the most important material factor making for the political power of a nation[10].

One of the important premises of realism is the anarchical structure of the international system since there is no central authority to govern the relations among States[11]. Thus, States are ultimately dependent on their own capabilities, or power, to further their national interests which is called as the "self help system"[12]. The most important national interest then becomes the survival of the State and States seek to maintain their autonomy, their political system and territorial integrity. In this context offensive realists argue that States should maximize power with the ultimate goal of hegemony as the best way to guarantee survival. According to

[7] Hans J. Morgenthau, "The primacy of the National Interest", *The American Scholar,* Volume 18 (2), 1949, pp. 207-212.
[8] Hans J. Morgenthau, *Politics among nations: The struggle for power and peace,* Alfred A. Knopf, 1948, p. 13.
[9] Hans J. Morgenthau, "The primacy of the National Interest", *supra* note 7, pp. 80-108.
[10] Hans J. Morgenthau, *Politics among nations: The struggle for power and peace*, *supra* note 8, p. 14.
[11] Kenneth Waltz, *Theory of International Politics,* Addison-Wesley Publishing Company, 1979, p. 66.
[12] *Ibid,* p. 111.

offensive realists, in such an international environment, States have to deal with their own security problem and ensuring security becomes the main concern of States that should strive for.

According to realists, the international system is unstable and due to the ongoing fight for power it is permanently changing. Due to the status of constant competition and confrontation, the system changes because although there are States with increasing power that are satisfied with their current position in the system (status quo powers) there are also States that are dissatisfied and face a constant incentive to change the distribution of power in their favor (revisionist states)[13]. According to Mearsheimer "great powers are always searching for opportunities to gain power over their rivals, with hegemony as their final goal. This perspective does not allow for status quo powers, except for the unusual state that achieves preponderance. Instead, the system is populated with great powers that have revisionist intentions at their core"[14].

Under realism assuming that States have only one goal, to maximize their power, and that hybrid threats are an instrument of the State, hybrid threats are presented essentially consistent with this theoretical framework. The hybridity of the concept is what makes it more effective and a more available tool for pursuing power interests[15]. Hybrid threats are a means for States to maintain and enhance their power that is inextricably linked to the advancement of national interests. In order to pursue their interests, States may employ hybrid threats and hybrid warfare in order to maximize their share of power at the expense of other States, depending on their political and strategic goals and the geopolitical context. Afterall, according to Morgenthau, "the political objective of war itself is not *per se* the conquest of territory and the annihilation of enemy armies but a change in the mind of the enemy which will make him yield to the will of the victor"[16].

What should be noted at this point is that hybrid means should be distinguished from the exercise of traditional influence and soft power in international relations, although a State may

[13]John Mearsheimer, "Structural Realism", in Tim Dunne, Milja Kurki, Steve Smith (Eds.) *International Relations Theories: Discipline and Diversity*, Oxford University Press, 2010, p. 79.
[14] John Mearsheimer, *The Tragedy of Great Power Politics*, W. W. Norton & Company, 2014, p.77.
[15] Ondřej Filipec, "Hybrid Warfare: Between Realism, Liberalism and Constructivism*", Central European Journal of Politics*, Volume 5(2), 2019, p. 57.
[16] Hans J. Morgenthau, *Politics among nations: The struggle for power and peace*, *supra* note 8, p. 15.

seek to enhance its impact by adding hybrid means[17]. On this note, Joseph Nye differentiates between two types of power; the "hard power" in terms of command and coercion, and the "soft power" as the ability to achieve goals in world politics because of attraction rather than coercion, also known as "the second face of power"[18]. Hybrid threats as a tool of coercion and hybrid warfare are presented as a means of hard power in the international scene.

2. Definition of hybrid threats

International organizations like NATO and the European Union, in addition to academia, are preoccupied with the idea of hybrid threats. Hybrid threats generated attention within NATO in 2010 and the definition of hybrid threats was incorporated into the NATO Capstone Concept as following: "*those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives"*[19]. According to NATO, hybrid threats will have fewer physical or political boundaries, particularly due to the effects of globalization and increased access to international resources and modern communications[20]. NATO asserts that hybrid threats combine military and nonmilitary, covert and overt means, including disinformation, deception, propaganda and sabotage, cyberattacks, economic pressure, the use of irregular armed groups, and the use of regular forces and hybrid methods are used to blur the lines between war and peace in order to destabilize the adversary and undermine society[21].

According to the European Commission, while definitions of hybrid threats vary and must remain flexible to respond to the changing nature of these threats, the concept aims to capture the mix of coercive and subversive activities, conventional and unconventional methods that can be used by State or non-State actors in a coordinated manner to achieve specific objectives

[17] Stefan Hadjitodorov and Martin Sokolov, "Blending New-generation Warfare and Soft Power: Hybrid Dimensions of Russia-Bulgaria Relations", *Connections: The Quarterly Journal*, 17 (1), 2018, p. 19.
[18] Joseph Nye, *Soft Power: The Means to Success in World Politics*, New York: Public Affairs, 2004, p. 5.
[19] North Atlantic Treaty Organization, "Input to a new NATO capstone concept for the military contribution to countering hybrid threats", 2010, p. 2.
[20] NATO, Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats, 2010, p. 3.
[21] NATO, "NATO's response to hybrid threats", 2019, available at: https://www.nato.int/cps/en/natohq/topics_156338.htm (last accessed: 20.12.2022)

while remaining below the threshold of officially declared warfare[22]. The Hybrid CoE, characterizes hybrid threats as coordinated and synchronized actions that use a variety of means to target the systemic vulnerabilities of democratic States and institutions; activities that exploit thresholds for detection and attribution and multiple interfaces; as well as activities designed to influence various forms of decision-making and to fulfill the agent's strategic goals while undermining the target's[23].

3. Escalation of hybrid threats to hybrid warfare

Hybrid threats combine different types of activities with varying intensities, long time frames, and changing geographies, while the actors behind them may operate in the shadows or "grey area" between acceptable and unacceptable, legal and illegal, using a combination of tools to enhance their efforts[24]. According Hybrid CoE, there is a potential escalation of hybrid threat action that could lead to hybrid warfare, beginning with the "priming phase", with interference (mainly psychological) that blurs situational awareness; the "destabilization phase", with the intensification of activities in the form of operations or campaigns to achieve the desired goal, creating the need for response and defense; and finally, "the coercion phase", in which activities reach the threshold of hybrid warfare, which involves a combination of means from all strategic domains with the use of force as the defining element[25]. RAND Corporation distinguishes the severity of the hybrid threat into persistent, i.e., low-threshold and non-military actions that do not violate international law and are very difficult to deter; moderate, i.e. direct and attributable coercive actions by nonmilitary means that exploit grey areas and are difficult to deter because they are below conventional thresholds; and aggressive, i.e., direct, threatening, and attributable quasi-military or military actions that violate international law and norms and can be deterred in advance[26].

[22] European Commission, "Joint Framework on countering hybrid threats a European Union response", Joint Communication to the European Parliament and the Council, 2016, p. 2: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

[23] Hybrid CoE, "Hybrid threats as a concept", https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ (last accessed: 20.12.2022).

[24] Georgios Giannopoulos, Hanna Smith, Marianthi Theocharidou, "The Landscape of Hybrid Threats: A conceptual model", Hybrid CoE, *Publications Office of the European Union*, 2021, p. 36

[25] *Ibid*, pp. 37-42.

[26] Michael Mazarr, Joe Cheravitch, Jeffrey Hornung, Stephanie Pezard, *What Deters and Why, Applying a Framework to Assess Deterrence of Gray Zone Aggression*, RAND Corporation, 2021, p.3.

B. Hybrid warfare

1. Origins and evolution of hybrid warfare

Theorists examine warfare historically as an evolutionary process influenced by societal pressures in addition to technology and the employment of military forces, thus the dual understanding of warfare as both an activity with numerous forms and an evolutionary process paves the way for a clearer understanding of hybrid warfare[27]. Hybrid warfare is a term used to describe modern warfare that encompasses a wide range of warfare techniques that do not conform to earlier notions of warfare, however, none of these techniques can truly be described as new and the military thought associated with them is rooted in history[28]. Hybrid warfare is not a recent phenomenon, since according to academics studying it, there are a number of historical conflicts that show hybrid warfare tactics have been used since ancient times. As NATO's Secretary General Jens Stoltenberg comments, "*the roots of hybrid warfare are as old as the Trojan horse, yet what has now changed is their scale, speed, and intensity*"[29].

Carl von Clausewitz, one of the most famous theorists of war, defined war as "*an act of violence intended to compel our opponent to fulfil our will*"[30]. Although warfare in the 21st century is characterized by major changes, it is still consistent with the fundamental nature of warfare as described by Clausewitz, and the underlying elements of war remain the same. Clausewitz concluded that regardless of the superficial appearance of war, the same factors are always at play. However, new weapons and increased lethality on the battlefield are changing our conceptions of warfare, and ongoing development challenges armed forces to constantly reexamine the ways in which war is conducted[31]. New types of warfare that combine conventional and unconventional tactics have emerged as a result of the evolution of warfare. The term hybrid warfare is used to describe the area where regular and irregular warfare overlap

---

[27] Tim McCulloh, Rick Johnson, "The Inadequacy of Definition and the Utility of a Theory of Hybrid Conflict: Is the "Hybrid Threat" New?", *JSOU Report* 13-4, 2013, p. 6.

[28] John Jacobs, Martijn Kitzen, "Hybrid Warfare", *Oxford Bibliographies*, 2021, available at: https://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-9780199743292-0260.xml (last accessed: 20.12.2022).

[29] Keynote speech by NATO Secretary General Jens Stoltenberg at the opening of the NATO Transformation Seminar, 2015, available at: https://www.nato.int/cps/en/natohq/opinions_118435.htm, (last accessed: 20.12.2022).

[30] Michael Howard, Peter Paret (eds), *Carl von Clausewitz, On War*, Princeton University Press, 1976.

[31] MacGregor Knox, Williamson Murray (eds.), *The Dynamics of Military Revolution 1300-2050*, Cambridge University Press, 2001, p. 175.

and merge into a new form of warfare[32]. The blending of conventional and irregular methods of warfare distinguishes such hybrid wars from their historical forms, as in the past conventional and irregular operations tended to take place concurrently but separately, rather than integrated, while operations by irregular combatants were usually subordinate to campaigns by conventional military forces[33]. Now, the hybridity of a conflict lies not only in the simultaneous use of all available means, but also in the way they are combined at the different levels of warfare: for example at the strategic level, nations might choose to support insurgent movements with conventional forces to weaken an adversary; at the operational level, a commander might use guerrilla forces to disrupt enemy lines of communication, or use a mixture of dispersion and concentration to prevent the enemy from massing his forces; while regular and irregular forces might work together tactically[34].

With the increasing emergence of irregular types of conflict in the early 21st century, hybrid warfare entered international discussion. In 2002, U.S. Major William J. Nemeth used the term "hybrid warfare" in reference to the conflict in Chechnya. He defined it as a conflict in which irregular and conventional tactics were combined with psychological operations and information operations and thus, according to him, hybrid warfare is to be understood in contrast to conventional warfare, in which regular authorized armies of States engage in combat against one another in accordance with predetermined set of rules[35]. One of the most important contributions to the hybrid warfare debate comes from Frank Hoffman, who in 2006 described the phenomenon as "*complex irregular warfare*". For Hoffman, hybrid wars differ from earlier wars in that they blur even at lower levels acknowledging that many wars in the past had regular and irregular components, but these effects were coordinated at the strategic level, even when fought in different theatres or in different formations yet in hybrid wars, these forces are also fused at the operational and tactical levels into the same force on the same battlefield[36].

[32] Frank G. Hoffman, "Conflict in the 21st Century: The Rise of Hybrid Wars", Potomac Institute for Policy Studies, 2007, p. 8.
[33] James Wither, "Making Sense of Hybrid Warfare", *Connections: The Quarterly Journal*, Volume 15 (2), 2016, p. 74.
[34] Stefano Marcuzzi, "Hybrid Warfare in Historical Perspectives", *NATO Foundation Defense College*, 2018, p. 7.
[35] William Nemeth, "Future war and Chechnya: a case for hybrid warfare", *Calhoun Institutional Archive of the Naval Postgraduate School*, 2002.
[36] Frank G. Hoffman, "Conflict in the 21st Century: The Rise of Hybrid Wars", *supra* note 32, p. 29.

