




ARTICLE



<https://doi.org/10.1057/s41599-023-01864-y>

OPEN

The concepts and laws applicable to hybrid threats, with a special focus on Europe

Susana Sanz-Caballero  ¹✉

In this paper, the consequences of the lack of definition of so-called hybrid threats is explored. Special attention was paid to the importance of the work already completed by the North Atlantic Treaty Organisation (NATO) and the European Union (EU) regarding the ever evolving types of actions associated with hybrid threats in the so called grey zone. The latter can be thought of as activities undertaken by one state that are harmful to another, albeit not legal acts of war, sometimes referred to as a malevolent manifestation of the concept of peace. The vastly different experiences of democratic and authoritarian states acting in the grey zone was also examined. In addition, the law applicable to hybrid threats was studied to determine if the legal framework is sufficiently adapted to repel state-sponsored and non-state-sponsored hybrid threats. In addition, the use of the European Convention on Human Rights in the struggle against hybrid threats in Europe and the limits to how state parties can react to hybrid threats established by this treaty was analysed. Lastly, the international rules of attribution of responsibility and difficulties associated with their application with respect to hybrid threats was considered. This article is structured in two parts. The first part explores the difficulty of defining hybrid threats, while the second presents the legal framework used to counter such threats, both at the international and European levels.

¹University Cardenal Herrera CEU, Valencia, Spain. ✉email: ssanz@uchceu.es

Introduction

The question of how to fight hybrid threats with the tools of the law is fundamental, but by no means straightforward.

The adjectives used in this context, such as hybrid, grey, asymmetric, unbalanced, and unconventional, are not always interchangeable and are indicative of the lack of stability in this field. Indeed, when we try to apply the law to such threats, we often find that the sands shift beneath our feet. Moreover, the international environment is becoming increasingly hybrid in nature. International law is meant to promote security, justice, cooperation, predictability, and common values, but hybrid activities play the opposite role. In this sense, Aurel Sari mentions “the tragedy of international law” in his work (Sari, 2019, p. 4).

The legal tools, procedures, and institutions that exist today were created primarily to prevent and mitigate Cold War controversies and so there is a school of thought that they may no longer be completely suited to preventing the highly disconcerting and complex covert operations of the so called grey zone. The latter may consist of activities undertaken by one state that are harmful to another, although not legal acts of war, which can be thought of as a malevolent manifestation of the concept of peace. Of note, the order of the international environment has shifted from being fairly stable, with all the players understanding where their enemies lay, to a much more volatile post-Cold War era, defined neither by open conflict nor by enduring peace. In this sense, hybrid threats exist, by their very nature, in the realm of legal uncertainty. They remain below the threshold of warfare because of their low intensity.

Education, prevention, monitoring, and raising social awareness are powerful tools to combat hybrid threats, although even military means may be necessary. Hence, it can also be argued that international law, or even any law, may not be needed to counter such threats. However, hybrid threats usually navigate between the troubled waters of what is legal, illegal, and alegal. Therefore, the law applicable to the grey zone is needed to identify whether specific activities fall within the limits of legal order, and if not, further legislation will again be required to counter that action or behaviour.

The law helps to determine any possible illegal conduct and identify the guilty actors behind it. In other words, in modern societies, there is no other way to mitigate or neutralise possible unlawful behaviours and actions, except through application of the law. Thus, the question then becomes whether new legal mandates or structures are needed to combat these hybrid tactics or whether those already in place are sufficient to respond to hybrid threats and/or low-intensity conflicts. Conversely, should international law and in particular, humanitarian law, be changed to adapt to unarmed hybrid campaigns? However, before responding to these questions, the concept of hybrid threat itself should first be explored in detail.

Hybrid threats are poorly defined

Hybrid threats pose a real risk to states because their objective is to destabilise the adversary through ever-increasing means and tactics, which are not easy to detect, let alone attribute to a perpetrator, whether it be a state or not (Lonardo, 2021, p. 1075). This is why some authors argue that rather than seeking a consensus in defining hybrid threats, it might be better to analyse when state vulnerabilities tend to appear and determine how to combat them (Hickman et al., 2018, p. 6; Papadimos and Stawicki, 2021). Nevertheless, it is difficult to confront threats if we do not know what these phenomenon are or anything about their configurations. Even so, malign asymmetric threats are on the rise and so states and international organisations are being forced to start considering what actions they might use to counter

them. It is therefore important to agree upon a definition of hybrid threats that is broad enough to include as wide a range of means of state destabilisation as possible.

The North Atlantic Treaty Organisation (NATO) and European Union (EU) have provided their own tentative definitions of hybrid threats, while the United Nations (UN) is moving more slowly in this regard¹ (Broeders et al., 2002, pp. 98). According to the 2010 NATO Strategic Concept, hybrid threats are “those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives”². As for the EU, the European External Action Service states that “hybrid campaigns are multidimensional, combining coercive and subversive measures, using both conventional and unconventional tools and tactics. They are designed to be difficult to detect or attribute. These threats target critical vulnerabilities and seek to create confusion and hinder swift and effective decision-making”³ (Galinek et al., 2019; Bazarkina, 2022). Nonetheless, rather than issuing a perfect definition of hybrid threats, which in fact does not exist because they vary in each case, both NATO and the EU advocate for the characterisation of such threats and provision of a list of their more general characteristics. Thus, their definition remains open to interpretation.

