Chapter 17

Legal Aspects of Hybrid Threats and Warfare

Katarzyna Zombory

Abstract

The chapter addresses the selected legal aspects of hybrid threats and warfare connected to certain branches of the international public and European Union (EU) law. The overarching objective of the chapter is to present a legal assessment of hybrid threats and delineate the scope of lawful countermeasures to respond to them, which is a prerequisite for swifter decision-making and enhancing the defensive capability of the EU. The author outlines the conceptual framework of hybrid warfare and hybrid threats, exemplified by the hybrid tactics used in the 2014 Russian invasion against Ukraine. The legal analysis of hybrid threats and warfare is carried out under rules governing the lawfulness of the resort to force (*jus ad bellum*), international law of armed conflicts (*jus in bello,* international humanitarian law), and human rights law. This analysis demonstrates that it is difficult to conclude whether the use of hybrid threats and warfare amounts to the use of force, and whether it triggers legal consequences attached to the existence of armed conflict, in terms of the right to self-defence and application of international humanitarian law, especially if a hybrid campaign does not involve the use of kinetic force. While balancing between war and peace, hybrid threats and warfare highlight how the traditional dichotomy underlying the law on the use of force works in favour of hybrid aggressors. Compared to the international legal framework, the EU's framework "theoretically" offers wider possibilities for a collective response to hybrid threats and campaigns compared with the North Atlantic Treaty Organization (NATO). This is because the EU framework enables invocation of the mutual solidarity clause (Article 222 Treaty on the Functioning of the EU) in situations that otherwise would not trigger a collective defence mechanism under Article 5 NATO Treaty.

Katarzyna Zombory (2024) 'Legal Aspects of Hybrid Threats and Warfare'. In: Katarzyna Zombory – János Ede Szilágyi (eds.) *Shielding Europe with the Common Security and Defence Policy. The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment,* pp. 755–800. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_17

Keywords: hybrid threats, hybrid warfare, information warfare, lawfare, collective defence

1. Introduction

War and warfare undoubtedly belong to the core domain of military alliances, such as the North Atlantic Treaty Organization (NATO) or the Rio Pact. The deteriorating global security environment prompted the European Union (EU), an economic "civilian power" rather than a military alliance, to increase its defence and military capacity, based on the concept of strategic autonomy, and to recently adopt its first quasi-military doctrine (the 2022 Strategic Compass for Security and Defence).[1] In its efforts for preventing and countering global security threats, the EU has increasingly focused on creating a coordinated response system for hybrid threats and hybrid campaigns, alone and in concert with the NATO. The growing concern about hybrid threats comes from the acknowledgement that both state and non-state actors are increasingly using hybrid tactics, including information manipulation, to interfere with democratic processes, which pose a growing security threat to the NATO and EU. Over the last decade, several EU Member States and the EU as a whole have been victims of multiple hybrid attacks, which warn how hybrid adversaries can identify and exploit existing vulnerabilities to achieve their strategic goals.

Russia's annexation of Crimea in 2014 and its recent armed aggression against Ukraine in February 2022 demonstrated that modern armed conflicts come with the highest level of military force combined with hybrid tactics and information manipulation.[2] As the NATO Secretary General Jens Stoltenberg puts it, the tactics used by hybrid adversaries are a dark reflection of the NATO's comprehensive approach, used to maintain peace and stability around the world.[3] This "dark reflection" denotes the emergence and proliferation of hybrid warfare – in which international law plays a crucial role as a strategic enabler and operating environment – primarily to gain advantage over law-abiding states. Hybrid warfare is a logical consequence of the rivalry between two visions of the international community and international legal order: the vision of the West, formulated under the influence of the United States, and the vision shared by Russia and China, which rejects the United States' global hegemony and demands a multipolar international community.[4] In the non-

1 Council of the European Union, *A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security*, Brussels, 21 March 2022, 7371/22.

2 Council of the European Union, *Council conclusions on a Framework for a coordinated EU response to hybrid campaigns*, Brussels, 21 June 2022, 10016/22, para. 1.

3 NATO, 2015.

4 For a detailed analysis of the problem, see: Mik, 2022; Aukia and Kubica, 2023.

Western narrative, one manifestation of the United States' hegemonic position is the unilateral and abusive interpretation of the law on the use of force by the NATO coalition. Non-Western actors perceive the NATO's 1999 Kosovo intervention (Operation Allied Force) as a violation of international law that remains unsanctioned. From the Russian perspective, the NATO is an illegal aggressor that acts under the guise of peacekeeping and crisis regulation and resorts to hybrid warfare; the NATO's conduct justifies and validates Russian countermeasures using an equal form of hybrid warfare.[5] As Najžer puts it straightforwardly, hybrid warfare is a tool of revisionist powers who seek to challenge the dominant world order.[6] In other words, we are witnessing a remodelling of the world's geopolitical landscape shaped after the end of the Cold War, in the process of which the use of hybrid warfare and weaponisation of international law is intrinsic.

This chapter's research objective is presenting a legal assessment of certain legal aspects connected to hybrid threats and warfare under various branches of the international public law and EU law. While this is a highly demanding if not an impossible task, analysing the legal framework applicable to hybrid conflicts and identifying its legal gaps should contribute to increasing the overall legal preparedness and legal resilience against hybrid threats in the EU and its Member States, even if there are no clear-cut answers to all the legal ambiguities. Delineating the scope of lawful countermeasures to prevent and respond to hybrid threats is a prerequisite for swifter decision-making and enhancing the EU's defensive capability. In section 2 of the chapter, the author addresses the terminological and conceptual framework of hybrid warfare and hybrid threats. Section 3 focusses on a legal analysis of hybrid threats and warfare carried out with respect to the following branches of international law: international law governing the lawfulness of the resort to force (*jus ad bellum*), international law of armed conflicts (*jus in bello*, international humanitarian law [IHL]), and human rights law. Section 4 of the chapter is devoted to the EU's approach to dealing with hybrid threats.

A legal assessment of hybrid threats and warfare is not possible without exploring the traditional dichotomy between war and peace that underlies the international legal regime on the use of force and law of armed conflicts. The reality of contemporary conflicts, which come with a combination of sophisticated non-kinetic and kinetic attacks that cannot be easily classified as either war or peace, prompts a dilemma reminiscent of the Schrödinger's paradox. In Schrödinger's famous experiment, the scientist argued that under certain conditions, the object of his experiment (a cat) can be simultaneously considered alive and dead. This chapter highlights the challenges posed by the use of hybrid threats and warfare for traditional legal classification, implying the unambiguous existence or non-existence of armed

5 See: the Federation Council of the Federal Assembly of the Russian Federation, 2019; Kremlin, Moscow, 2014. The Russian perspective and legal narrative are explained by Morten M. Fogt; see: Fogt, 2020, pp. 35–38, 47–49.

6 Najžer, 2020, p. 4.

conflict. This, with certain irony, can translate this chapter's research objective into the question of whether hybrid campaigns can substitute for Schrödinger's cat.

2. Concept and Means of Hybrid Threats and Warfare

2.1. Meaning of Hybrid Threats and Warfare

Throughout the past two decades, a considerable volume of scholarly works related to hybrid war has been published, resulting in an (over)abundance of definitions and ideas on what hybrid warfare is and how to term it properly.[7] The concept of hybrid warfare lies at the intersection of different disciplines, such as law, military doctrine, international relations, and security studies, which have employed various terms to describe the same phenomenon, such as low-intensive asymmetric warfare, fourth- or fifth-generation warfare, full-spectrum warfare, ambiguous warfare, grey-zone warfare, or sub-threshold warfare.[8] Following the Russian annexation of Crimea in 2014, NATO's term of choice has been "hybrid warfare".[9] In turn, EU documents employ the terms "hybrid threats" and "hybrid campaigns", avoiding the association with war and warfare.[10] This can be explained by the fact that the term "warfare" implies violent military activities, dealing with which is central for NATO; however, such activities lie on the outer periphery of the EU's mandate, while the word "threat" also covers less-intensive and non-violent acts and forms of confrontation.[11] Although several authors distinguish between these terms based on the intensity of the conflict and level of aggression,[12] legal challenges posed by hybrid warfare and hybrid threats are the same regardless of the denomination used. Therefore, this chapter uses both terms.

While the terms of hybrid threat and warfare are non-legal, they permeate the contemporary legal debate on the use of force. The reason for this is, on the one hand, the crucial role of law as a weapon and operating environment and, on the other, the consequences of the legal classification of hybrid conflicts on the targeted state or states' choice of defensive measures. Inherent to every legal debate is the attempt to define the notions under consideration and delineate their content. This seemingly basic task is not without significant difficulties in case of this chapter's

7 Besides numerous scientific articles, there have been several book-long accounts on hybrid warfare, e.g. Lasconjarias and Larsen, 2015; Mansoor, 2012; Najžer, 2020.
8 Fogt, 2020, p. 30.
9 Ibid.
10 See, e.g. Council of the European Union, *Council conclusions on a Framework for a coordinated EU response to hybrid campaigns*, Brussels, 21 June 2022, 10016/22.
11 Dinstein, 2011, pp. 9–10; Sari, 2017, p. 15.
12 See e.g. Lott, 2022, pp. 16–17; Sari, 2017, p. 15.

topic. This is because there is no common understanding of what hybrid warfare is, let alone a universally accepted definition. Nevertheless, legal considerations of hybrid threats and warfare must be anchored in a certain theoretical background.

It is believed that the first definition of hybrid threats and warfare was coined by Frank Hoffman, a United States military writer, in the early 2000s. According to Hoffmann, 'hybrid threats incorporate a full range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder'.[13] Hoffman notes that hybrid wars are polymorphous in nature and can be conducted by both states and various non-state actors. He argues that the potential for types of conflict that blur the distinctions between war and peace and between combatants and non-combatants is on the rise.[14] Hoffman's understanding of a hybrid war is highly reminiscent of the concept of political warfare already used by American diplomat George F. Kennan in the 1940s to describe the nature of the Soviet threat. According to Kennan,

> … political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures (as ERP), and "white" propaganda to such covert operations as clandestine support of "friendly" foreign elements, "black" psychological warfare and even encouragement of underground resistance in hostile states.[15]

Over the years, the conceptual idea of hybrid warfare has evolved, and many further definitions were proposed.[16] However, one aspect has been recurrent: A combination of various measures at the strategical, operational, and tactical level, with the goal of achieving strategical, political, and/or military advantages against another state, is inherent to the hybrid construct. The wide spectrum of means, both lawful and unlawful, including the legal framework and propaganda, effectively allow for the covered actions.[17] These elements permeate the NATO's discourse, where hybrid warfare is understood as a broad, complex, and adaptive combination of conventional and non-conventional means, as well as overt and covert military, paramilitary, and civilian measures, which are employed in a highly integrated design by state and non-state actors to achieve their objectives.[18] The EU, acknowledging that the definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature, also construes the concept as a mixture of not only

13 Hoffman, 2007, p. 29.
14 Ibid., p. 7.
15 Kennan, 1948, para. 1.
16 Twenty years of the development and evolution of the hybrid warfare concept are captured by Johnson, 2021, pp. 45–57; Bekić, 2022, pp. 142–151.
17 Fogt, 2020, pp. 30–31.
18 NATO, 2016, para. 72.

coercive and subversive activity but also conventional and unconventional methods (i.e. diplomatic, military, economic, and 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.[19]

The NATO's recognition of the evolving character of 21st-century warfare and its endorsement of the comprehensive military approach[20] has met with firm doctrinal response from non-Western powers. The Russian apprehension of hybrid warfare, often referred to as the Gerasimov doctrine after the Chief of General Staff of the Armed Forces of Russia, recognises the nature of NATO's involvement in the Arab Spring as hybrid operations. Russian military leadership, following the coloured revolutions in Africa and the Middle East, declared that the rules of war had changed because the role of non-military means of achieving political and strategic goals had grown to exceed the power of force of weapons in their effectiveness. According to Gerasimov, the applied methods of conflict have changed in the direction of broad use of political, economic, informational, humanitarian, and other nonmilitary measures, applied in coordination with the protest potential of the population. Such methods are supplemented by military means of a concealed character, such as actions involving informational conflict and special-operations forces.[21] As Bekić notes, by reversing the NATO's comprehensive military approach (Stoltenberg's "dark reflection"), the Gerasimov doctrine has set the stage for Russian hybrid countermeasures, as they featured prominently in the subsequent conflicts in Ukraine.[22]

The recent Chinese military doctrine focussing on aggressive influence operations can be seen as a response to the changing nature of contemporary conflicts; it is also reminiscent of the ancient Chinese military strategy that saw subduing the enemy without fighting and using stratagems for deceiving and outwitting the enemy as the supreme art of war.[23] The United States' military involvement in the First Gulf War, Balkan wars, and 2003 invasion of Iraq have lead Chinese military strategists to realise that non-military operations and non-kinetic capabilities are central to fighting and winning contemporary conflicts.[24] China's strategic framework, adopted in 2003 and known as the "three warfares" strategy, encompasses three interrelated elements – psychological, public opinion (media), and legal warfare – indicating

19 European Commission, *Joint Framework on countering hybrid threats. A European Union response*, Brussels, 6.4.2016 JOIN(2016) 18 final, p. 2.

20 The NATO's comprehensive military doctrine implies engagement in six main domains: political, military, economic, social, infrastructure, and information. See: the NATO's contribution to a comprehensive approach in NATO, 2013, Chapter 1, points 1–2.

21 The English translation of Valery Gerasimov's paper 'Tsennost' nauki v predvidenii', originally published in *Voenno-promyshlennyi kur'er* in February 2013, is provided by Fogt, 2020, pp. 35–36. See also Johnson, 2015.

22 Bekić, 2022, p. 147.

23 According to Sun Tzu, 2010, Chapter V. III., point 2, 'Hence to fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting' (translated by Lionel Giles).

24 Clarke, 2019, pp. 189–191.

a comprehensive approach to waging conflicts.[25] The three warfares are complementary and mutually reinforcing, and they are considered a force multiplier in military operations and political or diplomatic scenarios.[26] The purpose of the three warfares is to establish "discursive power," understood as the power to control perceptions and shape narratives that serve Chinese interests, while undermining those of an opponent.[27]

Among Western scholars, two main approaches or schools of thought have developed as regards the conceptual framework of the hybrid threat and warfare. The first school assumes that hybrid warfare is not a new concept, as the combination of different means of waging war using regular and irregular forces has been known since ancient times. The second school of thought believes that hybrid warfare is a novelty that prompts the need to develop entirely new responses to it. According to this approach, hybrid threats and warfare are more than a combination of different modes of waging war or simultaneous use of regular and irregular forces. The novelty lies in modern actors' blending of conventional and conventional means in a way that enables them to remain in the so called "grey zone" between war and peace and to achieve their goals without crossing the threshold of war, through their ability to plausibly deny any involvement in hostile activities.[28] The abundant range of innovative technologies available in the 21st century, as well as the resourcefulness of hybrid adversaries, undoubtfully amounts to another significant *novum* of hybrid warfare. Nevertheless, from a legal perspective, this debate is of more academic than practical significance.

Although there is no universally agreed definition of hybrid threats and warfare, certain common characteristics can be identified to describe hybrid activities and facilitate their early detection. Distinguishing features relate to both means employed by hybrid adversaries and the destructive results of concerted hybrid attacks.

