CHAPTER IV. THE IMPACT OF HYBRID THREATS

Violeta VASILIAUSKIENĖ

Mykolas Romeris University

Maironio str. 27, LT 44211 Kaunas, Lithuania

E-mail v.vasiliauskiene@mruni.eu

ORCID ID: 0000-0003-0743-4015

Abstract. *This chapter explores the concept of hybrid threats to state security, aiming to shed light on the complexities and challenges posed by this modern form of warfare. Hybrid threats, which blend conventional and non-conventional methods, are increasingly prominent in the international political arena, involving a mix of military, paramilitary, and civilian tactics that challenge traditional security frameworks. The primary objective of this research is to dissect the nature of hybrid threats, understand their implications for state security, and evaluate the effectiveness of current response strategies. The research questions guiding this study include: What defines hybrid threats and hybrid warfare? How do these threats exploit legal and systemic vulnerabilities? What are the political and security challenges posed by hybrid threats, and how can states effectively counter them? To address these questions, the research employs a multidisciplinary approach, combining qualitative analysis of existing literature, case studies of recent hybrid warfare incidents, and the theoretical exploration of international law and security studies. This methodology enables the creation of a comprehensive understanding of the evolving nature of hybrid threats and the multifaceted strategies employed by both state and non-state actors. The findings reveal that hybrid threats operate in a grey zone of conflict, utilizing a blend of cyber operations, disinformation campaigns, economic pressure, and conventional military tactics. These methods aim to create ambiguity, making it difficult for states to identify perpetrators and respond effectively. The study*

concludes that there is a need for clearer legal definitions and frameworks to govern hybrid warfare, ensuring that states can effectively respond to these emerging threats while adhering to international law. This chapter contributes to the growing body of knowledge on hybrid threats, offering insights into their nature.

Keywords: *hybrid threats, hybrid warfare, legal response to hybrid threats, international humanitarian law*

Introduction

Ever since the Trojan War, all means have been used to gain an advantage in war; as far as the ingenuity of the human mind allows, any methods are used. War is a state in which one goes beyond the limits of coexistence with one's neighbors, where the human mind and the greatest cruelty manifest in the pursuit of victory (Žilinskas, 2012, p. 1206). Regulating such relations has always posed a significant challenge. Historically, many wars have exhibited elements of "hybridity," often characterized by lawlessness and "unconventional" methods. The latter term implies an assumption that war can be regulated by international institutions (Johnson, 2018, p. 141). Modern hybrid warfare is distinctive because it challenges the post-World War II order, particularly US leadership in the global order. This form of warfare contests the dominance of Western military power and scientific thought. Emerging military powers, unable to directly confront the United States, are seeking to assert regional or global dominance through alternative means (Vasiliauskienė & Stumbrys, 2023, pp. 142–143).

"During the last twenty years, the global balance of power has been called into question by the emerging ambitions of China, India, Pakistan, and Iran. And they have someone to learn from – since the collapse of the Soviet Union, Russia has been a leader on the front of hybrid threats" (Vasiliauskienė & Stumbrys, 2023, p. 143). The primary characteristic of hybrid warfare is the continuous blend of

military and non-military methods of influence, presenting unique political challenges for both the military and security services (Dykyi & Kharchenko, 2016, p. 8). The terms "hybrid warfare" or "hybrid threat" are used synonymously with the terms "ambiguous warfare," "fourth or fifth-generation warfare," "non-linear warfare," "low-intensive asymmetric war," "unconventional warfare," or "full-spectrum warfare," indicating perhaps something new and different from the normal understanding of conventional "warfare" (Fogt, 2021, p. 30).

"In 1948 the USA Central Intelligence Agency was charged by the USA National Security Council with conducting espionage and counter-espionage operations abroad. It therefore was, for operational reasons, not to create a new agency for covert operations, but in times of peace to place the responsibility for them within the structure of the Central Intelligence Agency and correlate them with espionage and counter-espionage operations under the over-all control of the Director of Central Intelligence" (National Security Council Directive on Office of Special Projects, 1948; Vasiliauskienė & Stumbrys, 2023 p. 143). Covert operations were defined as activities conducted or sponsored by the government against hostile foreign states or groups, or in support of friendly foreign states or groups, designed and executed in such a way that US government involvement was not apparent to unauthorized individuals. If these operations were exposed, the US government could plausibly deny any responsibility. Specifically, such operations would include any covert activities related to: propaganda; economic warfare; preventive direct action, including sabotage, anti-sabotage, demolition, and evacuation measures; subversion against hostile states, including assistance to underground resistance movements, guerrillas, refugee liberation groups, and support for indigenous anti-communist elements in threatened countries of the free world. Such operations shall not include armed conflict by recognized military forces, espionage, counter-espionage, and cover and deception for military operations (National Security Council Directive on Office of Special Projects,

1948). It can be seen that this definition includes hybrid actions according to the current understanding, but does not call them "hybrid" actions. Speaking about the history of the use of the term, Solmaz (2022) notes that "the use of the term 'hybrid warfare' dates to the 1990s. To our best knowledge, the term 'hybrid warfare' first appeared in Thomas Mockaitis' book entitled *British Counterinsurgency in the Postimperial Era in 1995*." In later years several authors used the term with somewhat differing definitions, although in essence all indicated that "hybrid warfare" was a mode of warfare neither purely conventional nor irregular (Solmaz, 2022, Vasiliauskienė & Stumbrys, 2023, p. 143). Further mentions of hybrid warfare are related to the description of the strategy used by Hezbollah in the 2006 Lebanon War (Van Puyvelde, 2015; Vasiliauskienė & Stumbrys, 2023, p. 143).

