International Humanitarian Law and Hybrid Warfare

Piotr Łubiński

First published 2025

ISBN: 978-1-032-05717-0 (hbk)
ISBN: 978-1-032-05718-7 (pbk)
ISBN: 978-1-003-19885-7 (ebk)

Chapter 1

Hybrid threats

Below the threshold of hybrid warfare

DOI: 10.4324/9781003198857-2

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

1 Hybrid threats

Below the threshold of hybrid warfare

The primary challenge encountered by the author while writing this book was the frequent and interchangeable use of terms such as "hybrid threats", "hybrid war", and "hybrid warfare" without sufficient clarification.[1] This inconsistency has contributed to conceptual ambiguity and increased uncertainty regarding both the scope of their status and the application of relevant legal frameworks.[2] The author argues that a rigorous analysis of hybrid threats and hybrid warfare enables a nuanced understanding of their interconnectedness – two sides of the same coin, while also allowing for the identification of clear distinctions and thresholds.

These thresholds present another challenge, namely legal qualification. The author's position asserts that hybrid threats encompass a broad spectrum of actions, ranging from matters of international politics and diplomatic tensions to the prohibition of the use of force. In contrast, the means and methods of hybrid warfare span a continuum of actions regulated by the International Humanitarian Law.

This approach enhances the book's contribution to the study – the prime aim of the publication – namely, mapping the phenomenon of hybrid warfare and humanitarian law.

Therefore, the subsequent two chapters will also be interconnected. The aim is to make a clear distinction between hybrid threats and hybrid warfare. This chapter will examine hybrid threats as a distinct concept which, while overlapping with hybrid warfare, remains fundamentally different.

The central argument is that this conceptual confusion affects not only the legal classification of such phenomena but also the political, military, and legal responses to them. While the definitions of these terms continue to evolve, the author aims to demonstrate that, despite their shared doctrinal origins and

1 Weissmann, M. (2021) "*Conceptualizing and countering hybrid threats and hybrid warfare: the role of the military in the grey zone*", in Weissmann, M., Nilsson, N., Palmertz, B., and Thunholm, P. (eds), *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, 1st edn, London: I.B. Tauris, p. 63.

2 Cusumano, E., and Corbe, M. (2018) *A Civil-Military Response to Hybrid Threats*, 1st edn, Cham: Springer Nature, p. 19.

DOI: 10.4324/9781003198857-2

frequent discussion under a common framework, hybrid warfare and hybrid threats are distinct concepts governed by different legal regimes.

The motivation for examining these concepts both jointly and separately stems from their capacity to transcend legal frameworks and generate spill-over effects. This approach is grounded in the recognition that hybrid threats and hybrid warfare share a common foundation and possess the potential to destabilise the international legal order. Their key commonalities include law-fare, influence operations, violations of sovereignty with plausible deniability, and to some extent the erosion of the principle of distinction.

The spill-over effect and transcending legal regimes means that operations, such as, for example, cyber-attacks on Ukraine's banking infrastructure (which fall under the regulation of IHL), may extend beyond national borders due to the interconnected nature of financial systems. As a result, such attacks could impact banking institutions in EU countries, which are governed by different non-IHL international regulations. Similarly, the spill-over effect may apply to the disinformation narratives (in Ukraine IHL, elsewhere in Europe PIL), threats involving the use of nuclear weapons, and the terrorisation of both the civilian population in Ukraine (IHL) and Ukrainians residing abroad, as well as other populations outside the immediate armed conflict zone (PIL).

Together**,** these chapters will clarify the nature of these concepts and establish the threshold at which different legal frameworks apply. The overarching objective is twofold: first, to prove that hybrid threats are a distinct concept, and second, to introduce the threshold for hybrid warfare. Initially, the discussion will trace the joint evolution of the concepts of hybrid threats and hybrid warfare, before ultimately delineating the limits and legal framework of hybrid threats as distinct from its conceptual twin, hybrid warfare. This approach is provided with the understanding that, despite significant efforts to define them, both concepts remain fluid. As the former director of the European Centre of Excellence for Countering Hybrid Threats , Colonel Sönke Marahrens, aptly states, "it is all morphing".[3]

What is a hybrid?

It would be a disservice to the reader not to engage with Glenn's vivid depiction of hybridity. He illustrates this concept through the example of the most well-known hybrid in the animal kingdom, the mule, a cross-breed between a horse and a donkey. According to Glenn, a comprehensive understanding of the mule's capabilities necessitates an examination of the evolutionary development of both horses and donkeys. He argues that this analogy is equally applicable to the notion of hybrid conflicts, suggesting that these conflicts

3 Marahrens, S. "*The Russia-Ukraine conflict from a hybrid warfare perspective*", Defence Horizon Journal, 30 May. Available at: https://tdhj.org/blog/post/russia-ukraine-hybrid-warfare/ [Accessed 3 May 2025].

are best understood through alternative conceptual frameworks that provide greater clarity and insight.[4]

That is supported by a dictionary understanding of the notion. The Oxford English Dictionary provides that hybrid is "The offspring of two animals or plants of different species, or (less strictly) varieties; a half-breed, cross-breed, or mongrel".[5] According to the Merriam-Webster Dictionary, it is "something (such as a power plant, vehicle, or electronic circuit) that has two different types of components performing essentially the same function".[6]

The above definitions align with one of the general definitions of hybrid threats provided by The European Centre of Excellence for Countering Hybrid Threats in Helsinki:

> Hybrid threats are harmful activities that are planned and carried out with malign intent. They aim to undermine a target, such as a state or an institution, through a variety of means, often combined**.** Such means include information manipulation, cyberattacks, economic influence or coercion, covert political manoeuvring, coercive diplomacy, or threats of military force. Hybrid threats describe a wide array of harmful activities with different goals, ranging from influence operations and interference all the way to hybrid warfare.[7]

Even these basic definitions indicate several key observations regarding the nature of hybrid operations:

- different types of components performing essentially the same function.
- operations conducted according to a predefined plan.
- activities carried out with malign intent.
- the use of a variety of means.
- escalation up to the level of hybrid warfare.

Additionally, as the author aims to illustrate the evolution of this concept, reference will be made to an earlier (2019) definition of hybrid operations provided by the same centre, which states the following:

4 Glenn, R.W. 2009. "*Thoughts on hybrid conflict*", Small Wars Journal, p. 8. Available at: https://smallwarsjournal.com/jrnl/art/thoughts-on-hybrid-conflict [Accessed 10 February 2025].

5 Oxford English Dictionary, "*Hybrid, n. & adj.: meanings, etymology and more*", Oxford English Dictionary Online. Available at: https://www.oed.com/dictionary/hybrid_n [Accessed 10 February 2025].

6 Merriam-Webster Dictionary, "*Hybrid*", Merriam-Webster.com Dictionary. Available at: https://www.merriam-webster.com/dictionary/hybrid [Accessed 10 February 2025].

7 Hybrid CoE – The European Centre of Excellence for Countering Hybrid Threats (n.d.) "*Hybrid threats as a concept*", Hybrid CoE Blog. Available at: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ [Accessed 10 February 2025].

- coordinated and synchronised action, that deliberately targets democratic states' and institutions' systemic vulnerabilities, through a wide range of means (political, economic, military, civil and information).
- activities exploit the thresholds of detection and attribution as well as the border between war and peace.
- the aim is to influence different forms of decision-making at the local (regional), state**,** or institutional level to favour and/or gain the agent's strategic goals while undermining and/or hurting the target.[8]

This definition highlights the significance of coordination and synchronisation, as well as the integration of a diverse range of means, including military capabilities, which at that time meant greater incorporation of hybrid warfare means and methods. Regardless of whether the definition applies to a scenario involving military means, several fundamental aspects remain essential:

- coordination and synchronisation across a broad spectrum of means, often in combination (without specifying whether this applies across all domains or only two).
- the involvement of different components performing essentially the same function.

This brief introduction provides the context for a deeper exploration of the key actors and concepts related to hybrid threats within a chronological framework.

What is a threat?

> According to the Oxford Dictionary, a threat is defined as "a statement of an intention to inflict pain, injury, damage, or other hostile action on someone in retribution for something done or not done, such as responses to a threat"; it also categorises a threat as "a person or thing likely to cause damage or danger".[9] Meanwhile, Black's Law Dictionary defines a threat as "a communicated intent to inflict harm or loss on another person or their property", which includes elements of viable delivery and interactivity; it further describes a threat as "an indication of an approaching menace" which can apply to any person or entity likely to cause harm.[10] Both dictionaries indicate that the notion of threat, even in its literal sense, is not exclusively linked to armed conflict or similar acts. From the international perspective, the notion of threat is aligned with two concepts: the threat of use

8 Treverton, G.F., Thvedt, A., Chen, G., Lee, K., and McCue, M. (2020). "*Addressing hybrid threats. Helsinki: Hybrid CoE*", p. 10. Available at: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Treverton-AddressingHybridThreats.pdf [Accessed 10 February 2025].

9 Oxford University Press, Oxford English Dictionary, s.v. "*Threat*". Available at: https://www.oed.com [Accessed 10 February 2025].

10 Garner, B.A. (ed.) (2019) *Black's Law Dictionary*, 11th edn, St. Paul, MN: Thomson Reuters, s.v. "threat".

> of force and threat of the use of a nuclear weapon. The first concept is based on Article 2(4) of the UN Charter, which declares that all states shall refrain, in their international relations, from not only the use of force but also the threat against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the UN.[11] The prohibition of the threat of use of force was established through international consensus, and the international community accepts the prohibition of both the use and the threat.[12] Additionally, the 1969 Vienna Convention on the Law of Treaties states that any treaty obtained through threat or use of force is considered invalid.

The notion of threat is also regulated by the UN Treaty on the Prohibition of Nuclear Weapons, which explicitly prohibits both the use and the threat of use of nuclear weapons at 1 (d).[13] Despite the absence of major nuclear superpowers as signatories, the treaty reinforces the customary international norm prohibiting the threat or use of nuclear weapons. The matter of the use of Legality of the Threat or Use of Nuclear Weapons was also discussed by the ICJ Advisory Opinion.[14]

However, since the notion of threat in the realm of hybrid threats usually lacks specific international law qualifiers, it is difficult to precisely determine its exact meaning. Therefore, the author's position is that a threat consists of elements of international politics, extending to the use of force and acts of aggression. This indicates that hybrid threats may fall within a broad spectrum between the use of force and other forms of coercion to the level of acts which, as Lonardo eloquently put it, "are undesirable and dangerous behaviours by a political rival used to destabilise the adversary".[15]

11 The Organization and its Members, in pursuit of the Purposes stated in Article 1, shall act in accordance with the following Principles. 4) 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 General Assembly (UNGA).

1970 Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, UNGA Res 2625 (XXV), 24 October. United Nations, Charter of the United Nations, 24 October 1945, 1 UNTS XVI. Available at: https://treaties.un.org/doc/Publication/CTC/uncharter-all-lang.pdf, [Accessed 10 February 2025].

12 Kowalski, M., 2015. "*'Ius ad bellum' a systemowy charakter prawa międzynarodowego / 'Ius ad bellum' and the systemic nature of international law*", in Kwiecień, R. (ed.), *Państwo a prawo międzynarodowe jako system prawa / The State and International Law as a Legal System*, Lublin: Wydawnictwo KUL, p. 175–192, p. 176.

13 UN Doc. A/CONF.229/2017/8, UN Doc. CN.476.2017.TREATIES-XXVI-9 https://documents.un.org/doc/undoc/gen/n17/209/73/pdf/n1720973.pdf [Accessed 10 February 2025].

14 International Court of Justice (ICJ) (1996) "*Legality of the threat or use of nuclear weapons*", Advisory Opinion, ICJ Reports 1996, para. 95.

15 Lonardo, L. (2024) "*The seriousness of vagueness: introducing European law and policies against hybrid threats*", in Lonardo, L. (ed.), *Addressing Hybrid Threats: European Law and Policies*, Cheltenham: Edward Elgar Publishing, p. 1–22, p. 7.

Instead of qualifying each and every threat, the author will refer to the most relevant ones provided by the NATO STRATCOM COE. The list covers the following:

1) direct influence of public opinion
   a) establishing, funding, or supporting academic, educational, or cultural institutions.
   b) misinformation, fake news, or disinformation campaigns.
   c) setting up or supporting media and news channels; media ownerships and advertisement campaigns; pressuring journalists.
2) exacerbation of societal division
   a) funding, supporting, or promoting national, religious, or political extremist organisations.
   b) polarisation of political debates to subvert a specific policy program.
   c) exploitation of ethnic or cultural identities to undermine social cohesion.
3) agitation and civil unrest
   a) agitation of targeted societal, cultural, religious, or ethnic groups to call for policy change or initiate protests.
   b) disruption of political or economic processes through protests or boycotts.
   c) risk of radicalisation or violent escalation.
4) interference in elections
   a) foreign interference in elections to influence voting behaviour.
5) decreasing public trust in government
   a) decreasing public trust in government and military; discrediting target government and public institutions.
   b) undermining credibility and legitimacy of policies and operations.
   c) creating public insecurity through bribery, corruption scandals, blackmail, and extortion.
6) undermining governance and state functions
   a) foreign State sponsoring of a political party or actor.
   b) corruption and criminal networks, organised crime.
   c) establishing parallel informal government structures through information, education, and healthcare systems.
7) diplomatic pressure
   a) decrease diplomatic and domestic scope of action of target government through pressure, threat of force, intimidation, or coercion.
   b) discredit government to damage international reputation and relationships with allies.
   c) risk of becoming a platform for proxy conflict; regional instability.
8) economic leverage
   a) economic pressure, dependency on energy or resources, use of sanctions or incentives, disruption of business operations.

b) extraction of valuable resources from disputed territories.
c) marginalisation of local workforce; creating unsafe informal working conditions.
d) exacerbating economic disparities, social inequality, and poverty.

9) cyber operations
   a) disruption of communication flows and digital infrastructure.
   b) cyber-attacks as a statement of intent and capability.
   c) psychological impact on citizens and investors; political embarrassment and public insecurity.
10) terrorism and violent extremism
   a) national, religious, and political extremism.
   b) risk of domestic terrorism; resurgence of former terrorist organisations.
   c) ethnically motivated violence; escalation of socio-political protests; sectarian violence.
11) espionage
   a) financial, physical, security-related, and reputational losses.
   b) corporate, cyber, and political espionage.
12) territorial disputes
   a) regional instability; spill-over effects on other territorial disputes.
   b) strengthened separatist movements.[16]

All these examples provoke certain observations. Firstly, they are predominantly regulated by public international law. With the exception of a few cases, such as terrorism or cyber-attacks, these examples do not primarily relate to armed conflict. However, when escalated, they often reach a level where they exert significant influence not only on international relations but also on the use of force between states. Moreover, they may coexist within the realm of armed conflict, illustrating the spill-over effect of such phenomena.