2.2. Examples of Hybrid Threats and Warfare

A hybrid arsenal encompasses an extensive array of lawful and unlawful means; any actions designed to destabilise a given society can be used within a hybrid campaign.[29] Hybrid threats and warfare may consist of political activities; (dis)informational campaigns; and cyber, military, economic, and societal interventions. The toolbox of hybrid threats and warfare includes, without being exhaustive, cyberattacks, terrorism, organised crime, application of covert psychological operations, drug trafficking, inducing of migration flows, espionage, infiltration, kidnapping,

25 Martin, 2021.
26 Kania, 2016.
27 Cochran, 2020, pp. 3–4.
28 Bekić, 2022, p. 148; Fogt, 2020, pp. 33–34; see also Johnson, 2021, p. 47.
29 Parulski, 2016, pp. 11–12; Sanz Cabellero, 2023, p. 2. Measures undertaken by hybrid adversaries target the full spectrum of the society, affecting the given state's apparatus and population as a whole; hence, information influence plays a crucial role in hybrid conflicts.

economic leverage, media exploitation, use of unmarked special forces, mercenaries or proxy soldiers, intimidation and propaganda, or instrumental and abusive use of the legal framework.[30]

Fogt describes hybrid threats and warfare as a mixture of hybrid orchestrated non-kinetic and kinetic efforts, which may be based on, among others, (1) organised and controlled actions at the highest political and military levels supporting a clear long-term strategic vision; (2) unclear distinction between peace, crisis, and war and thus operations in various legal grey zones; (3) hybrid hostile engagement in terms of full-spectrum actions, including cyberspace and information activities; (4) strategy of denial regarding overall or effective control over non-state actors and motivation of civilians to participate in propaganda and cyberattacks; (5) protection and shielding of non-state actors and civilians participating in unlawful hybrid activities from national and international prosecution; (6) use of publicly controlled or influenced media and the private economic sector; (7) use of trade and economic state sanctions, that is, export or import restrictions, under the pretext of political and legal justification; (8) targeting of specific vulnerabilities of all possible counterparties, including defence alliances, individual states, international organisations, non-state actors, and foreign populations; (9) exploitation of existing weaknesses – such as lack of consensus in democracies and alliances, absence of political willingness to react, and reduced capacities to act with a timely response – and thus a reliance on late reaction instead of prompt action by opponents; and (10) use of "lawfare" for promoting one's own actions as legitimate and opponents' reactions as unlawful.[31]

Bachmann and Munoz Mosquera argue that hybrid adversaries resort to means based on indirect and multidisciplinary approaches (civil and military, legal and illegal, kinetic and non-kinetic, high-tech, etc.) to erode and delegitimise the internal and external prestige, reputation, and support of a superior military force, state apparatus, and/or international organisation; create confusion in general by questioning agreed political, religious, or territorial status quo; and build new dependencies and structures based on essential resources to support consolidated or imposed political, religious, or territorial changes.[32]

A distinctive feature of hybrid threats and warfare is the legal imbalance between law-abiding democratic states and illegally acting autocratic states or non-state actors.[33] Hybrid adversaries can attain legal asymmetry, which considerably limits

30 The NATO Strategic Communications Centre of Excellence provides for a systematised overview of hybrid threats and warfare identified in 30 case studies, by grouping them into the categories of diplomatic, information, military, economic, financial, intelligence, legal, and law enforcement measures; Heap, 2021, pp. 30–36. Another informative list of tools of hybrid threat activities is included in the joint report of the European Commission and Hybrid CoE on a conceptual model of hybrid threats; Giannopoulos, Smith and Theocharidou, 2021, pp. 33–35.

31 Fogt, 2020, p. 33.

32 Munoz Mosquera and Bachmann, 2016, p. 68.

33 For example, Fogt, 2020, p. 32; Sari, 2017, p. 26.

the countermeasures and defensive powers available to targeted states, through the instrumental use (weaponisation) of law, often referred to as lawfare and the exploitation of legal grey zones. The term "lawfare" denotes a method of warfare wherein law is used as a means of realising a military objective; in other words, it is the use of law as a weapon of war or, to quote Charles J. Dunlap, 'a cynical manipulation of the rule of law and the humanitarian values it represents'.[34] Instrumentalisation of law has the goal of manipulating the law by changing legal paradigms; creating confusion about the source of applicable law; and hampering consequent actions to identify the perpetrator, assign legal responsibility, and demand accountability.[35] Sari argues that hybrid adversaries aim to create legal asymmetry by (1) exploiting legal thresholds, complexity, and uncertainty; (2) generating legal ambiguity; (3) violating their legal obligations; and (4) utilising law and the legal process to create narratives and counter-narratives.[36]

Another distinctive tool of hybrid hostilities that commonly features in contemporary hybrid conflicts is information operations and influence activities, the conduct of which can be loosely termed as "information warfare". There is no clear definition or conceptual framework on information warfare. In general terms, it can be seen as a struggle to control or deny the confidentiality, integrity, and availability of information in all its forms, ranging from raw data to complex concepts and ideas.[37] Offensively, information warfare occurs when one side of a conflict seeks to impose its desired information state on the adversary's information and affect how target individuals or populations interpret or learn from the information they possess or collect. Defensive information warfare occurs when one side seeks to retain the ability to freely collect, interpret, and/or learn from its available information without outside interference.[38] Information warfare combines electronic warfare (including electronic countermeasures and jamming), cyberwarfare, and psychological operations, aimed at degrading the morale and well-being of a nation's citizens, such as by spreading false information through social media and news outlets.[39] Consequently, two main types of hybrid attacks with relation to the information environment can be identified: (1) attacks related to (dis)information that aim to provoke decision-making errors and (2) attacks that directly affect physical systems.[40] Countering information warfare and influence operations is particularly challenging due to the international human rights framework, which provides for wide guarantees of the right to freedom of expression. Determining what content falls within the ambit of freedom of expression and what qualifies as foreign interference is crucial, although

34 Dunlap, 2021, p. 4. For more accounts of lawfare, see: Dunlap, 2008; Kittrie, 2016; Kowalczewska, 2014; Munoz Mosquera and Bachmann, 2016; Veress, 2023.
35 Munoz Mosquera and Bachmann, 2015, pp. 26–27.
36 Sari, 2017, pp. 28–30.
37 Bingle, 2023.
38 Ibid.
39 Committee on Legal Affairs and Human Rights, 2018, p. 7.
40 Medina Llinàs, 2022, p. 39.

far from obvious. The example of Russian "troll factories" (or "troll farms") illustrates the challenges related to distinguishing the line between state interference and online activists' right to freedom of expression, and it highlights the scale of threat posed by information operations.[41]

Information warfare holds a paramount place in the military strategy and international relations of non-Western powers, such as Russia and China. It permeates the military doctrine of the Russian Federation, where it is associated with the "reflexive control theory" and constitutes a vital component of Russia's contemporary hybrid warfare strategy.[42] The aim of reflexive control actions is to influence the adversary's political or military plans, understanding of the situation, and decision-making processes, thereby taking control over their decisions and pushing them to make unfavourable political or military choices.[43] The major part of Russian reflexive control-based hybrid threat efforts are aimed at dividing Western allies and altering their collective decision-making processes.[44]

Recent frontier incidents in several EU Member States involving state-sponsored, artificially induced mass movement of irregular migrants provide further examples of hybrid tactics. The weaponisation of migrants, also termed "coercive engineered migrations", has been employed, such as on the Greece-Turkey border (2020) and the Lithuania-Belarus, Latvia-Belarus, and Poland-Belarus borders (2021), as a tool to compel the EU to make political and financial concessions, or in the case of the 2021 frontier incidents, to coerce the EU to withdraw its support for democratic movement in Belarus. The 2020 and 2021 border incidents exploited internal division among EU Member States on the issue of illegal migration, a vulnerability that became evident during the 2015 migration crisis.[45] The Prime Ministers of Poland, Lithuania, Latvia, and Estonia;[46] President of the European Commission Ursula von den Leyen; and President of the European Council Charles Michel explicitly labelled these hybrid operations as hybrid attacks to destabilise Europe.[47] In response to the 2021 hybrid attacks, the EU amended its sanctions regime to be able to respond to the instrumentalisation of migrants for political purposes and subsequently adopted restrictive measures (sanctions) on Belarus.[48]

41 Russian interference in the 2016 United States presidential elections has been alleged to involve Russian troll farms using divisive topics such as gun control and racial conflict to polarise voters and plant disinformation; Yablokov, 2022, p. 767.

42 Franke, 2015, pp. 11–12. While confusing the enemy and distorting the perception of real facts are key tactics of Russia's information war concept, reflexive control provides a theoretical foundation and tools for achieving it; Aukia and Kubica, 2023, pp. 34–35.

43 Aukia and Kubica, 2023, p. 35.

44 Ibid.

45 For the artificially engineered migration crisis, see: Bekić, 2022; Greenhill, 2010; Łubiński, 2021; Sari, 2023.

46 *Statement of the Prime Ministers of Poland, Lithuania, Latvia and Estonia on the hybrid attack on our borders by Belarus*, 2021.

47 European Commission, 2021a; European Commission, 2021b; European Council, 2021.

48 Council of the EU, 2021a; Council of the EU, 2021b.

The Russian Federation's 2014 intervention in Crimea is considered an archetypal example of a hybrid conflict.[49] The Russian campaign was carried out with a combination of various kinetic and non-kinetic means, which involved, among others, using proxy soldiers and unmarked special forces ("little green men"), provoking internal disturbances, conducting information operations, and making instrumental (mis)use of the international legal framework on the protection of national minorities and prevention of genocide.[50]

A cybercampaign to blur factual reporting and manipulate public opinion played a prominent role in the Russian hybrid arsenal used against Ukraine in 2014. Aside from social engineering and information warfare-style attacks, malicious software was installed in Ukrainian government and military artillery systems, while botnet attacks targeted Ukrainian websites and Ukrainian electoral systems.[51] An eye-opening research by John E. Arthur VI on the Russian cybernetwork operations in Estonia (2007), Georgia (2008), and Ukraine (2014) shows that Russia has long been using cyber and influence operations to support its military operations in the central regions of the former Soviet Bloc. Arthur demonstrates that a clear pattern can be identified in the Russian cybernetwork operations, which consist of three deliberate phases of cyber-support to potential Russian military operations, two of which include extensive inform-and-influence activities.[52]

The 2014 hybrid campaign involved large-scale use of legal arguments to support violent operations and other hybrid actions. Examples of how the Russian Federation used lawfare in the 2014 hybrid operation against Ukraine are plentiful: amending domestic laws on incorporation of territories into the Russian Federation, allowing the annexation of parts of neighbouring states following popular local referenda (in February–March 2014), modifying the law applicable to citizenship and using residency claims dating back to the Soviet Union and Russian Empire to grant Russian citizenship (April 2014); issuing Russian passports to claim the presence of Russian citizens in neighbouring regions (Abkhazia, South Ossetia, and Crimea);

49 Heap, 2021, p. 12. Although Russia had used a combination of military and non-military tactics in Georgia in 2008, they were only described as "hybrid" retrospectively.

50 Heap, 2021, p. 12; Parulski, 2016, pp. 12–15; Veress, 2023, pp. 35–36.

51 The sequence of Russian cybercampaigns' targets in 2014 was as follows: (1) Ukrainian populace, (2) governmental systems, (3) military systems, (4) Ukrainian websites, (5) Ukrainian electoral systems, and (6) Ukrainian utility systems; Arthur, 2020, pp. 51–52.

52 The first phase of Russian cybercampaigns tends to be a shaping operation, which creates conditions for the success of the decisive operation or kinetic attack; it targets, via malware, governmental and military organisations. The second phase is a sustaining operation, which focuses on information technology, media, and news targets and coincides with social media disinformation campaigns designed to dominate the information spectrum and create confusion. The final phase, disruption, focusses on dominating the adversary via inform-and-influence activities and computer network attacks. These attacks tend to consist of distributed denial-of-service/Structured Query Language injection-type attacks aimed at governmental and military targets; information technology, media, and news targets; and financial and business institutions. By attacking and disrupting such targets, Russia can effectively distract the targeted citizens from rapidly developing into an insurgency or organising a more robust means of defence; Arthur, 2020, pp. 52–53.

making attempts to use the United Nations (UN) Security Council to sanction the potential Russian opening of humanitarian corridors, using Kosovo and Libya as legal precedents for Russian actions; Russian courts sentencing Ukrainian officials *in absentia*; and Russian propaganda fabricating a legal case to justify the deployment of Russian "peacekeeping forces" in East Ukraine to prevent "a humanitarian catastrophe" caused by the "genocide" of Russian speakers in the region (examples from Voyger).[53]

Aside from the above-mentioned examples of instrumentalisation of law, the different narratives on the 1994 Budapest Memorandum on Security Assurances,[54] signed by the United States, Russia, Ukraine, and the United Kingdom in connection with Ukraine's accession to the 1968 Treaty on the Non-Proliferation of Nuclear Weapons,[55] show how the interpretation of international obligations can be used as lawfare. Signatories of the Budapest Memorandum pledged to respect the independence, sovereignty, and existing borders of Ukraine and to refrain from the threat or use of force against the territorial integrity or political independence of Ukraine, undertaking that none of their weapons will ever be used against Ukraine except in self-defence or otherwise in accordance with the UN Charter.[56] Russia breached these commitments by the annexation of Crimea in 2014 and subsequent aggression in Ukraine; however, Russian officials asserted that the loss of Ukraine's territorial integrity has resulted from complicated internal processes, which Russia and its obligations under the Budapest Memorandum have nothing to do with.[57] Such deliberate misinformation about the scope of treaty obligations and the attempt to negate the validity of an international treaty, which runs afoul of the principle *pacta sunt servanda*, demonstrates the lack of good faith and amounts to a case of treaty abuse, potentially giving rise to state responsibility.[58] Mosquera and Bachmann note that by distorting international law, Russia has engaged in hybrid warfare against not only Ukraine but also the entire NATO.[59] In this context, it is important to note that the 1994 Budapest Memorandum was purposefully designed to be ambiguous to allow its signatories to achieve significant goals. It provides a clear example of how legal ambiguities can become vulnerabilities that are exploited by hybrid adversaries.[60]

53 Voyger, 2015, p. 20.

54 *Memorandum on security assurances in connection with Ukraine's accession to the Treaty on the Non-Proliferation of Nuclear Weapons*, signed in Budapest on 5 December 1994, UN Treaty Series vol. 3007, No. 52241.

55 *Treaty on the Non-Proliferation of Nuclear Weapons*, concluded in Washington, Moscow, London on 1 July 1968, UN Treaty Series vol. 729, No. 10485.

56 Articles 1 and 2 of the Budapest Memorandum.

57 Statement of the Russian Minister of the Foreign Affairs, Alexander Lukashevich, of 12 March 2015, cited in Munoz Mosquera and Bachmann, 2015, p. 27.

58 Munoz Mosquera and Bachmann, 2015, p. 27.

59 Munoz Mosquera and Bachmann, 2016, p. 84.

60 For a detailed analysis of the 1994 Budapest Memorandum in the context of the Russia-Ukraine war, see Soldatenko, 2023.

The 2014 Russian hybrid attacks against Ukraine, the intensity of which reached its peak with the annexation of Crimea in February–March 2014, amounted to acts of aggression contrary to the prohibition of the use of force set forth in the UN Charter.[61] Although, in February 2022, the initial hybrid conflict transformed into a conventional high-intensity military conflict, this full-scale military conflict has constantly been a theatre of various hybrid operations, including, but not limited to, actions aimed at triggering energy, humanitarian, and food crises. The commercial blockade of Black Sea ports is an illustrative example of hybrid tactics used in the 2022 Russian military invasion against Ukraine. The blockade resulted in a disruption of Ukrainian grain exports. However, seen from a wider perspective, this not only deprived Ukraine of its key revenue source but also aimed to cause a food crisis at the regional and global levels. This further destabilised the situation in Africa and the Middle East and hobbled the already critical global security situation.[62] Overall, through its hybrid actions in 2022 and 2023, Russia aimed to reduce Western support for Ukraine and weaken the cohesion of NATO and the EU.[63]

3. Legal Assessment Under Public International Law

Hybrid threats and warfare can be examined from different angles with respect to different fields of public international law. First, hybrid threats and warfare are examined in the context of international law on the use of force (*jus ad bellum*) through the prism of prohibition on the use of force and the exceptions thereto, such as the right to individual and collective self-defence, and in the context of attribution of responsibility. The aim is to answer the following: (1) Can the use of hybrid threats and warfare trigger the right to individual or collective self-defence? (2) If military countermeasures are not a lawful response to hybrid activities, what defence measures can be lawfully implemented against aggression below the threshold of an armed attack? (3) Can hybrid adversaries face the responsibility for international wrongful acts on account of the use of hybrid threats and warfare? Second, hybrid activities are assessed from the perspective of IHL (*jus in bello,* law of armed conflicts), in terms of both international and non-international armed conflicts. Finally, hybrid threats and warfare are examined from the perspective of international human rights law to determine whether, and to what extent, countering hybrid threats can entail the curtailment of fundamental rights and freedoms.