The 2014 Russian invasion of Ukraine resulted in the illegal annexation of Crimea and the creation of two breakaway provinces in the Donbas and Luhansk regions, where the terms "hybrid war" and "hybrid threats" further entered the modern vocabulary (Bajarūnas & Keršanskas, 2016). Here, for the first time, we clearly saw that a completely different kind of conflict was taking place. Instead of a clear enemy, in Crimea we saw "green men" without distinguishing marks (Bajarūnas & Keršanskas, 2016). Russia's subtle – and initially concealed – political and military actions to incite unrest, generate internal dissent, manipulate political factions, and create confusion in Ukraine hindered both local and international awareness of the risks and threats to Ukraine. This allowed Russia to present the world with the fait accompli occupation and fragmentation of the state. The fact that Russian troops had disguised their national identities and directly supported insurgent forces in Donbas and Luhansk drew significant attention across Western Europe and prompted NATO to closely examine such activities (NATO, 2024, p. 13).

As Hybrid CoE[5] analysis notes, the topic of hybrid threats has become a dominant subject in Europe's security landscape. While some stakeholders may view it as a new issue, it is actually as old as conflict and warfare itself, now repackaged and enhanced by evolving security dynamics and new tools, concepts, and technologies that target vulnerabilities in unprecedented ways. The advancement of these tools increases the reach and effectiveness of hybrid threats in achieving several major strategic objectives, such as undermining public trust in democratic institutions, deepening unhealthy polarization both nationally and internationally, challenging the core values of democratic societies, gaining geopolitical influence and power by harming and undermining others, and impacting the decision-making capability of political leaders. Therefore, it is unsurprising that today's hybrid threats are regarded as serious and acute threats to the EU and its Member States, and are treated as such by policymakers across Europe (Giannopoulos et al., 2021, p. 6).

4.1. The search for the definition of hybrid threats

Speaking about the use of these terms, NATO (2024, p. 16) notes that "we can look to the meaning of the term hybrid to help clarify meaning. Although originally a noun, hybrid is also now used as an adjective. As a noun, hybrid refers to something composed of two different elements not normally combined, which in nature would be a new species. As an adjective, hybrid denotes something being of mixed character composed of different elements. In either form, the term refers to an unusual mating or joining together. Given that sense, we can say that with hybrid threats and hybrid warfare, the individual parts may not be new or novel. However, the combination of actions/activities is novel – although perhaps

5 Hybrid CoE is an international, autonomous network-based organization promoting a whole-of-government and whole-of-society approach to countering hybrid threats. Participation in the Centre's activities is open to all EU and NATO countries, and the number of Participating States has grown to include 36 states. https://www.hybridcoe.fi/

not unique – to traditional military conceptions of threats/ aggression and to civil authorities whose sensibilities of what constitutes a national security threat/ concern will be challenged to expand."

The term "hybrid threats" is appearing more and more often in modern international political discussions and other fields. Other terms employed include "hybrid warfare," "hybrid conflicts," "hybrid tactics," "hybrid confrontations," and "hybrid operations" (Bekkers et al., 2018, p. 6). As noted by Bekkers et al., "possibly the most accurate term for the phenomenon is 'multi-domain coercion'" (p. 6).

Speaking about international organizations, NATO has developed its definition of hybrid threats with the aim of creating a strategy to counter them. According to NATO (2010), hybrid threats are "those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives." NATO's interpretation of hybrid warfare depicts it as a mixture of military means and non-military means, including propaganda and cyber activities. NATO further notes, that hybrid warfare is "the highly integrated use of a wide range of overt and covert military, paramilitary and civilian means" (NATO, 2014). "This depiction describes a combination of political and nontraditional means of coercion and influence. These activities include the coercive use of military force and more subtle forms of harmful influence in the political and informational spheres." (Vasiliauskienė & Stumbrys, 2023, p. 144).

In its 2016 Joint Communication on the Joint Framework on Countering Hybrid Threats, the EU indicated that "definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature, the concept aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives

while remaining below the threshold of formally declared warfare" (European Commission, 2016). The document stresses that the aim of hybrid threats is usually to exploit "the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes" (European Commission, 2016). Examples include massive disinformation campaigns, or using social media to control the political narrative or to radicalize, recruit, and direct proxy actors. The communication also stresses that "hybrid threats aim to exploit a country's vulnerabilities and often seek to undermine fundamental democratic values and liberties" (European Commission, 2016). The European Commission's 2018 Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats further develops this point, noting that the aim in case of hybrid threats is also to "destabilise countries by undermining public trust in government institutions and by challenging the core values of societies" (European Commission, 2018). The document additionally mentions such examples as: cyber-attacks disrupting the economy and public services through targeted disinformation campaigns to enhance hostile military actions; and the danger posed by chemical, biological, radiological and nuclear-related threats, which fall into a category of their own because of the potential scale of the damage they can cause and the fact that they are difficult to detect and attribute, and complex to remedy.