Characterising hybrid threats. Without a doubt, reaching a consensus on a definition of hybrid threats that is acceptable for every stakeholder is exceedingly difficult (Winja, 2021). Nevertheless, it is particularly important to at least understand some of their characteristics. Hybrid threats revolve around the ideas of asymmetry, polymorphism, inequality, unaccountability, escalation, adaptability, multidimensionality, insidiousness, undetectability, gradualism, offensiveness, concealment, secrecy, ambiguity, opportunism, indeterminacy, disruption, manipulation, distortion, denial, ungovernability, misinformation, unlawfulness, usurpation, and amorality, among others⁴. On the one hand, this list of characteristics demonstrates that hybrid threats encompass a mixture of some truly unlawful acts but also some other simple, unethical behaviours and activities. On the other, the previously mentioned open-ended list implies that hybrid threats include any action, whether it be state-led or non-state led, designed to destabilise a given society.

Thus, hybrid threats consist of political activities, (dis)informational campaigns, and cyber, military, economic, and societal interventions. Moreover, although cyber-based threats are polemic, they represent only one of the domains in which hybrid threats may occur. Indeed, the ‘weapons’ used in the grey zone could include computers, border gates, fake news, drones, cyber-troll farms, radio stations, hijacked aircraft or ships, and spy balloons crossing into airspace not belonging to its jurisdiction of origin. A non-exhaustive list of hybrid threats would also include cyberattacks, terrorism, organised crime, drug trafficking, migration flows, economic or financial wars, media exploitation, and the application of covert psychological operations. The most updated catalogues of hybrid threats intertwine multiple political, economic, technical, social, informational, legal, diplomatic, scientific, and military risks (Galán, 2018, p. 3). In fact, nowadays any threat has a potential to become a hybrid threat because the nature of these hazards is that they are always evolving. The only exception to this is probably the case of a threat that is part of a declared war, whereby the strategy or action cannot then be considered hybrid.

The Centre of Excellence for Countering Hybrid Threats and the European Commission has identified different areas of vulnerability, including infrastructures, cyber spaces, the

economy, defence, intelligence, legal, political, and societal areas, space, distributed (dis)information, and public administrations (Com and Hybrid, CoE, 2021, pp. 26–36). Of note, some of the aforementioned activities, such as the sonic attacks upon American diplomatic agents in Cuba (ABC, 2021), could be seen as simple ‘incidents’. In the same vein, the state-sponsored mass movement of irregular migrants is a clear weaponisation of migrants. Examples of the latter are the events of May 2021 at the Moroccan–Spanish border or at the Belarusian–Lithuanian border in June 2021. Rather cynically, these migrants have been called ‘human bullets’ or their activity referred to as ‘migrant diplomacy’ (Mestre, 2021). Nonetheless, this strategy can also be labelled as a massive violation of national borders (Kotoulas and Pusztai, 2020, p. 4; Ploumis, 2021, p. 344).

Furthermore, some lawful activities such as supporting the self-determination of a territory, protecting nationals abroad, investing heavily in a particular foreign country, claiming sovereignty over a man-made island, or granting nationality to certain individuals are not unlawful per se, although some of their consequences could be unlawful (Hickman et al., 2018, p. 37). These consequences can include the recognition of a new state in a territory that is already part of an existing state or the annexation of a territory. Another highly effective hybrid tactic is seizing full control of a foreign state’s finances. Violation of the 1982 UN Convention on the Law of the Sea by unilaterally extending maritime boundaries in contravention of the intangibility of borders should also be mentioned. This is a way of reinterpreting history to create a new narrative, which is being leveraged to rewrite international rules that were carefully drafted after the Second World War.

The latter is known as the instrumental use of law: its misrepresentation by deliberately changing legal paradigms. Another manipulation often used by radicals to abolish public discourse critical to these groups is the abuse of legal procedures as a weapon of mass disinformation, as has been observed, for example, in the case of certain extremist Islamic factions. This can cause a powerful and damaging cooling effect on public dialogue in democratic societies (Lahmann, 2022, vol. 33, p. 411). Some of the latest hybrid threat activities observed are likely to have taken place in Ukraine in the aftermath of the Russian invasion and even before that, during the annexation of Crimea in 2014. Indeed, this conflict involves the contemporary tactics of the spread of propaganda, kinetic attacks, and espionage (Kong and Marler, 2022).

Democratic versus authoritarian regimes. Experience has shown that unscrupulous actors who confront law-abiding states are always one step ahead and can take advantage of the situation, manipulating it into unimaginable scenarios. Hybrid threats are often used by weaker actors against more powerful ones while using calculated ambiguity because the rules of the attribution of responsibility are not clearly applied in the grey zone. Indeed, hybrid threats are mainly used by those who cannot meet the military capabilities of their adversaries, applying a logic that includes the use of asymmetric means and procedures. This kind of strategy is used by an overlapping group of states, but also by parastatal actors, autonomous groups, proxies, authorised private military entities, paramilitaries, irregular actors, subversive elements, mercenaries, contractors, criminals, partisans, terrorist groups, drug traffickers, state and non-state-affiliated hackers, activists, and protesters, among others.

Many of these entities act under foreign influence, foreign orders, or are sponsored by a state, although this may not always be the case and sometimes, they act alone. Actors using hybrid threats often launch sophisticated (dis)information campaigns to

discredit law-abiding regimes, undermining their credibility by manipulating public opinion in open societies in which the flow of information is free. Autocracies tend to be more willing to use hybrid threats and proxies because they are less constrained by people’s reactions to their actions and they have more centralised decision-making processes compared to their democratic counterparts. Therefore, autocracies better serve the purposes of non-compliant actors and authoritarian regimes (Carment and Belo, 2020, p. 21).