States' approach to hybridity – the Chinese view

The strategic wisdom of Sun Tzu continues to inform modern doctrines, particularly within Chinese military thought. His assertion that "to subdue the enemy without fighting is the supreme skill"[17] encapsulates a philosophy that underpins contemporary Chinese approaches to hybridity – strategies that increasingly prioritise indirect, non-kinetic methods over conventional force. China plays an important role in the conceptualisation and implementation of hybrid threat strategies, often leveraging political, economic, informational,

16 NATO Strategic Communications Centre of Excellence, "*Strategic Communications Hybrid Threats Toolkit*". Available at: https://stratcomcoe.org/pdfjs/?file=/publications/download/Strategic-Communications-Hybrid-Threats-Toolkit.pdf?zoom=page-fit [Accessed 10 February 2025].

17 Sun Tzu, 1963. *The Art of War*, translated by S.B. Griffith, Oxford: Oxford University Press, ch. 3.

and legal tools in tandem to weaken adversaries without triggering traditional armed conflict. This evolution reflects a fusion of ancient principles with modern operational realities, where the lines between *ius in bello* and *ius ad bellum* are intentionally blurred. Two publications are essential to understanding this paradigm: "Unrestricted Warfare" (UW) by PLA Air Force colonels Qiao Liang and Wang Xiangsui, and the later formalisation of its principles in the "Three Warfares" (TW) doctrine – a cornerstone of China's strategic framework for hybrid operations. Two publications have marked the Chinese approach to hybridity: The first one is "Unrestricted Warfare" published by PLA Air Force colonels Qiao Liang and Wang Xiangsui, and the second one is the so-called "Three Warfares" concept, which develops the authors' findings.

Unrestricted warfare

The sentence, "Otherwise, the immortal bird of warfare will not be able to attain nirvana when it is on the verge of decline"[18] well reflects the unique language and character of the book and includes a reference to a combination of both means and methods of hybridity.[19] Published in 1999, the book appears to provide one of the earliest comprehensive introductions to the concepts of hybrid threats and hybrid warfare as they are understood today.

The work of the Chinese colonels is not an element of an official Chinese doctrine statement, as suggested by its title; rather it indicates a fusion of various types of threats with and without a militarised approach, ultimately advancing the concept of unrestricted warfare. Although the book predominantly presents hybrid threats from the outset, a key point of confusion arises: the blurring of the distinction between non-IHL hybrid threats and IHL-related hybrid warfare. Liang and Xiangsui describe unrestricted warfare as "using all means, including armed or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests".[20]

18 Qiao, L., and Wang, X., 1999. *Unrestricted Warfare*, Beijing: PLA Literature and Arts Publishing House, p. 5. English translation available at: https://www.c4i.org/unrestricted.pdf [Accessed 10 July 2021]. The translation begins with an FBIS Editor's Note and differs in pagination from the original Chinese edition. Initially the book subtitle was understood by many as "*China's Master Plan to Destroy America*", whereas the actual subtitle is "*Two Air Force Senior Colonels on Scenarios for War and the Operational Art in an Era of Globalization*" (p. 5). A very important matter concerns an issue with differing pagination in different translations. I refer to the English translation, found in vast spaces of the internet, available for example at https://www.c4i.org/unrestricted.pdf [Accessed 10 October 2021]. However, references to other translations in various literature provide different page numbers. To avoid any misunderstanding, my copy starts with the FBIS Editor's Note. The following selections are taken from "*Unrestricted Warfare*", a book published in China in February 1999 which proposes tactics for developing countries, in particular China, to compensate for their military inferiority vis-à-vis the US during a high-tech war.

19 Qiao, L., and Wang, X., *Ibidem*, p. 7.

20 Qiao, L., and Wang, X., *op. cit.,* p. 7.

They believe that "all the boundaries lying between the two worlds of war and non-war, of military and non-military, will be totally destroyed, and it also means that many of the current principles of combat will be modified, and even that the rules of war may need to be rewritten".[21]

Despite using militarised concepts, they discuss a number of threats which can be considered prime examples of contemporary hybrid threats: "trade wars, financial wars, and ecological wars as well as psychological warfare (spreading false information to intimidate the enemy and break his will); smuggling warfare (by attacking economic order); media warfare (manipulating public opinion); drug warfare (obtaining sudden and huge illicit profits by spreading disaster in other countries); network warfare; technological warfare (creating monopolies by setting standards independently); fabrication warfare (presenting a counterfeit appearance of real strength before the eyes of the enemy); resources warfare (grabbing riches by plundering stores of resources); economic aid warfare (bestowing favour in the open and contriving to control matters in secret); cultural warfare (leading cultural trends along in order to assimilate those with different views); and international law warfare (seizing the earliest opportunity to set up regulations)".[22] These are clear examples of actions which can be considered exclusively or predominantly as hybrid threats.

Furthermore, the authors emphasise the significance of integrating various forms of what they term "warfare", although their enumeration often includes elements that are not strictly related to warfare, encompassing also hybrid threats and hybrid warfare, namely; "Diplomatic warfare, Financial warfare, Conventional warfare, Network warfare, Trade warfare, Intelligence warfare, Resources warfare, Ecological warfare, Psychological warfare, Economic aid warfare, Space warfare**,** Regulatory warfare, Electronic warfare, Smuggling warfare, Sanction warfare, Drug warfare, Media warfare, Terrorist warfare, Virtual warfare (deterrence), Ideological warfare, Cultural warfare (leading cultural trends along in order to assimilate those with different views) and International Law warfare (seizing the earliest opportunity to set up regulations)".[23] They also make a small contribution toward identifying means and methods which can be applied in warfare: Guerrilla warfare, Tactical warfare, Bio-chemical warfare, Atomic warfare.[24] This enumeration is a fine example of the dominant character of the UW, i.e., dealing with HT yet leaving a gap open for HW. The authors provide the example of Hong Kong as a successfully orchestrated hybrid operation which combines financial warfare + regulatory warfare + psychological warfare + media warfare against financial speculation.[25] They also

21 Qiao, L., and Wang, X., *op. cit.*, p. 7.
22 Qiao, L., and Wang, X., *op. cit.*, p. 55.
23 Qiao, L., and Wang, X., *op. cit.*, p. 146.
24 Qiao, L., and Wang, X., *op. cit.*, p. 146.
25 Qiao, L., and Wang, X., *op. cit.*, p. 147.

quote Yue Fei, the military strategist during the Song Dynasty in China, who is said to have stated that "the subtle excellence of application lies in one-mindedness". This phrasing is nothing else but an underlying of the importance of orchestration and coordination, which is the core of a fully-fledged hybrid operation.

UW analysis results in a number of observations. Firstly, UW equalised military (AC related) methods with non-military ones, which is illustrated clearly by the following citation from UW:

> the boundaries between soldiers and non-soldiers have now been broken down, and the chasm between warfare and non-warfare nearly filled up, globalisation has made all the tough problems interconnected and interlocking, and we must find a key for that. The key should be able to open all the locks, if these locks are on the front door of war. And this key must be suited to all levels and dimensions, from war policy, strategy, and operational techniques to tactics; and it must also fit the hands of individuals, from politicians and generals to the common soldiers.[26]

Secondly, Unrestricted Warfare provides a distinctive perspective on hybrid threats and warfare, integrating both military and non-military strategies to exert pressure on adversaries. This publication introduces a comprehensive fusion of various influence forms, which may lead to the stretching or even violation of both *ius ad bellum* and *ius in bello*. The authors underscore the significance of coordination and orchestration in contemporary hybrid operations, as exemplified by their analysis of the situation in Hong Kong, which renders the publication, despite its title, mostly focused on hybrid threats.

Three warfares (San Zhong Zhanfa) – the hybrid threat perspective

Similar to "Unrestricted Warfare", "Three Warfares" (TW) also provides linguistic and conceptual blurs. The "Three Warfares" concept, officially introduced by the Central Military Commission (CMC)[27] in November 2003, draws inspiration from Sun Tzu's "The Art of War", reflecting the foundational principles of Chinese strategic thinking. It emphasises the importance of subduing the enemy through non-military means, particularly when facing a more powerful adversary. This approach highlights the critical role of political and psychological operations in achieving strategic objectives, extending beyond

26 Qiao, L., and Wang, X., *op. cit.*, p. 222.

27 Clarke, M. (2019) *China's Application of the 'Three Warfares' in the South China Sea and Xinjiang*, Orbis, Volume 63, No. 2, p. 191–208, p. 191. Available at: https://www.fpri.org/article/2019/06/chinas-application-of-the-three-warfares-in-the-south-china-sea-and-xinjiang/ [Accessed 10 July 2024].

traditional military power in shaping the outcomes of future conflicts.[28] Again the name of the concept indicates warfare but, in fact, it is also leaning toward hybrid threats, especially considering China's current lack of military engagement. The TW concept is intended to constitute the basic form of the PLS's soft power developed from previous strategic writings.[29]

The first element of TW is defined as "Psychological warfare conducted in two dimensions: an offensive one against the enemy's society and a defensive one that protects the state's society against the enemy's psychological attack". It is aimed at boosting fighting spirit in one's military and population.[30] Therefore, it resembles the warfare PYSOPS and does fall predominantly into the realm of hybrid warfare.

The second element of the TW is Public Opinion Warfare, which is defined as an operation orientated to generate public support domestically and internationally by transmitting selected information via various media. It aims to seize the political initiative or acquire a military victory. This type of operation is mostly conducted by mass media. Since the rapid development of internet-related media and channels of communication, Public Opinion Warfare aims not only at traditional media, such as newspapers and journals, but predominantly at electronic media. The main methods of public opinion warfare include guidance, control, alteration, suppression, and management[31] of narrative and content. And again, despite the militarised notion of warfare, Public Opinion Warfare could be considered as both HT and HW.

The last element in "Three Warfares" lies in legal warfare, known as lawfare. It is considered a "struggle for legal superiority by mobilising domestic and international laws to gain the political initiative and military victory. Methods of legal warfare include legal deterrence, legal attack, legal counterattack, legal binding, and legal protection".[32]

In conclusion, the "Three Warfares" concept represents the People's Liberation Army's (PLA) soft power strategy. This approach aligns closely with hybrid threats, particularly given China's current absence of direct military engagement. Although militarised in name, the "Three Warfares" concept primarily falls within the spectrum of hybrid threats rather than hybrid warfare, highlighting the multifaceted strategy China employs in modern conflict scenarios.

28 Lee, S. (2014) *China's "Three Warfares": Origins, Applications, and Organizations*, Journal of Strategic Studies, Volume 37, No. 2, p. 198–219, p. 200. Available at: https://www.tandfonline.com/doi/abs/10.1080/01402390.2013.870071 [Accessed 3 May 2025].

29 Sangkuk Lee (2014) *Ibidem*, p. 200.

30 Sangkuk Lee, *Ibidem*, p. 203.

31 Sangkuk Lee, *Ibidem*, p. 203.

32 Sangkuk Lee, *Ibidem*, p. 203.

Developments after unrestricted warfare and the three warfares

Chinese doctrine provides a number of other HT examples within a not fully identifiable blend of peacetime and wartime, especially in light of the strategy of a "military-civil fusion".;[33] for example, the use of non-armed non-state actors (NANSAs) by the Chinese government as a significant component in the creation of hybrid threats.[34] Proxies play a crucial role in enabling unlawful operations that fall below the threshold of armed conflict while allowing governments to maintain a degree of separation from attributable enforcement agents. Notably, such strategies have been employed in regions such as Hong Kong, Macao, and Taiwan. The Chinese government has strengthened its control by securing the cooperation of influential social elites while simultaneously marginalising potential opponents. The overarching objective is to suppress independence movements, erode local identities, and consolidate support for China's political system.[35] In 2003, the State-Owned Assets Supervision and Administration Commission was established to oversee state-owned economic entities and ensure their accountability for financial objectives,[36] which adds another dimension, namely the economic one.

In general, Chinese companies are expected to align their operations closely with government policy objectives and ideologies.[37] The aim is to establish a "united front" between the business sector and the government, enabling the strengthening of the party's influence over the private economy.[38] Private sector employees are educated about government policies and ideologies, with the anticipation that this "enlightenment" will guide their business decisions.[39] That indicates synergy between coordination of different forms of HT with the national economy.

The 2017 National Intelligence Law places a legal obligation on Chinese individuals. According to Chinese officials, this obligation extends to all citizens, as well as various social groups, enterprises, and institutions, requiring them to prevent and thwart espionage activities and uphold national security.

33 Saalman, L. (2021) "*China and its hybrid warfare spectrum*", in Weissmann, M., Nilsson, N., Palmertz, B., and Thunholm, P. (eds), *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, London: I.B. Tauris, p. 95–112, p. 99. Available at: http://dx.doi.org/10.5040/9781788317795.0013 [Accessed 19 June 2024].

34 Aukia, J. (2021) "*China as a hybrid influencer: non-state actors as state proxies*", Hybrid CoE Research Report 1. Helsinki: European Centre of Excellence for Countering Hybrid Threats, p. 8. Available at: https://www.hybridcoe.fi/wp-content/uploads/2021/06/20210616_Hybrid_CoE_Research_Report_1_China_as_a_hybrid_influencer_Non_state_actors_as_state_proxies_WEB.pdf [Accessed 22 July 2024].

35 Aukia, J. (2021) *Ibidem*, p. 18.

36 Aukia, J. (2021) *Ibidem*, p. 19.

37 Olson, S. (2020) "*Are private Chinese companies really private*?", *The Diplomat*, 30 September. Available at: https://thediplomat.com/2020/09/are-private-chinese-companies-really-private/ [Accessed 10 February 2025].

38 Stephen Olson, *Ibidem*.

39 Stephen Olson, *Ibidem*.

Civil organisations are expected to collaborate with national security agencies to educate, mobilise, and organise their personnel to counter-espionage activities. The ambiguous language of this law has led to questions regarding whether its purpose is defensive or offensive in terms of national security.[40]

The further development of Chinese doctrine indicates a dominant approach that emphasises hybrid threats, including the use of non-armed non-state actors and economic entities. This approach increasingly approaches the threshold of violating the prohibition on the use of force by blending peacetime and wartime tactics under the "military-civil fusion" strategy. Additionally, it involves collaboration between civil organisations and national security agencies, highlighting the synergy between them.

Is there a common denominator for the Chinese doctrine?