The concept of hybrid warfare was also referred to describe the 2006 war between Israel and Hezbollah in Lebanon. In the conflict, the vastly superior by conventional standards Israeli forces, failed due to the unexpectedly strong resistance of Hezbollah's irregular forces. The irregular Hezbollah tactics, later referred to as hybrid, caused significant losses for the Israeli Forces which had been relying only on high technology conventional weaponry. One common explanation for this unexpected outcome focuses on Hezbollah's integration of conventional and irregular capabilities. This war entailed regular and irregular methods of warfare that according to Stefano Marcuzzi "*created a synergistic effect*" by employing a lethal combination of conventional weapons with improvised weaponry suited for irregular warfare and ambush attacks[37]. Hybrid warfare advocates argued that this conflict was evidence of the validity of hybrid warfare, with Hezbollah seen as a paradigmatic hybrid adversary. The 2008 war between Georgia and Russia is also referred to as a "hybrid war" because Georgia experienced massive cyberattacks on its government, banks, and media websites in addition to the conventional conflict. In Europe, "hybrid warfare" is most often associated with Russia and its actions in Ukraine in 2014 and 2022. Russia's conquest of the Crimean Peninsula and its support for separatists in eastern Ukraine were presented as the culmination of hybrid warfare. Russia's ambition to preserve its sphere of influence in the center of the European continent was made clear with the start of offensive operations on February 24, 2022, when hybrid means were taken in addition to military action. Nevertheless, although the concept of hybrid warfare has emerged as one of the most contentious issues in the western world, the concept has yet to receive a precise and distinctive definition and the elements of this type of conflict are debated.

2. Definition of hybrid warfare

Reviewing the literature on the merging of conventional and unconventional means of warfare, certain basic ideas can be identified that guide the concept of hybrid warfare. Frank Hoffman analyzed hybrid warfare using the 2006 Lebanon War and Hezbollah tactics as an example. He argues that "hybrid wars" encompass a wide range of different warfare elements and that the concept captures the continuing effects of globalization, the proliferation of military

[37] Stefano Marcuzzi, "Hybrid Warfare in Historical Perspectives", *supra* note 34, p. 3.

technologies, and the information revolution[38]. Hoffman defines hybrid warfare as following: *"any adversary that simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism and criminal activities in the battle space to obtain their political objectives."*[39]. Hybrid wars in this sense incorporate a range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts and criminal disorder and can be increasingly characterized by a hybrid blend of traditional and irregular tactics, decentralized planning and execution, and non-State actors, using both simple and sophisticated technologies in innovative ways[40]. In hybrid warfare then, adversaries employ various forms of warfare to gain an asymmetric advantage. With this definition, it is clear that the use of irregular tactics in a hybrid war is not merely a means of weakening the adversary and thus overcoming him through conventional tactics, but the components of irregular forces become critical in such a conflict because they are operationally integrated with regular components[41].

Russell Glenn, a military strategist, defines "hybrid warfare" as: "An adversary that simultaneously and adaptively employs some combination of (1) political, military, economic, social and information means, and (2) conventional, irregular, catastrophic, terrorism, and disruptive/criminal warfare methods and it may include a combination of state and non-state actors"[42]. Glenn considers the impact on society that is the target of hybrid warfare. Referring to the Second Lebanon War in 2006 he noted that Hezbollah is more than a military force, and therein lies its real strength since it has political, social, diplomatic, and informational components that provide support for its military organization established by years of providing humanitarian aid, building physical infrastructure, educating Lebanese, and serving as medical provider that would remain even in the aftermath of military defeat[43].

Colonel John McCuen adds a societal element to the definition of "hybrid wars" believing that hybrid wars are a combination of symmetric and asymmetric warfare in which intervening forces conduct traditional military operations against enemy forces and targets, while at the

[38] Frank Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges" *Prism*, Volume 7(4), 2018, p. 38.
[39] Frank Hoffman, "Hybrid vs. Compound war", *Armed Forces Journal*, 2009, p.2.
[40] Frank Hoffman, "Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict", *Strategic Forum*, No. 240, 2009, p. 5.
[41] Maria Dourado, Alexandre Leite, Fábio Nobre, "Hybrid Warfare Vs. Gibridnaya Voyna: The Different Meanings of Hybrid Conflicts for West and Russia", *Revista da Escola de Guerra Naval*, Volume 26(1), 2020, p. 50.
[42] Russell Glenn, "Thoughts on 'hybrid' conflict", *Small Wars Journal*, 2009, p. 2.
[43] *Ibid.* p. 3.

same time, and more crucially, must attempt to gain control of the indigenous population of the combat zone by securing and stabilizing it[44]. Although McCuen emphasizes that "hybrid wars" will always involve direct fighting with conventional troops, he argues that hybrid warfare is successful when strategic objectives are achieved in both the physical and conceptual dimensions.

Russian military theorists have extensively examined changes in the character of warfare and the rise of new forms of warfare. However, an analysis of the concept of hybrid warfare by Russian military strategists reveals that there is a different focus and the Russian "*gibridnaya voyna"* revolves around the non-military spheres of politics, economy, social development, culture concept and defends an abstract battlefield where conflicting parties seek to destroy the socio-cultural cohesion of enemies and protect their own, whereas the US military thinkers rather focus on military activities[45].

Evgeny Messner, a Russian military theorist describes in his works the change in the nature of conflicts and predicts the increase of multidimensional wars using both regular and irregular activities, supported by information warfare[46]. According to Messner, one of the most distinguishing characteristics of this types of conflicts which he calls "subversion wars" is the prominence of the psychological/informational dimension where the main goal of war is not to conquer the enemy's physical territory but his mind, by the main means of propaganda and agitation and noted that in times of psychological war, neither victory in battle, nor territorial gains, are the goals themselves, but their main value is in their psychological effects[47]. According to him, this type of war is not limited to military activities, but it also includes successful political, economic, and social actions that can be used to influence the psyche of the masses[48].

Russian General Makhmut A. Gareev, widely regarded as Russia's leading military theorist, pointed out that technological warfare has fundamentally changed war since the methods and means of information warfare are much more sophisticated than before and he assumes that new measures will make possible to make better use of information and effectively wage a

[44] John McCuen, "Hybrid Wars". *Military Review*, Volume 88 (2), 2008, p. 108.
[45] Ofer Fridman, "Hybrid Warfare or Gibridnaya Voyna?", *The RUSI Journal*, Vol. 162, No. 1, 2017, p. 43.
[46]Evgeny Messner, "Lik sovremennoy voyny" (The Face of the Contemporary War), Buenos Aires: South American Division of the Institute for the Study of the Problems of War and Peace, 1959, p. 11.
[47] Ofer Fridman, "The Russian perspective on information warfare: conceptual roots and politicisation in Russian academic, political, and public discourse", *Defence Strategic Communications*, Volume 2, 2017, pp. 66-67.
[48] *Ibid.*

battle in the field of psychology[49]. He emphasizes that information warfare through systematic broadcasting of psychologically and ideologically biased materials of provocative nature, mixing partially truthful and false items of information can result in mass psychosis, despair, and feelings of doom and undermine trust in the government and armed forces and in general lead to the destabilization of the situation in those countries which become objects of information warfare[50]. In his book, Gareev frequently refers to the work of various Western scholars, showing that Russian military science was well aware of the ideas of the counterparts in the West and was able to respond to them and develop them further[51].

Since 2012, Russia's military strategy has been centered around the "Gerasimov Doctrine". General Valery Gerasimov speaks of "new generation warfare" with emphasis on information technologies, which has since been associated with Russian "hybrid warfare"[52]. Gerasimov explained how this new kind of warfare concentrates on the combined employment of diplomatic, economic, political, and other non-military means with direct military force instead of open warfare by citing the experience of the Arab Spring as an example[53]. According to Gerasimov, the rules of warfare have changed, and the importance of non-military means for achieving political and strategic goals has increased; in many cases, they surpass the power of weapons in their effectiveness[54]. Gerasimov acknowledges that many of the methods he mentions are not traditionally what one would call warlike activities, however, they are typical of 21st-century warfare and are even more significant than military means as they can reduce an adversary's fighting potential by causing social upheaval and fostering a climate of breakdown without resorting to overt violence[55]. In any case, according to Gerasimov, the armed forces play a crucial supporting role in modern combat.

[49] Miroslaw Banasik, "Russia's Hybrid War in Theory and Practice", *Journal on Baltic Security*, Volume 2(1), 2016, pp. 166- 167.
[50] Makhmut Gareev, *If War Comes Tomorrow? The Contours of Future Armed Conflicts*, Routledge, Abingdon, 1998, pp. 51-52.
[51] András Rácz "Russia's Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist", *The Finnish Institute of International Affairs*, Report 43, 2015, p. 35.
[52] Eugene Rumer, "The Primakov (Not Gerasimov) Doctrine in Action", *Carnegie Endowment for International Peace*, 2019, available at: https://carnegieendowment.org/2019/06/05/primakov-not-gerasimov-doctrine-in-action-pub-79254 (last accessed 20.12.2022).
[53] Valery Gerasimov, "The Value of Science Is in the Foresight – New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations", *Military Review*, 2016, p. 24.
[54] *Ibid.*
[55] Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War," *Moscow's Shadows*, 2014, available at: https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war (Gerasimov's Article: The value of science in prediction) (last accessed: 20.12.2022).

The above definitions of hybrid warfare prove that there is no clear and comprehensive definition. By examining the concept of hybrid warfare, we may draw the conclusion that despite some similarities in the tactics and strategies, there is still a significant difference in their points of view; the *"gibridnaya voyna"*, a literal translation from "hybrid warfare", does not reflect the exact same meaning[56]. While Russian conceptions tend to emphasize the significance of the psychological aspects of warfare, thus the use of non-military means, Western concepts emphasize a focus on the physical aspects, thus the military means of hybrid warfare. The Russian discussion of "gibridnaya voyna" differs from the Western discussion of hybrid warfare, despite the similarities, it proceeds from an understanding of "hybrid warfare" that focuses on the combination of military and non-military methods rather than on the reconciling of conventional and non-conventional military means[57].

3. Characteristics of hybrid warfare

Hybrid warfare has a number of key characteristics that make it unique from any other form of warfare. Specifically, in their analysis of hybrid warfare, theorists point to several characteristics of hybrid warfare, the most important of which are simultaneity, convergence, multimodality[58], and catastrophic[59].

Simultaneity describes the application of different modes of warfare at the same time and is highlighted as a dimension of hybrid warfare by all theorists. In particular, simultaneous action is where hybrid threats employ different types of conflict simultaneously to give the impression of overall coherence. An important element to mention is that in the hybrid threat, in addition to vertical escalation, which concerns the further intensity of military attacks on the battlefield, there is also horizontal escalation, i.e., the simultaneous shift of the attack from one domain to another, such as the possibility of shifting the attack from politics to the economy and from there to society and cyberspace, so that multiple attacks are waged on multiple levels, i.e., a

[56] Maria Dourado, Alexandre Leite, Fábio Nobre, *supra* note 41, p. 58.
[57] Markus Göransson, "Understanding Russian thinking on gibridnaya voyna", in Mikael Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm (eds.) *Hybrid Warfare Security and Asymmetric Conflict in International Relations*, I.B. Tauris, 2021, p. 83.
[58] Frank Hoffman, "Hybrid vs. Compound war", *supra* note 39.
[59] Russell W. Glenn, "Thoughts on "Hybrid" Conflict", *Small Wars Journal*, 2009, p.2

war on multiple dimensions[60]. Convergence on the other hand describes the fusion of different warfare elements into one threat, for instance the fusion of conventional and unconventional elements into one "hybrid" threat which is a distinctive characteristic of Hoffman's theory[61]. In this case for example, a hybrid threat may consist of a combination of professional soldiers, insurgents, terrorists, and criminals, and the element that links them all together is the fact that they have a common goal, they seek a common political outcome and thus they are considered to constitute a single threat. Multimodality is the general use of different warfare tools and actors during a conflict and can be defined as the extent to which an adversary can mix and apply different types of warfare. Russia is considered to have demonstrated the multimodality dimension of hybrid warfare in its actions to annex Crimea.

The catastrophic dimension that a hybrid warfare could reach, introduced by Russell Glen, is described as any man-made or natural incident which severely affects the population. It can be perceived as the impact on the environment, as *"any natural or man-made incident, including terrorism, which results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions"*[62].

[60] Ntamplia Eleni, "The Immigration issue as the vanguard of an asymmetric hybrid war", Master's Thesis, *Hellenic Army Academy – Technical University of Crete*, 2021, p. 34.
[61] Anna Nübel, "The Rise of New Types of War, A Case Study on Russian Hybrid Warfare in the Ukrainian Crisis in 2014", Master's Thesis, *University of Twente,* 2020, p. 28.
[62] Russell W. Glenn, "Thoughts on "Hybrid" Conflict", *supra* note 59, p.2: Definition of "catastrophic event" in Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 2010 (as amended in 2016), p. 28.

PART II. Hybrid threat domains

Hybrid threat actions concern two distinct dimensions: the physical and the conceptual, denoting the physical nature on the one hand and the non-physical or conceptual nature of the action on the other. Accordingly, one can distinguish in the physical dimension, the conventional and unconventional means of warfare, terrorism, and criminal behavior, and in the conceptual dimension, threats in the political and diplomatic, economic, information/media, social, information technology, scientific and technological, and legal domain. The domains should not be examined in isolation, as an effect on one domain is capable of causing cascade effects in another.