In contrast, democracies are scrutinised by their own media, public opinion, and the electorate. Thus, hybrid threats undermine democratic societies by provoking citizen distrust in state institutions, eroding trust in democracy itself and in specific democratic regimes, especially because they also jeopardise social cohesion. Of note, the real target of hybrid threats is the population of a given state, which is much more vulnerable in open and law-abiding societies. In fact, it has been argued that hybrid threats are “becoming the standard for disrupting a society’s ability to function” (Gaiser, 2019, p. 20). Indeed, the ambiguity inherent in hybrid threats challenges individuals who respect human rights and abide by international law in good faith. Law-abiding actors are more constrained than non-compliant actors because when the former act, they must respect the rule of law and ethics, whereas non-compliant actors interpret these lawful reactions as a weakness. Hence, law-abiding states are at a disadvantage because they are bound by international law when responding to hybrid threats, especially by the International Law of Human Rights. As a result, they never fight adversaries on the same terms as non-compliant states or actors (European Center of Excellence for Countering Hybrid Threats, 2021, p. 14).

Especially in Europe, any reaction to a hybrid threat from an EU member state must respect the European values recognised in Article 2 of the EU Treaty, including the rule of law, pluralism, equality, and human rights. Conversely, those planning a hybrid threat base their strategy on the idea that the victim state will adhere to legal and ethical standards. This is because if the latter does not respect the established order, citizen support for public institutions will fall, eroding the democratic system itself. From this perspective, adherence to democratic values is perceived as vulnerability (Lonardo, 2021, p. 1,080). In short, democratic states are more vulnerable to delegitimisation, discrediting by citizens, and negative international reactions. On the contrary, authoritarian states often have nothing to lose or fear in this sense because they are not accountable to their own population (Carment and Belo, 2018, p. 11). That said, there are other theories that autocrats sometimes enjoy broad support. As Przeworski argues, “when people cannot object, the absence of protests is uninformative: we cannot tell whether they do not protest because they believe that the government is acting in their best interest or because they fear repression” (Przeworski, 2022, pp. 15).

The law applicable to hybrid threats and the risks of ‘Lawfare’

Given the presence of hybrid threats, traditional rules-based order may be insufficient. This is because the application of international law is clearly contested by both non-state and state actors using hybrid threats to pursue their objectives, with one of the most recent examples of this being the actions of Russia in Ukraine. By annexing Crimea in 2014 and Donetsk, Kharkiv, Kherson, Luhansk, Mykolaiv, and Zaporizhzhia in 2022 and 2023, Russia violated the sacred principles of international law. By subsequently artificially issuing Russian passports to residents in the annexed Ukrainian territories, on a massive scale, Russia created a basis upon which to claim its right to protect its

nationals living abroad and to support these regions in declaring independence from Ukraine. Indeed, Russia is a leader in the use of legal arguments to support hybrid tactics (Chivvis, 2017, p. 3; Janičatová and Mlejnková, 2021, p. 313). One of its favourite hybrid tactics is to raise doubts about whether a given act is legitimate under international law. The confusion of implementing a new and controversial practice helps change the status quo and established norms, establishing an argument for *opinio juris*—the belief that an action was carried out as a legal obligation (Schmitt, 2017, p. 20). In fact, one of the goals of this strategy is to create a new norm of *lex ferenda* (‘with a view to a future law’).

It might be useful to give a few examples of this practice here. Firstly, it can be said that when China refused to enforce a Permanent Court of Arbitration ruling against its interests, it challenged the authority of the international courts (Sari, 2020, p. 8). Second, by using mercenaries in Syria and Libya, Turkey advanced without needing to send its troops abroad. Third, by attacking basic infrastructures such as electricity supplies to hospitals or the social security system, hackers caused panic and tried to discredit Spain’s state services. Fourth, when Boko Haram abducted 200 Nigerian schoolchildren, they used the media as a loudspeaker for its terrorist agenda (Bachmann, 2015, p. 90). Finally, by placing human shields near military objectives, Hamas prevented Israel from protecting itself from terrorism and undermined governmental support (Sari, 2020, p. 11). So, the question remains, is existing international law sufficient to cover current hybrid operations or should new norms be negotiated within the international community?

After the Second World War, the UN abolished the use of force, as set out in Article 2.4 of the Charter. The only exceptions to this prohibition are self-defence and the use of force when requested or authorised by the Security Council (Chapter VII of the Charter). In parallel, Article 2.7 of the Charter clarifies that nothing authorises the UN to interfere “in matters which are essentially within the domestic jurisdiction of any state.” The UN General Assembly Resolution 2625 (XXV)⁵, part of whose content is customary law, adds that:

(...) States have the duty to refrain from propaganda for wars of aggression (...), States have a duty to refrain from acts of reprisal involving the use of force (...), Every State has the duty to refrain from organising or encouraging the organisation of irregular forces or armed bands, including mercenaries, for incursion into the territory of another State (...), Every State has the duty to refrain from organising, instigating, assisting or participating in acts of civil strife or terrorist acts in another State or acquiescing in organised activities within its territory directed towards the commission of such acts, when the acts referred to in the present paragraph involve a threat or use of force.

Likewise, for decades, the four Geneva Conventions of 1949, and their two additional protocols of 1977, have provided sufficient guidelines for managing conventional wars through the *jus in bello* (international law regulating behaviour in war). However, in the present context of hybrid operations, the laws of war are vague, and their application is insufficiently clear. Thus, the UN and the Geneva Conventions are inadequate instruments for the purpose of de-escalating grey-zone conflicts. One of the main reasons for this is the opacity of activities taking place in the grey zone, as well as the regular involvement of non-state actors. In addition, state sovereignty is being challenged under international human rights law. As Rousseau stated, “The shift in emphasis in international law from sovereignty to humanitarian principles has created a gap between peace and war that State and non-State actors exploit through measures short of war” (Rousseau, 2017, p.

2). Furthermore, respect for the law, including the International Law of Human Rights, has come under constant scrutiny since the Second World War. While this increased legalism is undoubtedly a strength for democratic societies, in the age of social media, it is also challenging. Multiple misinterpretations of the law are fabricated and it is also invoked as a means to challenge the actions of our opponents (Sari, 2020, p. 11) or, conversely, it is used to justify our own actions.