61 *Charter of the United Nations*, adopted in San Francisco on 26 June 1945, XV UNCIO 335. See, e.g. European Council, 2014, para. 2; Wyrozumska, 2014, pp. 277–278.
62 Ionita, 2023.
63 Ibid.

3.1. Jus ad bellum

The international law governing the use of force rests upon the general prohibition of the threat or use of force between states, as expressed in Article 2 para. 4 UN Charter, which states that 'All Members shall refrain in their international relations from *the threat or use of force* against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations' (emphasis added). The ban on the unilateral use of force is a universally accepted norm of customary international law.[64] It constitutes one of the core values of the international community as a principal element of the international system of war prevention. In the UN Charter, the general prohibition of force is subject to two exceptions. They encompass, first, collective actions of the UN Security Council to maintain or restore international peace and security, implemented under Chapter VII of the UN Charter. Until the Security Council has taken collective actions, the state or states under attack can resort to individual or collective self-defence, which accounts for the second exception to the ban on the recourse to inter-state military action. Defensive use of force is permitted under Article 51 UN Charter, which states that the UN Charter does not impair 'the inherent right of individual or collective self-defence if *an armed attack* occurs against a Member of the United Nations' (emphasis added). The use of force in response to an armed attack is subject to the principles of proportionality, necessity, and immediacy, which aim to avoid escalation of conflicts through strict requirements for a permissive collective armed response.[65] The principle of self-defence, outlined in Article 51 UN Charter, provides a legal anchor for the collective defence mechanism enshrined in Article 5 of the NATO's founding treaty – the North Atlantic Treaty (hereinafter, the NATO Treaty)[66] – the cornerstone of the NATO Alliance, as well as in several regional collective defence mechanisms, such as those existing under the EU framework (mutual

64 Dörr and Randelzhofer, 2015, p. 203. The first international treaty on the renunciation of war as an instrument of international relations was adopted in 1928 (Briand-Kellog Pact), with which international law moved from *jus ad bellum* to *jus contra bellum*. For the historical development of the ban on the use of force, see, e.g. Dinstein, 2011, pp. 81–88; Dörr and Randelzhofer, 2015, pp. 204–207.

65 Fogt, 2020, pp. 69–70. For related case law of the International Court of Justice (ICJ), see, e.g. ICJ, *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America)*, Merits, judgement of 27 June 1986, https://www.icj-cij.org/sites/default/files/case-related/70/070-19860627-JUD-01-00-EN.pdf; ICJ, *Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America)*, judgement of 6 November 2003, https://www.icj-cij.org/sites/default/files/case-related/90/090-20031106-JUD-01-00-EN.pdf; ICJ, *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Rwanda)*, judgement of 19 December 2005, https://www.icj-cij.org/sites/default/files/case-related/116/116-20051219-JUD-01-00-EN.pdf.

66 *North Atlantic Treaty*, signed in Washington on 4 April 1949, UN Treaty Series vol. 34, Registration No. 541.

defence clause in Article 42 para. 7 of the Treaty on the EU) or within the Organization of American States (Article 3 para. 1 of the Inter-American Treaty of Reciprocal Assistance).[67]

According to the prevailing interpretation of Article 2 para. 4 UN Charter, prohibition of the 'threat and use of force' covers only the use of armed force, that is, military force, and it does not extend to "any" possible use of force.[68] Consequently, psychological or economic pressure, which often forms part of the hybrid arsenal, does not amount to the use of force within the meaning of Article 2 para. 4 UN Charter, unless combined with the use of armed forces.[69] Therefore, it can be established that targeting a state or states with hybrid threats and warfare, which do not involve violent acts, will not be considered waging "war" in the meaning of illegal use of force under Article 2 para. 4 UN Charter.[70] Neither does it qualify as "aggression" in terms of the UN General Assembly Resolution 3314 (XXIX) on the definition of aggression.[71] The 2014 Russian hostilities against Ukraine were considered acts of direct aggression in violation of the prohibition of threat or use of force, primarily because of the deployment of Russian armed forces in Ukraine and illegal acquisition of part of its territory, and not as a direct consequence of disinformation campaigns, cyberattacks, or weaponisation of law, also widely employed by Russia during the 2014 hybrid conflict.

The inherent right to self-defence under Article 51 UN Charter is not linked to the illegal "use of force" but is dependent on the existence of an "armed attack". The threshold for an armed attack is considered higher than that for the use of force, implying that all armed attacks classify as the use of force, but not every use of force qualifies as an armed attack.[72] According to the International Court of Justice (ICJ), the essential criteria that need to be considered when assessing whether hostilities level up to armed attack are their scale and effects.[73] Nonetheless, the relevant provisions of the UN Charter do not establish any gravity requirement, nor is the existence of the *de minimis* threshold for an armed attack undisputed in the international legal doctrine.[74] From the perspective of hybrid threats and warfare, the gap between the

67 *The Inter-American Treaty of Reciprocal Assistance*, signed in Rio de Janeiro on 2 September 1947, Organization of the American States Treaty Series Nos. 8 and 61 (also called the Rio Pact).

68 Dörr and Randelzhofer, 2015, pp. 208–209.

69 Dinstein, 2011, p. 88; Dörr and Randelzhofer, 2015, pp. 208–210. Nevertheless, such conduct may amount to a breach of the principle of non-interference in domestic affairs.

70 Instead of condemning the "resort to war", drafters of the UN Charter rephrased the term used in Article I of the 1928 Briand-Kellog Pact to 'threat or use of force'. The goal was to settle the discussion on the scope of the prohibition of war by prohibiting the deliberate initiation of force, whether or not the hostilities amounted to the normative condition of "war"; see: Lauterpacht, 1968, p. 62; Lesaffer, 2015, p. 54.

71 General Assembly Resolution 3314 (XXIX) Definition of Aggression, 14 December 1974, A/RES/3314(XXIX).

72 As recognised by the ICJ in *Nicaragua v. United States of America*, paras. 191–195; see also Dinstein, 2011, pp. 207–210; Hathaway, 2014, p. 214; Schmidt, 2015, p. 1119.

73 ICJ, *Nicaragua v. United States of America*, para. 195.

74 Fogt, 2020, pp. 63–64; Sari, 2017, pp. 23–24.

use of force and armed attack represents a serious obstacle for legal inter-operability, meaning there are difficulties related to the legal assessment of the situation and available countermeasures. In parallel, the gap between Article 2 para. 4 and Article 51 UN Charter creates an important advantage for hybrid adversaries by setting the stage for conducting hostilities at such a level of intensity or in a form that does not invest the targeted state with the right to use force in self-defence (as long as it is kept below the threshold for an armed attack).[75]

There have been several attempts at clearing the legal fog of hybrid war. Fogt suggests that in the face of low-intensity hybrid threats designed to remain below the threshold of an armed attack, the theory of "accumulation of events" can provide a useful tool to facilitate the threats' legal assessment. The asymmetric hybrid character of low-level use of force, flexibility in the intensity, and disinformation and fake news campaigns targeted at the entire papulation may collectively level up to an "armed attack".[76] The possibility of cumulatively weighting a series of acts to categorise them as an armed attack that justifies the right to use self-defence has been established by the ICJ[77] and has received support in the international legal doctrine.[78] In other words, the theory of accumulation of events provides the targeted state or states a legal possibility to exercise the right of self-defence in case of a hybrid campaign that otherwise is designed to remain below the threshold of an armed attack. Nevertheless, even if the accumulation of several low-intensity hybrid hostilities can be classified as an armed attack within the meaning of Article 51 UN Charter, it must be demonstrated that the hybrid hostilities originate from a specific state or non-state actor, and that they are attributable to those states or non-state actors, which, as the practice shows, is difficult due to the use of proxy actors, proxy networks, or a denial policy.

According to Dörr and Randelzhofer, the weapon-like destructive potential some attacks might develop using information technology legitimises an exception to the narrow interpretation of the term "force" in Article 2 para. 4 UN Charter as solely military force.[79] In extreme situations, computer network attacks against the information systems of another state might produce the effects of an armed attack triggering the right to self-defence under Article 51 UN Charter and allow the targeted state to respond by using armed force without violating Article 2 para. 4 UN Charter.

75 Sari, 2017, p. 23. There are several further legal issues connected to the use of force in legitimate self-defence that belong to complex legal grey zones: quality and quantity of the target of an armed attack (territory, infrastructure, military facilities, population, and person), burden of proof, and need of a possible intention; Fogt, 2020, p. 66.

76 Fogt, 2020, pp. 66–67.

77 *Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America*), para. 64. The ICJ examined the hostile incidents cumulatively to consider that they did not constitute an armed attack on the United States of the kind that, in line with the test used in the Nicaragua case, could have been qualified as a "most grave" form of the use of force, justifying the right to self-defence under Article 51 UN Charter.

78 Dinstein, 2011, pp. 206–207.

79 Dörr and Randelzhofer, 2015, p. 210; similarly, Dinstein, 2011, p. 212.

A similar approach is adopted by Dinstein, according to whom the main consideration while assessing weapons for the purpose of an "armed attack" within the meaning of Article 51 UN Charter is their consequential effects.[80] Thomas P. Jordan suggests that to determine whether a cyberattack constitutes an act of war, the ends sought from the attack should be examined. There is a substantial difference between a cyberattack to steal sensitive documents and a cyberattack to disable the targeted state's ability to control its nuclear arsenal or central weapons system – only the latter is an act of war, while the former is merely an act of espionage.[81] In light of these considerations, it can be argued that if a hybrid campaign involving, *inter alia*, a computer network attack was to cause severe damage to property or even human fatalities, or seriously affect the targeted state's defensive capacities, it could be qualified as an armed attack, thus investing the affected state with the right to defensive use of force.

The 2014 Russian operations in Ukraine have prompted the necessity to evaluate the right to collective self-defence in the event of a hybrid threat or warfare. In 2015, NATO Secretary General Jens Stoltenberg publicly declared that the Alliance and its allies are prepared to counter hybrid warfare as part of collective defence under Article 5 NATO Treaty.[82] The 2022 NATO Strategic Concept endorsed Stoltenberg's earlier declaration and confirmed that the hybrid operations against Allies could reach the level of an armed attack, which can eventually lead the North Atlantic Council to invoke Article 5 NATO Treaty.[83]

Nevertheless, a key feature of most hybrid threats and warfare is that they operate below the threshold of armed conflict and therefore do not allow for the activation of individual or collective self-defence within the meaning Article 51 UN Charter, Article 5 NATO Treaty, or other defence alliance treaties. Therefore, the lawful answer to hybrid threats or warfare is, in most cases, limited to peacetime cooperation and non-forcible countermeasures. At the domestic level, the victim state can answer to hybrid threats short of an armed attack by implementing measures belonging to the peacetime and crisis (public emergency) legal framework. If a hybrid threat merely constitutes a breach of the principle of non-intervention, which does not level up to

80 Dinstein, 2011, p. 212.

81 Jordan, 2016, pp. 56–57.

82 Warsaw Summit Communiqué; see: NATO, 2016. Pursuant to Article 5 NATO Treaty,

> The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.

83 A similar conclusion has been drawn with respect to malicious cyber-activities; see: NATO, 2022, paras. 25, 27.

an armed attack, it is still possible for the affected state to employ peaceful countermeasures, such as retaliatory measures through retorsions.[84] A more coordinated response is available under Article 4 NATO Treaty, which provides for a joint consultation forum for the Allies: 'The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened'.

The attribution of responsibility for hybrid operations to a particular state or non-state actor is a major difficulty, considering that states often use proxies to operate in the grey zone and avoid accountability. The state denial policy and covert operations by proxies and provocateurs, such as private military contractors and non-uniformed special forces, is central to hybrid warfare.[85] Moreover, global cyber-networks that hybrid adversaries commonly use allow different actors to commit acts of hostility while disguising their location or involvement. Even if the location from where a cyberattack was initiated can be identified, determining whether the attack was state-sponsored or whether the attackers operated under the protection of the state might still be an arduous task.

Holding a hybrid aggressor accountable requires establishing who had control over a given hybrid operation or who sponsored it.[86] If the given hybrid operation can be tracked back and attributed to a particular state actor, the rules of state responsibility codified in the draft Articles on the Responsibility of States for Internationally Wrongful Acts[87] are applicable. They establish two conditions for an action or omission of a state to be considered an internationally wrongful act: (1) The conduct of the state must be attributable to the state under international law, and (2) with such conduct, the state must have breached its international obligation.[88] They also provide for a set of rules governing the attribution of the actions and omissions to the state. Besides the clear-cut case wherein the actions or omissions of the state organs account for the conduct of the state, the conduct of a person or entity that is not a state organ, but is empowered by the state's law to exercise elements of governmental authority, can also lead to the attribution of wrongful conduct to the state if it acts in that capacity in the particular instance, even if it exceeds its authority or contravenes instructions.[89] What is important from the perspective of hybrid conflicts in which the use of proxies is commonplace is that the conduct of a person or group of persons is considered an act of a state under international law if that person or group of persons is in fact acting on the instructions of, or under the direction or

84 Karski and Mielniczek, 2019, p. 78.
85 Fogt, 2020, p. 74.
86 Sanz Cabellero, 2023, p. 6.
87 *Articles on Responsibility of States for Internationally Wrongful Acts*, UN General Assembly Resolution 56/83 of 12 December 2001, A/RES/56/83. Although the document has not been adopted as an international treaty, some of its contents reflect customary law; Sanz Cabellero, 2023, p. 6.
88 Article 2 of the Articles on Responsibility of States for Internationally Wrongful Acts.
89 Articles 4–5 and 7 of the Articles on Responsibility of States for Internationally Wrongful Acts.

control of, that state (i.e. conduct directed or controlled by the state).[90] A conduct not attributable to a state according to the previous rules will nevertheless be considered an act of that state under international law if the state acknowledges and adopts the conduct as its own.[91] Finally, several circumstances preclude the wrongfulness of conduct, such as when the act constitutes a lawful measure of self-defence taken in conformity with the UN Charter or is a countermeasure taken against another state in breach of its international obligations.[92]

By way of illustration, hostilities during the 2014 Russian-Ukrainian hybrid conflict that were performed by irregular forces (little green men) on the Crimean Peninsula can be attributed to the Russian Federation based on several provisions of the 2001 draft Articles on the Responsibility of States for Internationally Wrongful Acts. First, during an annual televised meeting with the Russian nation on 17 April 2014, President Putin (eventually) admitted that the "little green men" acting in Crimea were Russian servicemen.[93] This allowed a formal qualification of their activities as having been carried out by the Russian Federation itself based on Article 4 of the draft Articles. Second, in the light of President Putin's statement, the responsibility of the Russian Federation for the activity of irregular forces could also be based on Article 11 of the draft Articles, according to which the state bears international responsibility for an activity that it acknowledges and adopts as its own. These actions, attributed to the Russian Federation, constituted a breach of its international obligations, such as the obligation to refrain from the use of force against territorial integrity stemming from Article 2 Budapest Memorandum. Therefore, the conditions for considering that Russia committed an internationally wrongful act were formally met.