A. The physical dimension

1. Conventional/ regular means

In this context, the distinction between regular and irregular warfare is less clear than is often assumed. Some analysts, most notably Colin S. Gray, argue that the distinction itself is dangerous and problematic[63]. Hoffman distinguishes between conventional and unconventional conflict on the basis of largely subjective characteristics. In Hoffman's usage, "conventional" refers to the realm of interstate conflict, while "irregular" refers to the actions of nonstate actors[64]. Although there is no universally accepted definition for conventional warfare, it is usually described as "State-on-state conflict between organized, uniformed, professional military forces using massed firepower in open space away from civilians with the aim of destroying each other to gain and hold ground"[65].

The 2010 US Army Training Hybrid Threats Circular which was designed to enable planners to create training exercises against hybrid threats, defines "conventional" by its characteristics such as "anti-armor weapons, rockets, and command and control networks" or "sophisticated

[63] Colin Gray, 'Categorical Confusion? The Strategic Implications of Recognizing Challenges Either as Irregular or Traditional', *Strategic Studies Institute*, 2012, p. 27.
[64] Frank Hoffman, "Conflict in the 21st Century: The Rise of Hybrid Wars", *supra* note 32, p. 7.
[65] Sandor Fabian, "Irregular Versus Conventional Warfare: A Dichotomous Misconception", *Modern War Institute*, 2021, available at: https://mwi.usma.edu/irregular-versus-conventional-warfare-a-dichotomous-misconception/.

weapons, command and control, and combined arms tactics"[66]. The conventional capabilities are associated with the military capabilities of the State and include the usage of army, navy, and air force, joint combined arms maneuver warfare and firepower intensive conflicts[67]. Moreover, large units, divisions, fleets, air wings, heavily resourced joint combined arms maneuver warfare, quick decisive victories, the pursuit of new technologies, and annihilation goals are considered as the characteristics of conventional warfare[68]. A more useful and coherent means of distinguishing between conventional and irregular warfare is to define both according to how the parties adopting either approach seek to achieve victory. In this context, regular or conventional warfare is defined by the use of military technology and organizations structured with the goal of seeking combat with and destroying opposing forces[69].

2. Unconventional/ irregular means

Irregular warfare, on the other hand, is when a party avoids a decisive battle because of its conventional weakness and instead tries to defeat the enemy through other unconventional means. Irregular warfare arises from a situation where at least one of the combatants is at a disadvantage; where one or the other does not possess the means or the military power to challenge their rival directly[70]. Indicators of irregular warfare include guerrilla tactics and insurgency. Guerrilla tactics can be characterized as "hit-and-run raids and ambushes against local security forces" performed by "armed civilians"[71], while insurgency can be defined as "a rebellion against an authority when those taking part in the rebellion are not recognized as belligerents"[72].

The United States Department of Defense defines irregular warfare as a violent struggle among State and non-State actors for legitimacy and influence over the relevant populations which

[66] US Army, Training Circular 7-100 "Hybrid Threats", *United States Army Training and Doctrine Command*, 2010, p. 1
[67] Manon van Tienhoven, "Identifying 'Hybrid Warfare'", Master's Thesis, *University of Leiden*, 2016, p. 19.
[68] Fernando Reyeg, Ned Marsh, "Filipino way of war: irregular warfare through the centuries", Master's Thesis *Naval Postgraduate School, Monterey California,* 2011, p. 5.
[69] Stephen Biddle, 'Military Power', *Princeton University Press*, 2004, pp. 5-7.
[70] Russell Weigley, *The American way of war: a history of united states military strategy and policy*, Macmillan, 1973, p. xxii.
[71] James Kiras, "Irregular warfare: terrorism and insurgency in Strategy in the Contemporary World", in John Baylis, James Wirtz, Colin Gray (eds.), *Strategy in the Contemporary World*, Oxford: Oxford University Press, 2018, p. 188.
[72] Merriam-Webster Dictionary, Definition of "Warfare", http://www.merriam-webster.com/dictionary/warfare.

favors indirect and asymmetric approaches, though it may employ the full range of military and other capacities, in order to erode an adversary's power, influence, and will[73]. In the case of irregular warfare, success depends to a large extent not on the defeat of the armed forces but on winning the support or allegiance - or the will - of the population. Thus, psychological concepts such as credibility, legitimacy, and will are central to irregular warfare, as are power and influence in competing for the sympathy, support, and mobilization of various segments of the population[74]. More specific conceptualizations that have prevailed describe such a conflict as an asymmetric struggle between a government and a non-State actor, in which the latter hides among the civilian population and uses improvised explosive devices, suicide bombers, and small-scale "hit-and-run" tactics in densely populated urban areas to achieve its strategic goals[75].

Taking Hezbollah as an example, which is widely viewed as the epitome of a hybrid actor, it fundamentally lacked the conventional capabilities to directly challenge Israeli forces and instead used its capabilities to develop a sophisticated irregular strategy. The group developed over time its conventional capabilities in terms of rockets, artillery, anti-aircraft, anti-ship, and anti-tank weaponry but as its military strength grew over time it was supplemented by an asymmetric capability including criminal and terrorist networks[76]. During the First Chechen War, the Chechen insurgents knew that they could not defeat the Russians in a direct conflict because they were vastly outnumbered and lacked heavy equipment, thus instead, they chose to fight against the strength of the Russian army in the city, denying the army a clear front line and also using their network of contacts abroad, especially in the Middle East and Turkey, to procure equipment resulting in the defeat of between 45 and 95 thousand Russian soldiers by only 15 thousand Chechen insurgents[77]. In 2014, Russia supported an insurgency, the resistance movement against the legal Crimean government, through the use of "little green men" in Crimea who were storming Parliament and official buildings, blocking roads and streets, establishing checkpoints, organizing pro-Russian populations, and controlling the Crimean

[73] United States Department of Defense, Joint Publication 1-02: Dictionary of Military and Associated Terms (JP1-02), 2001, p. 280.
[74] Eric Larson, Derek Eaton, Brian Nichiprouk, Thomas Szayna, *Assessing Irregular Warfare. A Framework for Intelligence Analysis*, RAND, 2008, p. 11.
[75] Sandor Fabian, *supra* note 65.
[76] Tim McCulloh, Rick Johnson, *supra* note 27, p. 21.
[77] Petta Gomes da Costa, "Geopolitical Management through Irregular Actors", Athens: ATINER'S Conference Paper Series, No:POL2016-2110, 2016, p. 5

Peninsula, while another objective of Russia's irregular warfare was the regime change in Crimea[78].

3. Terrorism

While the melding of conventional and irregular warfare is by far the dominant feature of hybrid warfare, it is also important to examine the concepts of criminality and terrorism, which although are not as readily discussed or analyzed as conventional and irregular warfare, they are nonetheless central components of the most common definitions of hybrid warfare[79]. In very general terms, terrorism is an act or campaign of violence committed by an actor against non-combatants to instill fear or intimidate a large audience[80]. Terrorism is a controversial concept but can be defined as *"the illegitimate use of force to achieve a political objective by targeting innocent people"*[81]. A broader definition of terrorism, used as an indicator of the nature of warfare, is as follows: "1) an act of violence that produces widespread disproportionate emotional reactions such as fear and anxiety; 2) violence is systematic usually directed against symbolic targets; 3) the violence conveys messages and threats in order to communicate and gain social control"[82].

For example, the terrorist threat is believed to be one of the weapons used by the Islamic State to take the conflict beyond the borders of its territory and create an atmosphere of terror. Specifically, terrorist cells have carried out attacks outside Daesh territory with the aim of sending a message that goes far beyond the actual victims of the attacks; the Shiite population of Lebanon, Russia, and France, showcasing the kind of war the world is currently dealing with: a hybrid war in which the terrorist threat is one of the weapons used by the terrorists to take the conflict beyond the borders of their territory, bringing it directly into people's homes and creating an atmosphere of terror in communities[83]. A notable case in point is the

[78] Mehmet Seyfettin, "Hybrid Warfare Studies and Russia's Example in Crimea", *Akademik Bakış*, 2015, pp. 270-271.
[79] Andrew Dunn-Lobban, "Hybrid Warfare, Hybrid Threats and the Demarcation of Conflict, Thesis, University of New South Wales, 2016, p. 14.
[80]Igor Primoratz 'Terrorism', *The Stanford Encyclopedia of Philosophy*, 2015, <http://plato.stanford.edu/archives/spr2015/entries/terrorism/>.
[81] Walter Laqueur, *Terrorism*, Weidenfield and Nicholson, 1977, p. 7.
[82] Tore Bjorgo, *Root causes of Terrorism: myths, reality and ways forward*, Routledge, 2005, p. 120.
[83] Andrea Manciulli, "Daesh and the terrorist threat: from the Middle East to Europe", *Foundation for European Progressive Studies*, 2015, p. 10.

relationship between Iran and the powerful terrorist organization Hezbollah, whose agents have long been present and active in Europe as a part of their criminal enterprises and terrorist activities, with tentacles reaching practically everywhere in the world[84].

As Lawrence Freedman noted, terrorism is conceptually a primitive form of irregular warfare that seeks only limited impact[85]. Like criminal behavior, terrorism is most considered by proponents of the hybrid warfare concept to emphasize the variety of means employed by hybrid actors as hybrid threats, rather than to amount to a particular tactic or means of a hybrid warfare. Within hybrid warfare, the distinction between irregular warfare and terrorism is fraught with conceptual difficulties, therefore it is difficult to distinguish the effects of a hybrid actor using both the tools of irregular warfare and terrorism given the similarities between the two approaches[86].

4. Criminal behavior

Organized crime generally describes the actions of groups that are structured or organized in some way and whose goal is to obtain revenue through illegal activities including drug and arms smuggling, trafficking, narcoterrorism, illegal transfers of weapons, money laundering and the exploitation of gang networks as criminal activities. This criminal behavior is generally considered important in a hybrid strategic context because, first, it provides a source of revenue to fund the activities of hybrid actors and, second, criminality is viewed as a weapons system that undermines or destabilizes government, thus it used as a deliberate mode of warfare[87]. In hybrid warfare in particular, the generation of revenue through illicit activities is understood as a means to an end, a source of revenue to finance the hybrid actor's activities since criminal proceeds from these acts create funding for training and equipping hybrid forces[88].

A criminal enterprise may become a hybrid actor if it has a political goal beyond mere profit in order to undermine the governance of a State, similar to an insurgency. Criminal

[84] Georgios Giannopoulos et. al., *supra* note 24, p. 120.
[85] Lawrence Freedman, "The Counterrevolution in Strategic Affairs", *Dædalus*, Volume 140 (3), 2011, p. 26.
[86] Igor Primoratz, *supra* note 80.
[87] Andrew Dunn-Lobban, *supra* note 79, p. 15.
[88] John Davis, "Defeating Future Hybrid Threats: The Greatest Challenge to the Army Profession of 2020 and Beyond", *Military Review*, 2013, p. 22.

organizations with operations and networks in a target State constitute hybrid threats and a very useful tool for foreign State hybrid activities. The exploitation of criminal organizations could include utilizing established smuggling networks, the ability to provide forged documents, financial crime schemes or simply their ability to threaten, intimidate, pressure or harm strategically important individuals or groups in a specific situation for political purposes[89]. Economic power gained through money laundering and corruption can amplify gains in political influence by setting in motion a "virtuous circle of corruption" in which greater political power enables greater economic power[90]. Thus, criminal behavior as a hybrid threat is primarily a means to achieve other objectives, a means by which hybrid actors undermine the governance of a State while adding to the complexity and adaptability of a hybrid actor by disguising the hybrid threat as a criminal organization[91].

This is reflected in the classification of Mexican drug cartels as a hybrid threat since they conduct illegal activities but also seek political control by disrupting the governance of the Mexican State[92]. Besides, the Islamic State, which is referred to as a hybrid actor, has become one of the world's most wealthy terror groups by cultivating a self-sufficient shadow economy based on extortion, organized crime, and illicit oil sales[93]. In addition, criminal activities were part of Russia's actions in Ukraine, because since separated from Ukraine in 2014, crime, corruption and rebellion have flourished in the Russian-backed Donetsk, Luhansk and Crimea: "industrial-scale smuggling from coal to narcotics helped sustain the internationally unrecognized pseudo-states of Donbas; gangsters became militiamen; and money-laundering networks meanwhile bypassed sanctions"[94]. It is considered that the Crimean annexation has demonstrated the connection between crime and the Russian State since Kremlin is considered to have used criminality as an instrument of State policy[95].

