Finanziato dall'Unione europea
NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

digi

**Hybrid threats versus Democratic Resilience:
An analytical and practical toolkit**

Diego Mauri

Hybrid Warfare in Outer Space: Where Does International Law Stand Today?

Diego Mauri*

Hybrid Warfare in Outer Space: Where Does International Law Stand Today?

* Assistant Professor of International Law, Department of Law, University of Palermo. This research has been supported by the "Project Hybrid Threats versus Democratic Resilience: An Analytical and Practical Toolkit (HYDRA)", funded by the European Union within the"PRIN 2022 PNRR" program of the Italian Ministry of University and Research, CUP B53D23032490001.
This article is forthcoming in S. ZOLEA(ed.), *Comparative Visions in Space Law*, Roma Tre University Press.

Summary

1. Setting the Stage: Outer Space as Domain of (Hybrid) Warfare

In the aftermath of the Russian Federation's test of an anti-satellite weapon (ASAT) against its own *Cosmos-1408*, which took place on November 15, 2021, the reaction of several States – the US and EU Member States in the first place – was a heartfelt condemnation: as that ASAT test targeted a Soviet-era satellite placed on a Low Earth Orbit (LEO), fragments and *debris* generated by the kinetic impact will reasonably take years before descending in the atmosphere, thus endangering space activities for a significant lapse of time. The Russian conduct was labelled as «irresponsible behaviour in outer space»[1]. Less than a year later, the Russian representative at the UN General Assembly denounced an «extremely dangerous trend» taking place in the skies above Ukraine (against which the Russian Federation had been involved in an armed conflict since February 2022), namely the utilization of the Starlink system–owned and operated by a US-based company, SpaceX – by the Ukrainian armed forces[2].

Those are but instances of the importance of outer space for military activities carried out by States, inside as well as outside armed confrontation. Basing on those (and other) instances, many commentators have begun to conceive outer space as a «warfighting domain» or a «military domain», more precisely the *fourth* one (the first being 'land', the second 'sea', the third 'air', and the fifth 'cyber')[3].It is not difficult to grasp why: the outer space is teeming with military-sensitive technologies, such as satellites and systems for communications, transportation, navigation, global positioning, ISR (i.e. intelligence, surveillance, reconnaissance), early warning. Their role in contemporary societies' lives could hardly be overestimated.

More recently, the point has been made that, in addition to direct military confrontation, other state activities aiming at destabilizing opponents could be conducted in this domain: put differently, outer space too could become the theatre of «hybrid warfare». This concept–which literally exploded in recent years – has been crafted by several States and military alliances (mostly Western)[4]. According to NATO, hybrid

---

[1] *Statement by the High Representative of the Union for Foreign Affairs and Security Policy on behalf of the EU on the Russian Anti-Satellite Test on 15 November 2021*, 19 November 2021.

[2] *Statement by Deputy Head of the Russian Delegation Mr. Konstantin Vorontsov at the Thematic Discussion on Outer Space (Disarmament Aspects) in the First Committee of the 77th Session of the UNGA*, 22 October 2022.

[3] See more extensively S. MCCOSKER, *Domains of Warfare*, in B. SAUL, D. AKANDE (eds), *The Oxford Guide to International Humanitarian Law*, Oxford, 2020, p. 77, in particular p. 86.

[4] For a primer on hybrid warfare, see the seminal work of A. SARI, *Legal resilience in an era of grey zone conflicts and hybrid threats*, in *Cambridge Review of International Affairs*, 2020, p. 846; C. MARSCH, *The*

«threats» are «[c]oordinated and synchronized actions that deliberately target the systemic vulnerabilities of democratic states or institutions in order to reach strategic goals and create the desire effects»[5]. Conducts pertaining to the conceptual area of hybrid warfare are placed in a sort of 'grey area' between war and peace, which challenges rules and principles of international law as they currently exist.

The present paper aims to explore the connections between the concept of hybrid warfare and outer space from an international law perspective. To this end, it will delve into the concept of hybrid warfare, exposing difficulties associated with identifying a working definition thereof due to its essentially political – and thus contested – nature (section 2). The paper will then apply this concept to state and non-state activities that have been regularly carried out (or that will reasonably be in the near future) in outer space (section 3). The following section (4) will be dedicated to testing the adequacy of existing norms of international law as applicable to outer space activities to cope with the reality of hybrid warfare. Lastly and by way of conclusion, some trends emerging from recent practice will be pointed out (section 5).