‘Lawfare’ is the use of the law to deliberately twist and bend legal paradigms and is therefore, a key component of hybrid warfare (Bachmann and Muñoz Mosquera, 2015, p. 26.). The use of democratic norms and standards against democracy itself is a weaponisation of the law. It is also a strategy increasingly used as a hybrid tactic in the grey zone. Lawfare presupposes the abuse of legal procedures as a weapon of mass disinformation. This manipulation of norms has a crippling, nefarious effect on democratic societies. In fact, deliberate misinterpretations of the law are often meant to bring about changes in customary law through state practice. An example of this is China’s rights of transit passage through a strait in the South China Sea, which is in clear contradiction with the UN Convention on the Law of the Sea. This could expand the area China controls in this area without the need for force. Generally speaking, politically motivated use of the law is standard. What makes it a hybrid threat is any malicious intent to weaken states, subvert democratic governments, annex territories, breach previous international agreements, or maliciously access other markets, etc.

Thus, hybrid threats have generated a serious legality problem with regard to the laws of war, right to self-defence, legitimacy of pre-emptive measures, and use of countermeasures in response to these opaque offensive tactics. As already mentioned, an additional risk of hybrid threats is that they might change existing customary international law in these fields by reinterpreting legal norms in a misleading manner (Moeckli et al., 2022; Cardona, Sanz-Caballero, and Arrufat, 2022). The North Atlantic Treaty itself is insufficiently clear as to the threshold intensity an attack must reach to permit the use of the collective security mechanism established in its Article 5. By definition, hybrid adversaries avoid any overt use of force. Hence, if a hybrid operation does not reach the required intensity level, the use of force in self-defence will be out of the question and *jus ad bellum* (international law regulating the resort to force) and *jus in bello* will not apply. Therefore, without firing a shot, hybrid adversaries can achieve their objectives and evade retaliation. Moreover, the question of attribution and thus, accountability, may also raise difficulties because hybrid adversaries will always deny involvement in such activities.

Nonetheless, although hybrid adversaries may operate in a grey zone, they do not operate in a legal vacuum. International law in general, and international human rights law in particular, still apply. It is also important to note that countering hybrid threats is a state competence and state responsibility⁶. While countering hybrid threats requires close collaboration between NATO and the EU (Argumosa Pila, 2019, p. 10; Bajarūnas, 2020), the primary responsibility for responding to them lies with the target state (Gaiser, 2019, p. 19). Therefore, the actions and offences of hybrid adversaries must be examined through the lens of national law, especially national criminal law, including anti-terrorism legislation, domestic telecommunications law, counter-espionage rules, property rights, and all legislation against hate speech, cybercrime, and money laundering. As already stated, hybrid threats do not qualify as military actions and so they do not fall within the scope of international humanitarian law. Therefore, states are bound to deal with hybrid attacks by means of their own national legislation, usually by applying their national criminal code, although civil legislation is sometimes also

employed. Indeed, this is the case in illegal cyberspace operations that amount to espionage, theft, and property damage, or in hybrid actions involving human trafficking.

While the right to respond to hybrid attacks rests with the victim state, the role of NATO should not be ignored when one of its member states is the victim of such tactics. However, to trigger application of Article 5 of the North Atlantic Treaty, NATO must be completely certain about the origin and severity of the attack suffered by its member. Yet certainty is precisely what is lacking in any hybrid attack: by their nature, hybrid threats are unclear, opaque, and uncertain. When Article 5 is not applicable, which is usually the case, Article 4 of the Treaty then comes into play (Lanz Raggio, 2019, p. 36). Hence, hybrid threats can be addressed through this other provision, which stipulates that NATO members may “consult together whenever (...) the territorial integrity, political independence or security of any of the Parties is threatened”. Notwithstanding, as it stands today, the structure of NATO and its *raison d'être* is basically geared towards ensuring collective defence in inter-state conflicts, not countering hybrid threats through Article 4.

Regarding the EU, Article 42.7 of the EU treaty contains a clause on mutual assistance in the event of armed aggression, although, to date, this article has never been activated. However, the threshold for providing assistance is an armed aggression, meaning that hybrid threats are easily immune to this clause. Nonetheless, from among the tools the EU has at its disposal in the case of a threat, special attention should be paid to the solidarity clause in Article 222 of the Treaty on the Functioning of the EU in the case of natural or man-made disasters or terrorist attacks. Thus, in terms of the tools available to counter ongoing hybrid threats, it must be recognised that the EU is better equipped than other areas of the world to fight some specific types of attack. First, the EU has regulatory tools against disinformation; second, it has common trade policy regulation to tackle trade defence; third, the EU has instruments to deal with hostile foreign investment; fourth, it also has instruments to fight cyberspace crime; and lastly, the EU has Frontex, an agency whose responsibilities include countering border pressure (Lonardo, 2021).

In grey zone conflicts, both state and non-state actors often challenge legal and informational boundaries. Indeed, hybrid threats undermine the principle of good faith enshrined in Article 2.2 of the UN Charter (De Espona, 2019, p. 68). They maliciously produce legal ambiguity and blur the lines between what is ‘normal’ or not in international relations. They circumvent legal boundaries and, in so doing, prevent or at least hinder the application of any mutual assistance clauses such as those established for the EU, NATO, and UN in articles such as Article 222 of the Treaty on the Functioning of the EU, Article 42 of the EU Treaty, Article 5 of the NATO Treaty, and Article 51 of the UN Charter. Notwithstanding, hybrid threats are becoming increasingly sophisticated. While theoretically encompassing both violent and non-violent behaviour, it is rare for hybrid threats to reach a level of seriousness that can be considered the use of force, which therefore precludes the application of the principle of self-defence. Indeed, hybrid strategies do not usually reach a level of intensity that allows the victim state to first detect it and then intervene. Rather, they create a grey zone that is neither war nor peace (Army Air Force Center for Low Intensity Conflict, Langley Air Force Base, Virginia: 1987, p. 3; The Hague Centre For Strategic Studies, 2020; Kittichaisaree, 2017).