The Hybrid CoE indicates that an inherent characteristic of hybrid threats is the blurring of traditional dividing lines of various phenomena and the creation of ambiguity (Giannopoulos et al., 2021, p. 6). "Being 'under the radar' as much as possible is one of the characteristics of hybrid threat activities. … We are confronting a totally new situation today. The core values of Western societies, including openness and democratic decision-making, are being manipulated in order to compromise these very values" (p. 6). The Hybrid CoE (n.d.-a) defines a hybrid threat as an action carried out by state or non-state actors whose purpose is to harm or weaken the target by influencing its decision-making at the local,

regional, state, or institutional level.

Accordingly, the main features of hybrid threats according to the Hybrid CoE are:

1. Coordinated and synchronized actions deliberately targeting the systemic vulnerabilities of democratic states and institutions by various means.
2. Activities that exploit the limits of detection and attribution as well as different interfaces (war and peace, internal and external security, local and state, and national and international).
3. Activities aimed at influencing various forms of decision-making at the local (regional), state, or institutional level, and that are intended to further and/or implement the agent's strategic goals while undermining the target (Hybrid CoE, n.d.-b).

The Hybrid CoE further develops elements of the definition of hybrid threats in *The Landscape of Hybrid Threats: A Conceptual Model* (Giannopoulos et al., 2021).

When speaking about the question of the similarity of hybrid actions taken in isolation to the usual practice of states seeking influence, the Hybrid CoE observes that "we need to consider that in today's international system there may well be some new tools that we have not encountered before. Old tools might be used in a new way, or in a different context from what we are used to and surprising combinations can be created. This can challenge even the best prepared countries" (Giannopoulos et al., 2021, p. 11). The novelty of these threats comes from far-reaching globalization, hyperconnectivity, and digitization, which amplify their effectiveness and impact.

Thus, the Hybrid CoE proposes the following threshold for a regular threat turned hybrid:

"Ostensibly, it is when a hostile actor deliberately combines and synchronizes action, specifically targeting the systemic vulnerabilities in democratic societies in ways that have roots in tactics with which authoritarian states, revisionist

powers, rogue states and non-state networks that are seeking to undermine democratic state system have been trying to maintain their power, exert control and weaken opponents. …

Furthermore, there is a malign intent behind the action, characterized by the following:

- Using multiple synchronized tools (in principle, non-military) to create linear and non-linear effects […];
- Creating ambiguity (covert and plausible deniability) and hiding the real intent;
- Exhibiting deliberate threshold manipulation when it comes to detection and response
- Exploiting the seams of democratic society as well as between different jurisdictions;
- Often including a distraction element, such as action in one place, and a target somewhere else" (Giannopoulos et al., 2021, p. 11).

For the full understanding of hybrid threats, the Conceptual Model analyzes four main pillars: "actors (and their strategic objectives), tools applied by the actor, domains that are targeted, and phases (including the types of activity observed in each phase" (Giannopoulos et al., 2021, p. 11). The actor employing hybrid tactics "selects a combination of tools to achieve strategic objectives. These form the Hybrid Threats toolbox, which may vary depending on the actor in question (state actor, non-state actor) and its target. Each tool targets one or multiple domains or the interface between them. Tools can exploit, or even create a vulnerability in one or more domains, or take advantage of an opportunity. The objective can be achieved either by the direct effect of the tool on the domain or due to cascade effects. Activity in one domain may be aimed at affecting a completely different domain from the one where the activity was detected" (p. 12). The conceptual model developed by the Hybrid CoE further analyses the four elements and provides a visual representation.

4.2. Hybrid threats and hybrid warfare

The terms "hybrid threat" and "hybrid warfare" are often used as synonyms. After Russia's 2014 invasion, NATO Heads of State issued a communique that included the terms hybrid threat and hybrid warfare. The first reference combined the terms: "We will ensure that NATO is able to effectively address the specific challenges posed by hybrid warfare threats where a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design" (NATO, 2014, para. 13). Further references used threat and warfare interchangeably (NATO, 2024, p. 13). However, there are now efforts to define and delineate these terms. A suggestion has been put forward by the Hybrid CoE, where they underline that "this multidisciplinary analytical mosaic also blurs the picture of what the concept of Hybrid Threats actually entail. In this report the concept of Hybrid Threats is used as an umbrella concept, while hybrid warfare/war is part of the activity occurring under the Hybrid Threats umbrella" (Giannopoulos et al., 2021, p. 9).

The Assembly of the Council of Europe (2018) has noted that "there is no universally agreed definition of 'hybrid war' and there is no 'law of hybrid war.' However, it is commonly agreed that the main feature of this phenomenon is 'legal asymmetry,' as hybrid adversaries, as a rule, deny their responsibility for hybrid operations and try to escape the legal consequences of their actions. They exploit lacunas in the law and legal complexity, operate across legal boundaries and in under-regulated spaces, exploit legal thresholds, are prepared to commit substantial violations of the law and generate confusion and ambiguity to mask their actions."