"The first rule of Unrestricted Warfare", as the authors explains, "is that there are no rules, with nothing forbidden".[41] As Colonels Qiao/Xiangsui point out in their book, essentially, "everything is war". To summarise the Chinese approach, what is important from the international law perspective is the fact of blurring the boundaries between the civilian domain and the military one – yet leaning toward HT rather than HW, which adheres to Clarke's observations: "All boundaries lying between the two worlds of war and non-war, of military and non-military, will be totally removed".[42]

Such an approach affects both *ius ad bellum* and, to some extent, *ius in bello* principles (which will be discussed in the subsequent chapter). This leads to the conclusion that we are witnessing the emergence of a concept known as "hybridity with 'Chinese characteristics'".[43] This Chinese character represents the meaning and scope of "national security", or the role of the nation state[44] with dominance of non-military means and methods. According to Clarke, nation-state protection becomes the political and ideological security of the Party itself. China's "Three Warfares" is thus best understood primarily as a form of political warfare whose central purpose is to create and maintain political power for the CCP.[45] The Chinese model offers the broadest understanding of hybrid activity. It includes elements of the discussed concepts as well as a high degree of centralisation of the state in pursuit of its goals. In her survey, Saalman indicates that not only UW and TW, but also the general Chinese view on hybridity, is vested mainly in the nation's actions.

40 Aukia, J. (2021), *op. cit.*, p. 22.
41 Spalding, R. (2022) *War Without Rules: China's Playbook for Global Domination*, New York: Penguin Random House, p. 18.
42 Clarke, M. (2019) *op. cit.*, p. 191.
43 Clarke, M. (2019) *Ibidem*, p. 191.
44 Clarke, M. (2019) *Ibidem*, p. 96.
45 Clarke, M. (2019) *Ibidem*, p. 208.

And yet, despite China's effort to challenge the current international order through tactics involving political manipulation, deception, and information dominance, it is difficult to establish a single general rule for the Chinese doctrine, especially taking into consideration that the wording of the doctrine does include hybrid warfare and hybrid threats. These doctrinal considerations blur the line between *ius ad bellum* and *ius in bello*. General Spalding concludes that China's policy opposes the famous Clausewitz: Politics is the continuation of war by other means, and says: Politics is permanent, so is war.[46]

And again I will refer to Spalding's summary, which provides that war without rules is meant to be permanent.[47] With the findings of Hybrid CoE that China is on the rise as a proxy inducer,[48] one thing is certain – China has become an influential hybrid actor.

Russia's approach to hybridity

Russia's military doctrine primarily emphasises the militarised dimension of warfare. Its approach to modern warfare has been shaped by its experiences in armed conflicts in Chechnya and Georgia, as well as its military engagements against Ukraine. At the same time, Russia has demonstrated the capability to conduct a range of hybrid threat operations that either accompany or precede conventional military actions, including hybrid warfare itself. Therefore, the development of Russian concepts will be provided separately from both angles: hybrid threats and hybrid warfare. The proposed distinction is crucial because Russia's hybrid warfare cannot exist without preceding hybrid threats. However, there are numerous instances of Russian hybrid threats which do not escalate into full-scale hybrid warfare.

A defining characteristic of Russian hybrid threat operations is their strong emphasis on the information domain, accompanied by a blend of military and non-military means. Gierasimov recapitulated previous ideas in the journal *Voenno-promishlenniy kurier*, which was published in 2013. He stipulated the notion of "new generation warfare", which should "concentrate on the combined use of diplomatic, economic, political and other non-military methods with direct military force, instead of waging open war".[49] Gerasimov argued that non-military means of achieving political and strategic goals are often more effective than military ones. He also emphasised the importance of the information space, along with the extensive use of special forces and robotic

46 Spalding, R. (2022) *op. cit.*, 30.
47 Spalding, R. (2022) *op. cit.*, p. 18.
48 Aukia, J. (2021) *op. cit.*, p. 22.
49 Gerasimov, V. (2013) "*The value of science is in the foresight*", Voyenno-Promyshlennyy Kurier, 27 February. Translated in: Bartles, C.K. (2016) "*Getting Gerasimov Right*", Military Review, Jan–Feb, p. 23–29, p. 36. Available at: https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf [Accessed 3 May 2025].

weapons, such as drones.[50] This very blend of HT and HW supports the point made by the author.

Russia's hybrid threats' repertoire, which does not fall into the means and methods of the warfare-HW category, but in most cases coexists with influence operations, is as follows:

1) instrumentalisation of diasporas and Russia-linked institutions.
2) sabotage, vandalism, and intelligence activities.
3) cyber-attacks.
4) instrumentalisation of migration.[51]
5) damage to critical infrastructure.
6) radicalisation of the political narrative.
7) espionage.
8) economic pressure.
9) promoting social unrest.
10) clandestine operations.
11) territorial water violations.[52]

Russian hybrid threats and the role of influence operations

It is impossible to understand the Russian approach to hybridity without a reference to influence operations. The Russian doctrine, *maskirovka*/information operations, is so characteristic that it is inseparably connected with Russia's general concept of waging warfare as well as influencing other states through hybrid threats. Therefore, Russia has the capacity and capability to conduct information operations as a part of both their hybrid warfare as well as hybrid threats, making it a distinctly Russian trait.

It is beyond of the scope of this publication to point out one particular moment when Russia understood the influence and meaning of contemporary information operations. However, already Lenin underlined the importance of information warfare or propaganda in his "Lessons of the Moscow uprising". According to him, properly conducted propaganda had two main, equally important functions: first, to inform and mobilise his own forces/society and second, to shatter the morale of enemy troops.[53] In the 1960s,

50 Gerasimov, V. (2013) *Ibidem*.

51 Praks, H. (2024) "*Russia's hybrid threat tactics against the Baltic Sea region: from disinformation to sabotage*", Hybrid CoE Working Paper 32, May. Available at: https://www.hybridcoe.fi/wp-content/uploads/2024/05/20240530-Hybrid-CoE-Working-Paper-32-Russias-hybrid-threat-tactics-WEB.pdf [Accessed 3 May 2025].

52 Jungwirth, R., Smith, H., Willkomm, E., Savolainen, J., Alonso Villota, M., Lebrun, M., Aho, A., and Giannopoulos, G. (2023) *Hybrid Threats: A Comprehensive Resilience Ecosystem*, Luxembourg: Publications Office of the European Union.

53 Rácz, A. (2015) "*Russia's hybrid war in Ukraine: breaking the enemy's ability to resist*". Helsinki: The Finnish Institute of International Affairs, Report No. 43, p. 23. Available at: https://www.fiia.fi/wp-content/uploads/2017/01/fiiareport43.pdf [Accessed 3 May 2025].

Messner believed that a subversion-war was "first and foremost psychological" and argued that conquering "souls in the hostile state place the most important position".[54] Both Chechen wars clearly showed the importance of this element of modern conflicts.[55]

Russian doctrine paid particular attention to information operations both in and outside the scope of armed conflict, or from both HT and HW perspectives. Gareev said:

> systematic broadcasting of psychologically and ideologically biased materials of a provocative nature, mixing partially truthful and false items of information […] can all result in mass psychosis, despair and feelings of doom and undermine trust in the government and armed forces; and, in general, lead to the destabilisation of the situation in those countries, which become objects of information warfare, creating a fruitful soil for actions of the enemy.[56]

A similar approach was presented by Panarin popularising the role of information war.[57]

This lack of distinction between the time of peace and war is well reflected in the speech of General Staff officer/member Sergei Ivanov, who suggested in 2015 that Russia was under attack not by a specific country, but by various organisations using non-military means.[58] This perception contributed to a narrative of Russia being besieged by enemies, influencing its military policies. As a result, Russia views events like colour revolutions as security threats or domestic military danger.[59] This perspective shaped its military doctrines,

54 Cited in Jonsson, O. (2019) *The Russian Understanding of War: Blurring the Lines Between War and Peace*, Washington, DC: Georgetown University Press, p. 45.

55 Chechens were successful not only with the internet but also with traditional media. Chechens put in a significant effort and orchestrated a kind of embedded journalism. As a result, media were informed about Russian casualties and were generally critical of the government. In Putin's opinion, the society's low morale led to Russia's defeat. During the Second Chechen War, Russians were much more focused on placing domestic public opinion as the centre of gravity, limiting access of independent journalists. *Vide* Jonsson, O. (2019) *Ibidem*, p. 110.

56 M. Gareev, in Rácz, A. (2015) *op. cit.*, p. 35.

57 Göransson, M. (2021) "*Understanding Russian thinking on Gibridnaya Voyna*", in Weissmann, M., Nilsson, N., Palmertz, B., and Thunholm, P. (eds), *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, London: I.B. Tauris, p. 86.

58 Gareyev citation in Jonsson, O. (2019) *The Russian Understanding of War: Blurring the Lines between War and Peace*, Washington, DC: Georgetown University Press, p. 57.

59 Jonsson, O. (2019), *op cit.*, p. 92.

with the 2010[60] and 2014[61] doctrines emphasising the power of information warfare, recognising it as capable of achieving strategic objectives without traditional military force.

The umbrella wording which is key to understanding the Russian approach to influence operations is "reflexive control", in Russian: *refleksivnoje upravlenie* or *refleksivnyj control*.[62] It involves shaping an adversary's decision-making by strategically modifying information within a carefully orchestrated information campaign. The main objective of this manipulated information is to lead the opposing party into making decisions that have been predetermined by the creator of the altered information.[63] This concept, hailed by Vladimir Lefebvre, was pointed out by *inter alia* Wither as a significant Russian threat.[64] Russia has launched countless information operations targeting democratic governments, as well as similar campaigns during armed conflicts involving Russia. The challenge lies in the fact that elements of these operations such as specific narratives often overlap. The same false information is used in a coordinated and orchestrated manner both in armed conflicts and in countries not experiencing direct conflict. This blurring of lines makes it particularly difficult to distinguish between peacetime hybrid threats and HW methods used during armed conflicts.

The concept was codified in the Russian National Security Strategy and consists of the following elements: Power pressure (provocation and deterrence); Measures to present false information about the situation (deception, distraction and paralysis); Influencing the enemy's decision-making algorithm (exhaustion, divisions and suggestion); and Altering the decision-making time (pacification and overload).[65]

The role of information operations was also explained by another Russian military theorist, Pavel Kazarin. He argues that war should be interpreted beyond classical understanding, not limited only to armed conflict but as a sum of all features. He stated "that economic and information warfare" needed to be included in the analysis to reveal war's proper content. The economy being the foundation of a country's military strength, it could be

60 Russian Federation (2010) "*The Military Doctrine of the Russian Federation*". Approved by Presidential Edict on 5 February 2010, pkt 12 b. Available at: https://www.cndpindia.org/wp-content/uploads/2017/12/Russia-Military-Doctrine-2010.pdf [Accessed 3 May 2025].

61 Russian Federation (2014) "*The Military Doctrine of the Russian Federation*". Approved on 25 December 2014, pkt 15 a. Available at: https://rusmilsec.blog/wp-content/uploads/2021/08/mildoc_rf_2014_eng.pdf [Accessed 3 May 2025].

62 Kupiecki, R., and Legucka, A. (2023) *Disinformation and the Resilience of Democratic Societies*, Warsaw: Polski Instytut Spraw Międzynarodowych, p. 25.

63 Marahrens, S. (2024) *op. cit.*

64 Wither, J.K. (2016) *Making Sense of Hybrid Warfare*, Connections: The Quarterly Journal, Volume 15, No. 2, p. 73–87, p. 85. Available at: https://connections-qj.org/article/making-sense-hybrid-warfare [Accessed 3 May 2025].

65 Marahrens, S. (2024) *op. cit.*

weakened by varied means, especially nonviolent ones.[66] This is in line with the writings of Gorbunov and Bogdanov, who saw that the internal weakening of a state should include "the taking of informational, psychological, moral, climatic, and organisational measures, setting up and encouraging destructive opposition, and secretly fomenting and intensifying ethnic strife and ethnic conflicts".[67] Bogdanov and Chekinov addressed the issue of the influence of the Russian/world information sphere. They considered civic organisations as elements of foreign influence and compiled a concrete list of media outlets, religious organisations, cultural institutions, NGOs, public movements financed from abroad, and scholars engaged in research on foreign grants as potential components of a coordinated attack against Russia and other targeted countries. They also accused the United States (US) of operating a specialised internet 'troll' army and using social media for propaganda purposes.[68] Their writing had visible impact on Russian domestic regulations on the so-called foreign agents on the one hand and creating troll farms by Russians on the other. Gerasimov echoed this in a later speech in 2014. He saw the increasing importance of political, economic, diplomatic, and other measures and the demonstration of hidden measures, such as the use of NGOs and private military companies in Syria and Ukraine and Greenpeace activities in the Arctic.[69] As a result, the Russian concept encompasses computer network operations along with various other tactics, including psychological operations (PsyOps), strategic communications, influence operations, and tactics such as intelligence, counterintelligence, *maskirovka*, disinformation, electronic warfare, disruption of communications, degradation of navigation support, psychological pressure, and the dismantling of enemy computer capabilities[70] "a whole of systems, methods, and tasks to influence the perception and behaviour of the enemy, population, and international community on all levels".[71] To summarise, the Russian approach to the info operations lets us cite Gerasimov's voice again as a general summary of the Russian approach to hybridity. He famously said "Today, it is obvious that the line between peace and war is blurring. Non-military forms and means of struggle have received an unprecedented technological development and acquired a dangerous and

66 Jonsson, O. (2019) *op cit.*, p. 54.
67 Jonsson, O. (2019) *op cit.*, p. 62.
68 Chekinov, S.G., and Bogdanov, S.A. (2013) "*The nature and content of a new-generation war*", Military Thought, October–December, p. 12–23. Available at: http://www.eastviewpress.com/Files/MT_FROM%20THE%20CURRENT%20ISSUE_No.4_2013.pdf [Accessed 5 March 2025]. Cited in: Rácz, A. (2015), *op cit.*, p. 38.
69 Jonsson, O. (2019) *op cit.*, p. 1.
70 Giles, K. (2015) *Handbook of Russian Information Warfare*, Rome: NATO Defense College, p. 6.
71 Giles, K. (2015) *Ibidem*, p. 6.

sometimes violent nature", which indicates the direction and understanding of the Russian approach to both hybrid threats and hybrid warfare.[72]

Russian operations between hybrid warfare and hybrid threats

Considering the analysis presented, it is worth asking the critical question: is the Russian hybrid threat concept truly a separate and distinct concept in its own right? The author contends that Russia's repertoire of hybrid threats consistently precedes actual aggression, armed conflict, and hybrid warfare (as evidenced by the cases of Georgia and Ukraine). However, there are also instances in which hybrid threats are employed without an escalation into open armed conflict. Such threats may remain below the threshold of armed conflict for as long as Russia lacks the capacity to wage a full-scale war, or when hybrid operations alone prove sufficient, particularly if the targeted state demonstrates resilience. Regardless of the specific circumstances, Russia's approach to hybrid threats and hybrid warfare can be viewed as two sides of the same coin. Russia incorporates a broad spectrum of hybrid threats such as political, economic, humanitarian,[73] and other non-military measures to exert influence. The overt use of force often under the pretext of peacekeeping and crisis management must also be recognised as a component of Russia's strategy.[74]

The aggression against Ukraine in Crimea and the Donbas/Luhansk regions was preceded by prolonged hybrid threats operations, which thrived due to the ideal political, geographical, and military environment. For instance, Russian forces in Crimea faced limited resistance, resulting out of earlier prolonged hybrid threats operations. Perhaps the most defining feature of Russian hybrid operations are their population-centric approach, which seeks to shape public perception through information operations.[75] These tactics operate across both cyber and cognitive domains[76] and have even absorbed the already discussed *dezinformatsiya*, *maskirovka*, and, most notably, *reflexive control*.[77]

72 Jonsson, O. (2019), *op. cit.*, p. 1.

73 *Vide* for example COVID-related help to Italy; Luhn, A., 2020. *"'From Russia with Love'": Coronavirus disinformation and aid to Italy.* [online] Coda Story. Available at: https://www.codastory.com/disinformation/russia-coronavirus-aid-italy/ [Accessed 22 May 2025].