The 2001 draft Articles on the Responsibility of States for Internationally Wrongful Acts can provide an adequate framework to address state-sponsored hybrid threats and warfare. Nevertheless, they do not eliminate two main challenges relating to the attribution of responsibility for hybrid operations: hybrid threats that cannot be attributed

90 Article 8 of the Articles on Responsibility of States for Internationally Wrongful Acts.

91 Article 11 of the Articles on Responsibility of States for Internationally Wrongful Acts.

92 Articles 21–22 of the Articles on Responsibility of States for Internationally Wrongful Acts.

93 Earlier in 2014, President Putin denied on numerous occasions that the well-equipped troops operating in Crimea and wearing green uniforms without insignia had been part of the Russian armed forces. On 17 April 2014, President Putin, while opposing the use of the term "little green men," said, '… one cannot apply harsh epithets to the people who have made a substantial, if not the decisive, contribution to enabling the people of Crimea to express their will. They are our servicemen'. While answering the question of who were the little green men, President Putin replied,

… our goal was to ensure proper conditions for the people of Crimea to be able to freely express their will. And so we had to take the necessary measures in order to prevent the situation in Crimea unfolding the way it is now unfolding in southeastern Ukraine. We didn't want any tanks, any nationalist combat units or people with extreme views armed with automatic weapons. Of course, the Russian servicemen did back the Crimean self-defence forces. They acted in a civil but a decisive and professional manner ….

For the English transcript of the annual special Direct Line with Vladimir Putin of 17 April 2014, see President of Russia, 2014. For an account of Russia's use of unmarked special forces as a tool of the 2014 hybrid conflict in Ukraine, see: Wentzell, 2021.

to any state actor and difficulties related to identifying the hybrid aggressors before any attempts to establish the connection with any state actor. In the first case, when a non-state actor is identified as a hybrid aggressor, as a rule, the targeted state's domestic criminal law will apply in terms of the attribution of responsibility.[94] The latter problem justifies the need for novel approaches. For example, Thomas P. Jordan suggests regarding cyberattacks – a particularly challenging form of hybrid threats and warfare in terms of identifying the attackers – that governments from whose territories the cyberattacks are launched should be mandated to participate in identifying the attackers or face the presumption that the state itself was coordinating the attack.[95]

3.2. *Jus in bello*

The IHL (law of armed conflicts, *jus in bello*) is a body of international law that governs the conduct of hostilities during an armed conflict, to limit its effects for humanitarian reasons. *Jus ad bellum* is distinct from *jus in bello*, as the former's application is not contingent on the legality of the armed conflict; consequently, it applies regardless of whether there has been a legitimate derogation from the prohibition of the use of force laid down in Article 2 para. 4 UN Charter.[96] The codified legal framework for the IHL consists primarily of four Geneva Conventions for the Protection of War Victims adopted in 1949[97] (hereinafter referred to jointly as "the 1949 Geneva Conventions") and supplemented by two Additional Protocols of 1977: Additional Protocol I (AP I), relating to the protection of victims of international armed conflicts, and Additional Protocol II (AP II), relating to the protection of victims of non-international armed conflicts.[98]

94 Sanz Cabellero, 2023, p. 6.

95 Jordan, 2016, p. 56.

96 According to the International Committee of the Red Cross (ICRC), determination of the existence of an armed conflict and the related applicability of IHL depends on only the circumstances prevailing on the ground and not whether the use of force against another state is permitted under the UN Charter. Whether a state uses force in accordance with its right of self-defence, because it has been authorised to do so by a UN Security Council mandate, or in violation of the prohibition on the use of force, does not affect the determination of the existence of an international armed conflict; ICRC, 2016, para. 215; see also Moussa, 2008.

97 Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, adopted in Geneva on 12 August 1949, UN Treaty Series vol. 75, Reg. no. 970; Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, adopted in Geneva on 12 August 1949, UN Treaty Series vol. 75, Reg. no. 971; Geneva Convention Relative to the Treatment of Prisoners of War, adopted in Geneva on 12 August 1949, UN Treaty Series vol. 75, Reg. no. 972; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, adopted in Geneva on 12 August 1949, UN Treaty Series vol. 75, Reg. no. 973.

98 Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I), adopted in Geneva on 8 June 1977, UN Treaty Series vol. 1125, Reg. no. 17512; Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of non-international armed conflicts (Protocol II), adopted in Geneva on 8 June 1977, UN Treaty Series vol. 1125, Reg. no. 17513.

The nature of hybrid conflicts prompts questions about whether the IHL applies to hybrid threats and warfare and, if yes, to what extent. Hybrid conflicts, by definition, exploit the grey zone threshold of an armed conflict; therefore, they provoke uncertainty as to whether the given use of a hybrid threat or warfare triggers the law of armed conflicts. The issue goes far beyond academic debate, and its practical significance is that it allows one to determine the proper legal framework regulating the conduct of hostilities in the given hybrid conflict. Should the IHL be activated, it influences the application of international human rights law, especially as it affects the interpretation and scope of restrictions of certain rights and freedoms under the general human rights regime (see section 3.3 below). For example, during an armed conflict, adversary combatants become legitimate objects of attack, and civilians who directly participate in hostilities lose their general protection against dangers arising from military operations.[99]

The common Article 2 para. 1 of the 1949 Geneva Conventions provides that the IHL applies to all cases of 'declared war' or of 'any other armed conflicts', even if the state of war is not recognised by one of them. Instead of providing a legal definition, the 1949 Geneva Conventions introduced a fact-based approach to the notion of an armed conflict. By virtue of Article 2 para. 1 of the 1949 Geneva Conventions, IHL is applicable as soon as a state undertakes hostile military action(s) against another state.[100] According to the International Committee of the Red Cross (ICRC), how states characterise the armed confrontation does not affect the application of the 1949 Geneva Conventions if the situation evidences that the concerned state is effectively involved in hostile armed actions against another state. The fact that a state does not, for political or other reasons, explicitly refer to the existence of an armed conflict in a particular situation does not prevent it from being legally classified as such.[101]

The interpretation of the notion of "an armed conflict" under the common Article 2 para. 1 of the 1949 Geneva Conventions refers to military hostilities and armed actions, that is, the prevailing form of waging wars at the time of drafting of the 1949 Geneva Conventions. This approach has been supported by, among others, the International Criminal Tribunal for the Former Yugoslavia (ICTY), which holds 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' (emphasis added).[102] In light of such an interpretation, there is no legal basis to establish that hybrid conflicts that do not involve violent actions trigger the application of the 1949 Geneva Conventions and IHL. Nevertheless, the ICRC has recently begun to consider technological

99 See: Article 51 paras. 1–3 of the AP I.
100 ICRC, 2016, para. 209.
101 Ibid., para. 213.
102 ICTY, *The Prosecutor v. Duško Tadić*, Decision of 2 October 1995 on the Defence Motion for Interlocutory Appeal on Jurisdiction, Case No. IT-94-1-A, para. 70.

advancements, particularly the exponential increase in states' cyber-capabilities and their potential impact on the civilian population and infrastructure, for the applicability of the humanitarian law. According to the ICRC, cyberoperations that have effects similar to classic kinetic operations, result in the destruction of civilian or military assets, or cause the death or injury of soldiers or civilians may amount to an armed conflict within the meaning of Article 2 para. 1 of the 1949 Geneva Conventions, even if they are not carried out in conjunction with classic military operations.[103] From the perspective of IHL, these situations should not be treated as different from equivalent attacks conducted through more traditional means and methods of warfare. Peter Mauer, former President of the ICRC, argues that multiple strategies are needed to adapt IHL to today's hybrid kinetic-cyber realities. He suggests making logical legal interpretations from already existing legal concepts under the 1949 Geneva Conventions, such as the principles of distinction, proportionality, and precaution, arguing that through proper interpretation, it would be possible to make them applicable to cyberoperations in today's conflicts.[104]

Second, the subdivision between international armed conflicts and non-international armed conflicts, underlying the IHL, makes the legal assessment of a hybrid campaign even less straightforward. Based on factual and objective criteria (e.g. involvement of an armed force), if a given hybrid conflict meets the threshold of an armed conflict under common Article 2 para. 1 of the 1949 Geneva Conventions resulting in the activation of the IHL, further classification of the conflict as an international or non-international conflict is required. International armed conflict is understood as an armed conflict between two or more states. By contrast, non-international armed conflicts are restricted to the territory of a single state, involving either regular armed forces fighting groups of armed dissidents or armed groups fighting each other.[105] As Antonio Cassese points out, the division between these two subcategories of armed conflicts has a substantial practical impact: While international armed conflicts are subject to a wide range of rules, including those set out in the four 1949 Geneva Conventions and AP I, internal conflicts are governed only by a limited range of rules (common Article 3 of the 1949 Geneva Conventions and AP II).[106] The distinction is all the more important as non-international armed conflicts are nowadays the most prevalent form of armed conflict.[107]

The existence of an international armed conflict is not dependent on any threshold for the intensity of the armed confrontation or the duration of the hostilities. According to the ICRC, even minor skirmishes between armed (land, air, or

103 ICRC, 2016, para. 255. According to van den Bosch, the view that IHL is applicable below the threshold of attacks is not necessarily limited to cyberoperations and can even be applied to all non-destructive military operations such as information campaigns or disturbing operations such as jamming; van den Bosch, 2021, p. 219.

104 Mauer, 2023.

105 ICRC, 2004.

106 Cassese, 2008, pp. 5–6; ICRC, 2004.

107 ICRC, 2016, para. 194.

naval) forces can spark an international armed conflict and lead to the applicability of the humanitarian law.[108] As already mentioned, the ICRC accepts that cyberoperations having effects similar to classic kinetic operations might also amount to an international armed conflict if they result in the destruction of property or cause the death or injury of soldiers or civilians.

The legal category of non-international armed conflicts is vague and surrounded by legal uncertainties due to the non-defined criteria regarding the level of organisation for the non-state group, geographical scope of the internal armed conflict, and intensity of hostilities and control of territory.[109] Whether the internal hostilities level up to a non-international armed conflict determines the possibility of the use of force. A crisis below the threshold for a non-international armed conflict needs to be managed using national crisis and emergency law as well as law enforcement rules of engagement under a human rights regime. On the contrary, a conflict involving sufficient degree of organisation and intensity of hostilities to prompt the application of *jus in bello* for non-international armed conflicts will allow for more offensive rules of engagement, which, nevertheless, will be more restrictive and defensive than the rules of engagement for a full-scale international armed conflict.[110] Hybrid campaigns provide a fertile ground for circumventing (and abusing) the already uncertain threshold of a non-international armed conflict, making the legal assessment underlying strategic and political decision-making very challenging, especially in situations where hybrid adversaries target multiple states simultaneously with asymmetric means and different intensities.[111]

According to Fogt, the distinction between an international and non-international armed conflict in a hybrid warfare depends on the evidence of state attribution, which is a sensitive and highly political issue.[112] The attribution of hostilities to a given state actor is not without major difficulties, partly because of the state's denial policy and cover operations, which are the essence of hybrid tactics, and partly because of different requirements for state attribution adopted by different international courts. The ICJ upholds a strict requirement for a conduct to give rise to legal responsibility of the state, expecting that it must be proven that that state had "effective control" of the military or paramilitary operations ("effective control test").[113] By contrast, the ICTY has held that the ICJ's effective control requirement was not suitable for acts of organised groups (e.g. a military unit or, in case of war or civil strife, armed bands of irregulars or rebels), where the lower standard of

108 Ibid., paras. 236–237.
109 Fogt, 2020, p. 73.
110 Ibid., p. 74.
111 Ibid.
112 Ibid.
113 ICJ, *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America)*, para. 115.

"overall control" can be applied to attribute to a state the acts of such groups.[114] The ICJ's strict requirement of "effective control" legally allows the state to use non-state actors in the grey zone where the standard of attribution cannot be met.[115]

State practice shows that hybrid adversaries tend to conceal their involvement, using various means and methods, to avoid reaching the threshold of an international armed conflict. During the 2014 hybrid conflict, Russia employed unmarked forces (little green men) for its hostile operations in Crimea. Initially, Russian authorities successfully asserted that the little green men comprised persons of Crimean origin and formed part of the Ukrainian self-defence forces. Wentzel argues that, from a tactical viewpoint, the presence or absence of national insignia was of little importance.[116] The principal effect of the absence of national markings and the broader information operations campaign was to bolster Russia's strategic narrative that the events in Crimea were initially domestic in origin. Since, according to the Russian narrative, the little green men were not Russian soldiers, the Russian Federation could maintain plausible deniability of the military operation and disavow their actions within a sovereign state. More importantly, Russia's claim that the little green men were Ukrainian self-defence forces was meant to shift the classification of the conflict from an international conflict to a domestic one. Once labelled a domestic conflict, it was more difficult for Ukrainian authorities to address the international community and request foreign intervention onto its territory.[117] This simultaneously distracted the international community and facilitated Russia's subsequent actions – overt military operations to support the purported self-determination movement and incorporate Crimea into the Russian Federation.

3.3. Human Rights Law

Preventing and countering hybrid threats and warfare goes parallel with the curtailment of certain human rights and freedoms, although the scope of restrictions is limited by international law and depends on legal classification of the hybrid threats. The relevant legal regime regulating restrictions and derogations from human rights standards is anchored in both the international human rights

114 ICTY, *The Prosecutor v. Duško Tadić*, Appeals Chamber Judgment of 15 July 1999, Case No. IT-94-1-A, para. 120.

115 Fogt, 2022, p. 74.

116 Wentzell, 2021, p. 45.

117 Use of the little green men sufficiently concealed the Russian origin of the attack and gave more reluctant members of NATO grounds to debate whether or not an armed attack, rather than domestic unrest, has indeed occurred. Wentzell further argues that from a tactical viewpoint, the presence or absence of national insignia was of little importance. Had they considered the unmarked little green men exclusively as a domestic threat, the Ukrainian armed forces would have been constrained by their domestic legal regime concerning the use of force against their own people. However, it is more likely that upon recognising that there was foreign interference, the rules of IHL would have governed the conflict, and the Ukrainian armed forces would have only been required to distinguish combatants from non-combatants; Wentzell, 2021, pp. 45–47.

law and IHL, and it forms an inherent part of the legal assessment of hybrid threats and warfare. The Council of Europe's Committee of Legal Advisers on Public International Law (CAHDI) recommends that each case of a hybrid campaign must be assessed individually according to the relevant legal regime.[118] While international human rights law is relevant to both military and non-military actions carried out as part of hybrid threats and warfare, if the hybrid actions level up to an armed conflict (be it international or non-international armed conflict), then the IHL also becomes applicable and affects the interpretation and scope of restrictions on human rights and freedoms. In situations of armed conflict, the protections offered by human rights conventions and the IHL co-exist, as highlighted by the ICJ[119] and the European Court of Human Rights (ECtHR).[120] According to the ICJ and ECtHR, the relationship between the IHL and human rights law can unfold according to three scenarios: some rights may exclusively be matters of the IHL, others may exclusively be matters of human rights law, and some others may be matters of both these branches of international law.[121]

From the perspective of the European Convention on Human Rights (ECHR),[122] use of a hybrid threat and warfare would prompt different consequences depending on whether it occurs (1) in times of war, (2) in times of a public emergency other than war, or (iii) in peacetime when no armed conflict or public emergency exists.

According to Article 15 para. 1 ECHR, in times of "war" or "other public emergency" threatening the life of a nation, states may derogate from their obligations under the ECHR.[123] The formal condition for a valid derogation is an official declaration of the state of emergency by law at the domestic level.[124] Article 15 para. 2 ECHR excludes the possibility of derogation, even under a

118 CAHDI, 2018, para. 3.

119 ICJ, *Legality of the Threat or Use of Nuclear Weapons,* para. 25. See also ICJ, *The Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion of 9 July 2004, para. 106; ICJ, *Armed Activities on the Territory of the Congo (Democratic Republic of Congo (DRC) v. Uganda*, judgment of 19 December 2005, para. 216.