Solmaz (2022) notes that "As such, the idea of 'hybrid warfare' has continuously been subjected to conceptual stretching, and thus, today, it seems rather a vague and ambiguous concept. Yet still, a close investigation reveals that there are

five major interpretations of the concept of 'hybrid warfare' that are related yet different:

1. 'Hybrid Warfare' as the employment of synergistic fusion of conventional weapons, irregular tactics, terrorism, and criminal activities in the same battlespace.
2. 'Hybrid Warfare' as the combined use of regular and irregular forces under a unified direction.
3. 'Hybrid Warfare' as the use of various military and non-military means to menace an enemy.
4. 'Hybrid Warfare' as sub-threshold activities involving any mix of violent and non-violent means.
5. 'Hybrid Warfare' as a way of achieving political goals by using non-violent subversive activities."

One of the most famous researchers on hybrid warfare, Hoffman (2007, p. 28), has maintained that states can shift their regular forces to irregular units and employ non-traditional warfare tactics. Hoffman's notion of hybrid warfare, refers to nonstate actors with high-tech weapons and states who adopt irregular tactics. Hoffman's idea of hybrid warfare well describes what 21st-century insurgents such as Hezbollah, Hamas, the Taliban, ISIS, and the PKK have done over the last two decades. It also captures state-based irregular fighters, such as Russia's masked troops known as "little green men," China's maritime militias, and Iran's Quds Force. Thus, although non-state actors with sophisticated weapons and states who employ irregular tactics are not completely new, today they seem dominant in modern armed conflicts, as Hoffman forecasted correctly in 2007 (Solmaz, 2022; Vasiliauskienė & Stumbrys, 2023, p. 144). Hoffman (2009) also defined hybrid threats as "any adversary that simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism and criminal behaviour in the battle space to obtain their political objectives," and identified five characteristics of hybrid warfare that distinguish it: 1) modality

of actions – four action modules are distinguished in the area of military operations: conventional warfare, tactics characteristic of irregular groups, terrorism, and criminal actions; 2) synchronicity – all 4 types of actions are coordinated, take place at the same time and in the same space; 3) fusion – all actions of the warring groups aim for a common goal; 4) multimodality – different groups participate in military operations, characterized by a variety of tactics and weapons; and 5) criminality – an atmosphere of fear and mistrust is created in the space of military actions by means of criminal actions (Kilinskas, 2023; Vasiliauskienė & Stumbrys, 2023, p. 144).

The NATO reference curriculum on Hybrid Threats and Hybrid Warfare suggests a working definition of hybrid warfare: "Hybrid warfare is the creative use of hard, soft, and smart power by malign state or nonstate actors to achieve warlike objectives and political goals. Malign acts include a broad spectrum of military and nonmilitary instruments of coercive power beyond the conventionally conceived multidomain battlespace. Hybrid warfare encompasses politics, diplomacy, information, the economy, technology, the military and society, as well as dimensions like culture, psychology, legitimacy and morale. The coordinated performance of these malign acts occurs both overtly and covertly in the ambiguous grey zones of blurred interfaces: between war and peace, friend and foe, internal and external relations, civil and military, and state and nonstate actors, as well as in fields of responsibilities generally below the threshold of war or as an accompaniment to more regular armed conflict" (NATO, 2024, p. 16).

4.3. The response of international law– the prohibition of the use of force and hybrid warfare

Hybrid actions are often conducted in a way that would allow the perpetrating state to "fly below" the radar of the prohibitions established in international law, especially the prohibition of the use of force established in Article 1(4) of the UN

Charter (1945). "In practice, hybrid measures are designed to avoid being identified as clear violations of the Charter even when they do constitute an unlawful use of force. One way this is achieved is through an emphasis on covert action" (Cantwell, 2017). One goal of employing covert actions is to evade being directly associated with clear violations of international law. For perpetrators of hybrid warfare, covert methods are crucial because they exploit the vulnerabilities in the international enforcement system and foster inaction, particularly when aggressor states create uncertainty about the attribution or legality of their actions (Cantwell, 2017; Vasiliauskienė & Stumbrys, 2023, p. 147). "By definition, hybrid adversaries avoid any overt use of force. Hence, if a hybrid operation does not reach the required intensity level, the use of force in self-defence will be out of the question and jus ad bellum (international law regulating the resort to force) and jus in bello will not apply. Therefore, without firing a shot, hybrid adversaries can achieve their objectives and evade retaliation. Moreover, the question of attribution and thus, accountability, may also raise difficulties because hybrid adversaries will always deny involvement in such activities." (Sanz-Caballero, 2023).

Hybrid measures falling short of the use of force and measures in other fields usually do not violate Article 2(4). Disinformation, criminal activity, economic measures – all of these actions fall below the threshold of the use of force. However, such actions may be considered a form of interference, a prohibition implicit in Article 2(1) of the UN Charter (Cantwell, 2017). The General Assembly stated in 1965 that interference is the "subordination of the exercise of [a state's] sovereign rights." In 1970, the General Assembly stressed that there is a ban on intervention in the internal or external affairs of any other state along with "all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements" (Cantwell, 2017; UN General Assembly, 1970).

"The prohibition of the use of force is a cornerstone provision, *ius cogens* of

international law. The inherent right to self defence from an armed attack is established in Article 51 in UN Charter (1945). It states that every state has the right to defend itself in case if an armed attack occurs. However, the exact extent of the actions constituting armed attack is not as clear-cut. Armed actions of a state's armed forces will surely constitute armed attack in the sense of Article 51 and customary international law, but a question arises when the actions in question are low intensity or are perpetrated by irregular armed bands" Vasiliauskienė & Stumbrys, 2023, p. 146).