[89] Georgios Giannopoulos et. al., *supra* note 24, p. 24.
[90] Multinational Capability Development Campaign, "'A Deadlier Peril': The Role of Corruption in Hybrid Warfare", *Countering Hybrid Warfare Project*, 2019, p. 2.
[91] Andrew Dunn-Lobban, *supra* note 79, pp. 15-16.
[92] Sharon Cardash, Frank Cilluffo and Bert Tussing, 'HPSI Issue Brief: Mexico and the Triple Threat', 'The Hybrid Threat: Crime, Terrorism and Insurgency in Mexico', *A Joint CSL-HSPI Study*, 2011, pp. 11-15.
[93] Scott Jasper, Scott Moreland, 'The Islamic State is a Hybrid Threat: Why Does That Matter?', *Small Wars Journal*, Volume 10(12), 2014, pp. 1-2.
[94] David Klein, "Report: In Crimea and the Donbas, Organized Crime Reigns Supreme", *Organized Crime and Corruption Reporting Rroject*, 2022, available at: https://www.occrp.org/en/daily/16570-report-in-crimea-and-the-donbas-organized-crime-reigns-supreme (last accessed: 20.12.2022)
[95] Mark Galeotti, "Crime and Crimea: Criminals as allies and agents". *Radio Free Europe Radio Liberty*, 2014, http://www.rferl.org/content/crimea-crime-criminals-as-agents-allies/26671923.html (last accessed; 20.12.2022)

B. The conceptual dimension

As previously mentioned, hybrid strategies have gained much popularity in the 21st century as States seek to achieve their goals without the use of military force. Actors may employ a hybrid action without any desire to exert physical control in order to undermine the target State. Hybrid threats prove their effectiveness, as in most cases the State that employs them succeeds without the rest of the world noticing or being able to attribute the acts to it. It is a reality that the "battlefields of the future" are not only on the physical ground and do not always distinguish between a state of peace or war in their traditional meaning. It is claimed that there is no longer neither a clear distinction between the "state of war" and the "state of peace" nor possible to draw a definitive line between peaceful and aggressive relations: "We must stop thinking that war is when somebody is fighting, and peace is when there is no fighting"[96]. The idea of hybrid threats as part of not only a declared war but also an "undeclared war" is that they are designed to avoid being identified as clear violations of international law in order to exploit the weaknesses of the adversary and blur the lines between war and peace. According to Mark Galeotti "we will live in a world of permanent low-level conflict, often unnoticed, undeclared and unending, and one in which even our allies may also be our competitors"[97].

In the conceptual dimension, hybrid threats do not usually amount to acts of aggression thus they do not reach the level of warfare but operate at "gray zones". The gray zone is commonly understood as the hostile or adversarial interactions among competing actors below the threshold of conventional war and above the threshold of peaceful competition, employed by revisionist powers to attain their strategic aims without resort to conventional force and without triggering an international response[98]. In this context, hybrid activities are critical because they exploit the weakness of an international enforcement regime especially in cases where aggressor States have sown doubts about the imputability or legality of their conduct[99]. The main legal challenges or gaps for States being victims of such action are apart from the "gray zones" of international law and international humanitarian law, the legal constraints and

[96] Ofer Friedman, Russian Hybrid Warfare, *supra* note 6, pp. 157-160.
[97] Mark Galeotti, *The Weaponisation of Everything, A Field Guide to the New Way of War, supra* note 1, p. 5.
[98] James Dubik, Nic Vincent, "America's global competitions: the gray zone in context*", Institute for the Study of War*, 2018, p. 9.
[99] Douglas Cantwell, "Hybrid War as Strategy and Policy", *American Society of International Law*, Volume 21 (14), 2017.

restraints in peacetime and crisis which test the legal resilience of States[100]. This is particularly true among Western democracies who are embedded in a traditional understanding of international law, yet in the hybrid era, international law no longer fits with the reality on the ground[101]. In this area, hybrid threats aim at achieving highly strategic and overarching goals such as undermining public confidence in democratic institutions, deepening unhealthy polarization nationally and internationally, challenging the core values of democratic societies, gaining geopolitical influence and power by harming and undermining others, and compromising the decision-making capacity of political leaders[102].

1. Political and diplomatic domain

The term "political warfare" was employed by George Kennan in 1948 to describe the use of all means available to a nation, other than war, to achieve its national objectives including both overt and covert operations and various types of propaganda as well as covert operations that secretly support underground resistance in hostile States[103]. Hybrid threats in the political domain refer to the intentional use of political means to influence the political composition or decision-making in a State. The term "political" describes the calculated interaction between a government and a target audience, including the government of another State, the military, and/or the general population, in which governments use a variety of techniques to coerce certain actions and thereby gain a relative advantage over an opponent[104]. In a hybrid strategy, political means could be combined with violence, economic pressure, subversion, and diplomacy, but its main aspect is "the use of words, images, and ideas"[105]. The ultimate goal of the use of political means as a hybrid threat is to change an adversary's opinions and actions in favor of a State's interests without using military power since actors may seek to leverage the political domain to influence the target State or create favourable conditions for conducting hybrid threats. Political power can be used either within a country or in the diplomatic arena,

[100] Morten M. Fogt, "Legal Challenges Or "Gaps" By Countering Hybrid Warfare – Building Resilience In Jus Ante Bellum", *Southwestern Journal Of International Law*, Volume XXVII (1), 2020, p. 56.
[101] Mikael Weissmann, *supra* note 5, p. 76.
[102] Georgios Giannopoulos et. al., *supra* note 24, p. 6.
[103] George F. Kennan, "The Inauguration of Organized Political Warfare," *History and Public Policy Program Digital Archive*, 1948, p. 2.
[104] Wikipedia, "Political warfare", available at: https://en.wikipedia.org/wiki/Political_warfare
[105] Paul Smith, *On Political War*, Washington: National Defense University Press, 1989, p .2.

and the tools of this domain mainly target democratic processes, political organisations, and individuals[106].

The political domain is closely related to diplomacy, mainly because foreign policy can have a strong influence on domestic policy and the relationship between the two is often described as a "two-level game"[107]. Diplomacy is construed in its international dimension as the conduct of international relations and diplomatic power is typically deployed by States. Hybrid threats, particularly in the realm of diplomacy, aim to create divisions at the State or international level, support information campaigns, and interfere in the decision-making process[108]. They include, among others, persuasion, inducements, threats, and sanctions, as well as the drafting and tabling of resolutions, which can be expressions of political will or the basis for concrete action, by international organisations over which the State has some influence or in which it can find the support of like-minded States while the goal is often to isolate the target State from the international community in order to limit its room for manoeuvre and thus reduce its ability to pose a threat[109].

During the Cold War, the U.S. government used "political warfare" through a variety of mechanisms, including covert funding of noncommunist political parties in Europe and Japan, covert creation of journals and organizations to organize artists and intellectuals against communism, and financial and logistical support for dissidents behind the Iron Curtain[110]. Moreover, although military means were ultimately decisive, Russian interventions in 2014 relied heavily on diplomatic means and the mobilization of local political support among civilian groups to work toward the political goal of "restructuring" the Ukrainian State, with the aim of avoiding a clear and large-scale deployment of formed Russian units on Ukrainian territory or direct engagement in a long-term civil war and instead, civilians and allegedly organized civilian "self-defense forces" in Ukraine have been an important resource in Russian efforts to neutralize and counter the response of the Ukrainian central authorities as well as undermine the political legitimacy of the Ukrainian government[111].

---

[106] Georgios Giannopoulos et al., *supra* note 24, p.32.
[107]Robert Putnam, "Diplomacy and Domestic Politics: The Logic of Two-Level Games" *International Organization, Vol.* 42 (3), 1988, p. 434.
[108] Georgios Giannopoulos et al., *supra* note 24, p. 31.
[109] Janne Jokinen, Magnus Normark, "Hybrid threats from non-state actors: A taxonomy", *Hybrid CoE Research Report 6*, 2022, p. 23.
[110] Max Boot, Michael Doran, "Political Warfare", *Council on Foreign Relations*, 2013, p. 2.
[111] Roy Allison, "Russian 'deniable' intervention in Ukraine: how and why Russia broke the rules", *International Affairs* 90 (6), 2014, p. 1258.

2. Economic and energy domain

Hybrid threats in the economic domain entails the use or threat of use of economic means against a country to weaken its economy and thereby reduce its political and military power[112]. In this context, "economic warfare" includes the use of economic means to compel an adversary to change its policies or behaviour or to undermine its ability to conduct normal relations with other countries, while some common means of economic warfare include trade embargoes, boycotts, sanctions, tariff discrimination, the freezing of capital assets, the suspension of aid, the prohibition of investment and other capital flows, and expropriation[113]. The goal of a such a threat is to comprehensively weaken the target State and undermine public confidence in democracy and government as economic instruments may be used to exert political pressure or economic coercion to change a State's foreign policy stance, or to weaken the resilience of its economy, society, and security[114].

The economic domain is intimately tied to other domains, such energy and infrastructures, that can lead to economic dependency or serve as a tool for applying economic pressure. This is true in the context of hybrid threats. Large infrastructure projects are particularly vulnerable to becoming part of a hybrid threats strategy because once a pipeline, communications link, port, or other large piece of infrastructure is built, it cannot be moved, which in turn creates dependency since the supplier is vulnerable to demands from the customer to renegotiate the price of imports after the investment has already been made and the project is complete[115]. Russia has used both direct and indirect economic influence to affect European politics[116]. A closer look at the Russian-Ukrainian crisis reveals that energy was and is a far more important factor in hybrid action than is commonly assumed and Ukraine's high energy inefficiency and its dependence on Russian gas imports have led to Russia exerting economic pressure on Ukraine, while trying to discourage other European countries from supporting Ukraine with reverse gas supplies and touting the country's irreplaceable role in Europe's energy security[117]. Russia had already used energy as a foreign policy tool when it cut off natural gas supplies to

[112] The Britannica Dictionary, "Economic Warfare", available at: https://www.britannica.com/topic/economic-warfare (last accessed: 20.12.2022).
[113] *Ibid.*
[114] Georgios Giannopoulos et al., *supra* note 24, p. 29.
[115] Janne Jokinen, Magnus Normark, *supra* note 109, p. 19.
[116] Christopher Chivvis, "Understanding Russian "Hybrid Warfare" and What Can Be Done About it", *Rand Corporation*, 2017, p. 4.
[117] Michael Ruhle, Julijus Grubliauskas, "Energy as A tool of Hybrid Warfare", *NATO Defense College*, 2015, p.2.

Ukraine in the middle of winter in 2006 and 2009 to force Ukraine to agree on the price of gas[118].

Russia's indirect impact in Europe may be much more significant now that it is using hybrid means to undermine energy security in all NATO members states, not just in Ukraine, as part of its effort to counterbalance the alliance's strength in Europe and increase its global influence. In April 2022 the halt of gas supplies to Poland, Bulgaria, Finland, the Netherlands, Denmark, and Shell customers in Germany lead to a further increase in European gas prices[119], while in August, the Russian company proceeded with an indefinite shut down of its Nord Stream 1 gas pipeline, intensifying Europe's energy crisis[120]. Russia's State-owned gas giant company and its subsidiaries use the extensive network of natural gas pipelines built during the Soviet era to influence the politics and economies of many European countries[121]. By using the pipeline to escalate the conflict with Ukraine and by manipulating the markets and reducing supplies, Russia has taken advantage of Europe's dependency on energy to impose financial and political burdens and uses energy as a weapon. Since October 2022, Russia's sustained and extensive missile and drone attacks on Ukraine's energy grid as part of its hybrid warfare strategy have left millions of civilians without electricity, heat, water, and other essential services during the frigid winter months, with damage and destruction of civilian infrastructure being part of the Kremlin's strategy to terrorize civilians and increase pressure[122].

Apart from the above, it should be added that Russia’s war in Ukraine could cause according to the UN the largest food crisis in human history due to the Ukrainian grain export blockade by Russia and the consequent rise in global market prices of grains. For Russia, the global food crisis as a means of hybrid warfare is considered as a way to destabilize the world, and therefore to divert attention from the war in Ukraine and simultaneously serves as one of the levers to pressure Ukraine into negotiating with the extortionists and the West, into lifting sanctions

[118] Digital Forensic Center, “Deep dive: Hybrid Warfare”, available at: https://dfcme.me/en/deep-dive-hybrid-warfare/.
[119] Sarah Lohmann, “Russian Gas, Green Technology, and the Great Sacrifice”, *Georgetown Journal of International Affairs*, 2022, available at: https://gjia.georgetown.edu/2022/06/23/russian-gas-green-technology-and-the-great-sacrifice%EF%BF%BC/ (last accessed: 20.12.2022).
[120] The guardian, “Nord Stream 1: Gazprom announces indefinite shutdown of pipeline”, 2022, available at: https://www.theguardian.com/business/2022/sep/02/nord-stream-1-gazprom-announces-indefinite-shutdown-of-pipeline (last accessed: 20.12.2022)
[121] Digital Forensic Center, *supra* note 118.
[122] Olga Voitovych, Eliza Mackintosh, “Russian missile strikes pound Ukraine, knocking out power and putting entire country under air-raid alarm”, *CNN*, December 16, 2022, available at: https://edition.cnn.com/2022/12/16/europe/ukraine-russia-missile-strikes-friday-intl/index.html (last accessed: 20.12.2022)

imposed against Russia[123]. According to the High Representative of the EU for Foreign Affairs and Security Policy Josep Borrell, Russia attempts to use food as a war weapon and to create hunger in the world, in order to put pressure on the European Union, while its deliberate targeting of Ukrainian agricultural facilities and export routes have exacerbated the food price spike and the global food crisis[124].