74 Gardner, H. (2015) "*Hybrid warfare: Iranian and Russian versions of 'little green men' and contemporary conflict*", Research Paper, Rome: NATO Defense College, December, p. 4. Available at: https://css.ethz.ch/en/services/digital-library/publications/publication.html/195396 [Accessed 3 May 2025].

75 Abbasi, S.N., and Nasir, S. (2021) *Hybrid Warfare: A Reorientation of Russian Foreign Policy in Syria*, Pakistan Journal of International Affairs, Volume 4, No. 2, p. 187. Available at: https://pjia.com.pk/index.php/pjia/article/view/177 [Accessed 3 May 2025].

76 Rácz, A. (2015) *op. cit.*, p. 51.

77 Crowther, G.A. (2021) "*NATO and hybrid warfare: seeking a concept to describe the challenge from Russia*", in Weissmann, M., Nilsson, N., Palmertz, B., and Thunholm, P. (eds) *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, London: I.B. Tauris, p. 31.

That corresponds with Racz's observations on the requirements of a successful hybrid operation. He points out that the targeted country needs to be weak and divided, with corrupt officials. Second, the attacker needs to be militarily stronger than the target country to limit the defender's countermeasure potential.[78] Weakening a country before aggression is the task of hybrid threats. Militarily defeating it while manipulating the global audience, opposing the victim, and blaming the victim country for aggression or prolonged war are also aspects of hybrid threats.

What is certain is that Russia has mastered hybrid threats and its influence operations continue to challenge the sovereignty and stabilisation of other states through overt and covert means, and the hybrid operations expand not only against European states but also around the world. Moreover, these threats are frequently closely interconnected with the framework of hybrid warfare.

NATO's road to understanding of hybridity

Initially the concept of hybridity in the Western hemisphere revolved around the armed conflict, i.e., around the hybrid warfare dimension, with notable writings by US Major William Nemeth,[79] James N. Mattis[80] and Frank Hoffman.[81] Their references to military means and methods used by Hezbollah, Hamas, and Iraq's Fedayeen were a master case study of this method of warring.[82] At that time, Hoffman *et consortes* used all three types of hybridity, namely hybrid war, warfare, and threats interchangeably.[83] It can therefore be concluded that in the first decade of the twenty-first century the concept was changing to revolve mostly around armed conflict.[84]

At the outset, NATO had limited involvement in the understanding of the concept. An illustrative point is that the 2012 Chicago Declaration makes no mention of "hybridity", in contrast to the 2014 Wales Declaration, which begins by acknowledging that "Russia's aggressive actions against Ukraine have fundamentally challenged our vision of a Europe whole, free, and at

78 Racz, A., (2015). "*Russia's hybrid war in Ukraine: breaking the enemy's ability to resist*". Report No. 43. Helsinki: The Finnish Institute of International Affairs, p. 88.

79 Cusumano, E., and Corbe, M. (2018) *Ibidem*, p. 19.

80 Cusumano, E., and Corbe, M. (2018) *Ibidem*, p. 19.

81 Hoffman, F.G. (2007) *Ibidem*, p. 8.

82 Hoffman, F.G. (2007) *Ibidem*, p. 40.

83 In 2010, the US Secretary of Defense, Robert Gates, used the term hybrid warfare (…) to describe (..) the means that both state and non-state actors would employ to mitigate a conventional disadvantage against the US. *Vide* Gates, R.M., "*Quadrennial defense review report*", in Johnson, R. (2018) *Hybrid War and Its Countermeasures: A Critique of the Literature*, Small Wars & Insurgencies, Volume 29, No. 1, p. 145.

84 Mumford, A., and Carlucci, P. (2022) "*Hybrid warfare: the continuation of ambiguity by other means*", European Journal of International Security, p. 5.

peace" and references hybrid warfare five times.[85] However, since then, NATO's approach to hybridity has often been inconsistent, frequently using a diverse set of terms like warfare, attacks, threats, tactics, challenges, means, and campaigns to describe a similar concept.

The already mentioned 2014 Wales summit resulted in a declaration "that NATO is able to effectively address the specific challenges posed by hybrid warfare threats".[86] At the same time, the importance of cooperation between the military organisation NATO and the EU was emphasised[87] and the issues of common concern, including security challenges like cyber defenceand energy security, which fall into areas beyond a classical military contest It opened the space for the whole scope of non-IHL regulated threats.. At the time, NATO referred to hybrid warfare as a "wide range of overt and covert military, paramilitary, and civilian measures employed in a highly integrated design".[88] With blending of hybrid warfare and hybrid threats NATO was leaning mostly toward hybrid warfare, yet with an increasing role of non-military organisations, such as the EU, in combating the abovementioned (hybrid) threats.

The 2016 NATO Warsaw Summit addressed a wide range of issues, including both hybrid threats (HT) and hybrid warfare (HW). Point 5 of the final communiqué noted that "security challenges and threats originate from both the east and the south, from state and non-state actors". From a hybrid threats perspective, it emphasised that not all acts fall within the traditional categories of warfare. This includes tactics like terrorism, cyber-attacks, and other hybrid strategies that blur the line between conventional and unconventional warfare.[89] What was a very important statement was that "The primary responsibility to respond to hybrid threats or attacks rests with the targeted nation".[90] Simultaneously, it was noted that NATO was "prepared to assist an Ally at any stage of a hybrid campaign", as well as that "The Council could decide to invoke Article 5 of the Washington Treaty" when facing hybrid warfare.[91] At that time two concepts were discussed: hybrid warfare and hybrid attacks/threats, with the communiqué leaning toward addressing predominantly

85 Crowther, G.A. (2021) "*NATO and hybrid warfare: seeking a concept to describe the challenge from Russia*", in Weissmann, M., Nilsson, N., Palmertz, B., and Thunholm, P. (eds), *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, London: I.B. Tauris, p. 31.

86 Point 13 NATO (2014) "*Wales Summit Declaration*", 5 September. Available at: https://www.nato.int/cps/en/natohq/official_texts_112964.htm [Accessed 3 May 2025].

87 Point 14 NATO (2014) "*Wales Summit Declaration*", *Ibidem*.

88 Maronkova, B. (2021) "*NATO amidst hybrid warfare threats: effective strategic communications as a tool against disinformation and propaganda*", in *Disinformation and Fake News*, Singapore: Springer, p. 117–129.

89 NATO (2016) "*Warsaw Summit Communiqué*", 9 July. Available at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm [Accessed 3 May 2025].

90 Point 72 NATO (2016) "*Warsaw Summit Communiqué*". *Ibidem*.

91 Point 72 NATO (2016) "*Warsaw Summit Communiqué*". *Ibidem*.

hybrid warfare. The notion of the non-military character of the threat was reflected in the final communiqué, which commended:

> the joint declaration issued (…) by the NATO Secretary General, the President of the European Council, and the President of the European Commission, (…) aiming to take concrete actions together in areas including countering hybrid threats, enhancing resilience, and strengthening defence capacity.[92]

This broader approach highlights two key observations: first, hybrid threats constitute a distinct category; second, as these threats are primarily non-military and fall below the threshold of armed conflict, they cannot, and should not, be addressed solely by a predominantly military alliance such as NATO.[93] This underscores that countering hybridity necessitates a coordinated effort involving organisations, such as the EU.[94]

During the 2018 Brussels summit, much attention was paid to hybridity again, and hybrid attacks were named among other challenges.[95] Importantly, elements of the so-called hybrid challenges, such as disinformation campaigns, were included, alongside elements already mentioned in previous documents such as cyber activities.[96] The part dedicated to deterrence included cyber threats as part of a hybrid campaign.[97] The Brussels summit repeated "equating hybrid warfare (sic) with an armed attack, by asserting that" in cases of hybrid warfare, the Council could decide to invoke Article 5 of the Washington Treaty, as in the case of armed attack.[98] This confirms differing understandings of HT and HW (although the author is not entirely certain whether this was intentional). A legal-linguistic interpretation leads to viewing an armed attack as an element of *ius ad bellum* and a violation of the prohibition on the use of force. Therefore, it should be classified as a hybrid threat. Consequently, armed attack falls within the domain of *ius ad bellum* and hybrid threats, rather than being a hybrid means or method of warfare. Hybrid threats were also discussed during the 2019 London Declaration NATO summit.[99] Again, hybrid tactics were listed among the threats.[100]

92 Point 122 NATO (2016) "*Warsaw Summit Communiqué*", *Ibidem*.
93 Point 72 NATO (2016) "*Warsaw Summit Communiqué*". *Ibidem*.
94 Point 122 NATO (2016) "*Warsaw Summit Communiqué*", *Ibidem*.
95 Point 2 NATO (2018) "*Brussels Summit Declaration*", 11 July. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_07/20180713_180711-summit-declaration-eng.pdf [Accessed 3 May 2025].
96 Point 2 NATO (2018) "*Brussels Summit Declaration*". *Ibidem*.
97 Point 20 NATO (2018) "*Brussels Summit Declaration*". *Ibidem*.
98 Point 21 NATO (2018) "*Brussels Summit Declaration*". *Ibidem*.
99 NATO (2019) "*London Declaration*", 4 December, Point 3. Available at: https://www.nato.int/cps/en/natohq/official_texts_171584.htm [Accessed 3 May 2025].
100 NATO (2019) "*London Declaration*", Point 6.

Despite the eruption of the conventional armed conflict in Ukraine, the Madrid Summit of 2022 mentioned hybrid and asymmetric threats only twice in its closing declaration.[101] The summit was nonetheless foremost orientated on a new element – NATO's Strategic Concept (SC). Hybrid tactics as a threat to the NATO countries' democratic process were mentioned.[102] NATO's SC introduced a new notion - hybrid means.[103] Disinformation was again included in the repertoire of hybrid activities.[104] What was reiterated again was the message that "Hybrid operations against Allies could reach the level of armed attack and could lead the North Atlantic Council to invoke Article 5 of the North Atlantic Treaty".[105] Similarly to the previous declarations and communiqué, SC highlighted the role of the EU as a unique and essential partner for NATO in countering hybrid threats.[106] Therefore, the growing recognition of hybrid threats as a separate category not explicitly regulated by the International Humanitarian Law (IHL) underscores the increasing importance of understanding their nature and implications.

Similarly to previous summits, the list of threats presented in the 2023 Vilnius summit communiqué included hybrid threats. The broad concept of the hybrid actions introduced there was specified in reference to Russian actions and those of its proxies: "This includes interference in democratic processes, political and economic coercion, widespread disinformation campaigns, malicious cyber activities, and illegal and disruptive activities of Russian intelligence services".[107] It was repeated during the summit "that hybrid operations against Allies could reach the level of an armed attack and could lead the Council to invoke Article 5 of the Washington Treaty[108] as well as the fact the cyberspace contest may fall into the category of hybrid campaigns".[109]

During the anniversary summit in Washington, even greater attention was given to hybrid threats coming from both state and non-state actors.[110] The wording of the summit communiqué frequently referred to the already known wording of hybrid actions, which predominantly cover hybrid threats, such as sabotage, acts of violence, provocations at Allied borders, instrumentalisation

101 Point 6 and 10 NATO (2022) "*Madrid Summit Declaration*". Available at: https://www.nato.int/cps/en/natohq/official_texts_196951.htm [Accessed 3 May 2025].
102 NATO (2022) "*Strategic Concept*". Madrid: NATO, 29 June, p. 3, Point 7. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf [Accessed 3 May 2025].P.
103 Point 8 NATO (2022) "*Strategic Concept Madrid*", p. 4.
104 Point 13 NATO (2022) "*Strategic Concept (SC)*", p. 5.
105 Point 27 NATO (2022) "*Strategic Concept (SC)*", p. 7.
106 Point 43 NATO 2022 "*Strategic Concept (SC)*". *Ibidem.*, p. 10.
107 Point 18 NATO (2023) "*Vilnius Summit Communiqué*". Available at: https://www.nato.int/cps/en/natohq/official_texts_217320.htm [Accessed 3 May 2025].
108 Point 64 NATO (2023). *Ibidem.*
109 Point 66 NATO (2023). *Ibidem.*
110 Point 13 NATO (2024) "*Washington Summit Declaration*", 10 July. Available at: https://www.nato.int/cps/en/natohq/official_texts_227678.htm [Accessed 3 May 2025].

of irregular migration, malicious cyber activities, and electronic warfare, interference, disinformation campaigns, and malign political influence, as well as economic coercion.[111]

What is evident is that NATO continuously refers to the EU as an organisation of non-military character of the joint counter-hybrid efforts . This is due to the fact that several challenges, such as disinformation (although this could be also a part of an IHL government type of situation), migration, and maintaining stable governance lie far below the armed conflict threshold. Such threats are better addressed through political and law enforcement approaches, rather than within the framework of the IHL. However, the ambiguity surrounding what precisely triggers Article 5 creates a sense of unpredictability, particularly in the context of sustained hybrid pressure, as well as the fact that the number of the threats has to be addressed by law enforcement as well as military units in the environment below the threshold of armed conflict and use of force. The very recent destruction of critical sea bed infrastructure in the Baltic is a relevant example.[112]

EU approach to hybrid threats

The EU's approach is inherently defensive. The reason for presenting the work of various EU institutions lies in the fact that the EU has provided the most precise and comprehensive definitions, as well as the most well-developed concept of the counter-hybrid threats ecosystem. This framework positions hybrid threats below the threshold of armed conflict and serves as a starting point for identifying potential threats that affect democratic states.

From the EU's viewpoint, the differentiation between hybrid threats and warfare remained relatively unexamined before 2015. Since then, the EU took the pragmatic and policy-driven orientation approach to counter-hybrid strategies, describing them predominantly as hybrid threats.[113]

In April 2016, the High Representative (HR) for the Common Security and Defence Policy (CSDP) issued a joint framework on countering hybrid threats. This document sets the scene and provides a definition that confirms the non-armed conflict character of hybrid threats:

> While definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature, the concept aims to capture the mixture of coercive and subversive activity, conventional and unconventional

111 Point 20 NATO (2024) "*Washington Summit Declaration*", *Ibidem*.

112 NATO (2025) "*NATO Launches 'Baltic Sentry' to Increase Critical Infrastructure Security*", 3 May. Available at: https://www.nato.int/cps/en/natohq/news_232122.htm [Accessed 3 May 2025].