In the EU, NATO, and worldwide, states should be able to react and counter hybrid threats through proportionate countermeasures (both retaliatory and reprisal measures). However, the victim state’s response to hybrid threats will be limited by international law, especially by international human rights law.

Depending on the type of threat, other international legal norms such as sea, air, border, or refugee law or counterterrorism treaties, among others, might also apply. Unfortunately, there are serious difficulties in harmonising human rights law with the measures that victim states take when reacting to hybrid threats. These measures may, in turn, violate human rights, for example, when implementing anti-terrorist legislation, legislation to limit the internet, regulate the media, or change migration law.

Hybrid threats and the European Convention on Human Rights.

By analogy, in accordance with paragraph 2 of Articles 8 to 11 of the European Convention on Human Rights (ECHR), responses to hybrid threats should be established by law, pursue a legitimate aim, and be necessary for a democratic society. Of note, in the case of a large-scale hybrid or non-military action, European states can always invoke Article 17 of the ECHR in their favour. This article prohibits the abuse of rights and is closely related to the principle of good faith in international relations. Similarly, in the event of a national public emergency, Article 15 of the same convention allows state parties to suspend their obligations under the ECHR, except for the application of the right to life, prohibition of torture, slavery, the death penalty, and double jeopardy, as well as the principle of *nulla poena sine lege* (‘no punishment without law’)⁷. For example, during the COVID-19 pandemic, Serbia, Romania, North Macedonia, Albania, Georgia, Estonia, Moldova, Armenia, and Latvia notified the Secretary General of the Council of Europe that they would withdraw from their treaty obligations, providing their reasons for this decision.

In the legal case, *Big Brother Watch and others vs. United Kingdom* (request no. 58170/13, Judgement of 25 May 2021), the ECHR stated that the law restricting rights on national security grounds must be accessible, predictable, and detailed. They added that “before the intelligence services used selectors or search terms known to be connected to a journalist (...) the selectors or search terms had to be authorised by a judge or other independent and impartial decision-making body vested with the power to determine whether they had been ‘justified by an overriding requirement in the public interest’ and, in particular, whether a less intrusive measure might have sufficed to serve the overriding public interest” (paragraph 228 of the judgement). However, in the *Zana vs. Turkey* case (request no. 18754/91, Judgement of 25 November 1997) the Court did not condemn Turkey for its decision to ban incitements to violence, stating that incitement to violence cannot be considered a manifestation of the right to freedom of expression. In the same vein, in the *Seurot vs. France* case (request no. 57383/00, Judgement of 18 May 2004), on the dismissal of a teacher because of his writings, the Court found that the ECHR did not protect hate speech.

Additionally, Article 18 of the ECHR states that restrictions shall only be applied for the purpose for which they were prescribed, and so the victim state must be incredibly careful and strict about their application. For instance, some states have recently passed anti-terrorism, espionage, or anti-hate speech legislation that could obstruct the enjoyment of human rights. The problem is that in the grey zone it is exceedingly difficult to draw the line between, on the one hand, the freedom of expression of activists and citizens, and on the other, interference with the sovereignty of the victim state. Nonetheless, despite the aforementioned shortcomings of the ECHR, it would be wrong to think that international law is no longer fit or cannot deal with scenarios involving the increasing incidence of hybrid threats. Hybrid threats are not new. The problem is that we are now more aware of the dimensions of the problem and we have a common name for these risks. Unfortunately, almost anything now

qualifies as a hybrid threat. International law is more necessary than ever. Indeed, there are no alternatives for combating hybrid threats beyond international law; *sicut societas, sic ius* ('where there is society, there is law'). Thus, international institutions, including the UN, Council of Europe, NATO, and EU are bound to adapt their structures and procedures to cope with these new tactics in order to improve their resilience. However, finding consensus for reform might not be as necessary.

The major problem of the attribution of responsibility. States often use proxies to operate in the grey zone. However, the indication that a hybrid threat originated in the territory of a state is insufficient by itself to be able to attribute the act to that state. To attribute a specific act performed by a person or a group to a specific state, extremely strict conditions must be met, with this requiring the presence of several elements that are usually difficult to prove. This is why grey zone operations often produce easy rewards for those using such strategies and is also why deterrence with proxies or other entities operating in the grey zone often do not work. This is because opponents using the grey zone are not acting in good faith; they try to erode the entire international legal system. They cannot change the law *de jure* (legally recognised practices) and so they try to do it *de facto* ('that which exists in reality,' regardless of its legal basis and without preventing it from having legal effects). This is why it is so important that these adversaries are unmasked and identified, despite this being such a difficult task. If the aggressor is subject to international law, the rules on international responsibility will also obviously apply (López-Casamayor Justicia, 2019, p. 193; De Salas Claver, 2019, p. 139).

This is where the Articles on the Responsibility of States for Internationally Wrongful Acts of 2001⁸ and the Articles on the Responsibility of International Organisations of 2011⁹, drafted by the International Law Commission, come into play. Although these texts are not yet treaties, some of their contents express customary law. However, it is important to recognise that these texts only consider the international responsibility of the two established subjects of international law, namely, states and international organisations. To hold the aggressor accountable, it must be determined who had control over the operation or who sponsored the aggressors. Unfortunately, the International Law Commission does not consider the international responsibility of non-state actors in the drafts of these two texts. When a non-state actor is identified as responsible for a hybrid threat, the general rule is that the national criminal law of the victim state will be applied (De Wet, 2019, pp. 91–110).