3. Information/ media domain

"Information warfare" has been referred to as "actions taken to achieve superiority by affecting adversary information, information-based processes, information systems, and computer-based networks"[125]. Undoubtedly, information "weaponization" continues to be a defining characteristic of hybrid strategies with the use of information means as a hybrid threat. When social media is used for propaganda purposes, for the spread of disinformation and "fake news", in an attempt to control the perceptions of large groups of people, such activities constitute hybrid threats mainly for democratic societies. In contrast to typical cyberattacks, the purpose of a digital influence campaigns is to utilize computer systems against the target in a way that furthers the attacker's goals to influence how a society thinks, acts, and behaves and in certain situations even to make the target society dysfunctional as a whole, rather than to damage the functional integrity of such systems. Social media can and have already been used to "prepare the battlefield" by shaping the narrative for a specific audience-both decision makers and the general population-to achieve the desired effect and such conflicts, prepared and accompanied by active social media campaigns, seek to manipulate both sides' perceptions of the opposing side, their own populations, and the international community[126]. In particular, the use of media tools is probably the most common method of directing and influencing public opinion, whether on the Internet, in social networks, or through mass media coverage since

[123] Centre for strategic communication, Ministry of Culture and Information Policy of Ukraine "Grain as a Weapon. How Russian Aggression in Ukraine Threatens the World with Hunger", 2022, available at: https://spravdi.gov.ua/en/grain-as-a-weapon-how-russian-aggression-in-ukraine-threatens-the-world-with-hunger/ (last accessed: 20.12.2022).

[124] Josep Borrell, "The fight continues against the food insecurity that Russia's war is creating", *European Union External Action*, 2022, available at: https://www.eeas.europa.eu/eeas/fight-continues-against-food-insecurity-russia's-war-creating_en?s=232. (last accessed: 20.12.2022)

[125] Reto Haeni, "Information Warfare: An introduction", *The George Washington University, Cyberspace Policy Institute*, 1997, p. 4.

[126] Todor Tagarev, "Hybrid Warfare: Emerging Research Topics, *Information & Security: An International Journal*, 2018, p. 291.

apart from the ideal of enabling the free exchange of ideas in liberal democracies, media power is typically used to achieve two related but distinct goals: influencing States and societies through information, disinformation, propaganda, and the manipulation of information; as well as disrupting the channels of communication with the public and denying the adversary access to alternative sources of media dissemination[127].

Digital influence, in particular, can be used to undermine trust in political systems and institutions (such as democratic elections), disrupt and damage social cohesion, tear apart international alliances, and more, as such operations use a variety of deceptive and provocative tactics such as trolling, gaslighting, doxing, and the use of false social media profiles and videos and even more than technological attacks, they exploit psychological and emotional characteristics such as fear, insecurity and cognitive biases to take advantage of human weaknesses[128]. Disinformation in social media is not just a post that has been liked, shared or followed; rather, it is a powerful technique of multiplying cyber propaganda and the tools of this domain seek to shift the political discourse, to create or promote narratives, and to manipulate public opinion and sentiment while they may impair freedom of opinion and expression[129]. Another influencing strategy that has been used frequently in recent years is to promote engagement with information that may be wholly or partially accurate, particularly by eliciting emotional responses, which unlike disinformation and deception, the focus here is less on the message and more on getting people to propagate the message[130]. It must be noted that there is a strong connection between the information domain and intelligence since an actor deploying hybrid threats can either use intelligence capabilities to support planned or ongoing hybrid threat activities or influence the intelligence operations of the target State seeking to undermine the target State's ability as well as to develop and maintain situational awareness[131].

One of the best-known tools of the Russian hybrid strategy is the country's information operations and strategic communications[132]. In order to shape political narratives in other States, regions, or continents, Russia has conducted a broad, multifaceted influence campaign using all of the prior tools and techniques as well as a variety of new technological approaches

[127] Janne Jokinen, Magnus Normark, *supra* note 109, p. 27.
[128] James Forest, "Political Warfare and Propaganda: An Introduction", *Journal of Advanced Military Studies*, Volume 12(1), 2021, p. 15.
[129] Georgios Giannopoulos et al., *supra* note 24, p. 32.
[130] James Forest *supra* note 128, p. 22.
[131] Georgios Giannopoulos et al., *supra* note 24, p. 31.
[132] Christopher Chivvis, *supra* note 116, p. 3.

turning information into an instrument of national power and using it to create space for itself and its interests in the international environment and global public opinion[133]. Russia has been particularly investing in information infrastructure to dominate Western countries in news distributed over the Internet and in the media[134], such as online troll farms, armies of automated bot accounts, cyber-hacking units, and other tools so that it can pursue its objectives of influencing other countries. For example, the Russian efforts to influence the 2016 US presidential election is considered to represent an attempt to undermine the US led liberal democratic order with activities that demonstrated a significant escalation in directness, level of activity and scope of effort, through the use a messaging strategy that blended covert intelligence operations such as cyber activity with overt efforts by Russian Government agencies, State-funded media, third-party intermediaries and paid social media users or "trolls"[135].

Russia has been implementing a strategic approach in Ukraine since at least 2014 that depends heavily on Russia's concept of "information warfare", which consists of a deliberate disinformation campaign supported by actions of the intelligence organs designed to confuse the enemy and achieve strategic advantage at minimal cost[136]. As for the 2022 conflict in Ukraine, in addition to geopolitical, military, and economic actions, disinformation warfare represented Russia's main tool to justify its expansion in Ukraine in conventional military terms[137]. In this context, the Russian president ordered Russian forces to begin offensive operations against Ukraine, with the official goal, of "denazifying" Ukraine and stopping the "ongoing genocide of Russophones" in the country[138]. The Russian Defense Ministry announced victories in Crimea and Dombas and claimed air superiority over Ukraine reinforcing the Russian public's misleading perception of a light military operation in Ukraine, while Russian State television claimed that the Russian military could not withdraw, especially

[133] James Forest, *supra* note 128, pp. 24-25.
[134] Michael Kofman, Matthew Rojansky, "A closer look at Russia's hybrid war", *Kennan Cable*, No. 7, 2015, pp. 5-6.
[135] Intelligence Community Assessment, "Assessing Russian Activities and Intentions in Recent U.S. Elections", 2017, p. ii.
[136] Maria Snegovaya, "Putin's Information Warfare In Ukraine, Soviet Origins Of Russia's Hybrid Warfare", *Institute for the Study of War*, Report I, 2015, p. 7.
[137] Josias Guerrero, "Ukraine Conflict: Hybrid Warfare and Conventional Military Intervention", *Revista Seguridad y Poder Terrestre*, Volume 1(1), 2022, available at: https://ceeep.mil.pe/2022/07/07/ukraine-conflict-hybrid-warfare-and-conventional-military-intervention/?lang=en#post-20719-endnote-17. (last accessed: 20.12.2022)
[138] Tomasz Kamusella, "Democracy and Putin's obsession with a "nazi anti-Russia" Ukraine", *New Eastern Europe*, 2022, available at: https://neweasterneurope.eu/2022/03/07/democracy-and-putins-obsession-with-a-nazi-anti-russia-ukraine/. (last accessed: 20.12.2022)

after gaining control of Ukrainian airspace, which proved misleading and demonstrated the information narrative for future Russian escalations in Ukraine[139]. In addition, even before the war began, Russia had repeatedly used the same old tactics of "information warfare", such as assuming that the eastern expansion of NATO was the main cause of the invasion of Ukraine[140].

4. Social domain

Different means and tools are used in order to produce the social unrest required for hybrid strategies to persist or flourish with sociocultural divisions created, exacerbated, or exploited in the social/societal realm. The ultimate objective of this kind of activity is to influence the functioning of the target State in order to foster an environment that is conducive to hybrid operations, with particularly sensitive areas that are frequently debated in Western nations, such as unemployment, poverty, and education, making for easy targets while particularly alluring are issues that can start or perpetuate a crisis including the global financial crisis, illegal immigration, and terrorist acts[141]. In this case, it is believed that another aspect of Russia's hybrid tactics against the West is the "weaponization" of migrants, especially through the use of migrants from Africa, Central Asia, and the Middle East, apart from Ukraine, to destabilize Europe, in addition to the fact that Russia's hybrid actions also rage along the borders between the Russian proxy State of Belarus and Latvia, Lithuania, and Poland[142]. By generating migration waves that will destabilize Europe, Russia is harming the European continent without directly using military force against countries outside Ukraine[143].

Additionally, civil power is used as a tool for hybrid strategies in the form of protests, demonstrations, consumer boycotts, fundraising, and the like and although the use of civil society as a hybrid threat has a long history, this method became more prevalent during the Cold War with the most widely reported example of the Soviet intelligence that took control

[139] Institute for the Study of War, "Ukraine conflict update 11", 2022, https://understandingwar.org/backgrounder/ukraine-conflict-update-11. (last accessed: 20.12.2022)
[140] Tae Eun Song, "Information/Psychological Warfare in the Russia-Ukraine War: Overview and Implications", *Institute of Foreign Affairs and National Security*, 2022, p.2.
[141] Georgios Giannopoulos et al., *supra* note 24, p. 30.
[142] Daniel Kochis, "Russia's Weaponization of Migrants Hasn't Gone Away", *Washington Times*, 2022, available at: https://www.washingtontimes.com/news/2022/nov/16/russias-weaponization-of-migrants-hasnt-gone-away/ (last accessed: 20.12.2022)
[143] Elisabeth Braw, "Russia Is Taking Advantage of the Invasion-Stirred Migration Crisis", Foreign Policy, available at: https://foreignpolicy.com/2022/07/18/russia-ukraine-war-migration-food-crisis-putin/ (last accessed: 20.12.2022)

of parts of the antiwar and anti-nuclear protest movements in North America and Western Europe, turning them into hybrid actors against the Western alliance and its continued reliance on nuclear weapons as a deterrent[144]. In the 2022 Ukrainian conflict, The Russian Orthodox church is considered to have been serving as an instrument in the country's hybrid strategy against Ukraine by carrying out various goals and tasks set out by Russia's special services including active propaganda[145], while since the beginning of Russia's military intervention in 2014, pro-Moscow priests have been caught leading Russian ideological campaigns engaging in religious propaganda which is not limited to internal affairs[146].

5. Information technology domain

Information technology as a hybrid threat refers to the application of information technology means to gain access to target State networks or systems, through cyberattacks to influence political events and activities and for democratic manipulation. Although cyberspace may be a weapon in this more advanced idea of hybrid conflict, it nonetheless remains a multifaceted instrument employed by several players at various levels due to its offensive and defensive capabilities. Cyber power is used in a variety of forms, including the manufacture or modification of hardware for malicious purposes, cyber attacks by hackers, identity theft by organized cybercrime groups, phishing, interception and manipulation of data, modification of website content for propaganda or sabotage, suppression of web services, etc., as well as to intercept and monitor web-based communications and to manipulate and sabotage critical infrastructure that relies on web-based services[147].

Although cyber activities are still quite easy to conceal and tracing them to their originators is usually impossible, Russia has nonetheless been accused of malicious cyber activities several times in recent years and these activities have included tactics, techniques, and procedures that have significant overlap between cyber activism, cybercrime, and government organisations

[144] Janne Jokinen, Magnus Normark, *supra* note 109, p. 25.
[145] Oleksii Platonov ,"'Kremlin's agents in robes' – or the role of Russian Church in the Ukraine war", *Geneva solutions*, 2022, available at: https://genevasolutions.news/ukraine-stories/kremlin-s-agents-in-robes-or-the-role-of-russian-church-in-the-ukraine-war (last accessed: 20.12.2022).
[146] Tetyana Zhurman, "Religion as a Hybrid War Weapon to Achieve Russia's Geopolitical Goals", The Jamestown Foundation, Global Research & Analysis, 2021, available at: https://jamestown.org/religion-as-a-hybrid-war-weapon-to-achieve-russias-geopolitical-goals/ (last accessed: 20.12.2022).
[147] Janne Jokinen, Magnus Normark, *supra* note 109, p. 15.

conducting cyber attacks[148]. The cyberattacks carried out in Georgia in 2008-2009 are a good example of how cyberspace was used as a means of hybrid warfare for geopolitical interests. The hackers carried out the attacks from different countries and Georgia was left with an enormous loss of territories, an information vacuum and psychological pressure on the population. These types of attacks had a significant psychological impact, as in many cases these servers were used in media and communications facilities and hindered the government's ability to communicate effectively with the public[149]. In addition, on April 26, 2007, a cyberattack was perpetrated against the Estonian government's websites, culminating in a disruption of Internet service. First, the Estonian Prime Minister's website was attacked, then the President's, and shortly thereafter several ministries went down, while later, schools, television stations, and newspaper agencies were also paralyzed, as well as the banking system, triggering fears in society of an economic collapse[150]..