113 Cullen, P. (2021) "*A perspective on EU hybrid threat early warning efforts*", in Weissmann, M., Nilsson, N., Palmertz, B., and Thunholm, P. (eds) *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, London: I.B. Tauris, p. 44.

> methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors achieve their specific objectives while remaining below the threshold of formally declared warfare. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes. Massive disinformation campaigns, using social media to control the political narrative or to radicalise, recruit and direct proxy actors can be vehicles for hybrid threats.[114]

Since then, the Annual Joint Reports publication has indicated both potential threats as well as those measures undertaken by the EU to combat them. A Report in 2017 provided information about establishing the EU Hybrid Fusion Cell, developing strategic communication efforts, including the East Stratcom Task Force to counter disinformation campaigns, as well as details surrounding the launching of the European Centre for Countering Hybrid Threats in Finland to enhance cooperation and resilience.[115] The measures outlined in the report concerning resilience underscore the EU's prioritisation of countering hybrid threats across multiple domains. Key initiatives include the enhancement of cybersecurity through the implementation of the Network and Information Security (NIS) Directive and the establishment of public-private partnerships (PPPs) aimed at fostering cybersecurity research and innovation. Critical infrastructure protection has also been strengthened, particularly in sectors such as transport, energy, and finance. Within the transport domain, specific efforts have targeted aviation and maritime security to address vulnerabilities to hybrid threats. Energy security has been promoted through the diversification of gas supplies and the reinforcement of nuclear safety frameworks. Financial resilience has been advanced by bolstering cybersecurity within the banking sector and enacting more stringent anti-money laundering regulations.

In addition to these civilian measures, the EU has adopted a more robust approach, exemplified by the development of defence capabilities to counter hybrid threats, particularly through the lens of Article 222 of the Treaty on the Functioning of the European Union (TFEU) and Article 42(7) of the Treaty on European Union (TEU), both of which provide legal grounds for

114 European Commission and 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 – A European Union Response*" (Report, JOIN (2016) 18 final, 6 April 2016). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018 [Accessed 25 April 2025].

115 European Commission and 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 – A European Union Response*" (Report, JOIN(2017) 30 final, 19 July 2017). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0030 [Accessed 25 April 2025].

a collective response to hybrid attacks. From the outset, the EU has emphasised the necessity of deepened collaboration with NATO, including intelligence sharing, coordinated exercises, and broader efforts to enhance collective resilience.[116]

The 2018 Joint Report introduced the idea of expanding the East Stratcom Task Force and launching the Western Balkans Task Force, as well as the expansion of potential threats from the domain of space, by introducing integrated security measures into the EU Space Programme to protect critical space assets. Additionally, it reported on the Chimera exercise on biosecurity threats and improved emergency response coordination; it strengthened the EU cybersecurity strategy, including public-private partnerships, resilience for the energy and financial sectors, and improved cyber security incident response teams (csirts); combating radicalisation and disinformation, via improved measures for tackling extremist content online and increased cooperation with social media platforms. The EU also considered hybrid threats existing beyond its territory by launching Hybrid Risk Surveys in Moldova, Georgia, and Jordan and by strengthening cyber resilience programs in Ukraine, Africa, and Asia.[117]

Despite predominantly being below the armed conflict threshold character of these threats, the Joint report underlined cooperation with NATO in the form of the EU Operational Protocol – PACE17 exercises with NATO, as well as the upcoming PACE18 to further improve decision-making. The report discussed the Military Mobility issue to improve cross-border military transport in response to hybrid threats.[118]

The 2019 Report highlighted the growing impact of disinformation, prompting the launch of the Action Plan Against Disinformation in 2018. This included expanded monitoring of pro-Kremlin disinformation in the Western Balkans and Southern Neighbourhood. The economic aspects of hybrid threats were addressed through the Foreign Direct Investment (FDI) Screening Regulation (2019/452), aimed at safeguarding strategic industries. In the energy sector, the EU prioritised energy security by increasing Liquefied Natural Gas (LNG) imports and diversifying supply chains. The

116 European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2017) "*Joint Report ….on Countering Hybrid Threats – A European Union Response*", *op. cit.*, p. 4.

117 European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2018) "*Joint Report to the European Parliament, the European Council and the Council on the Implementation of the Joint Framework on Countering Hybrid Threats from July 2017 to June 2018*" (Report, JOIN (2018) 14 final, 13 June 2018). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018JC0014 [Accessed 3 May 2025].

118 European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2018) "*Joint Report ….on Countering Hybrid Threats – A European Union Response*", *op. cit.*

Galileo and Copernicus satellite systems were utilised for crisis response, enhancing the EU's resilience in critical infrastructure. To bolster cybersecurity, the EU enacted the Cybersecurity Act in 2019, strengthening its capacity to detect and respond to cyber threats. Additionally, the GOVSATCOM initiative was launched to provide secure satellite communications for EU institutions and member states. In response to the evolving threat landscape, the 2018 Election Package was introduced to counter foreign interference in democratic processes. The health sector's preparedness for biological and chemical attacks was also reinforced, including the development of specialised medical response plans under the EU Civil Protection Mechanism. The military dimension of hybrid threats was tested through EU-NATO Hybrid Crisis Protocols and coordinated Cyber Defence Exercises, ensuring comprehensive preparedness for complex, multi-domain challenges.[119] What is worth noting is that throughout the whole document, the word warfare is not mentioned.

The EU's strategic approach to countering hybrid threats and disinformation witnessed significant advancements in the 2020 and 2021 reporting periods, marked by a suite of institutional, legislative, and cooperative measures aimed at bolstering resilience across multiple domains. Central to the 2020 Report was the establishment of the Horizontal Working Party on Resilience and Hybrid Threats (HWP ERCHT) in July 2019, designed to enhance inter-institutional coordination, strategic communication, and counter-disinformation strategies. This initiative was supported by the expansion of the European External Action Service (EEAS) Strategic Communications Task Forces, which focused on countering malign narratives emanating from the East, South, and Western Balkans, as well as by continuous monitoring of the EU Code of Practice on Disinformation to ensure its efficacy.

Building upon this framework, the 2021 Report introduced further regulatory and institutional developments, notably the Critical Entities Resilience (CER) Directive and the Network and Information Systems Directive (NIS2), both aimed at fortifying cybersecurity across EU member states. In a parallel effort to address foreign interference in democratic processes, the European Parliament established the Special Committee on Foreign Interference in All Democratic Processes in the European Union, including Disinformation (INGE Committee), in June 2020. This body advocated for the creation of a joint operational mechanism to safeguard electoral systems, advancing the work of the European Cooperation Network on Elections (ECNE).

119 European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2018) "*Joint Report to the European Parliament, the European Council and the Council on the Implementation of the Joint Framework on Countering Hybrid Threats from July 2017 to June 2018*" (Report, JOIN (2018) 14 final, 13 June 2018). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018JC0014 [Accessed 3 May 2025].

Disinformation mitigation efforts were further reinforced through the European Commission's 2021 guidance to stakeholders on strengthening the Code of Practice on Disinformation. To support a more informed digital public sphere, the EU provided funding to the European Digital Media Observatory (EDMO) via the Connecting Europe Facility Programme, promoting collaboration between independent fact-checkers and academic institutions. Additionally, the Digital Education Action Plan (2021–2027) was introduced to enhance digital literacy and education across the Union, equipping citizens with the competencies required to critically engage with digital information environments.[120]

EU actions to prevent hybrid threats are correlated with the intellectual effort of the Helsinki-based European Centre of Excellence for Countering Hybrid Threats. Their definition covers the threats presented above. According to the COE, hybrid threats constitute "Coordinated and synchronised action that deliberately targets democratic states' and institutions' systemic vulnerabilities, through a wide range of means; The activities exploit the thresholds of detection and attribution as well as different interfaces (war-peace, internal-external, local-state, national-international, friend-enemy); influencing different forms of decision-making at the local (regional), state or institutional level to favour and/or obtain the agent's strategic goals while undermining and/or hurting the target".[121] Giannopoulos, G., Smith, H., and Theocharidou offer similar considerations.[122]

The EU has established a comprehensive framework for addressing hybrid threats, conceptualising them as a spectrum of coercive and subversive activities that remain below the threshold of the application of of international humanitarian law These threats, employed by both state and non-state actors, integrate conventional and unconventional methods to achieve strategic objectives while avoiding direct military confrontation. In response, the EU has implemented a range of measures, including strengthening cybersecurity, safeguarding critical infrastructure, and enhancing strategic cooperation with NATO. The EU's efforts are further reinforced by the European Centre of Excellence for Countering Hybrid Threats, based in Helsinki, which defines hybrid threats as coordinated actions designed to exploit systemic vulnerabilities and undermine the stability of targeted states.

120 "*Report on the Implementation of the 2016 Joint Framework on Countering Hybrid Threats*" (2018) *op. cit.*

121 Savolainen, J., Gill, T., Schatz, V., Ojala, L., Jakstas, T., Kleemola-Juntunen, P., Lohela, T. (ed.), and Schatz, V. (ed.) (2019) *Handbook on Maritime Hybrid Threats: 10 Scenarios and Legal Scans*, Hybrid CoE Working Papers, Helsinki: Hybrid CoE, p. 40. Available at: https://www.hybridcoe.fi/wp-content/uploads/2019/11/NEW_Handbook-on-maritime-threats_RGB.pdf [Accessed 3 May 2025].

122 Giannopoulos, G., Smith, H., and Theocharidou, M. (2020) "*The landscape of hybrid threats: a conceptual model*", European Commission, Ispra. PUBSY No. 123305, p. 41. Available at: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ [Accessed 3 May 2025].

Almost four horsemen of hybrid threats – definition proposal

The concepts of hybrid warfare, hybrid threat, and hybrid war were initially considered interchangeable. With an increasing number of operations not aligned to an armed conflict, predominantly in the information sphere, it became compelling to view hybrid threats and hybrid warfare as two distinct sides of the same coin.

Hybrid threats are harmful activities that are planned and carried out with malign intent. They aim to undermine a target, such as a state or an institution, through a variety of often combined means. Such means include information manipulation, cyber-attacks, economic influence or coercion, covert political manoeuvring, coercive diplomacy, or threats of military force. Hybrid threats describe a wide array of harmful activities with different goals, ranging from influence operations and interference all the way to hybrid warfare.[123]

Hybrid threats are primarily oriented toward democratic forms of governance and multilateral legal orders. Bilateralism and non-democratic forms of government appear more resilient to HT.[124]

Hybrid warfare and hybrid threats are understood here as two phases of the same phenomenon.[125] Similar findings are provided by Monaghan, who argues that hybrid threats and hybrid warfare occupy different spaces on the conflict spectrum. Hybrid threats are more likely to occur in the context of confrontation and the "gray zone", where the intensity of conflict is low but the probability of occurrence is high. In contrast, hybrid warfare belongs to the realm of armed conflict. These two concepts represent distinct phases and methods within the broader continuum of conflict.[126]

Most of the above discussion about the concepts of hybrid threats leads to the conclusion that the role of the media, especially in modern crowd mobilisations, cannot be overlooked. It encompasses not only historical examples such as Rwanda, but also contemporary instances, such as the Rohingya ethnic cleansing, the influence of ISIS, anti-Ukrainian propaganda in Russian media, Brexit, and the deep polarisation within democratic societies.

Considering the above together with the factors that create an environment conducive to hybrid operations could make it easier to identify potential threats as well as legal thresholds. In general, the success of hybrid threat operations is rooted in the identification and exploitation of the inherent structural vulnerabilities within the target states. Corruption plays a crucial role in infiltrating the various sectors of the target country, including its political, administrative, economic, defence, law enforcement, intelligence, social, and media systems. States that are impoverished, poorly governed, have a weak commitment to democracy and human rights, and are marked by ethnic and social tensions are especially

123 Giannopoulos, G., Smith, H., and Theocharidou, M. (2020) *op. cit.*, p. 41.
124 Johnson, R. (2021) *op.cit.*, p. 45.
125 Weissmann, M. (2021) *op.cit.*, p. 17–26.
126 Sean Monaghan (2019) *op. cit.* , p. 87.

susceptible to hybrid offensives.[127] McCulloch lists a number of elements of the successful hybrid campaign, such as a favourable "temporal, geographic, socio-cultural, and historical context", "a specific ideology within the hybrid force that shapes an internal narrative for the organisation", "deviation from conventional military strategies in pursuit of long-term survival", "asymmetry between hybrid forces and their potential adversaries" and a situation in which "a hybrid force incorporates both conventional and unconventional elements".[128]

Therefore, it is most compelling to locate hybrid threats and actions below the threshold of armed conflict. Hybrid threats constitute "the mixture of coercive and subversive activity, conventional and unconventional methods (i.e diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of warfare".[129] Or, as the author understands from the legal point of view, acts below the armed attack threshold or violation of the use of force in light of articles 2(4) and 51 of the UNC.[130] This very broad spectrum includes acts that range from elements of international politics up to the level of aggression. Once the threshold is crossed, we enter the realm regulated by the law of armed conflict, where hybrid warfare means and methods dominate. It does not, however, clear all doubts.

Firstly, what needs to be emphasised is the intrinsic nature of hybrid operations. They may be collaborative and joint in character. While each individual threat may not surpass the threshold of the mentioned Armed Conflict (AC) or violate the prohibition resulting from *ius ad bellum*, when combined, they may achieve objectives equivalent to the threshold of the use of force or constitute a "dispersed" armed attack. Typically, in international law, each situation is considered separately. However, hybrid threats should be scrutinised from the same centralised/orchestrated perspective. This parallels criminal law, where the concept of a criminal enterprise provides for punishment of even the less serious crimes committed within a larger scheme owing to the mere fact of participation in an organised group. This approach resonates with Giannopoulos *et consortes*, who articulate it as "a cascade effect, wherein activity in one domain may aim to affect a completely different domain from the one where the activity was detected".[131] This may lead to a situation where international lawyers and the security community miss the chance to grasp the bigger picture.

127 Racz, A. (2015) *op. cit.*, p. 88.

128 McCulloh, T. (2014) "*The inadequacy of definition and the utility of a theory of hybrid conflict: is the 'hybrid threat' new?*", School of Advanced Military Studies, Army Command and General Staff College, Fort Leavenworth, p. 24. Available at: https://apps.dtic.mil/sti/pdfs/ADA611608.pdf [Accessed 3 May 2025].

129 Cullen, P. (2021) "*A perspective on EU hybrid threat early warning efforts*", in Weissmann, M. et al (eds), *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, 1st edn, London: I.B. Tauris, p. 48.

130 United Nations (1945), "*Charter of the United Nations*", 24 October 1945, 1 UNTS XVI.

131 Giannopoulos, G., Smith, H., and Theocharidou, M. (2020) *op. cit.*, p. 12.

Secondly, certain acts play a dual role. The same narrative can be extended to the realm regulated by the law of armed conflict as well as to other states where IHL is not applicable. This makes hybrid threats truly one side of the coin, with hybrid warfare being the other.