2. What Is in a Name: 'Hybrid Warfare' andRelated Concept

The concept of hybrid 'warfare' – sometimes referred to also as hybrid 'attacks' or 'threats', depending on source and context – hasbeen experiencing a period of incredible success. If the definition proposed above is accepted[6], one could easily rebut that the concept itself is as old as humanity: in the célèbre *The Art of War*, Sun Tzu affirmed that «[t]he supreme art of war is to subdue the enemy without fighting»[7].While this sentence (dating back the sixth century BC) cleverly captures the inherent feature of the concept of hybrid warfare – that is, targeting the enemy through means that fall short of war in its proper sense –, it must be noted at the outset that technological advances have made possible forms and degrees of intrusiveness and confrontation that was simply unimaginable few decades ago (let alone millennia ago!). Considering this, one cannot but

---

Grey Zone and Hybrid Conflict. A Conceptual Introduction, in M. REGAN, A. SARI, *Hybrid Threats and Grey Zone Conflict*, Oxford, 2024, p. 31.

[5]M. HÖYHTYÄ, S. UUSIPAAVALNIEMI, *The space domain and the Russo-Ukrainian war: Actors, tools, and impact*, Hybrid CoE Working Paper 21, September 2023, available at <https://www.hybridcoe.fi/wp-content/uploads/2023/01/20230109-Hybrid-CoE-Working-Paper-21-Space-and-the-Ukraine-war-WEB.pdf>.

[6] See *supra*, section 1.

[7]SUN TZU, *The Art of War*, translated by J.J.L. DUYVENDAK, S. YANG, S. YUAN, Stansted, 1998, p. 37.

notice the structural difference between the conducts that are relevant for the contemporary conceptand those relevant for the ancient one.

Turning to how hybrid warfare is understood today, it is helpful to rapidly sketch a biography of that concept. The institutional framework in which it was conceived and tested is the Organization of the North Atlantic Treaty (NATO). In the 2010 Strategic Concept, NATO Member States took into consideration the reality of cyberattacks, arguing that«[f]oreign militaries and intelligence services, organised criminals, terrorist and/or extremist groups can each be the source of such [cyber] attacks»[8].In another document specifically dealing with hybrid warfare, the parallel notion of hybrid 'threats' was defined as «those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives»[9].

While back then what Member States had mostly in mind were terrorist attacks by non-state actors (both on Western soil and abroad)[10], a new reality was making its way in the international arena, as in 2007 Estonia was famously targeted by a cyberattack causing a 'Distributed Denial of Service' (DDoS) and allegedly attributable to a Russia-backed hacktivist group[11].In the following years, NATO and its Member States progressively applied the concept of hybrid warfare to conducts attributable to state actors, namely the Russian Federation and China.

In the aftermath of the Russian invasion of Crimea in February 2014, NATO States adopted a declaration not only condemning that act, but also stressing the importance of building a defensive strategy vis-à-vis «hybrid warfare threats [*sic*], where a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design»[12].Such reference to hybrid warfare was far from fortuitous: as is known, the Russian Federation resorted to non-state groups (the so-called «Little Green Men») to infiltrate Crimea and join forces with irregular troops located there[13].Simultaneously, another key security actorin the European continent, i.e. the European Union (EU), began to show interest in the topic: in 2015, both the EU Defense

[8]NATO, *Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*, adopted 19-20 November 2010, para. 12.
[9]The document is quoted in M. AARONSON ET AL., *NATO Countering the Hybrid Threat*, in *Prism*, 2011, p. 111, at p. 115.
[10]Back then, the US-led *Global War on Terror* was actively conducted. For a critical appraisal of such 'war' from the angle of international law, see M.E. O'CONNELL, *The Legal Case against the Global War on Terror*, in *Case Western Reserve Journal of International Law*, 2004, p. 349.
[11] See M. ROSCINI, *World Wide Warfare* – Jus ad bellum *and the Use of Cyber Force*, in A. VON BOGDANDY, R. WOLFRUM (eds), *Max Planck Yearbook of United Nations Law*, 2010, p. 85.
[12]NATO, *Wales Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*, 5 September 2014, para. 13.
[13]T.D. WENTZELL, *Russia's Green Men: The Strategic Storytellers of Hybrid Warfare*, in *Canadian Military Journal*, 2021, p. 42.