Cyberattacks are an integral part of Russia's hybrid strategy since they were used by Russia as early as the Georgia-Russia conflict in 2008, most notably during Russia's annexation of Crimea in 2014, and through its continued support of militant rebel groups in eastern Ukraine over the years. It is widely alleged that Russia has "cyber warriors" who have developed capabilities and tools and interfere with other countries' achievements, secret files, and information systems, as in the same context Russia was accused in 2016 of trying to influence the U.S. presidential campaign[151]. As for the current conflict in Ukraine, Russian forces began their offensive actions on February 24, while simultaneous cyber-attacks were carried out against Ukraine, damaging key government websites such as the Ministry of Foreign Affairs, infrastructure, and others, while later two of Ukraine's largest credit institutions, were attacked[152]. Ukraine was the target of 43 documented cyberattacks between May 2014 and March 2022, 56% of which can be explicitly traced to Russia as the threat actor[153]. The target sectors of these attacks are the financial and energy sectors to spread panic and insecurity by disrupting services, the telecommunications sector mainly involving disinformation and defacing public websites, the public and government sectors to spread disinformation from

[148] Sandor Fabian, "The Russian hybrid warfare strategy – neither Russian nor strategy", *Defense & Security Analysis*, 2019, p. 319.
[149] *Ibid.*
[150] Anzhela Parulua, Hybrid Warfare – Contemporary Concept in Georgia's External Security", Master's thesis, *Tallinn University of Technology*, 2018, p. 42.
[151] Christopher Chivvis, *supra* note 116, p. 3.
[152] Josías David, *supra* note 137.
[153] Headmind Partners, "Cyberattacks in hybrid warfare: the case of Russia/Ukraine War", 2022, available at: https://www.headmind.com/en/cyberattacks-hybrid-warfare/. (last accessed: 20.12.2022).

official sources or simply shut down their services, and finally the citizens themselves through phishing and hacking their email and social media accounts[154]. In addition, since the invasion, the European Union has seen a number of cyberattacks on critical energy infrastructure, particularly green technologies. In particular, Germany's renewable energy sector has been affected by cyberattacks since the invasion of Ukraine. On February 24, for example, a cyberattack on a satellite providing services to Ukraine disabled 5,800 wind turbines in Germany and Central Europe[155], while on April 12, another cyberattack on a German wind energy company caused the daylong shutdown of the remote control systems of 2,000 wind turbines while a turbine manufacturer company also discovered a security incident on March 31 that forced it to shut down its information-technology systems[156].

6. Scientific and technological domain

It is possible to use scientific and technological means, including technological innovations, as a hybrid threat strategy, in part or in full, to advance a political or economic agenda. New technologies have a catalytic effect on hybrid tools and strategies because they improve the prerequisites for hybrid action, increase the number of hybrid actors, and assist in expanding both the scope of their activities and their chances of success. In hybrid warfare, artificial intelligence technology in particular is seen as driving an evolution in which dominance in information and understanding may prove critical by increasing the speed, precision, and efficiency with which information can be harnessed and put into action, as artificial intelligence will allow groups to mimic, influence, and change behaviour, thereby affecting the social and economic impact of hybrid conflict[157]. In addition, public services, both government and private, are increasingly being shifted to privately owned technology platforms, and such developments invite attempts to control and manipulate the activities of technology companies

[154] *Ibid.*
[155] Joseph Henry, "Europe Cyberattack Results to 'Massive' Internet Outage | About 5,800 Wind Turbines Went Offline", *Tech Times*, 2022, available at: https://www-techtimes-com.cdn.ampproject.org/c/s/www.techtimes.com/amp/articles/272624/20220305/europe-cyberattack-results-massive-internet-outage-5-800-wind-turbines.htm. (last accessed: 20.12.2022).
[156] Catherine Stupp, "European Wind-Energy Sector Hit in Wave of Hacks", *The Wall Street Journal*, 2022, available at: https://www.wsj.com/articles/european-wind-energy-sector-hit-in-wave-of-hacks-11650879000#:~:text=European%20Wind-Energy%20Sector%20Hit%20in%20Wave%20of%20Hacks,governments%20move%20to%20transition%20away%20from%20Russian%20fuel?msclkid=7f9116ddc7cd11ec9178cad5c4c63099. (last accessed: 20.12.2022).
[157] Ralph Thiele, "Artificial Intelligence – A key enabler of hybrid warfare", *Hybrid CoE Working Paper 6*, 2020, p. 5.

to gather information, influence, interfere, and disrupt[158]. The Covid-19 pandemic showcased an example of how new technologies can be used as a tool since before the virus emerged the production of vaccines and protective equipment was centralized in a few countries, but when it emerged, the public and government agencies were willing to pay almost any price to obtain them[159], which resulted in both criminal activity and the so-called "vaccine diplomacy" by countries where governments were in power.[160].

Apart from the above there is growing concern about hybrid threats in the space-based services domain as more countries and commercial actors engage in space and the increasing use of and dependence on space for national security has led more countries to consider developing their own counterspace capabilities that can be used to disrupt or destroy space systems[161]. Space-based services include communications, remote sensing, and science and exploration and most instruments that can target the space domain leverage the linkage of space assets to other domains, as it is closely linked to the military/defense, economic, infrastructure, information, and intelligence domains, and the potential cascading effects if these domains are compromised even temporarily[162].

7. Legal domain

It is a reality that hybrid actions not only pose a challenge to international peace and security, but also undermine the current legal framework by challenging the rules of the game of international law[163]. The legal domain refers to the set of legal rules, measures, processes, and institutions, including their normative and substantive manifestations, that are or can be used in a hybrid threat campaign to achieve legal or non-legal effects[164]. Law can become a toolbox with which potential adversary actors can exert influence, which means they play a significant

[158] Janne Jokinen, Magnus Normark, *supra* note 109, pp. 25-26.
[159] *Ibid.*
[160] Michael Leigh: "Vaccine diplomacy: soft power lessons from China and Russia?", *Bruegel Blog*, 2021, available at: https://www.bruegel.org/2021/04/vaccine-diplomacy-soft-power-lessons-from-china-and-russia/. (last accessed: 20.12.2022).
[161] Weeden, Brian, and Vicotria Samson, eds. 2019. *Global Counterspace Capabilities: An Open Source Assessment*. Secure World Foundation, 2020, p. ix.
[162] Georgios Giannopoulos et al., *supra* note 24, pp. 27-28.
[163] Sascha Bachmann, Andres Mosquera, "Lawfare and hybrid warfare – how Russia is using the law as a weapon", Amicus Curiae, Issue 102, 2015, p. 27.
[164] Georgios Giannopoulos et al., *supra* note 24, p. 30.

but very complex new role in the threat maps, because when an adversary operates across legal boundaries and obfuscates its actions, the adversary's decision-making processes are undermined[165]. However, hybrid threats in this domain and the actions behind hybrid strategies are difficult for a State to identify as use of coercive force because they are designed to remain below certain thresholds for detection or response, and the actions taken by the hostile actor are not explicitly or necessarily illegal or may be part of normal lawful activities[166]. A hybrid threat campaign in this domain may be supported by an actor using a variety of legal tools, such as exploiting legal thresholds, gaps, complexity, and uncertainty; evading its legal obligations; avoiding accountability; exploiting the target State's non-compliance with the law; exploiting the target State's lack of legal interoperability; using its own regulatory powers under domestic law; and using law and legal processes to create narratives and counternarratives[167].

For example, following Russia's annexation of Crimea in 2014 and subsequent occupation of eastern Ukraine, President Putin declared that Russia had intervened under international law "to defend the rights of the Russian-speaking population living abroad", underscoring Russia's consistent use of "lawfare" to support its broader goals[168]. On this legal battlefield, Russia has put forward a series of legal and normative arguments to justify its coercive actions in Crimea and to support the process of "deniable" intervention aimed at blurring the legal and the illegal and creating pretexts for justification, in part by exploiting some areas of uncertainty in international law, claiming to intervene by invitation, citing some previous cases of intervention, while making unsubstantiated claims about "facts", such as threats against Russians and Russian speakers and pointing to the Western focus on protecting people and Kosovo's secession from Serbia[169]. These weak assertions were probably made not with the expectation that they would convince of the legitimacy of Russian actions, but to create sufficient uncertainty in the international community at large, especially among EU states, to limit punitive Western reactions[170].

[165] Tiina Fem, "Laws in the Era of Hybrid Threats." *Hybrid CoE Strategic Analysis,* 2017, p. 2.
[166] *Ibid,* p.3.
[167] Georgios Giannopoulos et al., *supra* note 24, pp. 30-31.
[168] Sascha Bachmann, Andres Mosquera, *supra* note 163.
[169] Roy Allison, "Russian 'deniable' intervention in Ukraine: how and why Russia broke the rules", *supra* note 111, pp. 1259-1260.
[170] *Ibid.*

C. Cross – domain deterrence

Deterrence is considered the most important tool and the foundational strategy for countering hybrid threats because it can prevent them from developing in the first place. However, the characteristics of hybrid warfare complicate the traditional deterrence calculus and necessitate updating the traditional approach to deterring modern hybrid threats[171]. Deterrence is defined as the practice of discouraging or restraining a nation-state from taking unwanted actions involving an effort to stop or prevent an action, and is distinguished in classic literature in two categories: deterrence by denial and deterrence by punishment[172]. The first three waves of deterrence theories that emerged after World War II focused on conventional deterrence in the event of aggression, including the possible use of nuclear weapons, while the fourth wave of deterrence theories developed in the post-Cold War period in response to real-world developments focused on asymmetric threats[173]. Given the increasing number of ways and means by which hostile acts can be committed and their cross-domain nature, strategists have begun to engage in the application of deterrence in new domains and cross-domain deterrence (CDD) in both traditional and new domains[174]. Cross-domain deterrence is defined as "the use of threats in one domain, or some combination of different threats, to prevent actions in another domain that would change the status quo"[175]. In this context, it is argued that the cross-domain deterrence which in the classical deterrence theory is a concept developed predominantly in a military context, is also applicable to new challenges of deterring aggression in the in the domains of space and cyberspace[176] as well as to the hybrid domain[177].

Hybrid Coe's Deterrence Playbook suggests that the deterrence theory and practice can be applied to deal with activities below the threshold of military response, as hybrid threats,

[171] Sean Monaghan (ed.), *Countering Hybrid Warfare,* Multinational Capability Development Campaign Project (MCDC), 2019, p. 35.
[172] Michael J. Mazarr, "Understanding Deterrence", *RAND Corporation, 2018,* p.2.
[173] Jeffrey Knopf, "The Fourth Wave in Deterrence Research", *Contemporary Security Policy*, Volume 31(1), 2010, pp. 1-2.
[174] Tim Sweijs, Samuel Zilincik, "The Essence of Cross-Domain Deterrence", in Frans Osinga, Tim Sweijs (eds.), *Deterrence in the 21st Century—Insights from Theory and Practice*, Netherlands Annual Review of Military Studies 2020, Springer, 2021, p.131.
[175] Jon Lindsay, Erik Gartzke, "Introduction: Cross-Domain Deterrence, From Practice to Theory", in Erik Gartzke, Jon Lindsay (eds.), *Cross-Domain Deterrence: Strategy in an Era of Complexity*, Oxford University Press, 2019, p.6.
[176] King Mallory, 'New Challenges in Cross-Domain Deterrence', *RAND Corporation,* 2018, p. 6.
[177] Tim Sweijs, Samuel Zilincik, *Cross Domain Deterrence and Hybrid Conflict*, The Hague Centre for Strategic Studies, The Hague, 2019, p. 10.

emanating from hostile State and non-State actors[178]. Dealing with challenges posed by hybrid threats requires effective deterrence that combines resilience and crisis response and goes well beyond military-centric classical deterrence thinking, as a hostile actor may pursue hybrid activities outside the military domain and therefore deterrence requires a range of military and nonmilitary response options[179]. In this context, deterrence by denial aims to increase resilience and minimize the consequences of hybrid attacks by securing the following: the political domain, by preventing dependences of political parties and organization or influences over political decision-making; the military domain for homeland resilience; the economic domain by ensuring the security and diversity of strategic resources and combating corruption; the social domain through education and situational awareness; infrastructures, through physical and nonphysical measures; and the information domain, through proactive and transparent cooperation with the media[180]. Deterrence by punishment for a coordinated response through horizontal escalation include: military measures calibrated to maintain proportionality while maximizing coercive potential; measures focused on the political domain ranging from travel restrictions to expulsion of diplomats and revocation of voting rights in international organizations; economic measures, such as sanctions and financial penalties; civil measures related to upholding the rule of law; and in the information domain, measures to ensure media transparency and counter misinformation and disinformation, while in the cyber domain, development of offensive cyber measures[181]. Deterrence by denial concerns all phases and severity levels of hybrid threats, while deterrence by punishment can be achieved mainly in the coercion phase/aggression level of hybrid threats.