To summarise the best definition based on a general concept rather than a descriptive approach to every threat, let me refer to the one coined by Hybrid COE and IISS. It is a "Coordinated and synchronised action, that deliberately targets democratic states' and institutions' systemic vulnerabilities, through a wide range of means (political, economic, military, civil and information), 2) Activities exploit the thresholds of detection and attribution as well as the border between war and peace, and 3) The aim is to influence different forms of decision-making at the local (regional), state, or institutional level to favour and/or gain the agent's strategic goals while undermining and/or hurting the target.[132] Another angle is presented by Jokinen and Normark, according to whom "The landscape of hybrid threats can be described as a continuum that encompasses conditions of peaceful influencing, interference and warfare aimed at priming, destabilisation or coercion by the hybrid threat actor of the targeted society".[133]

I propose an imperfect, albeit as general as possible, definition of hybrid threats

Violation or Not Distinction – The blending of civilian and military domains is a common feature in many of the concepts discussed above. However, it is not a defining element of hybrid threats. This is because the principle of distinction is a well-established cornerstone of International Humanitarian Law (IHL). While violations of this principle occur in armed conflict, hybrid threats primarily operate below the threshold of armed conflict. Nevertheless, the deliberate blurring of military and civilian spheres during peacetime is a characteristic of hybrid threats, posing significant challenges to the multi-domain security environment.

- plausible deniability and/or violation of state sovereignty. The lack of official attribution allows the execution of hybrid threats up to the level of violation of state sovereignty: this may include up to the level of the use of force and an armed attack:
  a. espionage.[134]
  b. sabotage.[135]

132 Weissmann, M. (2021) "*Conceptualizing and countering hybrid threats and hybrid warfare: the role of the military in the grey zone*", in Weissmann, M. et al (eds), *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, 1st edn, London: I.B. Tauris, p. 64.

133 Jokinen, J. and Normark, M. (2022) "*Hybrid threats from non-state actors: a taxonomy*", Hybrid CoE Research Report No. 6, June, p. 7.

134 Lanoszka, A. (2019) *op. cit.*, p. 178–179.

135 Lanoszka, A. (2019) *op. cit.*, p. 178–179.

  c. criminal disorder, whereby the belligerent's agents engage in hit-and-run attacks.[136]
  d. Fifth columns: groups of individuals, usually acting covertly, embedded within a much larger population which they seek to undermine.[137]
  e. Unmarked soldiers who are armed but lack the insignia that would identify them and their home government, proxies, cartels.
  f. Border skirmishes.
- cyber domain: another element of hybridity lies in cyberspace.[138] All actors use cyberspace for hardware attacks as well as for resourcing disinformation:
  - disinformation and online propaganda up to the level of the use of force and an armed attack (HT/HW).[139]
  - cyber-attacks up to the level of the use of force and an armed attack (HT/HW).
- lawfare – instrumentalisation and violation of international law for the purpose of hybrid threats.

To summarise, hybrid threats combine a wide range of non-IHL regulated means and methods to target vulnerabilities across the whole of society in order to undermine the functioning, unity, or will of their targets by degrading and subverting the *status quo*. This kind of strategy is used by revisionist actors to gradually achieve their aims without triggering decisive responses, including armed ones.[140] What seems universal for "hybrid threats" is the synchronised use of a broad continuum of instruments designed to remain below the thresholds of detection, attribution, and, foremost, retaliation,[141] or to provide otherwise to stay below the threshold of armed conflict and armed attack.

What has to be underlined from the perspective of the legal framework is that hybrid threats do not fall into the armed conflict spectrum. As such, hybrid threats should not be regulated by humanitarian law.

Defining the threshold: where do hybrid threats begin?

Hybrid threats manifest themselves in various legal shades, presenting a full spectrum of acts, from those akin to aggression, through hybrid threats that

136 Lanoszka, A. (2019) *op. cit.*, p. 178–179.
137 Lanoszka, A. (2019) *op. cit.*, p. 178–179.
138 Johnson, R. (2021) "*Hybrid warfare and counter-coercion*", in Johnson, R., Kitzen, M., and Sweijs, T. (eds), *The Conduct of War in the 21st Century: Kinetic, Connected and Synthetic*, London: Routledge, p. 47.
139 Lanoszka, A. (2019) "*Russian Hybrid Warfare*", *op. cit.*, 178–179.
140 Sean Monaghan (2019) *op. cit.*, p. 87.
141 Balcaen, P., Du Bois, C., and Buts, C. (2021) "*A game-theoretic analysis of hybrid threats*", in *Defence and Peace Economics*, p. 1. Available at: https://doi.org/10.1080/10242694.2021.1875289 [Accessed 3 May 2025].

necessarily involve the use or threat of force as defined by Article 2(4) of the UN Charter, or to acts which are merely international unpleasantries. An understanding of the relationship between hybrid threats and the applicable international law enables elaborating an appropriate framework to represent the phenomenon. Effective countermeasures require a thorough mapping of these threats and reliance on existing legal frameworks; – after all, repackaging of old concepts does not alter their essence.

Participants in the international legal order strive to avoid being labelled as aggressors, as such a designation not only constitutes a violation of the UN Charter but also harms their reputation in the eyes of the global community. A key characteristic of hybrid threats is their reliance on non-military means and methods to achieve multiple objectives, including military ones, across multiple domains. These operations are often deliberately designed to remain below the threshold of direct force or an armed attack.[142] While international law provides clear definitions for terms such as "armed attack", "use of force", "threat or use of force", and "aggression",[143] the hybrid threats environment introduces ambiguity, which is aggravated by the cascade effect.[144]

Whether and how hybrid threats violate the prohibition of the use of force in international relations will be explored in the subsequent section.

Hybrid threats and the use of force and the threat of use of force

Hybrid threats operate in a grey area and include the use of force leading to violations of states' sovereignty. The historical account of the Briand-Kellogg Pact reveals that the absence of repercussions for breaches ultimately leads to the further deterioration of legal order. When Japan launched an offensive against China in 1937, it euphemistically referred to its aggression as an "incident" or "*Shina jihen*", translated as the "China Incident", rather than calling it a "war", which would have had legal and diplomatic implications under international law.[145] Japan labelled the conflict an "incident" to downplay its scale and avoid triggering formal wartime responsibilities under treaties such as the League of Nations Covenant. Likewise, Mussolini's Italy described the 1935–36 annexation of Abyssinia as a "*civilising mission*" or "*pacification expedition (spedizione di pacificazione)*". By avoiding the term "war", Mussolini aimed to present Italy's campaign as both morally justified and

142 von Heinegg, W.H. (2020) *Internationally Legal Responses to Hybrid Threats*, Israel Yearbook on Human Rights, Volume 50, Brill Nijhoff, p. 218.

143 Klabbers, J. (2015) "*Intervention, "armed intervention, armed attack, threat to peace, act of aggression, and threat or use of force: what's the difference?*", in Weller, M. (ed.), *Oxford Handbook of the Use of Force in International Law*, Oxford: Oxford University Press, p. 488.

144 Giannopoulos, G., Smith, H., and Theocharidou, M. (2020) *op. cit.*, p. 12.

145 Duara, P. (2008) *Decolonization: Perspectives from Now and Then*, London: Routledge, p. 105–106.

legally permissible.[146] These understatements played a role in undermining the freshly established norms governing the use of force in international relations. The very wording, "an incident" or "an expedition", is not significantly different from the wording "a special military operation".

Article 2(4) of the UN Charter declares that all states 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 UN.[147] This principle is not unlimited; the inherent right of individual or collective self-defence and the exercise of UNSC powers under Chapter VII of the UN Charter, including the authorisation of military action, are considered legitimate exceptions.[148] The prohibition of the use of force was established through international consensus, and the international community accepts the prohibition of the use of force as well as the threat of the use of force.[149]

What constitutes a challenge is that the elements of hybrid operations often fall below the threshold of *ius ad bellum*. This is why certain states use hybrid means and methods to weaken the multilateral international consensus.

What constitutes the use of force under Article 2(4) of the United Nations Charter?

General prohibition of the use of force by one state against another was introduced by the UNC Article 2(4): "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".

The most serious and manifest illegal use of force against another state in violation of Article 2(4) was detailed in the General Assembly Resolution 3314

146 Baer, G.W. (1976) *Test Case: Italy, Ethiopia, and the League of Nations*, Stanford: Hoover Institution Press, p. 218.

147 UNGA Res 2625 (XXV) (24 October 1970). *The Organization and its Members, in pursuit of the Purposes stated in Article 1, shall act in accordance with the following Principles.*
4) 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. United Nations General Assembly (1970) *UNGA Res 2625 (XXV)*, 24 October. Available at: https://treaties.un.org/doc/Publication/CTC/uncharter-all-lang.pdf [Accessed 3 May 2025]. United Nations (1945) *Charter of the United Nations*, 24 October, 1 UNTS XVI. Available at: https://treaties.un.org/doc/Publication/CTC/uncharter-all-lang.pdf [Accessed 3 May 2025].

148 Blokker, N. (2000) *Is the Authorization Authorized? Powers and Practice of the UN Security Council to Authorize the Use of Force by Coalitions of the Able and Willing*, European Journal of International Law, Volume 11, No. 3, p. 541.

149 Kowalski, M. (2015) "*Ius ad bellum – systemowy charakter prawa międzynarodowego" / "Ius ad bellum – the systemic character of international law*", in Kwiecień, R. (ed.) *Państwo a prawo międzynarodowe jako system prawa / The State and International Law as a Legal*, Lublin, p. 176.

(XXIX) of 1974[150] and subsequently reaffirmed in the Kampala Amendment on the crime of aggression:

> Article 8 bis Crime of aggression
>
> 1. For the purpose of this Statute, 'crime of aggression' means the planning, preparation, initiation or execution, by a person in a position effectively to exercise control over or to direct the political or military action of a State, of an act of aggression which, by its character, gravity and scale, constitutes a manifest violation of the Charter of the United Nations.
>
> 2. For the purpose of paragraph 1, 'act of aggression' means the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations. Any of the following acts, regardless of a declaration of war, shall, in accordance with United Nations General Assembly resolution 3314 (XXIX) of 14 December 1974, qualify as an act of aggression:

a) The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof;
b) Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State;
c) The blockade of the ports or coasts of a State by the armed forces of another State;
d) An attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State;
e) The use of armed forces of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement;
f) The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State;
g) The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State

150 UN General Assembly (1974) "*Definition of Aggression*", 14 December, A/RES/3314. Available at: https://undocs.org/en/A/RES/3314(XXIX) [Accessed 3 May 2025].

> of such gravity as to amount to the acts listed above, or its substantial involvement therein.[151]

Even a brief analysis of hybrid threats indicates that they are unlikely to reach a result equal to the use of armed forces and fall into the category of prohibited use of force. The hybrid threat result must cause physical damage in order to be considered a use of force under Article 2(4) of the UN Charter. Hybrid threats which result "in death, injury, or significant destruction would likely be viewed as a use of force".[152] Harold Koh provides a number of examples of cyber activity that would constitute a use of force, for example: "(1) operations that trigger a nuclear plant meltdown; (2) operations that open a dam above a populated area causing destruction; or (3) operations that disable air traffic control resulting in airplane crashes".[153]

As of now, there are only a few examples of hybrid threats that have evolved or may be considered similar to acts of aggression: the so-called "little green men" and the annexation of Crimea; as well as very recent apprehension of Russian operatives allegedly planting explosive devices intended to destroy an aircraft that crashed in Koh requirements. At the same time, many hybrid threats may fall within the spectrum of interventions that undermine the sovereignty and political independence of other states.

Hybrid threats and the threat of use of force

Another question which has to be raised is whether hybrid threats are similar to the threat of use of force. In general, the prohibition of the threat of use of force has a customary and peremptory character,[154] similar to the prohibition of the use of force. In the Nuclear Weapons Advisory Opinion, the ICJ confirmed that the threat of use of force is equally unlawful as the actual use of force[155] The concept of threats is not a novel one. States were referring to threats on a number of occasions, *vide* Iran – Israel, North Korea, and the US.[156] Threats were also addressed directly or indirectly in a number of UNSC

151 International Criminal Court (2010) "*Amendments on the Crime of Aggression to the Rome Statute of the International Criminal Court*", Kampala, 11 June. Available at: https://asp.icc-cpi.int/iccdocs/asp_docs/RC2010/AMENDMENTS/CN.651.2010-ENG-CoA.pdf [Accessed 3 May 2025].

152 Borgen, C. (2012) "*Harold Koh on International Law in Cyberspace*", OpinioJuris. Available at: http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/ [Accessed 3 May 2025].

153 Borgen, C. (2012) *op. cit.*

154 Lagerwall, A., Dubuisson, F., and Weller, M. (2015) "*The Threat of the Use of Force and Ultimata*", in Weller, M. (ed.), *The Oxford Handbook of the Use of Force in International Law*, Oxford: Oxford University Press, p. 910.

155 International Court of Justice (1996) "*Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion)*", ICJ Rep 226.

156 Lagerwall, A., Dubuisson, F., and Weller, M. (2015) *op. cit.*, p. 911.

resolutions.[157] The threat of use of force necessitates a specific demand issued by one state, or a coalition of states, against another, alongside a specific threat of use of force. Brownlie's definition provides that "A threat of force consists in an express or implied promise by a government of a resort to force conditional on non-acceptance of certain demands of that government".[158]

Threats of force can be state issued or formally accepted within the context of collective security. For instance, in Resolution 678 (1990), the UN Security Council authorised the use of force against Iraq unless Iraq withdrew from Kuwait by a set deadline. The North Atlantic Treaty Organization (NATO) issued a threat of force in line with Resolution 836 (1993), while calling for the removal of heavy weapons from areas designated as safe zones by the UN in Bosnia and Herzegovina. In 1999, an international contact group threatened use of force unless the parties involved in the Kosovo conflict swiftly reached a political resolution in line with the Security Council resolutions.[159]

Importantly, the nature of the threat of use of force is the same as the use of force. As previously established, "force" refers to armed force; therefore, a number of non-military hybrid threats are excluded. Their legal status is fairly clear, as the UN Charter prohibits armed threats as well.[160] There are a few examples of such coercive measures accompanied by demands and threats for targeted states: "rearmament, military manoeuvres, establishment of military bases on the territory of a foreign State, bellicose declarations, concentration of troops along the borders, general mobilisation, and propaganda in favour of a war of aggression".[161]

The above excludes most of the hybrid threats discussed earlier, yet, at the same time, international public opinion has witnessed some such acts: for instance the Russian military build-up before engagement,[162] as well as aggressive language threatening countries engaged in support of Ukraine with an armed attack or articulating nuclear threats.