120 ECtHR, *Hassan v. the United Kingdom*, judgement of 16 September 2014, Application No. 29750/09, paras. 102–103. In the past, the IHL framework was considered *lex specialis* to the human rights framework; nowadays, however, it is accepted that both legal areas are applicable at the same time and mutually influence each other's application.

121 ICJ, *The Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion of 9 July 2004, para. 106; ICJ, *Armed Activities on the Territory of the Congo (Democratic Republic of Congo (DRC) v. Uganda*, judgement of 19 December 2005, para. 216; ECtHR, *Hassan v. the United Kingdom*, para. 102.

122 *Convention for the Protection of Human Rights and Fundamental Freedoms*, adopted in Rome on 4 November 1950, ETS No. 005 (hereinafter referred to as ECHR).

123 Article 15 para. 1 ECHR states that
In time of war or other public emergency threatening the life of the nation any High Contracting Party may take measures derogating from its obligations under this Convention to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with its other obligations under international law.

124 Council of Europe, 2022, para. 53.

state of emergency, with respect to the right to life (Article 2 ECHR), prohibition of torture (Article 3 ECHR), prohibition of slavery or servitude (Article 4 para. 1 ECHR), and prohibition of punishment without law (Article 7 ECHR). Further non-derogable rights stem from additional Protocols to the ECHR (the right to *ne bis in idem*, as well as the protection against the death penalty),[125] while some rights are considered non-derogable, even if they are not expressly specified in the ECHR or its Protocols (e.g. the right to a fair trial and the right to an effective remedy).[126]

Based on Article 15 para. 2 ECHR, lawful use of force validates derogations from the otherwise non-derogable right to life. Deaths resulting from lawful acts of war constitute an exemption from the absolute protection under Article 2 ECHR. By the same token, the non-derogable status of the prohibition of death penalty does not exclude capital punishment in respect of acts committed in times of war or imminent threat of war.[127] The ECtHR is not required to interpret the meaning of "war" in Article 15 para. 1 ECHR. According to the prevailing view, the term "war", enabling far-reaching derogations from human rights under Article 15 paras. 1–2 ECHR, should be understood as an "armed conflict" (international or non-international) within the meaning of the common Article 2 of the 1949 Geneva Conventions.[128] Schabas suggests that it should be interpreted in light of the test used by the ICTY in the *Tadić* case, which implies that a "war" within the meaning of Article 15 para. 1 ECHR exists whenever there is a resort to armed force or protracted armed violence.[129] By referencing the understanding of "armed conflict" under the IHL, it seems justified to conclude that hybrid hostilities can activate the most far-reaching derogations from human rights if they involve the use of armed force, or *mutatis mutandis*, resulting in the destruction of civilian or military assets or death or injury of soldiers or civilians, even if they are not carried out in conjunction with classic military operations (see section 3.2 above). If a hybrid campaign meets the threshold of an armed conflict, it has two consequences: (1) derogation from Article 2 ECHR is allowed, and (2) the IHL becomes applicable as *lex specialis* to the international human rights law and determines if the lethal use

125 Article 3 of Protocol No. 6 to the Convention for the Protection of Human Rights and Fundamental Freedoms concerning the Abolition of the Death Penalty, ETS No. 114; Article 2 of Protocol No. 13 to the Convention for the Protection of Human Rights and Fundamental Freedoms, concerning the abolition of the death penalty in all circumstances, ETS No. 187); and Article 4 para. 3 of Protocol No. 7 to the Convention for the Protection of Human Rights and Fundamental Freedoms, ETS No. 117.

126 Council of Europe, 2022, paras. 71–75.

127 Article 2 of Protocol No. 6 to the Convention for the Protection of Human Rights and Fundamental Freedoms concerning the Abolition of the Death Penalty.

128 Fogt, 2020, p. 94.

129 See: ICJ, *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America)*, para. 115; Schabas, 2015, pp. 594–595.

of force is lawful.[130] Similarly, the existence of an armed conflict triggering the application of the IHL also affects the interpretation of the provisions of Article 5 ECHR (right to liberty and security). This can occur only in cases of international armed conflict, where the taking of prisoners of war and detention of civilians who pose a threat to security are accepted features of the IHL, and Article 5 ECHR could be interpreted as permitting such broad powers.[131]

A public emergency other than war that allows states to derogate from human rights, although not from the Article 2 of the ECHR, covers exceptional situations of crisis or emergency that affect the whole population and constitute a threat to the organised life of the community.[132] To enable derogations from human rights obligations under Article 15 para. 1 ECHR, the effects of a crisis situation must be actual or imminent, must involve the whole nation, and threaten the continuance of organised life of the community; moreover, the crisis or danger should be exceptional, meaning that normal measures or restrictions, permitted by the ECHR for public safety, health, and order, must be inadequate.[133] Following the terrorist attacks of 11 September 2001, the ECtHR has taken the stand that the requirement for public emergency under Article 15 para. 1 ECHR (a threat to the life of the nation) does not need to be understood narrowly as a threat of serious physical damage and loss of life, but it can extend to a menace to the institutions of government or the existence of a civil community.[134] Not every public emergency constitutes a threat to the life of the nation to justify derogations from the ECHR; however, states enjoy a wide margin of appreciation in assessing whether the life of nation is threatened by a public emergency and can consider a

130 Fogt, 2020, p. 94. The ICJ's 1996 *Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons* contains a good illustration of the interplay between human rights and IHL with respect to the right to life. While considering whether the use of nuclear weapons violates the right to life guaranteed in Article 6 para. 1 International Covenant on Civil and Political Rights, the ICJ concluded that

> The protection granted by the International Covenant on Civil and Political Rights does not cease in times of war, except by virtue of Article 4 of the Covenant whereby certain provisions may be derogated from in a time of national emergency. Respect for the right to life is not, however, such a provision. In principle, the right not arbitrarily to be deprived of one's life applies also in hostilities. The test of what is an arbitrary deprivation of life, however, then falls to be determined by the applicable lex specialis, namely, the law applicable in armed conflict which is designed to regulate the conduct of hostilities. Thus, whether a particular loss of life, through the use of a certain weapon in warfare, is to be considered an arbitrary deprivation of life contrary to Article 6 of the Covenant, can only be decided by reference to the law applicable in armed conflict and not deduced from the terms of the Covenant itself.

See: ICJ, *Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons*, para. 25.

131 *Hassan v. United Kingdom*, paras. 102–105.

132 ECtHR, *Lawless v. Ireland (no. 3)*, judgement 1 July 1961, Application No. 332/57, para. 28.

133 The test applied to assess whether a situation constitutes a public emergency threatening the life of the nation was formulated by the ECHR in the "Greek Case": Denmark, Norway, Sweden, Netherlands v. Greece, Applications Nos. 3321/67, 3322/67, 3323/67, 3344/67, opinion of the Sub-Commission, 4 October 1969; see also Schabas, 2015, p. 595.

134 ECtHR, A. *and Others v. the United Kingdom*, judgement of 19 February 2009, Application No. 3455/05, para. 179.

broad range of factors in determining the nature and degree of the actual or imminent threat.[135] The hybrid threat or warfare below the threshold of an armed conflict could become a valid ground for derogation from the ECHR obligations if it created a public emergency involving an actual or imminent threat to the existence of the nation. In such a case, safeguards under the ECHR would continue to apply, subject to possible derogations, which nevertheless could not encompass the safeguards under Articles 2, 3, and 4 paras. 1 and 7 of the ECHR. In situations short of armed conflict, the IHL framework as such would not be applicable.

The state practice of derogating from their ECHR obligations in times of public emergency can be exemplified by the notifications made by Ukraine following the Russian intervention in 2014. Ukraine derogated from the ECHR (and the International Covenant on Civil and Political Rights [ICCPR]) for the first time in June 2015 on the grounds of the international armed conflict ongoing on its territory since 2014. Since the first notification, more than 20 further derogation notifications have been filed, reflecting the evolution of the armed conflict between Ukraine and Russia.[136] The initial notifications were made in the context of hybrid conflict culminating in the annexation of Crimea, while the notifications made from March 2022 onwards took place in the context of a full-scale armed conflict. Ukraine authorities justified their first derogations in June 2015 with the needs of the anti-terrorist operations conducted by Ukrainian forces in certain areas of the country (Donetsk and Luhansk) against armed aggression from the Russian Federation.[137] Initially, Ukraine exercised the right of derogation from its obligations established in Article 5 (right to liberty and security), Article 6 (right to a fair trial), Article 8 (right to respect for private and family life), and Article 13 (right to an effective remedy) ECHR, as well as in Article 2 para. 3 and Articles 9, 12, 14, and 17 ICCPR. Later, Ukraine derogated from several other human rights obligations under the ECHR and ICCPR as well.[138] Some of the derogations were considered void, as they effected non-derogable rights, either *expressis verbis* based on the ECHR and its Protocols or based on customary international law (e.g. the right to *ne bis in idem*, right to an effective remedy, or right to a fair trial).[139] According to the Council of Europe's interpretation, this does not invalidate Ukrainian derogation as a whole, which remains valid, but only that part of the rights for which the derogation is allowed.[140] The non-derogable rights, even if derogated from, continue to apply, meaning that derogation does not affect these rights and cannot be used to interfere with them. The Ukrainian derogations from human rights obligations complied with the formal conditions under Article 15 para. 1 ECHR, considering that

135 Ibid., paras. 179–180; see also Schabas, 2015, pp. 595–596.

136 For a detailed analysis of Ukraine's derogations from its human rights obligations, see Council of Europe, 2022, p. 2.

137 Secretariat General, 2015.

138 *Legal Analysis of the derogation made by Ukraine under Article 15 of the European Convention of Human Rights and Article 4 of the International Covenant on Civil and Political Rights*, para. 82.

139 Ibid., paras. 71–75.

140 Ibid., para. 80.

when declaring the derogation and state of emergency, Ukraine relied on its national laws. For example, Ukraine relied on Resolution No. 462-VIII of the Verkhovna Rada in the June 2015 notification, on amendments to several national laws implementing specific derogatory measures in 2016, and on martial law declaring an emergency and imposing derogatory measures since February 2022.[141]

All notifications on derogations filed by Ukraine since 2015 referred to one ground for the derogation – armed aggression of the Russian Federation. In the 2015 notification, Ukraine referred to the annexation and temporary occupation by the Russian Federation of the integral part of Ukraine – the Autonomous Republic of Crimea and the city of Sevastopol – as a result of armed aggression against Ukraine, involving 'both regular Armed Forces of the Russian Federation and illegal armed groups guided, controlled and financed by the Russian Federation'.[142] The 2022 notifications referred to 'military aggression of the Russian Federation against Ukraine' as grounds for derogation.[143] Although the 2014 Russian-Ukrainian conflict is considered an archetypical example of a hybrid campaign, the derogations notified in 2015 were substantiated by the existence of an armed aggression and not by the use of non-kinetic means also widely employed in the conflict. Although the Ukrainian case-study is not the most apposite example of a derogation under Article 15 ECHR for a hybrid threat and warfare not involving military means, it showcases the practical functioning of the derogation clause in the context of a hybrid campaign. It has been suggested that in the 2021 migration crisis on the Polish/Latvian/Lithuanian-Belarussian border, which was considered to involve hybrid attacks that used coercive engineered migration, invoking the derogation clause under Article 15 ECHR could have been a viable option for the targeted states, especially considering that all three of them invoked public emergency measures. A situation of instrumentalised migration could be qualified as a public emergency where the situation reaches the level of prohibited use of force and validates the derogation from human rights obligations.[144]

The third possible scenario involving the effect of hybrid actions under the human rights framework refers to situations where the hostilities do not amount to armed conflict or a public emergency threating the nation. The derogation clause in Article 15 ECHR is not applicable, nor is the IHL.[145] In peacetime, no derogation from human rights obligations is possible, while restrictions on human rights and freedoms guaranteed in the ECHR can be imposed only in accordance with the limitation clauses specifically provided for in the ECHR. In accordance with para. 2 of Articles 8, 9, 10, and

141 Ibid., paras. 58–59.

142 *Notification – JJ7979C Tr./005-185 – Ukraine – Derogation to the Convention on the Protection of Human Rights and Fundamental Freedoms*, p. 2.

143 Secretariat General, 2022, p. 3.

144 Huttunen, 2024.

145 Nevertheless, according to the ECtHR, lack of a formal derogation under Article 15 of the ECHR does not prevent the court from considering the context and provisions of IHL when interpreting and applying the ECHR rights in peacetime, e.g. Article 5; see: *Hassan v. United Kingdom*, para. 104.

11 ECHR, as well as Article 2 para. 3 of Protocol No. 4 to the ECHR,[146] the protection of national security or public safety can constitute valid grounds for curtailment of human rights. Any response to hybrid threats and warfare leading to human rights restrictions must not only pursue a legitimate aim, such as national security, but also be prescribed by law and be necessary in a democratic society. Moreover, Article 18 ECHR prohibits the states from applying the restrictions permitted under the ECHR for any purpose other than those for which they have been prescribed.

The Parliamentary Assembly of the Council of Europe has expressed a concern that certain Member States have already taken measures (e.g. surveillance measures, blocking of websites, expulsion of foreigners, and criminal convictions for online statements) that prompt questions concerning the respect for human rights, primarily the right to freedom of expression, along with the right to information, right to respect for one's privacy, and right to the freedom of movement.[147] A 2018 Recommendation of the Parliamentary Assembly envisaged the development of new legal standards to prevent and combat hybrid threats and warfare, which was followed by a Parliamentary Assembly resolution with that aim.[148] However, the CAHDI considered that developing new legal standards to prevent and combat the threats of "hybrid war" is premature at this stage, considering the absence of a common understanding as to what a "hybrid war" is.[149]

When considering hybrid threats and warfare from the perspective of the international human rights law, it is exceedingly difficult to balance the interests of national security and states' sovereignty with freedom of expression, right to privacy, and other individual human rights and freedoms. That combined with the legal asymmetry between hostile actors and democratic states and the fear of eventual "hypocrisy costs"[150] can hamper an effective response to hybrid threats; this further enhances the likelihood of the success of hybrid actions. The human rights agenda,

146 Protocol 4 to the European Convention for the Protection of Human Rights and Fundamental Freedoms, securing certain Rights and Freedoms other than those already included in the Convention and in the First Protocol thereto, signed on 16 September 1963, ETS No. 46.

147 Parliamentary Assembly of the Council of Europe, *Legal challenges related to hybrid war and human rights obligations*, Resolution 2217 (2018).

148 Parliamentary Assembly of the Council of Europe, Recommendation 2130 (2018) on the 'Legal Challenges Related to Hybrid War and Human Rights Obligations', 26 April 2018; Parliamentary Assembly of the Council of Europe, *Legal challenges related to hybrid war and human rights obligations*, Resolution 2217 (2018).

149 *Opinion of the CAHDI On Recommendation 2130 (2018) of the Parliamentary Assembly of the Council of Europe – 'Legal Challenges Related to Hybrid War and Human Rights Obligations'*, para. 5.