The main provisions of the Articles on Responsibility of States for Internationally Wrongful Acts of 2001, provide that two conditions must be met for an action or omission of a state to be considered an internationally wrongful act. First, the act or omission must be attributed to the state according to international law and, second, this state must have breached an international obligation (Article 2). The articles on state responsibility also consider the conduct of a person or entity that is not a state organ but is "empowered by the law of that State to exercise elements of the governmental authority" and "shall be considered an act of the State under international law, provided the person or entity is acting in that capacity in the particular instance" (Article 5). Furthermore, the Articles state that the conduct of organs of the state or of persons or entities empowered to exercise governmental authority should be considered an act of the state, even if they exceed their powers or contravene orders (Article 7).

Likewise, the conduct of a person or group of people will be considered an act of state whenever following the instructions of a

state or under the direction or control of a state when implementing the conduct (Article 8). Similarly, "the conduct of a person or a group of persons shall be considered an act of a State under international law if the person or group of persons is in fact exercising elements of the governmental authority in the absence or default of the official authorities and in circumstances such as to call for the exercise of those elements of authority" (Article 9). Article 11 is a closing provision whereby any conduct that is not attributable to a state according to the previous provisions will, nevertheless, be ascribed to that state in the event that it accepts and adopts this conduct as its own. Thus, the aforementioned Articles provide sufficient room to combat state-sponsored hybrid tactics, both 'with' and 'within' international law. However, two main problems remain: first, hybrid threats that are not attributable to a state, and second, the question of identifying the hybrid aggressors themselves.

Conclusions

Despite the ongoing unresolved debate over the real need for a definition of hybrid threats, there is an international consensus that hybrid threats represent a growing security problem. Addressing these threats is a major challenge because, in addition to being a never-ending task, this process erodes democracy from within. The grey zone is the arena in which actors operate on the fringes of legality. Threats in the grey zone are always evolving and so our responses must also be proactive and flexible. Hybrid operations constantly and surreptitiously undermine the ability of states to function. If a state uses hybrid capabilities, it will be acting contrary to its obligations under international law, in a non-transparent manner, and against the principle of good faith. Hybrid threats also run counter to the principle of non-interference in domestic affairs. Thus, although they are short of open warfare, hybrid threats clearly evade the idea of the peaceful resolution of disputes.

Hybrid threats exploit the vacuum of law, but law is needed to address these same threats. While prevention, social awareness, and education are also required to counter hybrid threats, the law is paramount because actors using such threats move between the realms of what is legal, illegal, and alegal. Unless an attack is lethal, law-abiding states should not apply the law of armed conflict in response to hybrid tactics. It is important that this rule remain unchanged. Nor is redefinition of the meaning of the terms 'force', 'aggression', 'war', 'intimidation', or 'conflict' necessary because the inclusion of hybrid threat attacks within these concepts would only add confusion.

In general, peacetime law applies to hybrid threats, which forces law-abiding states to carefully measure their responses and fully respect human rights, placing them in a precarious position. In this respect, democratic regimes can become prisoners of ethical standards and rule-of-law principles because they must not retort against aggressors with weapons or other means. This is because hybrid threats must be countered by using the law in good faith. Importantly, international law should not be bypassed when responding to hybrid threats, rather it must be applied with determination and further developed. Thus, dismantling the current international legal system is not required, although the system should be made more resilient to better deal with these threats. In addition, awareness, preparation, prevention, counterintelligence, diplomacy, and strategic communication are all required, although these needs do not undermine the critical importance of international law and its institutions as they currently stand.

The potential damage that hybrid threats could cause to international peace and stability should not be underestimated: the covert way in which they show up can confuse law-abiding

states. This makes hybrid threats one of the main ongoing challenges to world order. Nevertheless, these risks have probably always been present throughout history, with political groups, whether state or non-state actors, always having attempted to upset the stability of their perceived rivals using these tactics. Hence, in some ways, hybrid threats are endogenous to the international political system. What makes them special is that they attempt to surreptitiously circumvent the law, making their detection and attribution particularly difficult. The novelty of hybrid threats in the 21st century is the multifaceted forms they now often adopt, usually through the application of new technologies, as well as the exponential speed of their propagation. Hybrid threats can cause critical damage to basic infrastructure, making them an immensely powerful weapon both in times of peace and of war. Notwithstanding, such threats must be tackled using the means of the law, as well as through prevention, resilience, and education.

Both the current international and national legal systems, especially their civil and criminal branches, are sufficient to counter these risks. In any case, is there even an alternative to enforcement through the law? Can a solution against hybrid threats not firmly anchored in legal standards be praised? Moreover, can illegal means be used to counter these threats and what would an illegal response look like? It is worth remembering that state responsibility comes first in the fight against hybrid threats. However, states should not solely rely on international law to solve all these problems. While international law must remain the overall guiding framework to deal with hybrid threats, each state should also legislate at the domestic level. States need clear national norms regarding cyberspace, migration, drugs, money laundering, human trafficking, infrastructures, and privacy law, among others, because these are some of the principal vulnerabilities leveraged by hybrid tactics. States should also enact comprehensive national defence legislation and cyber security laws sooner rather than later. Furthermore, they should legislate on their diplomatic services to update their functions and capacity to face these threats in their everyday work. Thus, international law cannot and should not replace state law in this respect.

Data availability

Data sharing is not applicable to this research because no data were generated or analysed.