157 *Vide* United Nations Security Council (1964–1985) *Selected Resolutions*: Res.186 (4 March 1964), Res.187 (13 March 1964), Res.326 (2 February 1973), Res.411 (30 June 1977), Res.487 (19 June 1981), Res.573 (4 October 1985), UN Docs S/RES/186; S/RES/187; S/RES/326; S/RES/411; S/RES/487; S/RES/573.

158 Brownlie, I. (1963) *International Law and the Use of Force by States*, Oxford: Clarendon Press. Quoted in: Lagerwall, A., Dubuisson, F., and Weller, M. (2015) "*The threat of the use of force and ultimata*", in Weller, M. (ed.), *The Oxford Handbook of the Use of Force in International Law*, Oxford: Oxford University Press, p. 913.

159 Weller, M. (2015) "*Part I introduction: international law and the problem of war*", in Weller, M. (ed.), *The Oxford Handbook of the Use of Force in International Law*, Oxford: Oxford University Press, p. 19–20.

160 Lagerwall, A., Dubuisson, F., and Weller, M. (2015) *op. cit.*, p. 912.

161 Lagerwall, A., Dubuisson, F., and Weller, M. (2015) *op. cit.*, p. 913.

162 Jankovic, S. and Roeben, V. (2024) *The Threat of Russia's Force in Ukraine*, Journal on the Use of Force and International Law, Volume 11 , No. 1–2, p. 87–110.

What constitutes an armed attack under Article 51 of the United Nations Charter?

Under Article 51 of the UN Charter, states are entitled to self-defense if "an armed attack occurs against a Member of the United Nations". The debate over what constitutes an "armed attack" has persisted for many decades. It revolves around whether an armed attack should be understood as only the "most grave forms of the use of force" or if it also includes "less grave forms" of force.[163] Those attacks can be orchestrated by states and non-state actors.[164]

The understanding of what constitutes the occurrence of an armed attack of a certain gravity has always been crucial due to the fact that it triggers the right to lawful self-defense.

From the perspective of hybrid threats it could be observed that states use violence that constitutes a form of attack but not an armed attack, as foreseen in Article 51 of the UNC.

The notion of an armed attack necessarily requires resorting to arms and is therefore even less applicable to hybrid threats than general prohibition of the use of force.

Article 39 of the United Nations Charter as potential remedy for hybrid threats

Apart from more popular concepts dealing with the use of force, such as the crime of aggression and armed attack, Article 39 of the UNC (United Nations Charter) provides that

> The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations or decide what measures shall be taken in accordance with Articles 41 and 42 to maintain or restore international peace and security.

The ambiguity over the crime of aggression was resolved after several years by the Kampala Amendment.

While the assessment of threats to peace and breaches of peace is addressed separately by the UN Charter, there remains a clear central concept, a

163 *Vide* Military and Paramilitary Activities in and against Nicaragua, supra note 35, para. 191. *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, Judgment of 19 December 2005, [2005] ICJ Rep. 168, at 222 paras. 146–47. For state-centred statements see *Oil Platforms (Islamic Republic of Iran v. United States of America)*, Judgment of 6 November 2003, [2003] ICJ Rep. 161, at 186–187, 190–191 paras. 51, 61.; *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion of 9 July 2004 [2004], ICJ Rep. 136, at 194 para. 139. at 194 para. 139.

164 Arnold, R. (ed.) (2008) *Law Enforcement within the Framework of Peace Support Operations*, Leiden: Martinus Nijhoff, p. 14.

contested boundary, and overlapping areas of ambiguity between the two.[165] Most importantly, both concepts play a crucial role in the framework of hybrid operations. These threats include, *inter alia*, hybrid aggressor-induced or -exploited economic crises, energy insecurity, cybersecurity, disinformation, and transborder crime.[166]

"Threat to the peace" is the broadest and most encompassing concept derived from Article 39. In theory, the UN Security Council (UNSC) may identify a threat to peace arising from various actions by states. In practice, this term encompasses a wide array of scenarios, including armed conflicts, treatment of refugees, violations of peace accords, severe human rights abuses, illicit arms trafficking, the imposition of particular political systems within a state, discrimination against foreign economic interests in defiance of international standards, and the closure of ports to foreign vessels. The term is sufficiently expansive to encompass other circumstances as well. Article 39 grants the Security Council the authority to take preventative action even prior to the outbreak of armed conflict. Moreover, the notion of a "threat" to peace encompasses preventive measures that extend beyond scenarios of "imminent attacks".[167] In the context of hybrid situations, it is particularly important to highlight the ongoing debate about whether the actions of the Security Council (SC) are confined to conflict prevention or extend to broader measures addressing general threats, rather than being limited to specific conflicts. This debate has significantly influenced the Security Council's deliberations (and, to some extent, its actions) on issues such as non-proliferation, counterterrorism, the illicit exploitation of natural resources, and climate change. These topics often fall into the category of hybrid operations, especially given that Article 39 provides a legal basis for SC actions not only in the context of interstate conflicts (the classic example of a "threat to the peace") but also in internal situations.[168]

The list of threats to peace provided by the Commentary to the UNC includes those which may fall into the category of hybrid means and methods. The threats are divided into several categories, including: classical security threats; proliferation and arms control; terrorism; internal armed conflicts; and piracy (though limited to measures in Somali waters and not the Gulf of Guinea)[169]. Additional categories include threats to human security, such as

165 Krisch, N. (2012) "*Ch.VII action with respect to threats to the peace, breaches of the peace, and acts of aggression, Article 39*", in Simma, B., Khan, D.-E., Nolte, G., Paulus, A., and Wessendorf, N. (eds), *The Charter of the United Nations: A Commentary*, Volume II, 3rd edn, Oxford: Oxford University Press, p. 1279–1280.

166 European Parliamentary Research Service (2019) "*EU Response to Hybrid Threats*". Available at: https://www.europarl.europa.eu/RegData/etudes/IDAN/2019/637946/EPRS_IDA(2019)637946_EN.pdf [Accessed 3 May 2025].

167 Krisch, N. (2012) *op. cit.*, p. 1280.

168 Krisch, N. (2012) *op. cit.*, p. 1280.

169 Krisch, N. (2012) *op. cit.*, p. 1280–1283.

the protection of populations from genocide, war crimes, ethnic cleansing, and crimes against humanity; the protection of civilians in armed conflicts; human rights violations; conflict prevention and stabilization; and, potentially crucial in the context of hybrid threats, violations of democratic principles. Such measures were taken against Haiti, Sierra Leone, and Côte d'Ivoire.[170] What has to be underlined is that the violation of democratic standards as such does not constitute a threat to peace.[171]

Despite the fact that the Security Council practice usually does not rely on breach of peace and turns to the broader concept of a "threat to the peace", the concept itself is interesting, especially from a hybrid operations perspective.[172] In general, the "Breach of peace" denotes a situation more serious than a mere threat, yet one not escalated to the level described in the Definition of Aggression.[173] On the other hand, aggression is always considered as a breach of peace.[174] From a definitional standpoint, a breach of the peace is typically characterised by hostilities between the armed forces of two States. Also a breach of the peace can exist if force is used by or against an effective independent de facto regime which is not recognised as a State. The term should be understood to include "all situations in which a 'threat to the peace' is no longer merely a threat but has already materialised".[175]

It is up-to the Security Council to define what qualifies as a threat to peace and a breach of peace. The UN Charter entrusts the Security Council with the decision of whether to take action in a particular situation, and there is no obligatory requirement for the Council to issue a determination under Article 39. While the Council's authority in establishing what constitutes a threat to peace, breach of peace, or aggression under Article 39 has limits, it is not boundless. The Security Council frequently engages in discussions regarding the extent of its jurisdiction under Article 39.[176] As a result, the concepts are versatile and flexible.

These instruments are not perfect. There are limitations intrinsically related to the structure of the UN Security Council's P5, especially when one P5 member gravely violates very basic principles of international law. And yet, despite these limitations, the concept of a threat of peace/breach of peace is especially interesting, particularly in the context of the grey area of hybrid operations. Hence, the notion of a threat to peace as well as a breach of peace enables not only the classification within the current legal structure but, more

170 Krisch, N. (2012) *op. cit.*, p. 1284–1290.
171 Nico Krisch (2012) *op. cit.*, p. 1288.
172 Krisch, N. (2012) *op. cit.*, p. 1294.
173 Kleczkowska, A. (2022) "*Nord stream explosions as a breach of the peace*". Available at: http://opiniojuris.org/2022/10/31/nord-stream-explosions-as-a-breach-of-the-peace/ [Accessed 3 May 2025].
174 Krisch, N. (2012) *op. cit.*, p. 1294.
175 Krisch, N. (2012) *op. cit.*, p. 1294.
176 Krisch, N. (2012) *op. cit.*, p. 1276–1277.

importantly, incorporates them into the collective security apparatus, offering a robust solution, particularly when addressing hybrid threats.

The principle of non-intervention

At the core of the international legal framework governing state conduct lies the principle of non-intervention, which serves as a foundational norm in regulating the use of hybrid threats. This principle is deeply embedded in customary international law and codified in several key legal instruments. Most prominently, Article 2(1) of the United Nations Charter enshrines the principle of sovereign equality of states, while Article 2(4) explicitly prohibits the threat or use of force in international relations. Furthermore, Article 2(7) delineates the scope of domestic jurisdiction, affirming that the United Nations is not authorised to intervene in matters that are essentially within the internal affairs of any state.[177]

Complementing these provisions, the International Law Commission's (ILC) Articles on State Responsibility (2001) provide additional normative guidance.[178] Articles 20 and 22 articulate the circumstances under which the wrongfulness of an internationally wrongful act may be precluded, such as valid consent or countermeasures. Articles 49 to 51 further elaborate on the conditions and limitations of proportional countermeasures available to states in response to violations of international obligations. Historical treaty law also supports the non-intervention principle.[179] The 1936 International Convention on Broadcasting prohibits the transmission of propaganda intended to incite insurrection or otherwise disturb the internal order or security of another state.[180] This instrument illustrates early recognition of the risks associated with information-based interference, which has become a central feature of contemporary hybrid threats.

Importantly, the jurisprudence of international courts and tribunals has consistently upheld the non-intervention norm. In landmark decisions, such as those of the International Court of Justice (ICJ), the threshold for unlawful intervention has been clarified, especially regarding coercive measures that infringe upon the political or territorial integrity of states without the use of direct force.[181]

177 Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI.

178 International Law Commission (2001) "*Draft articles on responsibility of states for internationally wrongful acts*", II(2) *Yearbook of the International Law Commission*, p. 26.

179 Kress, C. (2015) "*The ICJ and the 'principle of non-use of force'*", in Weller, M. (ed.) *Oxford Handbook of the Use of Force in International Law*, Oxford: Oxford University Press, p. 563.

180 *International Convention on the Use of Broadcasting in the Cause of Peace* (adopted 23 September 1936, entered into force 2 April 1938) 186 LNTS 301.

181 Inter alia; *Corfu Channel Case (UK v. Albania)* [1949] ICJ Rep. 4., *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States)* [1986] ICJ Rep. 14.,

In the context of hybrid threats – characterised by ambiguity, deniability, and the strategic use of non-military means – the principle of non-intervention remains a critical legal benchmark. It delineates the boundary between lawful influence and unlawful coercion, serving as a conceptual and legal constraint on the conduct of both state and non-state actors engaged in hybrid operations.

Conclusions

As Colonel Sönke Marahrens suggests, perhaps hybridity is all morphing, and pursuing a black stone definition makes no sense.[182] Hybrid warfare and hybrid threats operate in spectrums and should be seen as two sides of the same coin, blurring the lines between the IHL and the law enforcement paradigm. Superpowers and regional players alike practise or advocate for the blurring of the line between war and peace. Hybrid threats easily fall into an inverted version of Clausewitz's formula: war is no longer the continuation of politics by other means, but politics is war waged by other means; therefore, politics is one of the instruments and one of the embodiments of war.[183]

Despite the challenges, there are common universal traits, for hybrid threats are operations in the spectrum of what the author calls the "Four (Three and a Half) Horsemen of Hybridity":

1) the cyber domain (including cyber-attacks and disinformation).
2) violation of the principle of distinction (noting that distinctions in the context of hybrid threats differ from those applicable in armed conflict).
3) violation of the principle of sovereignty, often accompanied by plausible deniability.
4) lawfare.

Bibliography

Books and Book Chapters

Arnold, R. (ed.) (2008) *Law Enforcement within the Framework of Peace Support Operations*. Leiden: Martinus Nijhoff.

Democratic Republic of the Congo v. Uganda (2005) ICJ Rep. 168, *Rio Tinto Zinc Corporation v. Westinghouse Electric Corporation* [1978] AC 547 – This case examined extraterritorial jurisdiction and the extent to which states can impose legal authority beyond national borders without violating the principle of non-intervention.

182 Marahrens, S. (2024) *Personal Interview with Colonel Sönke Marahrens, COE director*, 26 June 2023, Helsinki.

183 Davydenko, L. (2024) "*The development Of Russia's hybrid war doctrine*", TDHJ.org, 25 March 2024. Available at: https://tdhj.org/blog/post/development-russia-hybrid-war-doctrine/ [Accessed 3 May 2025].

Baer, G.W. (1976) *Test Case: Italy, Ethiopia, and the League of Nations*. Stanford: Hoover Institution Press.
Brownlie, I. (1963) *International Law and the Use of Force by States*. Oxford: Clarendon Press.
Clarke, M. (2019) 'China's application of the "three warfares" in the South China Sea and Xinjiang', *Orbis*, 63(2).
Crowther, G.A. (2021) 'NATO and hybrid warfare: seeking a concept to describe the challenge from Russia', in Weissmann, M., Nilsson, N., Palmertz, B. and Thunholm, P. (eds) *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. London: I.B. Tauris.
Cullen, P. (2021) 'A perspective on EU hybrid threat early warning efforts', in Weissmann, M., Nilsson, N., Palmertz, B. and Thunholm, P. (eds) *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. London: I.B. Tauris.
Cusumano, E. and Corbe, M. (2018) *A Civil-Military Response to Hybrid Threats*. 1st ed. Cham: Springer Nature.
Duara, P. (2008) *Decolonization: Perspectives from Now and Then*. London: Routledge.
Garner, B.A. (ed.) (2019) *Black's Law Dictionary*. 11th ed. St. Paul: Thomson Reuters.
Giles, K. (2015) *Handbook of Russian Information Warfare*. Rome: NATO Defense College.
Göransson, M. (2021) 'Understanding Russian Thinking on Gibridnaya Voyna', in Weissmann, M., Nilsson, N., Palmertz, B. and Thunholm, P. (eds) *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. London: I.B. Tauris.
Johnson, R., Kitzen, M. and Sweijs, T. (eds) (2021) *The Conduct of War in the 21st Century: Kinetic, Connected and Synthetic*. London: Routledge.
Jonsson, O. (2019) *The Russian Understanding of War: Blurring the Lines Between War and Peace*. Washington: Georgetown University Press.
Klabbers, J. (2015) 'Intervention, armed intervention, armed attack, threat to peace, act of aggression, and threat or use of force: what's the difference?', in Weller, M. (ed.) *Oxford Handbook of the Use of Force in International Law*. Oxford: Oxford University Press.
Kowalski, M. (2015) '"Ius ad bellum" a systemowy charakter prawa międzynarodowego/ "Ius ad bellum" and the systemic nature of international law', in Kwiecień, R. (ed.) *Państwo a prawo międzynarodowe jako system prawa / The State and International Law as a Legal System*. Lublin: Wydawnictwo KUL.
Kress, C. (2015) 'The ICJ and the "principle of non-use of force"', in Weller, M. (ed.) *Oxford Handbook of the Use of Force in International Law*. Oxford: Oxford University Press.
Krisch, N. (2012) 'Ch.VII action with respect to threats to the peace, breaches of the peace, and acts of aggression, Article 39', in Simma, B., Khan, D.-E., Nolte, G., Paulus, A. and Wessendorf, N. (eds) *The Charter of the United Nations: A Commentary, Volume II*, 3rd edn. Oxford: Oxford University Press.
Kupiecki, R. and Legucka, A. (2023) *Disinformation and the Resilience of Democratic Societies*. Warsaw: Polski Instytut Spraw Międzynarodowych.
Lagerwall, A., Dubuisson, F. and Weller, M. (2015) 'The threat of the use of force and ultimata', in Weller, M. (ed.) *Oxford Handbook of the Use of Force in International Law*. Oxford: Oxford University Press.
Lonardo, L. (2024) 'The seriousness of vagueness: introducing European law and policies against hybrid threats', in Lonardo, L. (ed.) *Addressing Hybrid Threats: European Law and Policies*. Cheltenham: Edward Elgar Publishing.