The International Court of Justice (hereinafter ICJ) has stated that "the Court sees no reason to deny that, in customary law, the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces" (ICJ, 1986). In the *Nicaragua v. United States of America* (1986) case, the ICJ held the view that "a mere frontier incident" – however this should be defined – does not qualify as an "armed attack" (Fogt, 2021, p. 63), thus requiring the gravity of an offensive in order to invoke the self-defense right of the state. However, Fogt (2021) argues that this restrictive and cautious interpretation has been rejected by some states and various scholars: "It seems, indeed, most convincing to depart from the view of a gravity requirement expressed by the ICJ in the Nicaragua case and regard any attack which results in or is likely to cause destruction of property and injury or loss of life as an 'armed attack,' which justifies state self-defence subject to the jus ad bellum principles of necessity and proportionality. A proportionate response to a small-scale attack, which could be conducted as part of a hybrid warfare, would in itself be limited in scale and effect in order to be lawful" (p. 63).

The question of whether multiple incidents can in accumulation constitute an armed attack is addressed by the theory of accumulated events. According to

Fard et al. (2023), "ICJ has affirmed the existence of a threshold for distinguishing between "the most extreme forms" and "less extreme forms" of the use of armed force. The theory of the accumulation of incidents refers to a series of minor incidents that have accumulated until they reach the threshold of armed conflict". This doctrine, also known as the "spiking" theory, involves a series of minor incidents accumulating until they reach the level of an armed attack, and some governments use it to justify their right to self-defense. Although this theory previously had limited support, it has gained traction as governments grapple with the significant challenges posed by transnational terrorist attacks (Fard et al., 2023).

"When applied to malicious cyber activities in the context of international law, normative aggregation may be appropriate where a series of acts can be attributed to a single State. As with normative aggregation in domestic criminal law, individual malicious cyber activities do not have to constitute a standalone wrongful act if, in the aggregate, the consequences of state action constitute a breach of an international obligation. Under international law, this theory of aggregation is called the Accumulation of Events Theory, or Nadelstichtaktik" (McLaughlin, 2023). In other sources, this is called needle-prick or pin-prick aggression.

McLaughlin (2023) asserts that the key criterion for determining if cyber or other hybrid activities qualify as an armed attack that justifies the right to self-defense is whether their effects are comparable to those caused by a kinetic weapon. To aggregate the cumulative impact of malicious activities that individually fall short of this threshold, their consequences and actions must be causally and temporally linked and attributable to a single source. The process of accumulating events starts with the initial identifiable wrongful act and continues until the activity stops. Any self-defense measures taken must be both proportionate and necessary for the effective exercise of self-defense. In addressing hybrid activities, proportionality and necessity depend on what is needed to disrupt either the

capacity or the will of the offending nation to persist in its wrongful conduct (McLaughlin, 2023; Vasiliauskienė & Stumbrys, p. 147).

In analogue with cyber activities, McLaughlin (2023) states that "When applied to malicious cyber activities in the context of international law, normative aggregation may be appropriate where a series of acts can be attributed to a single State. As with normative aggregation in domestic criminal law, individual malicious cyber activities do not have to constitute a standalone wrongful act if, in the aggregate, the consequences of state action constitute a breach of an international obligation. Under international law, this theory of aggregation is called the Accumulation of Events Theory, or Nadelstichtaktik (needle prick)." Fogt (2021) states that "the accumulation of events theory is of particular importance when discussing hybrid threats and warfare designed to stay under the triggering threshold. The asymmetric hybrid character of the low-level use of force, the flexibility regarding intensity and rapid adaptability coupled with disinformation and fake news targeted at the entire society as such may collectively constitute an 'armed attack' and, thus, justify a necessary and proportionate act in self-defence" (p. 66).

The question of attribution remains: one still has to establish whether this string of actions may be attributed to one or more specific states or a non-state group. "Both the standard evidence of attribution to such hybrid attacks to a specific state or non-state actor group, and the determination of the necessary scale and frequency of small attacks required remains unclear. On the one hand, this makes the accumulation of theory a most difficult jus ad bellum justification to apply for the state claiming self-defence or collective self-defence, but it does open the legal door of self-defence of the victim state by a series of hybrid acts" (Fogt, 2021, p. 67).

"Many other jus ad bellum issues of state self-defense also have the character of complex legal gray zones covered by uncertainties such as: the quality and quantity of the target of an armed attack (a person, unit, military facilities,

infrastructure or territory), the standard of burden of proof, the need of a possible intention (mens rea element), a duration or gravity requirement, or whether accumulation of "small" events suffices".

(Fogt, 2021, p. 66). This allows states to stay in apparent legality speaking about self-defence rules, but still conduct hybrid actions and hybrid warfare against other states.