Also recently examined is the prospect of a fifth wave of theory that extends the concept of deterrence across the spectrum of hybrid threats, continuing the elements of previous waves on psychology, the role of military force, the central role of State actors, but also adding new elements, including the prevalence of nonmilitary hybrid threats, the unprecedented complexity, diversity, and interconnectedness, a large sub-state component, and a shift away from punishment to denial through resilience[182]. Like any strategy, deterrence has its limits, for the lower limit of deterrence is tolerance of the least serious hybrid threats and lack of attribution as well as the complexity of the cross-domain logic of deterrence make it necessary

[178] Vytautas Keršanskas, "Deterrence: Proposing a more strategic approach to countering hybrid threats", Hybrid CoE Paper 2, 2020.
[179] *Ibid*, pp. 7-8.
[180] Sean Monaghan, *supra* note 171, pp. 45-46.
[181] *Ibid*, p. 57.
[182] Hybrid CoE, "Deterring hybrid threats: Towards a fifth wave of deterrence theory and practice", *supra* note 1,

to address hybrid threats even beyond deterrence[183]. In this respect the common threat of hybrid warfare within the Euro-Atlantic area presents an opportunity for NATO and the European Union to develop their strategic partnership even further in cooperation as well as in parallel, coordinated and complementary ways[184]. Since the deterrence policy of NATO as a military alliance is based on a rapid military response in the case of hybrid warfare, the EU offers a variety of policy tools that can be used in the context of hybrid threats[185]. This indicates that NATO and the EU could form an effective institutional tandem that has a wide range of political and military tools at its disposal[186].

[183] *Ibid*, pp. 31-33.
[184]Alexandros Papaioannou, "Strengthening EU-NATO relations", *NATO Review*, 2019, available at: https://www.nato.int/docu/review/articles/2019/07/16/strengthening-eu-nato-relations/index.html, (last accessed: 20.12.2022).
[185] Peter Pindjak, "Deterring hybrid warfare: a chance for NATO and the EU to work together?", *NATO Review*, 2014, available at: https://www.nato.int/docu/review/articles/2014/11/18/deterring-hybrid-warfare-a-chance-for-nato-and- the-eu-to-work-together/index.html, (last accessed: 20.12.2022)
[186] *Ibid.*

Conclusion

From the above analysis, it can be concluded that the concept of hybrid threats has its origins in history and although hybrid threats have evolved over time due to technological advances, the basic concept has remained the same: to serve the interests of a State or a group by harming the adversary without or by not only using direct military force, and occasionally in such a way that the other side is not even aware of it[187]. Hybrid threats, cited as one of the greatest challenges to international security in the twenty-first century, have attracted the attention of several academic and military analysts in recent years. Events in Ukraine, Syria, and other conflict zones have demonstrated the sensitivity of modern society and militaries to such operations and have led to a sudden increase in attention to hybrid threats. In the case of international actors, the use of hybrid threats can ensure that their primary objectives can be achieved with minimal effort and, in most cases, without the use of force, while depriving the target of the ability to defend itself. In the meantime, hybrid warfare has the potential to symbolize the conflict of the twenty-first century, a new type of direct yet indirect combat with short and medium term consequences that cannot be predicted.

In the coming years, hybrid strategies will continue to grow, gain more adherents, and take multiple forms. Hybrid threats may become increasingly aggressive and numerous as attempts to mitigate their impact and identify the most effective protection and control measures in most cases are made without a clearly identifiable attacker and without clear means to address them. Because the development of a specialized hybrid threat strategy against a State cannot always be considered an act of aggression, hybrid threats are portrayed as even more important than conventional warfare in democratic societies. Against this backdrop, hybrid threats are a complicated and multidimensional phenomenon. Therefore, a holistic, cross-domain approach for countering hybrid threats that includes as most important political, military, diplomatic, social, information and economic means is considered essential. The actions taken to counter hybrid threats or mitigate their effects are beyond the capabilities of any single actor and require coordinated efforts and a comprehensive strategy. Countering hybrid threats requires a wide range of tools to be successful. Finding coordinated responses at a higher level requires not

[187] Toumpani Margarita, *supra* note 3, p. 44.

only bringing together existing State actors, but also merging and integrating civilian and military instruments and involving international and non-governmental organizations[188].

Last but not least, to better understand this phenomenon, efforts must be made to develop deterrence mechanisms, detect hybrid threats as early as possible, share information among States and among specialized organizations, build cyber defense capabilities, as well as develop effective tools to punish those who support, promote, or directly employ hybrid attack methods, whether individuals, organizations, or nations. The aggressive activities of recent years have taken the entire world by surprise, and many have argued that the actions the world has witnessed are an expression of a new and revolutionary strategic concept of hybrid warfare. Although the specific characteristics of this concept are still debated, there is widespread agreement that the focus of the main actors today has shifted from traditional military capabilities to non-military means, and that the human mind is considered the primary battlefield [189]. Therefore, understanding the concept of hybrid threats and its cross-domain implications should not be just a theoretical endeavor, but a top priority for government agencies and international organizations to address the phenomenon in a comprehensive and holistic manner, leading to an improved international security environment.

[188] Aurelian Raţiu, "Countering Hybrid Threats by Integrating Civilian-Military Capabilities", *International Scientific Conference The Knowledge Based Organization*, Volume. 22 (1), 2016, p. 109.
[189] Sandor Fabian, *supra* note 148, p. 322.

List of Sources

Books

Bjorgo Tore, *Root causes of Terrorism: myths, reality and ways forward*, Routledge, 2005

Fridman Ofer, *Russian "Hybrid Warfare": Resurgence and Politicisation*, Hurst & Company, 2018

Galeotti Mark, *The Weaponisation of Everything, A field Guide to the New Way of War*, Yale University Press, 2002.

Gareev Makhmut, *If War Comes Tomorrow? The Contours of Future Armed Conflicts*, Jacob Kipp (ed.), Frank Cass Publishers, 1998.

Howard Michael, Paret Peter (eds), *Carl von Clausewitz,On War*, Princeton University Press, 1976

Knox MacGregor, Murray Williamson (eds.), *The Dynamics of Military Revolution 1300-2050*, Cambridge University Press, 1st edition, 2001

Laqueur Walter, *Terrorism*, Weidenfield and Nicholson, 1977

Larson Eric, Eaton Derek, Nichiprouk Brian, Szayna Thomas, *Assessing Irregular Warfare. A Framework for Intelligence Analysis*, RAND, 2008

Mazarr Michael, Cheravitch Joe, Hornung Jeffrey, Pezard Stephanie, *What Deters and Why, Applying a Framework to Assess Deterrence of Gray Zone Aggression*, RAND Corporation, 2021

Monaghan Sean (ed.), Countering Hybrid Warfare, Multinational Capability Development Campaign Project (MCDC), 2019

Morgenthau Hans, *Politics among nations: The struggle for power and peace,* Alfred A. Knopf, 1948

Nye Joseph, *Soft Power: The Means to Success in World Politics*, New York: Public Affairs, 2004

Smith Paul, *On Political War*, Washington: National Defense University Press, 1989

Sweijs Tim, Zilincik Samuel, *Cross Domain Deterrence and Hybrid Conflict*, The Hague Centre for Strategic Studies, The Hague, 2019

Waltz Kenneth, *Theory of International Politics*, Addison-Wesley Publishing Company, 1979

Weigley Russell, *The American way of war: a history of united states military strategy and policy*, Macmillan, 1973

Articles

Allison Roy, "Russian 'deniable' intervention in Ukraine: how and why Russia broke the rules", *International Affairs* 90 (6), 2014

Bachmann Sascha, Mosquera Andres, "Lawfare and hybrid warfare – how Russia is using the law as a weapon", Amicus Curiae, Issue 102, 2015

Banasik Miroslaw, "Russia's Hybrid War in Theory and Practice", *Journal on Baltic Security, Vol. 2, No. 1*., 2016

Biddle Stephen, 'Military Power', *Princeton University Press*, 2004

Boot Max, Doran Michael, "Political Warfare", *Council on Foreign Relations*, 2013

Braw Elisabeth, "Russia Is Taking Advantage of the Invasion-Stirred Migration Crisis", Foreign Policy, available at: https://foreignpolicy.com/2022/07/18/russia-ukraine-war-migration-food-crisis-putin/

Cantwell Douglas, "Hybrid War as Strategy and Policy", *American Society of International Law*, Volume 21 (14), 2017.

Cardash Sharon, Cilluffo Frank and Tussing Bert, 'HPSI Issue Brief: Mexico and the Triple Threat', 'The Hybrid Threat: Crime, Terrorism and Insurgency in Mexico', A Joint CSL-HSPI Study, 2011

Chivvis Christopher, "Understanding Russian "Hybrid Warfare" and What Can Be Done About it", *Rand Corporation*, 2017

Daniel Kochis, "Russia's Weaponization of Migrants Hasn't Gone Away", *Washington Times,* 2022, available at: https://www.washingtontimes.com/news/2022/nov/16/russias-weaponization-of-migrants-hasnt-gone-away/

Davis John, "Defeating Future Hybrid Threats: The Greatest Challenge to the Army Profession of 2020 and Beyond", *Military Review,* 2013

Dourado Maria, Leite Alexandre, Nobre Fábio, "Hybrid Warfare Vs. Gibridnaya Voyna: The Different Meanings of Hybrid Conflicts for West and Russia", *Revista da Escola de Guerra Naval,* Volume 26(1), 2020

Dubik James, Vincent Nic, "America's global competitions: the gray zone in context'", Institute for the Study of War, 2018

Dunn-Lobban Andrew, "Hybrid Warfare, Hybrid Threats and the Demarcation of Conflict, Thesis, *University of New South Wales*, 2016

Fabian Sandor, "Irregular Versus Conventional Warfare: A Dichotomous Misconception", *Modern War Institute,* 2021, available at: https://mwi.usma.edu/irregular-versus-conventional-warfare-a-dichotomous-misconception/

Fabian Sandor, "The Russian hybrid warfare strategy – neither Russian nor strategy", *Defense & Security Analysis*, 2019

Filipec Ondřej, "Hybrid Warfare: Between Realism, Liberalism and Constructivism*", Central European Journal of Politics,* Volume 5 (2), 2019

Fogt Morten, “Legal Challenges Or “Gaps” By Countering Hybrid Warfare – Building Resilience In Jus Ante Bellum”, *Southwestern Journal Of International Law*, Vol. XXVII:1, 2020

Forest James, “Political Warfare and Propaganda: An Introduction”, *Journal of Advanced Military Studies*, Volume 12(1), 2021

Freedman Lawrence, ‘The Counterrevolution in Strategic Affairs’, *Dædalus*, Volume 140(3), 2011

Fridman Ofer, “Hybrid Warfare or Gibridnaya Voyna?”, *The RUSI Journal*, Volume 162(1), 2017

Fridman Ofer, “The Russian perspective on information warfare: conceptual roots and politicisation in Russian academic, political, and public discourse”, *Defence Strategic Communications*, Volume 2, 2017

Galeotti Mark, “Crime and Crimea: Criminals as allies and agents”. *Radio Free Europe Radio Liberty*, 2014, http://www.rferl.org/content/crimea-crime-criminals-as-agents-allies/26671923.html

Galeotti Mark, “The ‘Gerasimov Doctrine’ and Russian Non-Linear War,” Moscow’s Shadows, 2014, available at: https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war.

Gerasimov Valery, “The Value of Science Is in the Foresight – New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations” Military Review, 2016, (Originally published in Military-Industrial Kurier, 27 February 2013.)

Giannopoulos Georgios, Smith Hanna, Theocharidou Marianthi, “The Landscape of Hybrid Threats: A conceptual model”, *Publications Office of the European Union*, 2021

Glenn Russell, “Thoughts on “Hybrid” Conflict*”, Small Wars Journal*, 2009

Göransson Markus, “Understanding Russian thinking on gibridnaya voyna”, in Mikael Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm (eds.) Hybrid Warfare Security and Asymmetric Conflict in International Relations, I.B. Tauris, 2021, p. 83.

Gray Colin, ‘Categorical Confusion? The Strategic Implications of Recognizing Challenges Either as Irregular or Traditional’, *Strategic Studies Institute*, 2012

Guerrero Josias, “Ukraine Conflict: Hybrid Warfare and Conventional Military Intervention”, Revista Seguridad y Poder Terrestre, Volume 1(1), 2022, available at: https://ceeep.mil.pe/2022/07/07/ukraine-conflict-hybrid-warfare-and-conventional-military-intervention/?lang=en#post-20719-endnote-17.