Maronkova, B. (2021) 'NATO amidst hybrid warfare threats: effective strategic communications as a tool against disinformation and propaganda', in Jayakumar, S., Ang, B. and Anwar, N.D. (eds) *Disinformation and Fake News*. Singapore: Springer.

Qiao, L. and Wang, X. (1999) *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House. Available at: https://www.c4i.org/unrestricted.pdf

Saalman, L. (2021) 'China and its hybrid warfare spectrum', in Weissmann, M., Nilsson, N., Palmertz, B. and Thunholm, P. (eds) *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. London: I.B. Tauris.

Spalding, R. (2022) *War Without Rules: China's Playbook for Global Domination*. New York: Penguin Random House.

Sun Tzu (1963) *The Art of War*. Translated by S.B. Griffith. Oxford: Oxford University Press.

Weissmann, M. (2021) 'Conceptualizing and countering hybrid threats and hybrid warfare: the role of the military in the grey zone', in Weissmann, M., Nilsson, N., Palmertz, B. and Thunholm, P. (eds) *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. 1st edn. London: I.B. Tauris.

Weissmann, M., et al. (eds) (2021) *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. London: I.B. Tauris.

Weller, M. (2015) 'Part I introduction: international law and the problem of war', in Weller, M. (ed.) *Oxford Handbook of the Use of Force in International Law*. Oxford: Oxford University Press.

Journal Articles and Papers

Abbasi, S.N. and Nasir, S. (2021) 'Hybrid Warfare: A Reorientation of Russian Foreign Policy in Syria', *Pakistan Journal of International Affairs*, 4(2). Available at: https://pjia.com.pk/index.php/pjia/article/view/177

Balcaen, P., Du Bois, C. and Buts, C. (2021) 'A Game-Theoretic Analysis of Hybrid Threats', *Defence and Peace Economics*, 32(7). Available at: https://doi.org/10.1080/10242694.2021.1875289

Blokker, N. (2000) 'Is the Authorization Authorized? Powers and Practice of the UN Security Council to Authorize the Use of Force by Coalitions of the Able and Willing', *European Journal of International Law*, 11(3).

Chekinov, S.G. and Bogdanov, S.A. (2013) 'The Nature and Content of a New-Generation War', *Military Thought*, October–December. Available at: http://www.eastviewpress.com/Files/MT_FROM%20THE%20CURRENT%20ISSUE_No.4_2013.pdf

Gerasimov, V. (2013) 'The Value of Science Is in the Foresight', *Voyenno-Promyshlennyy Kurier*, 27 February. Translated in: Bartles, C.K. (2016) 'Getting Gerasimov Right'. *Military Review*, January–February.

Glenn, R.W. (2009) 'Thoughts on Hybrid Conflict', *Small Wars Journal*, 2(1). Available at: https://smallwarsjournal.com/jrnl/art/thoughts-on-hybrid-conflict

Jankovic, S. and Roeben, V. (2024) 'The Threat of Russia's Force in Ukraine', *Journal on the Use of Force and International Law*, 11(1–2).

Johnson, R. (2018) 'Hybrid War and Its Countermeasures: A Critique of the Literature', *Small Wars & Insurgencies*, 29(1).

Lee, S. (2014) 'China's "Three Warfares": Origins, Applications, and Organizations', *Journal of Strategic Studies*, 37(2).

Marahrens, S. (2024) 'The Russia-Ukraine Conflict From a Hybrid Warfare Perspective', *Defence Horizon Journal*. Available at: https://tdhj.org/blog/post/russia-ukraine-hybrid-warfare/

Mumford, A. and Carlucci, P. (2022) 'Hybrid Warfare: The Continuation of Ambiguity by Other Means', *European Journal of International Security*, 8(2).

Savolainen, J., Gill, T., Schatz, V., Ojala, L., Jakstas, T., Kleemola-Juntunen, P., Lohela, T. (ed.) & Schatz, V. (ed.) (2019) *Handbook on Maritime Hybrid Threats: 10 Scenarios and Legal Scans*. Hybrid CoE Working Papers. Helsinki: Hybrid CoE. Available at: https://www.hybridcoe.fi/wp-content/uploads/2019/11/NEW_Handbook-on-maritime-threats_RGB.pdf

von Heinegg, W.H. (2020) 'Internationally Legal Responses to Hybrid Threats', *Israel Yearbook on Human Rights*, 50.

Wither, J.K. (2016) 'Making Sense of Hybrid Warfare', *Connections: The Quarterly Journal*, 15(2). Available at: https://connections-qj.org/article/making-sense-hybrid-warfare

Cases

Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment of 19 December 2005, [2005] ICJ Rep. 168.

Corfu Channel Case (UK v. Albania) [1949] ICJ Rep. 4.

International Court of Justice (1996) *Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion)*, ICJ Rep 226.

International Court of Justice (ICJ) (1996) *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, ICJ Reports 1996.

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion of 9 July 2004, [2004] ICJ Rep. 136.

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States) [1986] ICJ Rep. 14.

Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment of 6 November 2003, [2003] ICJ Rep. 161.

Rio Tinto Zinc Corporation v. Westinghouse Electric Corporation [1978] AC 547.

Treaties and Conventions

Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI.

International Convention on the Use of Broadcasting in the Cause of Peace (adopted 23 September 1936, entered into force 2 April 1938) 186 LNTS 301.

International Criminal Court (2010) *Amendments on the Crime of Aggression to the Rome Statute of the International Criminal Court*, Kampala, 11 June. Available at: https://asp.icc-cpi.int/iccdocs/asp_docs/RC2010/AMENDMENTS/CN.651.2010-ENG-CoA.pdf

Russian Federation (2010) *The Military Doctrine of the Russian Federation*. Approved by Presidential Edict on 5 February 2010

UN General Assembly (1970) *UNGA Res 2625 (XXV), 24 October*. Available at: https://treaties.un.org/doc/Publication/CTC/uncharter-all-lang.pdf

United Nations General Assembly (1974) *Definition of Aggression, A/RES/3314, 14 December*. Available at: https://undocs.org/en/A/RES/3314(XXIX)

United Nations (1945) *Charter of the United Nations*, 24 October, 1 UNTS XVI. Available at: https://treaties.un.org/doc/Publication/CTC/uncharter-all-lang.pdf

United Nations (2017) *UN Doc. A/CONF.229/2017/8, UN Doc. CN.476.2017. TREATIES-XXVI-9*. Available at: https://documents.un.org/doc/undoc/gen/n17/209/73/pdf/n1720973.pdf

United Nations General Assembly (UNGA) (1970) *Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in accordance with the Charter of the United Nations*, UNGA Res 2625 (XXV), 24 October.

United Nations Security Council (1964–1985) *Selected Resolutions: Res.186, Res.187, Res.326, Res.411, Res.487, Res.573*. UN Docs S/RES/186; S/RES/187; S/RES/326; S/RES/411; S/RES/487; S/RES/573.

Reports and Online Sources

Aukia, J. (2021) *China as a Hybrid Influencer: Non-state Actors as State Proxies. Hybrid CoE Research Report 1*. European Centre of Excellence for Countering Hybrid Threats. Available at: https://www.hybridcoe.fi/wp-content/uploads/2021/06/20210616_Hybrid_CoE_Research_Report_1_China_as_a_hybrid_influencer_Non_state_actors_as_state_proxies_WEB.pdf

Davydenko, L. (2024) *The Development Of Russia's Hybrid War Doctrine*, TDHJ.org, 25 March 2024. Available at: https://tdhj.org/blog/post/development-russia-hybrid-war-doctrine/

European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2016) *Joint Report to the European Parliament and the Council on the Implementation of the Joint Framework on Countering Hybrid Threats – A European Union Response* (JOIN(2016) 18 final, 6 April 2016). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018

European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2017) *Joint Report to the European Parliament and the Council on the Implementation of the Joint Framework on Countering Hybrid Threats – A European Union Response* (JOIN(2017) 30 final, 19 July 2017). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0030

European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2018) *Joint Report to the European Parliament, the European Council and the Council on the Implementation of the Joint Framework on Countering Hybrid Threats from July 2017 to June 2018* (JOIN(2018) 14 final, 13 June 2018). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018JC0014

European Parliamentary Research Service (2019) *EU Response to Hybrid Threats*. Available at: https://www.europarl.europa.eu/RegData/etudes/IDAN/2019/637946/EPRS_IDA(2019)637946_EN.pdf

Gardner, H. (2015) *Hybrid Warfare: Iranian and Russian Versions of "Little Green Men" and Contemporary Conflict*. Research Paper. Rome: NATO Defense College.

Available at: https://css.ethz.ch/en/services/digital-library/publications/publication.html/195396

Giannopoulos, G., Smith, H. and Theocharidou, M. (2020) *The Landscape of Hybrid Threats: A Conceptual Model*. European Commission, Ispra. PUBSY No. 123305. Available at: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

Hybrid CoE – The European Centre of Excellence for Countering Hybrid Threats (n.d.) 'Hybrid Threats as a Concept'. Available at: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

International Law Commission (2001) *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, II(2) *Yearbook of the International Law Commission*.

Jokinen, J. and Normark, M. (2022) *Hybrid Threats from Non-State Actors: A Taxonomy*. Hybrid CoE Research Report No. 6.

Jungwirth, R., Smith, H., Willkomm, E., Savolainen, J., Alonso Villota, M., Lebrun, M., Aho, A. and Giannopoulos, G. (2023) *Hybrid Threats: A Comprehensive Resilience Ecosystem*. Luxembourg: Publications Office of the European Union.

Kleczkowska, A. (2022) *Nord Stream Explosions as a Breach of the Peace*. Available at: http://opiniojuris.org/2022/10/31/nord-stream-explosions-as-a-breach-of-the-peace/

McCulloh, T. (2014) *The Inadequacy of Definition and the Utility of a Theory of Hybrid Conflict: Is the "Hybrid Threat" New?* School of Advanced Military Studies, Army Command and General Staff College. Available at: https://apps.dtic.mil/sti/pdfs/ADA611608.pdf

NATO Strategic Communications Centre of Excellence (n.d.) *Strategic Communications Hybrid Threats Toolkit*. Available at: https://stratcomcoe.org/pdfjs/?file=/publications/download/Strategic-Communications-Hybrid-Threats-Toolkit.pdf?zoom=page-fit

Olson, S. (2020) 'Are Private Chinese Companies Really Private?', *The Diplomat*, 30 September. Available at: https://thediplomat.com/2020/09/are-private-chinese-companies-really-private/

Praks, H. (2024) *Russia's Hybrid Threat Tactics Against the Baltic Sea Region: From Disinformation to Sabotage. Hybrid CoE Working Paper 32*. Available at: https://www.hybridcoe.fi/wp-content/uploads/2024/05/20240530-Hybrid-CoE-Working-Paper-32-Russias-hybrid-threat-tactics-WEB.pdf

Rácz, A. (2015) *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*. Report No. 43. Helsinki: The Finnish Institute of International Affairs

Russian Federation (2014) *The Military Doctrine of the Russian Federation*. Available at: https://rusmilsec.blog/wp-content/uploads/2021/08/mildoc_rf_2014_eng.pdf

Treverton, G.F., Thvedt, A., Chen, G., Lee, K. and McCue, M. (2020) *Addressing Hybrid Threats*. Helsinki: Hybrid CoE. Available at: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Treverton-AddressingHybridThreats.pdf

Websites

Borgen, C. (2012) *Harold Koh on International Law in Cyberspace*, OpinioJuris. Available at: http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/

Luhn, A. (2020) 'From Russia with Love': Coronavirus Disinformation and Aid to Italy. *Coda Story*. Available at: https://www.codastory.com/disinformation/russia-coronavirus-aid-italy/

Merriam-Webster Dictionary (n.d.) 'Hybrid'. Available at: https://www.merriam-webster.com/dictionary/hybrid

NATO (2014) *Wales Summit Declaration*, 5 September. Available at: https://www.nato.int/cps/en/natohq/official_texts_112964.htm

NATO (2016) *Warsaw Summit Communiqué*, 9 July. Available at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO (2018) *Brussels Summit Declaration*, 11 July. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_07/20180713_180711-summit-declaration-eng.pdf

NATO (2019) *London Declaration*, 4 December. Available at: https://www.nato.int/cps/en/natohq/official_texts_171584.htm

NATO (2022) *Madrid Summit Declaration*, 29 June. Available at: https://www.nato.int/cps/en/natohq/official_texts_196951.htm

NATO (2022) *Strategic Concept*. Madrid: NATO, 29 June. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

NATO (2023) *Vilnius Summit Communiqué*. Available at: https://www.nato.int/cps/en/natohq/official_texts_217320.htm

NATO (2024) *Washington Summit Declaration*, 10 July. Available at: https://www.nato.int/cps/en/natohq/official_texts_227678.htm

NATO (2025) *NATO Launches "Baltic Sentry" to Increase Critical Infrastructure Security*, 3 May. Available at: https://www.nato.int/cps/en/natohq/news_232122.htm

Oxford English Dictionary (n.d.) 'Hybrid, n. & adj.: Meanings, Etymology and More'. Available at: https://www.oed.com/dictionary/hybrid_n

Oxford University Press, Oxford English Dictionary, s.v. "threat". Available at: https://www.oed.com