Received: 13 October 2022; Accepted: 19 June 2023;

Published online: 29 June 2023

Notes

- United Nations General Assembly: Developments in the field of information and telecommunications in the context of international security. Report of the Secretary-General, A/74/120, 24 June 2019; UNITED NATIONS GENERAL ASSEMBLY: Open-ended Working Group in the field of information and telecommunications in the context of international security. Third substantive session. Chair's summary, A/AC/290/2021/CR.P.3.
- NATO: *Active engagement, modern defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government in Lisbon Strategic*, November 2010, available at: https://www.nato.int/cps/en/natohq/official_texts_68580.htm.
- NATO: External Action Service: *A Europe that protects: Countering hybrid threats*, June 2018, available at https://www.eeas.europa.eu/node/46393_en.
- Council of Europe. Committee on Legal Affairs and Human Rights: *Legal challenges related to hybrid war and human rights obligations*, Doc. 14044 and 14048, reference 4217, 20 June 2018.
- United Nations General Assembly: A/RES/2625 (XXV), Declaration 2625 (XXV) on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, 24 October 1970.

- Council Of The European Union: Complementary efforts to enhance resilience and counter hybrid threats, Doc. 14972/19, 10 December 2019, p. 3.
- European Court of Human Rights: Guide to Article 15. Derogation in time of emergency, August 2022, available at: https://www.echr.coe.int/documents/Guide_Art_15_ENG.pdf.
- Available at <https://legal.un.org>.
- Available at <https://legal.un.org>.

References

- ABC (2021) El misterioso síndrome de La Habana se extiende ya a más de 130 funcionarios de EEUU, 14 May 2021
- Argumosa Pila J (2019) El discurso de la guerra híbrida. Informe de la cátedra de estudios estratégicos, 2 de enero de 2019, p. 10
- Army–Air Force Center for Low Intensity Conflict (1987) LANGLEY AIR FORCE BASE, VIRGINIA: Low intensity conflict. Imperatives for success, Clic Papers, 1987
- Bachmann SD, Muñoz Mosquera AB (2015) Lawfare and hybrid warfare-how Russia is using the law as a weapon. In: *Amicus Curiae*, summer 2015, issue 102, pp. 25–28
- Bachmann S-D (2015) Hybrid wars: the 21st-century's new threats to global peace and security. *Scientia Militaria*, South African J Military Stud 43,(1):77–98
- Bajarūnas E (2020) Addressing hybrid threats: priorities for the EU in 2020. In: *European View*, 2020, accessible at <https://doi.org/10.1177/1781685820912041>
- Bazarkina DY (2022) Countermeasures for hybrid threats: the experience of the European Union and its Member States. In: *Herald of the Russian Academy of Sciences*, 2022, available at: <https://link.springer.com/article/10.1134/S1019331622100033>
- Broeders D, De Busser E, Cristiano F, Tropina T (2002) Revisiting past cyber operations in light of new cyber norms and interpretations of International Law: inching towards lines in the sand? *J Cyber Policy*, 2002, pp. 97–135, available at: <https://www.tandfonline.com/doi/full/10.1080/23738871.2022.2041061>
- Cardona J, Sanz-Caballero S, Arrufat A (2022) La protección internacional de la persona, Tirant, 2022
- Carment D, Belo D (2018) War's future: the risks and rewards of grey-zone conflict and hybrid warfare, Policy Paper Canadian Global Affairs Institute, Oct 2018, p. 11
- Carment D, Belo D (2020) Gray-zone conflict management, in *European, Middle Eastern & African Affairs*, summer 2020, p. 21
- Chivvis CS (2017) Understanding Russian “Hybrid Warfare” and what can be done about it. In: *Rand Testimonies*, 2017, p. 3, available at: <https://www.rand.org/pubs/testimonies/CT468.html>
- Council of Europe (2018) Committee on legal affairs and human rights: legal challenges related to hybrid war and human rights obligations, Doc. 14044 and 14048, reference 4217, 20 Jun 2018
- Council of The European Union (2019) Complementary efforts to enhance resilience and counter hybrid threats, Doc. 14972/19, 10 Dec 2019
- De Espona, RJ (2019) Las operaciones militares en el ámbito cognitivo: aspectos jurídicos. In: *Cuadernos de estrategia no. 201, límites jurídicos de las operaciones actuales: nuevos desafíos*, IEEEE, Ministerio de Defensa, 2019, p. 68, available at www.ieee.es
- De Salas Claver J (2019) De la flecha al ratón. Consideraciones jurídicas de las operaciones ofensivas en el ciberespacio. In: *Cuadernos de estrategia no. 201, límites jurídicos de las operaciones actuales: nuevos desafíos*, IEEEE, Ministerio de Defensa, 2019, pp. 133–174
- De Wet E (2019) The invocation of the right to self-defence in response to armed attacks conducted by armed groups: Implications for attribution. *Leiden J Int Law* 32(1):91–110
- European Commission & European Centre of Excellence for Countering Hybrid Threats (2021) The landscape of hybrid threats: a conceptual model. 2020 Report, OPEU, Luxembourg, 5 Feb 2021
- European External Action Service (2018) A Europe that protects: Countering hybrid threats, Jun 2018, available at https://www.eeas.europa.eu/node/46393_en
- European Center of Excellence for Countering Hybrid Threats (2021) The–future of cyberspace and hybrid threats. In: *Hybrid CoE Trend Reports*, no. 6, Apr 2021, p. 14, available at: www.hybridcoe.fi
- European Court of Human Rights (2022) Guide to Article 15. Derogation in time of emergency, Aug 2022, available at: https://www.echr.coe.int/documents/Guide_Art_15_ENG.pdf
- Gaiser L (2019) NATO-EU Collaboration on hybrid threats. Cooperation out of necessity with potential consequence on international legal framework. In: *National security and the future*, Vol. 20 No. 1-2, 2019, p. 20, available at: hrcak.srce.hr
- Galán C (2018) Amenazas híbridas. Nuevas herramientas para viejas aspiraciones. In: *Elcano Documentos de Trabajo*, 20/2018, p. 3
- Galinek D, Steingartner W, Vinko Z (2019) Cyber rapid response team: an option within hybrid threats. In: 2019 IEEE 15th International Scientific Conference