4.4 Hybrid warfare and laws of war

When analyzing hybrid warfare, questions and issues arise regarding jus in bello or international humanitarian law (IHL). Hybrid warfare tactics frequently operate in ways that evade the direct scrutiny of international law. This includes IHL, which comes into play when the activities of the parties meet the threshold of an armed conflict (Vasiliauskienė & Stumbrys, 2023, p. 148). "The beginning of an armed conflict is the moment from which the application of the full regime of one or another international humanitarian law begins. Therefore, it can be said that the classification of the situation as an armed conflict is a legal fact of extraordinary importance" (Žilinskas, 2008, p. 92).

Accurately determining the existence of an armed conflict has significant and extensive implications in international law. The Use of Force Committee of International Law Association has stressed that "the existence of armed conflict has many significant impacts on the operation of international law beyond the well-known fact that during armed conflict international humanitarian law (IHL) will apply and states party to an armed conflict (or other emergencies) may have the right to derogate from some human rights obligations. In addition, states that provide asylum to persons fleeing the violence of armed conflict will have the duty to do so; treaty obligations may be implicated; the law of neutrality may be triggered; arms control agreements are affected, and United Nations forces engaged in armed conflict will have rights and duties not applicable in operations

outside of armed conflict. These are just some of the areas of international law that are affected by the outbreak of armed conflict." (Use of Force Committee, 2010, p. 33). The most crucial implication is that only during an armed conflict can parties exercise the rights of belligerents. Attempting to exercise these rights outside of an armed conflict risks infringing upon fundamental human rights that are upheld during peacetime (Vasiliauskienė, 2012, p. 182).

The existence of armed conflict "changes the level of protection of the right to life. In peacetime, the state may use force to maintain order, including the taking of life, but this must be absolutely necessary and strictly proportionate to the objectives pursued, according to human rights standards. In armed conflict, the deprivation of life is analysed under IHL norms, which impose quite different standards and proportionality requirements" (Vasiliauskienė, 2012, p. 182). Furthermore, a state responding in a proportionate and necessary manner in self-defense can only use force against persons and objects if it fulfils the requirements of IHL (Fogt, 2021, p. 73). An object is a legitimate target if it constitutes a military objective and if the use of force against this target is proportionate and conducted with lawful methods and means, and all feasible precautions have been taken. (Fogt, 2021, p. 73).

The International Criminal Tribunal for the former Yugoslavia (hereinafter ICTY), in the *Prosecutor v. Dusko Tadic* (1995) case, elaborated on the definition of an armed conflict, which since has been cited on numerous occasions and has become accepted as a textbook definition of armed conflict, which had not been provided for in the Geneva Conventions on the laws of war, Common article 2. The ICTY states that "an armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organised armed groups or between such groups within a State" (*Prosecutor v. Dusko Tadic*, 1995, para. 70).

The UN High Commissioner for Human Rights' Special Rapporteur on

Human Rights and Terrorism defines an "armed conflict as a situation requiring that there be military operations and the use of military materiel. Long-accepted requirements for a showing of armed conflict include the use of military (rather than police) forces, the use of military (as opposed to police) weaponry and materiel, and the use of military (as opposed to police) operations." (Koufa, 2004, p. 9).

The Committee on the Use of Force of the International Law Association explored the concept of armed conflict under international law and concluded in 2010 that the definition of armed conflict provided in the *Prosecutor v. Dusko Tadic* (1995) case is supported by additional sources. The committee identified two critical elements of armed conflict: the presence of organized armed groups and engagement in combat activities of a certain intensity (Use of Force Committee, 2010, p. 2; Vasiliauskienė & Stumbrys, 2023, p. 149).

Challenges arise with both components of this definition. "Speaking about the organisational aspect, in case of the activity of states, the organisational criterion does not raise questions, as state is *ipso facto* considered an organised entity fully capable to participate in an armed conflict. But a different question arises, of attribution of particular hybrid action to the state. In case of hybrid actions, the states aim to "hide" behind proxies, armed groups, green men etc., therefore it is difficult to ascertain the organisator of hybrid actions and thus the existence of armed conflict. Furthermore, the intensity criterion is even more problematic. Manifestations of hybrid warfare in many cases do not amount to armed actions, but in totality may incur consequences similar to armed actions. Therefore a question arises whether the accumulation of actions could be considered together in order to determine whether the threshold for armed conflict has been crossed." (Vasiliauskienė & Stumbrys, 2023, p. 149).

As noted, the consequences of this determination are significant: a situation that falls just below the threshold for a non-international armed conflict will be addressed under national crisis and emergency (martial) laws and law enforcement

rules within a human rights law framework, possibly with or without military support from the state or its allies (Fogt, 2021, p. 74). Conversely, a situation that meets the criteria for armed conflict would trigger responses governed by IHL. Fogt further suggests that if a hybrid campaign and non-state armed resistance are scaled back and hostilities diminish, the threshold for a non-international armed conflict may no longer be met, leading to the reapplication of peacetime jus ad bellum (p. 74). Consequently, many questions remain unresolved.

Conclusions

The term "hybrid threats" is increasingly prevalent in international political discourse, encompassing various forms such as hybrid warfare, hybrid conflicts, and hybrid operations. NATO defines hybrid threats as involving adversaries using a mix of conventional and non-conventional methods to achieve their objectives, including propaganda and cyber activities. Similarly, the EU describes hybrid threats as a blend of coercive and subversive activities aimed at exploiting vulnerabilities and creating ambiguity to hinder decision-making. The Hybrid CoE highlights that hybrid threats blur traditional boundaries, exploiting systemic vulnerabilities and influencing decision-making at multiple levels. These threats are characterized by coordinated actions, deliberate ambiguity, and the use of both old and new tools in innovative ways, challenging even well-prepared states due to the effects of globalization, hyperconnectivity, and digitization.