150 The term "hypocrisy costs" denotes symbolic political reputational costs that can be imposed when there exists a real or perceived disparity between a professed commitment to liberal values and/or international norms and demonstrated state actions that contravene such a commitment. They are operationalised in a manner such that once a government or its leadership has publicly committed itself to a principle, canny observers can use those positions, and their command of information, to expose the distance between discourse and practice. Hypocrisy costs can further enhance the likelihood of success of hybrid actions carried out by hybrid adversaries; for an example of coercive engineered migration, see: Blake-Martin, 2023.

which questions absolute state sovereignty, might at times collide with the UN Charter and has been identified as a major challenge to the international security architecture.[151]

4. Legal Assessment Under the EU Law and Policies

4.1. Hybrid Threats within the EU Common Defence and Security Policy

Countering of hybrid threats forms an integral part of the Strategic Compass for Security and Defence, the first quasi-military strategy of the EU approved by the Council of the EU on 21 March 2022. It establishes a common strategic vision for the EU's security and proposes several concrete actions in four main domains: act, secure, invest, and partner. The action plan under the Strategic Compass sets out, among others, main objectives related to countering hybrid threats. These include the (1) creation of the EU Hybrid Toolbox, consisting of various instruments to prepare for and respond in a coordinated manner to a wide spectrum of hybrid threats; (2) creation of the Hybrid Fusion Cell to enhance situational awareness through strategic analysis and assessments of hybrid threats; and (3) establishment of the EU Hybrid Rapid Response Teams to secure short-term and targeted assistance to EU Member States in case of a hybrid campaign.[152] Moreover, the Strategic Compass envisages measures to counter foreign information manipulation and interference (FIMI) taking place within broader hybrid campaigns, such as by developing the EU toolbox to address and counter the FIMI. These actions are to be implemented in parallel to enhance further counter-hybrid cooperation with NATO.

The significance attributed to countering hybrid threats, evidenced by its fully-fledged place in the Strategic Compass, is a consequence of several years of policymaking for hybrid threats long preceding the adoption of the Strategic Compass. The EU's policymaking for addressing hybrid threats began in the aftermath of the 2014 Russian annexation of Crimea and the beginning of the Donbas conflict. In 2015, the Council of the EU adopted conclusions on the Common Defence and Security Policy, calling for a joint framework with actionable proposals to counter hybrid threats and foster the resilience of the EU and its Member States. The first comprehensive policy document, the *Joint Framework on Countering Hybrid Threats – A European Union Response*[153] was issued in 2016 by the European Commission and High Representative

151 Hathaway, 2014, pp. 217–222; Sanz Caballero, 2023, p. 5.

152 Strategic Compass for Security and Defence, 2022, p. 22.

153 European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats – a European Union response*, Brussels, 6 April 2016, JOIN(2016) 18 final.

of the Union for Foreign Affairs and Security Policy; this was followed by the 2016 EU *Operational Protocol for Countering Hybrid Threats 'EU Playbook'*[154] and the *2018 Joint Communication on Increasing Resilience and Bolstering Capabilities to Counter Hybrid Threats*.[155] In 2020, a mapping of almost 200 measures related to enhancing the EU's resilience against hybrid threats, implemented under the auspices of the EU, was made public.[156] A highly relevant policy document, the *Council Conclusions on a Framework for a Coordinated EU Response to Hybrid Campaigns*,[157] was adopted in June 2022 to support the development of the EU Hybrid Toolbox and counter the FIMI actions as envisaged in the 2022 Strategic Compass. These conclusions have been adopted in light of Russia's armed aggression against Ukraine, which, as the Council of the EU acknowledged, was 'combined with hybrid tactics, cyberattacks, foreign information manipulation and interference, economic and energy coercion and an aggressive nuclear rhetoric'.[158] The *Annual Progress Report on the Implementation of the Strategic Compass for Security and Defense*, published in March 2023, recognised that the use of hybrid tactics against the EU and its Member States has been exacerbated by Russia's invasion of Ukraine, which has witnessed hybrid tactics such as the instrumentalisation of food, irregular migration, energy, and lawfare.[159]

4.2. Coordinated and Collective Response to Hybrid Threats under the EU Legal Framework

The primary responsibility for countering hybrid threats and campaigns relates to national security and defence and lies with the EU Member States. Nonetheless, many Member States face similar or common threats that target cross-border infrastructures or networks and can be addressed more efficiently with a coordinated response at the EU level, using instruments envisaged by the EU treaties and policies. The 2016 *Joint Framework on Countering Hybrid Threats – A European Union Response* and the 2022 *Council Conclusions on a Framework for a Coordinated EU Response to Hybrid Campaigns* provide an overview of the instruments and policies that are most suitable for a coordinated response to malicious hybrid activities at the EU level.

154 European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, *Joint Staff Working Document. EU operational protocol for countering hybrid threats 'EU Playbook'*, Brussels, 5 July 2016, SWD(2016) 227 final.

155 European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament, the European Council and the Council. Increasing resilience and bolstering capabilities to counter hybrid threats*, Brussels, 13 June 2018, JOIN(2018) 16 final.

156 European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, *Joint Staff Working Document. Mapping of measures related to enhancing resilience and countering hybrid threats*, Brussels, 24 July 2020, SWD(2020) 152 final.

157 Council of the European Union, *Council Conclusions on a Framework for a coordinated EU response to hybrid campaigns*, Brussels 21 June 2022, 10016/22.

158 Ibid., para. 1.

159 High Representative of the Union for Foreign Affairs and Security Policy, 2023, p. 11.

Decisions on a coordinated EU response should be made on a case-by-case basis, and several guiding principles must be observed, as laid down in the 2022 Council Conclusions. The coordinated countermeasures in response to hybrid campaigns should serve to protect democratic values, processes, and institutions, as well as the integrity, security, and strategic interests of the EU, its Member States, and their citizens; they need to provide for attainment of the objectives of the EU, particularly the Common Foreign and Security Policy objectives set out in the Treaty on EU (TEU) and Treaty on the Functioning of the EU (TFEU); they shall be based on a shared situational awareness among the Member States and correspond to the needs of the specific situation at hand; and finally, they should consider the broader context of the EU's external relations with the state concerned by the response. More importantly, if seen from the legal perspective, the decision on a coordinated EU response shall ensure that the envisaged countermeasures (1) 'respect international law', (2) 'protect fundamental rights and freedoms', (3) 'support international peace and security', and (4) are '*proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact* of each particular hybrid campaign' (emphasis added).[160]

In many cases, a decision on a lawful and proportionate response to hybrid campaigns is contingent on the attribution. The process of attribution, most importantly legal and political attribution, is understood as assigning responsibility for a malicious hybrid activity to a specific state or non-state actor and consists of different levels.[161] Under the existing EU framework, the attribution is a sovereign national prerogative, a political decision made by EU Member States on a case-by-case basis.[162] The Member States' decision on attribution should be based on all-source intelligence, in which they can rely on the assistance of the EU Single Intelligence and Analysis Capacity framework, which combines civilian and military intelligence to produce all-source intelligence assessments, particularly the Hybrid Fusion Cell. However, hybrid threats and campaigns are often designed in such a way as to create ambiguity around their origins and hinder decision-making processes, which makes attribution a principal legal challenge impeding EU Member States' effective response. In the 2022 Council Conclusions, the Council of the EU affirmed that not all measures forming part of a coordinated EU response to hybrid campaigns require assigning responsibility to a state or non-state actor.[163] Measures covered by the Framework for a Coordinated EU Response can be tailored to the degree of certainty that can be established in each case. When coordinated attribution is not possible or public attribution is not in the best interest of the EU and its Member States,

160 *The EU Framework for a Coordinated Response to Hybrid Campaigns*, para. 8.

161 Some types of hybrid threats also require a technical attribution, such as in case of cyber-incidents, where the process of technical attribution involves using information technology forensics to evaluate technical artefacts and evidence to gather knowledge about the attacker's actions; see: Bendiek and Schulze Attribution, 2021, p. 10.

162 Council conclusions of a Framework for a coordinated EU response to hybrid campaigns, paras. 14 and 17.

163 Ibid., para. 18.

well-calibrated asymmetric actions from the toolbox covered by the framework can be implemented on a case-by-case basis, providing that they comply with international law and receive due approval.[164]

According to the Council of the EU's conclusions, when the perpetrator of a hybrid campaign can be identified "with a high degree of certainty", asymmetric and proportionate measures in line with international law may be taken, to either prevent or respond to a hybrid campaign.[165] Member States' response is not limited to hybrid campaigns that are classified as internationally unlawful acts; they can also be triggered by malicious activities that do not classify as such but are considered unfriendly acts.[166] The EU toolbox includes various countermeasures in areas such as diplomatic, political, military, economic, and strategic communication. Countermeasures based on the Framework on a Coordinated EU Response to hybrid threats can encompass measures falling within the foreign, security, and defence policy, such as (1) preventive measures, including capacity and confidence building measures; (2) cooperative measures, (3) stability building measures, including public diplomacy and diplomatic engagement with the involved state actor; (4) restrictive measures (sanctions); and (5) measures to support Member States, upon their request, which choose to exercise their inherent right of individual or collective self-defence as recognised in Article 51 UN Charter.[167] Category 5 refers to collective defence under the mutual assistance clause in Article 42 para. 7 TEU[168] and the solidarity clause under Article 222 TFEU.[169]

The solidarity clause, laid down in Article 222 TFEU, provides that the EU and its Member States can act jointly in a spirit of solidarity if a Member State is the object of "a terrorist attack" or victim of a "natural or man-made disaster".[170] Article 222 TFEU allows for an EU action as well as direct assistance by one or several Member States to a targeted Member State.[171] EU action under Article 222 para. 1 TFEU is implemented

164 Ibid.

165 Ibid., para. 14.

166 Ibid.

167 Ibid., paras. 14–15. The objective of measures within foreign, security, and defence policy are to strengthen prevention, encourage cooperation, facilitate the mitigation of immediate and long-term threats, and influence the behaviour of potential aggressors in the long term.

168 *Treaty on European Union of 13 December 2007* – consolidated version, Official Journal of the European Union C/202 of 7 June 2016.

169 *Treaty on the Functioning of the European Union of 13 December 2007* – consolidated version, Official Journal of the European Union C/202 of 7 June 2016.

170 Both terms are defined in Article 3 of Council Decision 2014/415/EU. A "terrorist attack" means a terrorist offence as defined in Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism, while "disaster" means any situation that has or may have a severe impact on people, the environment, or property, including the cultural heritage.

171 The solidarity clause was introduced by the Treaty of Lisbon as a political response to different terrorist attacks, such as those in New York in 2001 and Madrid in 2004, as well as to natural disasters such as the floods in Central Europe in 2002. The location of Article 222 TFEU in Part V TFEU concerning the external action by the EU underlines that the sources of these threats are, at least in part, seen to be outside the EU, even though the events dealt with in Article 222 TFUE occur on the territory of the Member States and not externally; see: Erlbacher, 2019, p. 1691.

by applying Council Decision 2014/415/EU,[172] which sets out the conditions of invocation of the solidarity clause and the available means of reaction. The solidarity clause is designed as a subsidiary tool of last resort, as the affected Member States may invoke it only if they consider that the crisis clearly overwhelms the response capabilities available to them, after having exploited the possibilities offered by existing means and tools at the national and EU levels.[173] The affected Member State addresses the invocation of Article 222 TFUE to the Presidency of the Council of the EU. The European Commission and EU High Representative identify the relevant EU instruments that can best contribute to the response to the crisis. In their respective areas of competence, they are both responsible for taking all the necessary measures provided under those instruments, identifying military capabilities with the support of the EU Military Staff, identifying and proposing the use of instruments and resources falling within the remit of EU agencies, and producing regular integrated situational awareness and analysis reports.[174] Invocation of the solidarity clause triggers coordination at the Council of the EU level (Integrated Political Crisis Response arrangements).[175] Application of the solidarity clause under Article 222 para. 1 TFEU stems from the EU's general obligation of solidarity towards its Member States, expressed as the obligation to mobilise all instruments at its disposal, including the military resources made available by the Member States, to assist a Member State at the request of its political authorities in the event of a terrorist attack, to protect democratic institutions and the civilian population from any terrorist attack, and to prevent the terrorist threat in the territory of the Member States. In situations involving direct assistance by one or several Member States to a Member State under Article 222 para. 2 TFUE, Council Decision 2014/415/EU does not apply. The obligation of mutual assistance between Member States is expressed in a less extensive manner than the solidarity obligation incumbent on the EU towards its Member States. Each Member State has the sovereign right to choose the most appropriate means to comply with its own solidarity obligation towards the affected Member State.[176]

If a hybrid attack includes an armed aggression, it can trigger the invocation of the mutual assistance clause (also referred to as the mutual defence clause) set forth in Article 42 para. 7 TEU. It guarantees that

> If a Member State is the victim of *armed aggression* on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the United Nations Charter. (emphasis added)

172 Council Decision 2014/415/EU of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause, Official Journal of the European Union, 1 July 2014, L 192/53.
173 Article 4 para. 1 of Council Decision 2014/415/EU.
174 Article 5 para. 2 of Council Decision 2014/415/EU.
175 Joint Framework on countering hybrid threats, p. 16.
176 Declaration No. 37 on Article 222 of the Treaty on the Functioning of the European Union, Official Journal of the European Union, 7 June 2016, C 202/349.

Article 42 para. 7 TEU imposes a legally binding obligation on Member States to provide 'aid and assistance by all the means in their power' to a Member State that is the victim of armed aggression in its territory. However, the exact nature of aid and means of assistance can be determined by each Member State differently. Article 42 para. 7 TEU does not require Member States to take military action; military assistance remains only one possible means of aid.

Unlike the solidarity clause under Article 222 TFEU, the mutual assistance clause foresees Member States' action only, providing for a direct country-to-country support, without a previously determined procedure of implementation that needs to be followed. Member States implement the mutual assistance clause bilaterally with the Member State invoking it, which, at least in theory, allows for a prompter, more flexible, and tailored response.[177] Any cooperation between the Member States under Article 42 para. 7 TEU should respect the specific character of the Member States' security and defence policy and comply with the commitments under the NATO, which remains the foundation of its member states' collective defence and the forum for its implementation.[178] As Ramopoulos notes, insertion of Article 42 para. 7 TUE in the text of the Treaties does not transform the EU into a defence or military alliance but instead conveys a strong political message.[179]

The key question from the point of view of legal assessment of hybrid threats and warfare from the perspective of EU law is whether and when hybrid operations can be classified as an armed aggression under Article 42 para. 7 TEU or a terrorist attack or man-made disaster under Article 222 TFEU to enable a collective response. EU policy papers confirm that "multiple serious hybrid threats" can amount to armed aggression and thus fall within the ambit of Article 42 para. 7 TEU.[180] However, it is believed that the solidarity clause is more likely to be used in the case of hybrid attacks that combine criminal and subversive actions without military means.[181] The Council of the EU has recognised that while the use of military force can be an integral component of some state actors' hybrid tactics, they might also use hybrid tactics as a substitute for armed aggression.[182]

177 Ramopoulos, 2019, p. 282; see also Nováky, 2017.

178 Council conclusions of a Framework for a coordinated EU response to hybrid campaigns, para. 15.

179 Ramopoulos, 2019, p. 282.

180 *Joint Framework on countering hybrid threats*, p. 16. For a recent study on the applicability of Article 42 para. 7 in response to hybrid threats, see: Deen, Zandee and Stoetman, 2022.

181 European Commission and The High Representative of the Union for Foreign Affairs and Security Policy, *Joint Report to the European Parliament and the Council on the implementation of the Joint Framework on countering hybrid threats – European Union response*, Brussels, 19 July 2017, JOIN(2017) 30 final, p. 16. The practice shows that states might be more willing to invoke Article 42 para. 7 TEU than Article 222 TFEU, even when the underlying crisis is not of a military nature, due to the more flexible and less regulated framework of mutual assistance compared to the solidarity clause, which does not entail handing over of political coordination to the Council Presidency, as in the procedure of Article 222 para. 1 TFEU. Nevertheless, any definite conclusions cannot be well-founded, as Article 42 para. 7 TEU has so far been invoked only once, by France in 2015, following the terrorist attacks in Paris. For more, see Bakker et al., 2016, pp. 22–29.