- on Informatics, 2019, available at: <https://ieeexplore.ieee.org/abstract/document/9119292>
- Hickman K, Weissman M, Nilsson N, Dominik S, Gunneriusson H, THUNHOLM P (2018) Hybrid threats and asymmetric warfare: What to do?. Conference Proceedings Swedish Defence University, February 2018, p. 6, accessible at eprints.bournemouth.ac.uk
- Janičatová S, Mlejnková P (2021) The ambiguity of hybrid warfare: a qualitative content analysis of the United Kingdom's political–military discourse on Russia's hostile activities". In: *Contemporary Security Policy*, 2021, vol. 42, no. 3, pp. 312–344
- Kittichaisaree K (2017) *Public International Law of cyberspace*, 2017
- Kong W, Marler T (2022) Ukraine's lessons for the future of hybrid warfare. In: *National Interest*, 25 Nov 2022
- Kotoulas IE, Pusztai W (2020) Migration as a weapon. Turkey's hybrid warfare against the European Union, Foreign Affairs Institute, 2020, p. 4
- Lahmann H (2022) Infecting the mind: establishing responsibility for trans-boundary disinformation. *Eur J Int Law* 33(2):411–440
- Lanz Raggio M (2019) El conflicto en las sombras: aspectos generales y elementos jurídicos de las operaciones en la zona gris". In: *Cuadernos de estrategia* no. 201, límites jurídicos de las operaciones actuales: nuevos desafíos, IEEE, Ministerio de Defensa, 2019, pp. 17–55
- Lonardo L (2021) EU Law against hybrid threats. A first assessment, in *European Papers*, 2021, vol. 6, pp. 1075–1096
- López-Casamayor Justicia A (2019) Armas letales a la luz del derecho internacional humanitario: legitimidad y responsabilidad. In: *Cuadernos de estrategia* no. 201, límites jurídicos de las operaciones actuales: nuevos desafíos, IEEE, Ministerio de Defensa, 2019, pp. 177–216
- Mestre J (2021) Las balas humanas de Mohammed VI, in *OK Diario*, 24 May 2021
- Moeckli D, Shah S, Sivakumaran S (2022) *International Human Rights Law*, OUP, 2022
- NATO (2010) Active engagement, modern defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government in Lisbon Strategic, November 2010, available at: https://www.nato.int/cps/en/natohq/official_texts_68580.htm
- Papadimos T, Stawicki SP (2021) Hannah Arendt's prognostication of political animus in america: social platforms, asymmetric conflict, and offset strategy. *Open J Philos* 2021, 11, 1, accessible at: <https://www.scirp.org/journal/paperinformation.aspx?paperid=107003>
- Ploumis M (2021) Comprehending and countering hybrid warfare strategies by utilizing the principles of Sun Tzu. *J Balk Near East Stud* 24(2):344–364. <https://doi.org/10.1080/19448953.2021.2006005>
- Przeworski A (2022) Formal models of authoritarian regimes: a critique. In: *European Papers*, vol. 6, no. 2, <https://doi.org/10.2139/ssrn.4033720>
- Rousseau K (2017) International law and military strategy: changes in the strategic operating environment. *J Natl Secur Law Policy* 9(1):2
- Sari A (2019) Legal resilience in an era of grey zone conflicts and hybrid threats. In: *Exeter Centre for International Law Working Paper Series*, 2019, no. 1, p. 6, accessible at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3315682
- Sari A (2020) Hybrid threats and the law. Concepts, trends and implications. In: *Hybrid CoE Trend Report* 3, Apr 2020, p. 8
- Schmitt MN (2017) Grey zones in the International Law of cyberspace. *Yale J Int Law Online* 42(2):1–21
- The Hague Centre for Strategic Studies (2020) Hybrid conflict. Neither war, nor peace, 10 Jan 2020, <https://hcss.nl/report/hybrid-conflict-neither-war-nor-peace/>
- United National General Assembly (2019) Developments in the field of information and telecommunications in the context of international security. Report of the Secretary-General, A/74/120, 24 Jun 2019
- United Nations General Assembly (1970) Declaration 2626 (XXV) on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, A/RES/2625 (XXV), 24 Oct 1970
- United Nations General Assembly (2019) Open-ended Working Group in the field of information and telecommunications in the context of international security. Third substantive session. Chair's summary, A/AC/290/2021/CR.P.3
- Wijnja K (2021) Countering hybrid threats: does strategic culture matter? In: *Defence Studies*, 2021, <https://www.tandfonline.com/doi/abs/10.1080/14702436.2021.1945452?tab=permissions&scroll=top>

Acknowledgements

This article was conducted within the framework of projects PID2021-126765NB-I00 MICINN and AICO/2021/099 GVA from the Universidad Cardenal Herrera and the Valencian regional government, respectively. I would also like to thank Kailey Elisabeth Kirkham for revising the text and for her insights.

Author contributions

The sole author is responsible for all aspects of the study.

Competing interests

The author declares no competing interests.

Ethical approval

This article does not contain any studies with human participants performed by the author.

Informed consent

This article does not contain any studies with human participants performed by the author.

Additional information

Supplementary information The online version contains supplementary material available at <https://doi.org/10.1057/s41599-023-01864-y>.

Correspondence and requests for materials should be addressed to Susana Sanz-Caballero.

Reprints and permission information is available at <http://www.nature.com/reprints>

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2023