Hadjitodorov Stefan and Sokolov Martin, “Blending New-generation Warfare and Soft Power: Hybrid Dimensions of Russia-Bulgaria Relations”, *Connections: The Quarterly Journal,* 17 (1), 2018

Haeni Reto, “Information Warfare: An introduction”, *The George Washington University, Cyberspace Policy Institute,* 1997

Headmind Partners, “Cyberattacks in hybrid warfare: the case of Russia/Ukraine War”, 2022, available at: https://www.headmind.com/en/cyberattacks-hybrid-warfare/.

Henry Joseph, “Europe Cyberattack Results to 'Massive' Internet Outage, About 5,800 Wind Turbines Went Offline”, *Tech Times,* 2022, available at: https://www-techtimes-com.cdn.ampproject.org/c/s/www.techtimes.com/amp/articles/272624/20220305/europe-cyberattack-results-massive-internet-outage-5-800-wind-turbines.htm.

Hoffman Frank, “Conflict in the 21st Century: The Rise of Hybrid Wars”, *Potomac Institute for Policy Studies*, 2007

Hoffman Frank, “Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges” *Prism*, Vol. 7, No. 4, 2018

Hoffman Frank, “Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict”, *Strategic Forum*, No. 240, 2009

Hoffman Frank, “Hybrid vs. Compound war”, *Armed Forces Journal*, 2009

Institute for the Study of War, “Ukraine conflict update 11”, 2022, https://understandingwar.org/backgrounder/ukraine-conflict-update-11.

Jacobs John, Kitzen Martijn, “Hybrid Warfare”, *Oxford Bibliographies*, 2021

Jasper Scott, Moreland Scott, ‘The Islamic State is a Hybrid Threat: Why Does That Matter?’, *Small Wars Journal*, Volume 10(12), 2014

Jokinen Janne, Normark Magnus, “Hybrid threats from non-state actors: A taxonomy”, *Hybrid CoE Research Report 6,* 2022

Josep Borrell, “The fight continues against the food insecurity that Russia’s war is creating”, European Union External Action, 2022, available at: https://www.eeas.europa.eu/eeas/fight-continues-against-food-insecurity-russia’s-war-creating_en?s=232

Kamusella Tomasz, “Democracy and Putin’s obsession with a “nazi anti-Russia” Ukraine”, *New Eastern Europe*, 2022, available at: https://neweasterneurope.eu/2022/03/07/democracy-and-putins-obsession-with-a-nazi-anti-russia-ukraine/.

Kennan George, “The Inauguration of Organized Political Warfare,” *History and Public Policy Program Digital Archive*, 1948

King Mallory, “New Challenges in Cross-Domain Deterrence”, *RAND Corporation,* 2018

Kiras James, “Irregular warfare: terrorism and insurgency in Strategy in the Contemporary World”, in John Baylis, James Wirtz, Colin Gray (eds.), *Strategy in the Contemporary World*, Oxford University Press, 2018

Kiras James, “Irregular warfare: terrorism and insurgency in Strategy in the Contemporary World”, in John Wither James, “Making Sense of Hybrid Warfare”, *Connections: The Quarterly Journal*, Volume 15 (2), 2016

Klein David, “Report: In Crimea and the Donbas, Organized Crime Reigns Supreme”, Organized Crime and Corruption Reporting Rroject, 2022, available at: https://www.occrp.org/en/daily/16570-report-in-crimea-and-the-donbas-organized-crime-reigns-supreme

Knopf Jeffrey, “The Fourth Wave in Deterrence Research”, *Contemporary Security Policy*, Volume 31(1), 2010

Kofman Michael, Rojansky Matthew, “A closer look at Russia’s hybrid war”, *Kennan Cable,* No. 7, 2015

Lindsay Jon, Gartzke Erik, “Introduction: Cross-Domain Deterrence, From Practice to Theory”, in Erik Gartzke , Jon Lindsay (eds.) *Cross-Domain Deterrence: Strategy in an Era of Complexity,* Oxford University Press, 2019

Lohmann Sarah, “Russian Gas, Green Technology, and the Great Sacrifice”, *Georgetown Journal of International Affairs*, 2022, available at: https://gjia.georgetown.edu/2022/06/23/russian-gas-green-technology-and-the-great-sacrifice%EF%BF%BC/

Manciulli Andrea, “Daesh and the terrorist threat: from the Middle East to Europe”, *Foundation for European Progressive Studies*, 2015

Marcuzzi Stefano, “Hybrid Warfare in Historical Perspectives”, *Nato Foundation Defense College*, 2018

Mazarr Michael, “Understanding Deterrence”, *RAND Corporation, 2018*

McCuen John, “Hybrid Wars”. *Military Review*, Volume 88 (2), 2008

McCulloh Tim, Johnson Rick, “The Inadequacy of Definition and the Utility of a Theory of Hybrid Conflict: Is the “Hybrid Threat” New?”, *JSOU Report* 13-4, 2013

Mearsheimer John, “Structural Realism”, in Tim Dunne, Milja Kurki, Steve Smith (Eds.) *International Relations Theories: Discipline and Diversity*, Oxford University Press, 2010

Morgenthau Hans, “The primacy of the National Interest”, *The American Scholar*, Volume 18(2), 1949

Nemeth William, “Future war and Chechnya: a case for hybrid warfare”, *Calhoun Institutional Archive of the Naval Postgraduate School,* 2002

Ntamplia Eleni, "The Immigration issue as the vanguard of an asymmetric hybrid war", Master’s Thesis, *Hellenic Army Academy – Technical University of Crete*, 2021

Nübel Anna, “The Rise of New Types of War, A Case Study on Russian Hybrid Warfare in the Ukrainian Crisis in 2014”, Master’s Thesis, University of Twente, 2020

Papaioannou Alexandros, “Strengthening EU-NATO relations”, NATO Review, 2019, available at: https://www.nato.int/docu/review/articles/2019/07/16/strengthening-eu-nato-relations/index.html.

Parulua Anzhela, Hybrid Warfare – Contemporary Concept in Georgia’s External Security”, Master’s thesis, Tallinn University of Technology, 2018

Petta Gomes da Costa, “Geopolitical Management through Irregular Actors", Athens: ATINER'S Conference Paper Series, 2016

Pindjak Peter, “Deterring hybrid warfare: a chance for NATO and the EU to work together?”, NATO Review, 2014, available at: https://www.nato.int/docu/review/articles/2014/11/18/deterring-hybrid-warfare-a-chance-for-nato-and- the-eu-to-work-together/index.html.

Platonov Oleksii , "'Kremlin's agents in robes' – or the role of Russian Church in the Ukraine war", *Geneva solutions*, 2022, available at: https://genevasolutions.news/ukraine-stories/kremlin-s-agents-in-robes-or-the-role-of-russian-church-in-the-ukraine-war

Primoratz Igor, "Terrorism", *The Stanford Encyclopedia of Philosophy*, 2015, <http://plato.stanford.edu/archives/spr2015/entries/terrorism/>.

Putnam Robert, "Diplomacy and Domestic Politics: The Logic of Two-Level Games" *International Organization, Voume.* 42 (3), 1988

Rácz András, "Russia's Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist", *The Finnish Institute of International Affairs,* Report 43, 2015

Raţiu Aurelian, "Countering Hybrid Threats by Integrating Civilian-Military Capabilities", *International Scientific Conference The Knowledge Based Organization*, Volume 22(1), 2016

Reyeg Fernando, Marsh Ned, "Filipino way of war: irregular warfare through the centuries", Master Thesis Naval Postgraduate School, Monterey California, 2011

Robinson Linda, Helmus Todd, Cohen Raphael, Nader Alireza, Radin Andrew, Magnuson Madeline, Migacheva Katya, "The Growing Need to Focus on Modern Political Warfare", *RAND Corporation*, 2019

Ruhle Michael, Grubliauskas Julijus, "Energy as A tool of Hybrid Warfare", *Nato Defense College*, 2015

Rumer Eugene, "The Primakov (Not Gerasimov) Doctrine in Action", *Carnegie Endowment for International Peace*, 2019, available at: https://carnegieendowment.org/2019/06/05/primakov-not-gerasimov-doctrine-in-action-pub-79254

Seyfettin Mehmet, "Hybrid Warfare Studies and Russia's Example in Crimea", *Akademik Bakış*, 2015

Snegovaya Maria, “Putin’s Information Warfare In Ukraine, Soviet Origins Of Russia’s Hybrid Warfare”, *Institute for the Study of War*, Report I, 2015

Stupp Catherine, “European Wind-Energy Sector Hit in Wave of Hacks”, *The Wall Street Journal*, 2022, available at: https://www.wsj.com/articles/european-wind-energy-sector-hit-in-wave-of-hacks-11650879000#:~:text=European%20Wind-Energy%20Sector%20Hit%20in%20Wave%20of%20Hacks,governments%20move%20to%20transition%20away%20from%20Russian%20fuel?msclkid=7f9116ddc7cd11ec9178cad5c4c63099

Sweijs Tim, Zilincik Samuel, “The Essence of Cross-Domain Deterrence”, in Frans Osinga, Tim Sweijs (eds.), *Deterrence in the 21st Century—Insights from Theory and Practice,* Netherlands Annual Review of Military Studies 2020, Springer, 2021

Tae Eun Song, “Information/Psychological Warfare in the Russia-Ukraine War: Overview and Implications”, *Institute of Foreign Affairs and National Security*, 2022

Tagarev Todor, “Hybrid Warfare: Emerging Research Topics, *Information & Security: An International Journal,* 2018, p. 291.

Thiele Ralph, “Artificial Intelligence – A key enabler of hybrid warfare”, *Hybrid CoE Working Paper 6*, 2020

Tienhoven Manon, “Identifying ‘Hybrid Warfare’”, Master’s Thesis, *University of Leiden*, 2016

Tiina Fem, “Laws in the Era of Hybrid Threats.” *Hybrid CoE Strategic Analysis,* 2017

Toumpani Georgia, “Hybrid Threats: A new menace in International Era and the Presence of Russia in the Balkan Peninsula”, *Master Thesis, University of Peloponnese*, 2019

Voitovych, Olga, Mackintosh Eliza, “Russian missile strikes pound Ukraine, knocking out power and putting entire country under air-raid alarm”, *CNN*, December 16, 2022, available at:

https://edition.cnn.com/2022/12/16/europe/ukraine-russia-missile-strikes-friday-intl/index.html

Weissmann Mikael, "Conceptualizing and countering hybrid threats and hybrid warfare", in Mikael Weissmann, Niklas Nilsson, Björn Palmertz, Per Thunholm (eds.), Hybrid Warfare Security and Asymmetric Conflict in International Relations, I.B. Tauris, 2021.

Zhurman Tetyana, "Religion as a Hybrid War Weapon to Achieve Russia's Geopolitical Goals", The Jamestown Foundation, Global Research & Analysis, 2021, available at: https://jamestown.org/religion-as-a-hybrid-war-weapon-to-achieve-russias-geopolitical-goals/

Other

European Commission, "Joint Framework on countering hybrid threats a European Union response", Joint Communication to the European Parliament and the Council, 2016, p. 2. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

Centre for strategic communication, Ministry of Culture and Information Policy of Ukraine "Grain as a Weapon. How Russian Aggression in Ukraine Threatens the World with Hunger", 2022, available at: https://spravdi.gov.ua/en/grain-as-a-weapon-how-russian-aggression-in-ukraine-threatens-the-world-with-hunger/

Intelligence Community Assessment, "Assessing Russian Activities and Intentions in Recent U.S. Elections", 2017.

Keynote speech by NATO Secretary General Jens Stoltenberg at the opening of the NATO Transformation Seminar, 2015

Merriam-Webster Dictionary, Definition of "Warfare", http://www.merriam-webster.com/dictionary/warfare.

Multinational Capability Development Campaign, "'A Deadlier Peril': The Role of Corruption in Hybrid Warfare", Countering Hybrid Warfare Project, 2019

NATO, "NATO's response to hybrid threats", 2019, available at: https://www.nato.int/cps/en/natohq/topics_156338.htm

North Atlantic Treaty Organization, "Input to a new NATO capstone concept for the military contribution to countering hybrid threats", 2010

The European Centre of Excellence for Countering Hybrid Threats, "Deterring hybrid threats: Towards a fifth wave of deterrence theory and practice", Hybrid CoE Paper 12, 2022.

The European Centre of Excellence for Countering Hybrid Threats, "Hybrid threats as a concept", https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

The Britannica Dictionary, "Hybrid", available at: https://www.britannica.com/dictionary/hybrid

The Britannica Dictionary, "Economic Warfare", available at: https://www.britannica.com/topic/economic-warfare

United States Department of Defense, Joint Publication 1-02: Dictionary of Military and Associated Terms (JP1-02), 2001

US Army, Training Circular 7-100 "Hybrid Threats", *United States Army Training and Doctrine Command*, 2010