182 Council conclusions of a Framework for a coordinated EU response to hybrid campaigns, para. 16.

The 2016 *Joint Framework on Countering Hybrid Threats* has called on the European Commission and EU High Representative to examine the applicability and practical implications of Article 222 TFEU and Article 42 para 7 TEU in case a wide-ranging and serious hybrid attack occurs, but such an assessment has not been accomplished yet. A clearer specification of the thresholds for and consequences of invoking either clause in the event of a hybrid threat could significantly enhance the EU's ability to promptly counteract hybrid hostilities in line with the common operational protocol. Although embarking on negations on purely hypothetical thresholds would be counterproductive, creating a common frame of reference among EU Member States through regular simulations and joint exercises could prevent situations where some states could question the legitimacy of the invocation and subsequently refrain from rendering meaningful assistance.[183]

So far, the Member States' practice does not provide any examples of invoking either the mutual assistance or solidarity clause to counter hybrid threats. The artificially engineered migration surge on the Poland-Belarus, Lithuania-Belarus, and Latva-Belarus borders in 2021, identified by EU officials as hybrid attacks, was dealt with by the affected countries without resorting to either Article 42 para. 7 TEU or Article 222 TFEU. The three targeted countries successfully managed the hybrid attacks with domestic crisis regulations on public emergency,[184] and they were supported by the EU's restrictive measures imposed on Belarus. So far, it has been argued that the EU's response to hybrid threats and warfare remains overly circumspect, as the EU is deferring, on the one hand, to national governments to protect themselves and to NATO on the other.[185]

5. Conclusions

In 1952, Hersch Lauterpacht famously wrote that 'if international law is, in some ways, at the vanishing point of law, the law of war is, perhaps even more conspicuously, at the vanishing point of international law'.[186] If the law of war is already at the vanishing point of international law, the emergence of hybrid threats and warfare has pushed it even further into the abyss, for which military and legal scholars have coined the term "grey zone." Waging war with a hybrid arsenal makes contemporary conflicts an alternative example of the Schrödinger's cat paradox, which pins down the dilemma wherein war exists and at the same time it does not. One may argue

183 Deen, Zandee and Stoetman, 2022, p. 22.
184 For an extensive study of the domestic regulations on the public emergency regime in these states, which enabled an effective response to hybrid threats, see: Nagy and Horváth, 2020.
185 Tallis and Šimečka, 2017, pp. 21–22.
186 Lauterpacht, 1952, p. 382.

that unlike the paradox in Schrödinger's quantum experiment, this contradiction can be easily resolved by distinguishing war in the material sense, meaning factual hostilities between states (*de facto* combat), and war in the technical sense, which denotes the normative condition of the state of war (*de jure* state of war).[187] However, the hybrid incidents the world has witnessed in the last two decades, as well as the legal and military debate surrounding them, clearly show that the legal and political assessment of hybrid conflicts is far from that easy.

When assessed in relation to the prohibition of the threat and use of force (Article 2 para. 4 UN Charter) and the right to self-defence (Article 51 UN Charter), hybrid campaigns highlight several specific challenges that the use of unconventional contemporary warfare poses to the international system of war prevention. Prohibition of the use of force under Article 2 para. 4 UN Charter refers to armed force; therefore, classifying hybrid campaigns that do not involve violent military acts as illegal use of force is contrary to the prevailing interpretation of Article 2 para. 4 UN Charter, although some consideration has recently been given to the weapon-like destructive potential of cyberattacks. The threshold for an armed attack enabling the right to self-defence under Article 51 UN Charter is higher than that required to consider hostilities as illegal use of force under Article 2 para. 4 UN Charter; therefore, it is even more difficult to conclude that the use of hybrid threats and warfare would trigger the right to self-defence. Hybrid adversaries deliberately act at such a level of intensity that normally does not allow the targeted state to use forcible measures in self-defence. In the aftermath of the 2014 Russian hybrid operation in Ukraine, the NATO declared that hybrid operations could reach the level of armed attack that could lead to the invocation of Article 5 NATO Treaty. However, it is not clear whether such operations would require any violent acts by hybrid adversaries to trigger the NATO's collective defence mechanism. Otherwise, states targeted with hybrid threat or warfare below the threshold of an armed attack are limited in their response to non-forcible countermeasures and peacetime regulations.

The nature of hybrid conflicts, which combine kinetic and non-kinetic means of warfare, makes it difficult to determine whether the use of hybrid threats and warfare qualifies as an armed conflict that activates the application of IHL, and if yes, whether it triggers the IHL regime for an international or non-international armed conflict. The 1949 Geneva Conventions were drafted at a time when kinetic warfare prevailed, and currently there is no legal basis to establish that hybrid conflicts, which do not involve violent actions, trigger the application of the 1949 Geneva Conventions. Nevertheless, the ICRC has recently begun considering the technological advancements and impact of cyber-capabilities for the applicability of humanitarian law. The experience of the 2014 hybrid conflict between Russia and Ukraine shows that the threshold enabling the application of the IHL for an international armed conflict can easily be averted. The international community's reluctance to declare the existence of an international armed conflict, entailing the risk

187 Dinstein, 2011, pp. 9–10; Greenwood, 1987, p. 283; Lauterpacht, 1968, p. 65.

of escalating violence and possibly activating collective self-defence, can successfully be exploited by hybrid adversaries by using hybrid threats and warfare, such as the use of unmarked forces and the denial policy.

When countering hybrid threats and warfare, states are bound to respect human rights law. The relevant legal regime regulating restrictions on and derogations from human rights obligations is anchored in both the international human rights law and the IHL, and it needs to be assessed individually on a case-by-case basis. Hybrid campaigns can prompt different consequences depending on whether they occur (1) in times of armed conflict, (2) in times of public emergency other than armed conflict, or (3) in peacetime when no armed conflict or public emergency exists. In times of war or other public emergencies threatening the life of the nation, states may derogate from their human rights obligations pursuant to Article 15 ECHR. During armed conflict, the ECHR enables the most far-reaching derogation of human rights, even from the otherwise non-derogable right to life set forth in Article 2 ECHR. In times of public emergencies other than armed conflict, states can derogate from certain human rights obligations, although not from Article 2 ECHR. Hybrid threats or warfare below the threshold of an armed conflict can become a valid ground for derogation from the ECHR regime if the triggering public emergency involves an actual or imminent threat to the existence of the nation and when the normal restrictions permitted by the ECHR for the interests of national security are inadequate. Hybrid hostilities that do not amount to armed conflict or a public emergency threating the life of the nation cannot legitimise any derogations from the human rights obligations under the ECHR. Any response to hybrid threats and warfare entailing restrictions on the enjoyment of individual human rights and freedoms need to be prescribed by law, must pursue a legitimate aim (e.g. interests of national security), and should be necessary in a democratic society. Countering hybrid threats and warfare under the international human rights law paradigm highlights that the main challenge is balancing the interests of national security and state sovereignty with the enjoyment of individual human rights, such as the right to privacy.

In the EU domain, hybrid threats and campaigns can trigger various measures envisaged in the EU treaties and policies, primarily in the area of foreign, security, and defence policies, including the collective response under Article 42 para. 7 TEU (mutual assistance) and Article 222 TFEU (obligation of solidarity). Such measures should be decided on a case-by-case basis; comply with both the international law and the EU's strategic interests; and ultimately be well-calibrated and proportionate to the scope, scale, duration, intensity, complexity, sophistication, and impact of each hybrid campaign. It requires optimal situational awareness, often lacking in cases of a concerted hybrid threat or campaign. A coordinated response at the EU level can be instigated against malicious hybrid activities that constitute internationally wrongful acts and against those that are merely considered unfriendly acts. The attribution of responsibility for hybrid activities to a particular state or non-state actor is not a precondition for the implementation of countermeasures at the EU level; nevertheless, some measures (e.g. sanctions) can only be targeted. Compared

to the international legal framework, the framework of the EU (compared to NATO) "theoretically" offers wider possibilities for a collective response to hybrid threats and campaigns by enabling the invocation of the mutual solidarity clause (Article 222 TFEU) in situations that otherwise could not trigger the collective defence mechanism under Article 5 NATO Treaty. Nevertheless, the possible application of Article 222 TFEU or Article 42 para. 7 TEU (mutual defence clause) to hybrid attacks has not yet been assessed or implemented in practice.

The analysis in this chapter demonstrates that it is hardly possible to generally and unequivocally conclude whether the use of hybrid threats and warfare leads to *de facto* combat that amounts to the use of force, and whether it triggers legal consequences attached to the existence of armed conflict, especially if the hybrid campaign does not involve the use of kinetic force. Balancing between war and peace, hybrid warfare could indeed substitute for Schrödinger's cat. It aptly highlights how the international community and international legal order thrives on the traditional dichotomy between war and peace – a dichotomy that is hardly compatible with the realities of international relations and works in favour of hybrid aggressors.[188] Facilitating the application of existing international standards to hybrid threats and warfare through a clearer interpretation of the relevant thresholds and legal consequences would amount to effective "lawmunition", translating into better preparedness and resilience. However, in the author's opinion, any interpretation or re-interpretation of the existing international standards, albeit necessary, should be guided by the spirit of the UN Charter, which seeks to protect our children and grandchildren from the scourge of war.[189]

188 George F. Kennan, 1948, para. 1, expressed that concern already in 1948:
We have been handicapped however by a popular attachment to the concept of a basic difference between peace and war, by a tendency to view war as a sort of sporting context outside of all political context, by a national tendency to seek for a political cure-all, and by a reluctance to recognize the realities of international relations – the perpetual rhythm of struggle, in and out of war.

189 Teleological interpretation is an imperative that stems from the interpretation guidelines contained in Article 31 para. 1 of the *Vienna Convention on the Law of Treaties*, adopted in Vienna on 23 May 1969, UN Treaty Series vol. 1155, Reg. no. 18232.

References

Arthur, J.E. (2020) 'Russian Cyber Campaigns in Support of Military Operations', *American Intelligence Journal*, 37(1), pp. 49–53.

Aukia, J., Kubica, L. (2023) 'Russia and China as hybrid threat actors: The shared self-other dynamics', *Hybrid CoE Research Reports*, *The European Centre of Excellence for Countering Hybrid Threats*, March 2023. [Online]. Available at: https://www.hybridcoe.fi/wp-content/uploads/2023/04/NEW_Hybrid_CoE_Research_Report_8_web.pdf (Accessed: 31 January 2024).

Bakker, A., Biscop, S., Drent, M., Landman, L. (2016) *Spearheading European Defence. Employing the Lisbon Treaty for a Stronger CSDP.* The Hague: Netherlands Institute of International Relations Clingendael.

Bekić, J. (2022) 'Coercive Engineered Migrations as a Tool of Hybrid Warfare', *Croatian Political Science Review*, 59(2), pp. 141–169; https://doi.org/10.20901/pm.59.2.06.

Bendiek, A., Schulze, M. (2021) *Attribution – a Major Challenge for EU Cyber Actions. An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW.* Berlin: German Institute for International and Security Affairs; https://doi.org/10.18449/2021RP11.

Bingle, M. (2023) 'What is Information Warfare?', *The Henry M. Jackson School of International Studies, University of Washington*, 25 September 2023. [Online]. Available at: https://jsis.washington.edu/news/what-is-information-warfare (Accessed: 31 January 2024).

Blake-Martin, D. (2023) 'Interview – Kelly Greenhill', *E-International Relations*, 5 February 2023. [Online]. Available at: https://www.e-ir.info/2023/02/05/interview-kelly-greenhill (Accessed: 31 January 2024).

van den Bosch, B. (2021) 'Fighting a war without violence. The rules of International Humanitarian Law for military cyber-operations below the threshold of 'attack'' in Johnson, R., Kitzen, M., Sweijs, T. (eds.) *The Conduct of War in the 21st Century: Kinetic, Connected and Synthetic*. London: Routledge, pp. 211–222; https://doi.org/10.4324/9781003054269-19.

CAHDI (2018) 'Opinion of the CAHDI: On Recommendation 2130 (2018) of the Parliamentary Assembly of the Council of Europe – "Legal Challenges Related to Hybrid War and Human Rights Obligations"', *Council of Europe*, 2018. [Online]. Available at: https://rm.coe.int/opinion-of-the-cahdi-on-recommendation-2130-2018-of-the-parliamentary-/1680907884 (Accessed: 31 January 2024).

Cassese, A. (2008) 'Current Trends in the Development of the Law of Armed Conflict' in Gaeta, P., Zappalà, S. (eds.) *The Human Dimension of International Law: Selected Papers*. New York: Oxford Academic Press, pp. 4–38; https://doi.org/10.1093/acprof:oso/9780199232918.003.0001.

Clarke, M. (2019) 'China's Application of the 'Three Warfares' in the South China Sea and Xinjiang', *Orbis*, 63(2), pp. 187–208; https://doi.org/10.1016/j.orbis.2019.02.007.

Cochran, E.S. (2020) 'China's "Three Warfares": People's Liberation Army Influence Operations', *International Bulletin of Political Psychology*, 20(3), pp. 1–24.

Committee on Legal Affairs and Human Rights (2018) 'Legal Challenges Related to Hybrid War and Human Rights Obligations', *Parliamentary Assembly of the Council of Europe*, 6 April. [Online]. Available at: https://pace.coe.int/en/files/24547 (Accessed: 31 January 2024).

Council of Europe (2022) 'Legal Analysis of the Derogation Made by Ukraine under Article 15 of the European Convention of Human Rights and Article 4 of the International Covenant on Civil and Political Rights', *Council of Europe*, November 2022. [Online]. Available at: https://rm.coe.int/legal-analysis-of-the-derogation-made-by-ukraine-under-article-15-of-t/1680aa8e2c (Accessed: 31 January 2024).

Council of the EU (2021a) 'Belarus: EU Adopts 5th Package of Sanctions Over Continued Human Rights Abuses and the Instrumentalisation of Migrants', *Council of the EU and the European Council*, 2 December. [Online]. Available at: https://www.consilium.europa.eu/en/press/press-releases/2021/12/02/belarus-eu-adopts-5th-package-of-sanctions-over-continued-human-rights-abuses-and-the-instrumentalisation-of-migrants/ (Accessed: 31 January 2024).

Council of the EU (2021b) 'Belarus: EU Broadens Scope for Sanctions to Tackle Hybrid Attacks and Instrumentalisation of Migrants', *Council of the EU and the European Council*, 15 November. [Online]. Available at: https://www.consilium.europa.eu/en/press/press-releases/2021/11/15/belarus-eu-broadens-scope-for-sanctions-to-tackle-hybrid-attacks-and-instrumentalisation-of-migrants/ (Accessed: 31 January 2024).

Deen, B., Zandee, D., Stoetman, A. (2022) *Uncharted and uncomfortable in European defence. The EU's mutual assistance clause of Article 42(7).* The Hague: Netherlands Institute of International Relations Clingendael.

Dinstein, Y. (2011) *War, aggression, and self-defence*. 5th edn. Cambridge: Cambridge University Press; https://doi.org/10.1017/CBO9780511920622.

Dörr, O., Randelzhofer, A. (2015) 'Article 2(4)' in Simma, B., Khan D.-E., Nolte, G., Paulus A., Wessendorf, N. (eds.) *The Charter of the United Nations: A Commentary, Volume I*. 3rd edn. Oxford: Oxford University Press.

Dunlap, C.J. (2001) 'Law and Military Interventions: Preserving Humanitarian Values in 21st Conflicts' presented at *Humanitarian Challenges in Military Interventions Conference* (29 November 2001). [Online]. Available at: https://scholarship.law.duke.edu/faculty_scholarship/3500/ (Accessed: 31 January 2024).

Dunlap, C.J. (2008) 'Lawfare Today: A Perspective', *Yale Journal of International Affairs*, Winter 2008, pp. 146–154.