The terms "hybrid threat" and "hybrid warfare" are often used as synonyms. However, there are now efforts to define and delineate these terms. The Hybrid CoE suggests that "hybrid threats" is used as an umbrella concept, while "hybrid warfare" is part of the activity occurring under the hybrid threats umbrella. The characteristics of hybrid warfare are modality of action, synchronicity, fusion, multimodality, and criminality. Hybrid warfare is the creative use of hard, soft, and smart power by malign state or nonstate actors to achieve warlike objectives

and political goals.

Hybrid actions are often conducted in a way that would allow the perpetrating state to evade the prohibitions established in international law, especially the prohibition of the use of force established in Article 1(4) of the UN Charter. Disinformation, criminal activity, economic measures – all of these actions fall below the threshold of the use of force. However, such actions may be considered a form of interference, a prohibition implicit in Article 2(1) of the UN Charter. The theory of accumulated events suggested by some scholars in the field of self-defense would allow multiple hybrid actions to be considered as armed attack, triggering the right to self-defense. However, the question of attribution may be problematic, and the state must follow the requirements of necessity and proportionality when responding in self-defense.

Hybrid warfare raises significant questions regarding IHL, particularly in how these conflicts evade direct scrutiny under IHL standards. IHL applies once activities reach the threshold of an armed conflict, which has extensive implications including shifts in contractual obligations, refugee rights, and arms control standards. During an armed conflict, the protection of the right to life transitions from peacetime human rights norms to IHL standards. The ICTY's *Prosecutor v. Dusko Tadic* case provides a widely accepted definition of armed conflict, involving organized armed groups and combat activities of a certain intensity. However, hybrid warfare complicates this definition, as states often use proxies to obscure involvement, challenging the identification of the true organizers and the cumulative assessment of hybrid actions. If a situation falls below the threshold of an armed conflict, it is managed under national laws and human rights frameworks, but meeting the threshold triggers IHL governance. Consequently, many aspects of hybrid warfare's interaction with IHL remain unresolved, underscoring the complexity of applying traditional legal frameworks to modern conflicts.

References

1. Bajarūnas, E., & Keršanskas, V. (2016). Hybrid threats: Analysis of content, challenges posed, and measures to overcome. *Lithuanian Annual Strategic Review*, *16*(1), 123–170. http://dx.doi.org/10.2478/lasr-2018-0006
2. Bekkers, F., Meessen, R., & Lassche, D. (2018). *Hybrid conflicts: The new normal?* TNO. https://www.tno.nl/publish/pages/7427/tno-2019-hybride.pdf
3. Cantwell, D. (2017). Hybrid warfare: Aggression and coercion in the gray zone. *ASIL Insights, 21*(14). https://www.asil.org/insights/volume/21/issue/14/hybrid-warfare-aggression-and-coercion-gray-zone
4. Council of Europe. (2018). *Legal challenges related to hybrid war and human rights obligations*. Committee on Legal Affairs and Human Rights, Rapporteur: Mr. Boriss Cilevičs, Latvia. https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24547&lang=en
5. Dykyi, E., & Kharchenko, S. (2016). *Hibridinis Rusijos karas: Ukrainos patirtis Baltijos šalims*. Generolo Jono Žemaičio Lietuvos karo akademija.
6. European Commission. (2016). Joint Communication to the European Parliament and the Council. Joint framework on countering hybrid threats: A European Union response (No. JOIN(2016) 18 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018
7. European Commission. (2018). Joint Communication to the European Parliament and the Council. Increasing resilience and bolstering capabilities to address hybrid threats (No. JOIN(2018) 16 final). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN%3A2018%3A16%3AFIN
8. Fard, M. A., Hatami, M., & Azadbakht, F. (2023). The theory of accumulation of events in the appeal to international self-defence. *International Law Review*, *40*(70). https://doi.org/10.22066/cilamag.2023.706167
9. Fogt, M. (2021). Legal challenges or "gaps" by countering hybrid warfare – Building resilience in jus ante bellum. *Southwestern Journal of International Law*, *27*(1), 28–100. https://www.swlaw.edu/sites/default/files/2021-03/2.%20Fogt%20%5B28-100%5D%20V2.pdf
10. Giannopoulos, G., Smith, H., & Theocharidou, M. (2021). *The landscape*

of hybrid threats: A conceptual model. Publications Office of the European Union. https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf

11. Hoffman, F. G. (2007). *Conflict in 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies.
12. Hoffman, F. G. (2009, October 1). Hybrid vs. compound war. The Janus choice: Defining today's multifaceted conflict. *Armed Forces Journal*. http://armedforcesjournal.com/hybrid-vs-compound-war
13. Hybrid CoE. (n.d.-a). *Hybrid threats*. Retrieved July 20, 2024. https://www.hybridcoe.fi/hybrid-threats
14. Hybrid CoE. (n.d.-b). *Hybrid threats as a concept*. Retrieved July 20, 2024. https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon
15. Johnson, R. (2018). Hybrid war and its countermeasures: A critique of the literature. *Small Wars & Insurgencies*, *29*(1), 141–163. https://doi.org/10.1080/09592318.2018.1404770
16. Koufa, K. K. (2004). *Terrorism and human rights: Final report* (E/CN.4/Sub.2/2004/40). United Nations Economic and Social Council. Commission on Human Rights. Sub-Commission on the Promotion and Protection of Human Rights. https://www.refworld.org/reference/themreport/unsubcom/2004/en/65285
17. Kilinskas, K. (2023). *Hibridinis karas*. Visuotinė lietuvių enciklopedija. https://www.vle.lt/Straipsnis/hibridinis-karas-124426
18. McLaughlin, M. (2023, February 3). Deterring the next invasion: Applying the accumulation of events theory to cyberspace. *Opinio Juris*. https://opiniojuris.org/2023/03/02/deterring-the-next-invasion-applying-the-accumulation-of-events-theory-to-cyberspace
19. National Security Council. (1948). *Directive on Office of Special Projects*. https://history.state.gov/historicaldocuments/frus1945-50Intel/d292
20. NATO. (2010, August 25). *Bi-SC input to a new NATO capstone concept for the military contribution to countering hybrid threats*. https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf

21. NATO. (2014, September 5). *Wales NATO Summit communiqué* [Press release]. http://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en
22. NATO. (2024). *Hybrid threats and hybrid warfare: Reference curriculum*. https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf
23. Nicaragua v. United States of America, Merits, Judgment, I.C.J. Reports 1986, p. 14. https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf
24. Prosecutor v. Dusko Tadic, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, International Criminal Tribunal for the former Yugoslavia, IT-94-1-A, 2 October 1995. https://www.icty.org/x/cases/tadic/acdec/en/51002.htm
25. Sanz-Caballero, S. (2023) The concepts and laws applicable to hybrid threats, with a special focus on Europe. *Humanit Soc Sci Commun* 10, 360, https://doi.org/10.1057/s41599-023-01864-y
26. Solmaz, T. (2022, February 25). Hybrid warfare: One term, many meanings. *Small Wars Journal*. https://smallwarsjournal.com/jrnl/art/hybrid-warfare-one-term-many-meanings
27. United Nations General Assembly. (1970). Declaration on principles of international law concerning friendly relations and cooperation among states in accordance with the Charter of the United Nations. G.A. Res. 25/2625, Oct. 24, 1970. http://www.un-documents.net/a25r2625.htm
28.
29. United Nations Charter. (1945). https://www.un.org/en/about-us/un-charter/full-text
30. Use of Force Committee, International Law Association. (2010). *Final report on the meaning of armed conflict in international law*. https://www.rulac.org/assets/downloads/ILA_report_armed_conflict_2010.pdf
31. Van Puyvelde, D. (2015, May 7). Hybrid war – does it even exist? *NATO Review*. https://www.nato.int/docu/review/articles/2015/05/07/hybrid-war-does-it-even-exist/index.html

32. Vasiliauskienė, V., & Stumbrys, V. (2023). Problematic aspects of the legal definition of hybrid warfare. *Public Security and Public Order*, *33*, 142–153. https://ojs.mruni.eu/ojs/vsvt/issue/view/477
33. Žilinskas, J. (2008). Ginkluoto konflikto samprata tarptautinėje humanitarinėje teisėje ir jos taikymo problemos moderniuose ginkluotuose konfliktuose [The concept of armed conflict in international humanitarian law and problems of its applicability in modern armed conflicts]. *Jurisprudencija*, *104*(2), 91–100. https://ojs.mruni.eu/ojs/jurisprudence/article/view/2625
34. Žilinskas, J. (2012). "Teisingo karo" doktrina ir jos atspindžiai mūsų dienomis ["Just war" doctrine and its reflections in our times]. *Jurisprudencija, 19*(3), 1201–1214. https://ojs.mruni.eu/ojs/jurisprudence/article/view/80

MYKOLAS ROMERIS UNIVERSITY

Public Security Academy

TRANSFORMATIONS, CHALLENGES AND SECURITY

Collective monograph

Mykolo Romerio universitetas

MYKOLAS ROMERIS UNIVERSITY

Public Security Academy

TRANSFORMATIONS, CHALLENGES AND SECURITY

Collective monograph

Mykolo Romerio universitetas

Vilnius, 2024

Reviewed:
Prof. dr. Badri Gechbaia (Batumi Shota Rustaveli State University)
Prof. dr. Tadeuz Trocikowski (Cuiavian University in Włocławek)

Editor-in-chief:
Prof. habil. dr. Žaneta Simanavičienė

Approved for publication by the Council of the Public Security Academy of Mykolas Romeris University, at the sitting on 13 September 2024. Resolution No. 1VS-8.

All publishing rights are reserved. This book, or any part of it, may not be reproduced, edited, or otherwise distributed without the permission of the publisher.
The bibliographic data of the publication is available on the portal of the Lithuanian Integrated Library Information System (LIBIS) "ibiblioteka.lt".

ISBN: ISBN 978-609-488-096-4 (El. - PDF)
ISBN 978-609-488-097-1 (Print)

© Mykolas Romeris University, 2024