Erlbacher, F. (2019) 'Article 222' in Kellerbauer, M., Klamert, M., Tomkin, J. (eds.) *The EU Treaties and the Charter of Fundamental Rights. A Commentary.* 1st edn. Oxford: Oxford University Press, pp. 1690–1696.

European Commission (2021a) '2021 State of the Union Address by President von der Leyen', *European Commission*, 15 September. [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701 (Accessed: 31 January 2024).

European Commission (2021b) 'Von der Leyen on Belarus: The EU Has the Will, the Unity and the Resolve to Face This Crisis', *European Commission*, 23 November. [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/AC_21_6254 (Accessed: 31 January 2024).

European Council (2014) 'Statement of the Heads of State or Government on Ukraine', *Council of the EU and the European Council*, 6 March. [Online]. Available at: https://www.consilium.europa.eu/media/29285/141372.pdf (Accessed: 31 January 2024).

European Council (2021) 'Remarks by President Charles Michel After His Meeting with the Prime Minister of Poland, Mateusz Morawiecki, in Warsaw' *Council of the EU and the European Council*, 10 November. [Online]. Available at: https://www.consilium.europa.eu/en/press/press-releases/2021/11/10/intervention-du-president-charles-michel-a-l-issue-de-sa-rencontre-avec-le-premier-ministre-polonais-mateusz-morawiecki-a-varsovie (Accessed: 31 January 2024).

Federation Council of the Federal Assembly of the Russian Federation (2019) 'Statement of the Federation Council of the Federal Assembly of the Russian Federation', *Federation Council*, 10 April. [Online]. Available at: http://council.gov.ru/en/activity/docs/en/104357/ (Accessed: 31 January 2024).

Fogt, M.M. (2020) 'Legal Challenges or 'Gaps' by Countering Hybrid Warfare: Building Resilience in Jus ante Bellum', *Southwestern Journal of International Law*, 27(1), pp. 28–100.

Franke, U. (2015) *War by non-military means. Understanding Russian information warfare*, Stockholm: Försvarsdepartementet.

Giannopoulos, G., Smith, H., Theocharidou, M. (2021) *The Landscape of Hybrid Threats: A conceptual model*. Luxembourg: Publications Office of the European Union; https://doi.org/10.2760/44985.

Greenhill, K.M. (2010) 'Weapons of Mass Migration: Forced Displacement as an Instrument of Coercion', *Strategic Insights*, 9(1), pp. 116–160.

Greenwood, C. (1987) 'The concept of war in modern international law', *International and Comparative Law Quarterly*, 36(2), pp. 283–306.

Hathaway, O.A. (2014) 'Fighting The Last War: The United Nations Charter In The Age Of The War On Terror' in Shapiro, I., Lampert, J. (eds.) *Charter of the United Nations: Together with Scholarly Commentaries and Essential Historical Documents*. New Haven: Yale University Press, pp. 210–224; https://doi.org/10.12987/9780300182538-011.

Heap, B. (ed.) (2021) *Strategic Communications Hybrid Threats Toolkit. Applying the principles of NATO Strategic Communications to understand and counter grey zone threats*. Riga: NATO Strategic Communications Centre of Excellence.

Hoffman, F.G. (2007) *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Studies.

Huttunen, J. (2024) 'Countering Instrumentalised Migration: The case for Border Closure Through a Derogation under the ECHR', *EJIL:Talk! Blog of the European Journal of International Law*, 2 January 2024. [Online]. Available at: https://www.ejiltalk.org/countering-instrumentalised-migration-the-case-for-border-closure-through-a-derogation-under-the-echr/ (Accessed: 31 January 2024).

International Committee of the Red Cross (2004) *What is International Humanitarian Law. Legal factsheet.* [Online]. Available at: https://www.icrc.org/en/download/file/240610/what_is_ihl.pdf (Accessed: 31 January 2024).

International Committee of the Red Cross (2016) *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*. 2nd edn. Cambridge: Cambridge University Press. [Online]. Available at: https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949/article-2/commentary/2016 (Accessed: 31 January 2024).

Ionita, C.-C. (2023) 'Conventional and hybrid actions in the Russia's invasion of Ukraine', *Security and Defence Quarterly*, 44(4), pp. 5–20; https://doi.org/10.35467/sdq/168870.

Johnson, R. (2021) 'Hybrid Warfare and Counter-Coercion' in Johnson, R., Kitzen, M., Sweijs, T. (eds.) *The Conduct of War in the 21st Century: Kinetic, Connected and Synthetic*. London: Routledge, pp. 45–57; https://doi.org/10.4324/9781003054269-5.

Johnson, D. (2015) 'Russia's Approach to Conflict – Implications for NATO's Deterrence and Defence', *Research Division-NATO Defense College Rome*, 2015/111, pp. 1–12.
Jordan, T.P. (2016) 'The Law of Armed Conflict, Unconventional Warfare, and Cyber Attacks', *American University National Security Law Brief*, 6(2), pp. 37–58.
Kania, E. (2016) 'The PLA's Latest Strategic Thinking on the Three Warfares', *China Brief Volume*, 16(13). [Online]. Available at: https://jamestown.org/program/the-plas-latest-strategic-thinking-on-the-three-warfares/ (Accessed: 31 January 2024).
Karski, K., Mielniczek, P. (2019) 'The notion of hybrid warfare in international law and its importance for NATO', *NATO Legal Gazette,* 2019/39, pp. 67–80.
Kennan, G.F. (1948) '269. Policy Planning Staff Memorandum', *Office of the Historian*, 4 May 1948. [Online]. Available at: https://history.state.gov/historicaldocuments/frus1945-50Intel/d269 (Accessed: 31 January 2024).
Kittrie, O.F. (2016) *Lawfare: Law as a Weapon of War.* Oxford: Oxford University Press; https://doi.org/10.1093/acprof:oso/9780190263577.001.0001.
Kowalczewska, K. (2014) 'Lawfare: inter arma… leges arma?', *Międzynarodowe Prawo Humanitarne*, 2014/5, pp. 38–53.
The Kremlin, Moscow (2014) 'Address by President of the Russian Federation', *President of Russia*, 18 March. [Online]. Available at: http://en.kremlin.ru/events/president/news/20603 (Accessed: 31 January 2024).
Lasconjarias, G., Larsen, J.A. (eds.) (2015) *NATO'S Response to Hybrid Threats*. 1st edn. Rome: NATO Defense College.
Lauterpacht, H. (1952) 'The problem of the revision of the law of war', *British Yearbook of International Law*, 1952/29, pp. 360–382.
Lauterpacht, E. (1968) 'The Legal Irrelevance of the State of War', *American Society of International Law Proceedings*, 1968/62, pp. 58–67; https://doi.org/10.1017/S0272503700014919.
Lesaffer, R. (2015) 'Too Much History: From War as Sanction to the Sanctioning of War' in Weller, M. (ed.) *The Oxford Handbook of the Use of Force in International Law.* 1st edn. Oxford: Oxford University Press, pp. 35–55; https://doi.org/10.1093/law/9780199673049.003.0002.
Lott, A. (2022) *Hybrid Threats and the Law of the Sea. Use of Force and Discriminatory Navigational Restrictions in Straits*. 1st edn. Leiden: Brill-Nijhof, pp. 16–36; https://doi.org/10.1163/9789004509368_004.
Łubiński, P. (2021) 'Hybrid Warfare or Hybrid Threat – The Weaponization of Migration as an Example of the Use of Lawfare – Case Study of Poland', *Polish Political Science Yearbook*, 2021/51, pp. 1–13; https://doi.org/10.15804/ppsy202209.
Medina Llinàs, M. (2022) 'Hybrid attacks on critical infrastructure' in Bargués, P., Bourekba, M., Colomina, C. (eds.) *Hybrid threats, vulnerable order.* Barcelona: Barcelona Centre for International Affairs.
Mik, C. (2022) 'Russia's Aggression against Ukraine: a Clash of Two Visions of the International Community and International Law', *Polish Review of International and European Law*, 12(2), pp. 57–113; https://doi.org/10.21697/2022.12.2.5.
Martin, M. (2021) 'China's Three Information Warfares', *Proceedings*, vol. 147/3/1,417, March 2021. [Online]. Available at: https://www.usni.org/magazines/proceedings/2021/march/chinas-three-information-warfares (Accessed: 31 January 2024).

Mansoor, P.R. (2012) 'Hybrid Warfare in History' in Murray, W., Mansoor, P.R. (eds.) *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*. New York: Cambridge University Press.

Mauer, P. (2023) 'Strategies for Reconciling International Humanitarian Law and Cyber Operations: A Q&A with Dr. Peter Maurer', *Digital Front Lines*. [Online]. Available at: https://digitalfrontlines.io/2023/07/11/strategies-for-reconciling-international-humanitarian-law-and-cyber-operations/ (Accessed: 31 January 2024).

Moussa, J. (2008) 'Can jus ad bellum override jus in bello? Reaffirming the separation of the two bodies of law', *International Review of the Red Cross*, 90(872), pp. 963–990; https://doi.org/10.1017/S181638310900023X.

Munoz Mosquera, A.B., Bachmann, S.D. (2015) 'Lawfare and hybrid warfare – how Russia is using the law as a weapon', *Amicus Curiae*, 2015/102, pp. 25–28; https://doi.org/10.14296/ac.v2015i102.2433.

Munoz Mosquera, A.B., Bachmann, S.D. (2016) 'Lawfare in Hybrid Wars: The 21st Century Warfare', *Journal of International Humanitarian Legal Studies*, 7(1), pp. 63–87; https://doi.org/10.1163/18781527-00701008.

NATO (2013) *Allied Command Operations Comprehensive Operations Planning Directive Interim Version 2.0 (COPD V 2.0)*. Brussels: NATO Unclassified.

NATO (2015) 'Keynote Speech by NATO Secretary General Jens Stoltenberg at the Opening of the NATO Transformation Seminar', *NATO*, 25 March. [Online] Available at: https://www.nato.int/cps/en/natohq/opinions_118435.htm (Accessed: 31 January 2024).

NATO (2016) 'Warsaw Summit Communiqué', *NATO*, 9 July. [Online]. Available at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm (Accessed: 31 January 2024).

NATO (2022) 'NATO 2022 Strategic Concept: Adopted by Heads of State and Government at the NATO Summit in Madrid 29 June 2022', *NATO*, 29 June. [Online]. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf (Accessed: 31 January 2024).

Najžer, B. (2020) *The Hybrid Age: International Security in the Era of Hybrid Warfare*. 1st edn. London: I. B. Tauris; https://doi.org/10.5040/9780755602544.

Nagy, Z., Horváth, A. (eds.) (2022) *Emergency Powers in Central and Eastern Europe: From Martial Law to COVID-19*. 1st edn. Budapest-Miskolc: Ferenc Mádl Institute of Comparative Law, Central European Academic Publishing; https://doi.org/10.47079/2022.znah.epicaee.1.

Nováky, N.I.M. (2017) 'The Invocation of the European Union's Mutual Assistance Clause: A Call for Enforced Solidarity', *European Foreign Affairs Review*, 22(3), pp. 357–375; https://doi.org/10.54648/eerr2017030.

Parulski, K. (2016) 'Legal Aspects of Hybrid Warfare in Ukraine', *Zeszyty Naukowe AON*, 4 (105), pp. 5–27.

President of Russia (2014) 'Direct Line with Vladimir Putin', *President of Russia*, 17 April 2014. [Online]. Available at: http://en.kremlin.ru/events/president/news/20796 (Accessed: 31 January 2024).

Ramopoulos, T. (2019) 'Article 42 TEU' in Kellerbauer, M., Klamert, M., Tomkin, J. (eds.) *The EU Treaties and the Charter of Fundamental Rights. A Commentary*. 1st edn. Oxford: Oxford University Press, pp. 277–282.

Sanz Caballero, S. (2023) 'The concepts and laws applicable to hybrid threats, with a special focus on Europe', *Humanities and Social Sciences Communications*, 2023/10, pp. 1–8; https://doi.org/10.1057/s41599-023-01864-y.

Sari, A. (2017) 'Hybrid Warfare, Law and the Fulda Gap', *University of Exeter – Law School*. [Online]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2927773 (Accessed: 31 January 2024).

Sari, A. (2023) 'Instrumentalized migration and the Belarus crisis: Strategies of legal coercion', *Hybrid CoE Paper No. 17, The European Centre of Excellence for Countering Hybrid Threats*, April 2023. [Online]. Available at: https://www.hybridcoe.fi/wp-content/uploads/2023/04/20230425-Hybrid-CoE-Paper-17-Instrumentalized-migration-and-Belarus-WEB.pdf (Accessed: 31 January 2024).

Schabas, W.A. (2015) *The European Convention on Human Rights. A Commentary*. 1st edn. New York: Oxford University Press; https://doi.org/10.1093/law/9780199594061.001.0001.

Schmitt, M.N. (2015) 'The Use of Cyber Force and International Law' in Weller, M. (ed.) *The Oxford Handbook of the Use of Force in International Law*. 1st edn. Oxford: Oxford University Press, pp. 1110–1130; https://doi.org/10.1093/law/9780199673049.003.0053.

Secretariat General (2015) 'JJ7979C Tr./005-185', *Council of Europe*, 10 June. [Online]. Available at: https://rm.coe.int/09000016804896cf (Accessed: 31 January 2024).

Secretariat General (2022) 'JJ9325C Corrigendum Tr./005-287', *Council of Europe*, 2 March. [Online]. Available at: https://rm.coe.int/1680a5b0b0 (Accessed: 31 January 2024).

Soldatenko, M. (2023) 'Constructive Ambiguity of the Budapest Memorandum at 28: Making Sense of the Controversial Agreement', *Lawfare Foreign Relations & International Law*, 7 February 2023. [Online]. Available at: https://www.lawfaremedia.org/article/constructive-ambiguity-of-the-budapest-memorandum-at-28-making-sense-of-the-controversial-agreement (Accessed: 31 January 2024).

Sun Tzu (2010) *The Art of War: timeless military strategy from 6th Century China* (transl. Lionel Giles). Rookhope: Aziloth Books.

Tallis, B., Šimečka, M. (2017) *Collective Defence in the Age of Hybrid Warfare*. Prague: Institute of International Relations. [Online]. Available at: https://www.iir.cz/priloha?page=collective-defence-in-the-age-of-hybrid-warfare&p=1&type=news_cs (Accessed: 31 January 2024).

Veress, C. (2023) 'Kisebbségi jogok felhasználása hibrid hadviselési eszközként' [Using minority rights as a hybrid warfare tool], *Nemzetközi tevékenység*, 2023/1, pp. 29–40; https://doi.org/10.35926/HSZ.2023.1.3.

Voyger, M. (2015) 'Russia's Use of 'Legal' as an Element of its Comprehensive Warfare Strategy', *LandPower Magazine*, 1(2), p. 20.

Wentzell, T.D. (2021) 'Russia's Green Men: The Strategic Storytellers of Hybrid Warfare', *Canadian Military Journal*, 22(1), pp. 42–48.

Wyrozumska, A. (2014) 'The Opinion by the Legal Advisory Committee to the Minister of Foreign Affairs of the Republic of Poland on the Annexation of the Crimean Peninsula to the Russian Federation in Light of International Law', *Polish Yearbook of International Law*, 2014/34, pp. 275–278; https://doi.org/10.7420/pyil2014l.

Yablokov, I. (2022) 'Russian disinformation finds fertile ground in the West', *Nature Human Behaviour*, vol. 6, pp. 766–767; https://doi.org/10.1038/s41562-022-01399-3.

Statement of the Prime Ministers of Poland, Lithuania, Latvia and Estonia on the hybrid attack on our borders by Belarus (2021) gov.pl, 23 August 2021. [Online]. Available at: https://www.gov.pl/web/nato-en/statement-of-the-prime-ministers-of-poland-lithuania-latvia-and-estonia-on-the-hybrid-attack-on-our-borders-by-belarus (Accessed: 31 January 2024).