Ministers and the European External Action Service discussed hybrid warfare and called for shared actions at the supranational level[14]. NATO and the EU eventually joined their efforts in 2017, setting up a Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)[15].

Hybrid warfare has since then been regularly referred to in NATO and EU official documents dealing with security[16], up to the 2022 Strategic Concept[17]. Here, interestingly, the potential sources of hybrid threats are identified not only in Russia, but also in China[18]. Even if not quoted, reference here must be understood to China's interests in the South China Sea and the Taiwan Strait, a region where military escalation is believed to beplausiblein the near future[19].

Having said this, one may inquire what is the actual *content* of the notion of hybrid warfare. As this has been understood as featuring conventional and non-conventional means, put in place either by state and non-state actors, covertly or overtly, to exploit democratic States's structural vulnerabilities and weaken them, one may rightfully conclude that virtually *anything*that is done *against* the interests of Western States and that exploits their vulnerabilitieswould be included in the concept. As a confirmation, some authors have described the concept as a «contested» one, working as a mere «catch-all phrase or buzzword»[20].

For the purposes of the present contribution, it seems more useful to leave aside definitional quandaries and to focus on *specific* domains (or instances) in which the concept of hybrid warfare is believed to articulate. These include – but are not limited to – cyberattacks against critical infrastructure, disinformation campaigns (e.g.,on political

[14]See EEAS, *Food-for-thought paper "Countering Hybrid Threats"*, 8887/15, 13 May 2015.For more on the European stance vis-à-vis hybrid warfare, see L. LONARDO, *The seriousness of vagueness:introducing European law and policies against hybrid threats*, in L. LONARDO (ed), *Addressing Hybrid Threats. European Law and Policies*, Cheltenham-Northampton, 2024, p. 1.

[15]See NATO, *Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*, 6 December 2016. As of today, after the adhesion of Albania, the Hybrid CoE is composed of 36 Members, including all EU and NATO Member States.

[16] See NATO, *Brussels Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels*,11-12 July 2018, para. 13; ID., *Brussels Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels*,14 June 2021, para. 31. For the legal implications of those declarations, see*infra*section4.

[17]NATO, *2022 Strategic Concept. Adopted by the Heads of State and Government at the NATO Summit in Madrid*, 29 June 2022.

[18]*Ibidem*, para. 13.

[19]See MARSCH, *The Grey Zone and Hybrid Conflict. A Conceptual Introduction*, cit., p. 33.

[20]E. REICHBORN-KJENNERUD, P. CULLEN, *What is Hybrid Warfare?*, in *Norwegian Institute of International AffairsPolicy Brief*, 2016, p. 1.

elections)[21],boosting migratory routes[22], and illegal, unreported and unregulated fishing (so-called IUU fishing) on the high seas adjacent to States' Exclusive Economic Zones (EEZ)[23].As one may easily note, the variety of those areas requires that each one of them be addressed severally, that is, one the one hand, with regard to its inherent features, and, on the other hand, taking into account the legal framework that applies specifically.

In addition to this, it is worth noting that all definitions of hybrid warfare and related concepts embrace also the 'vulnerabilities' of the intended targets. This is due to the fact that States that are members of the relevant organizations (NATO and the EU) are democratic systems based on the rule of law and the respect of fundamental rights: hybrid warfare can prove particularly effective against those systems, as their margin of reactions is restrained by numerous norms (e.g., as laid down in domestic Constitutions and enshrined in human rights treaties). As a result, the discussion around the topic of hybrid warfare is centered in the notion of legal 'resilience', which describes the effort to put in place preventive and mitigatory measures against hybrid threats, without jeopardizing core democratic values[24].

Turning now to the topic that this paper addresses, it is worth noting that NATO States have expressly identified outer space as a domain where hybrid warfare can – and actually *is* – conducted. In the already mentioned 2022 Strategic Concept, it is acknowledged that «authoritarian actors challenge [NATO Member States'] interests, values and democratic way of life», and that those actors «conduct malicious activities in cyberspace and space»[25]. The recent practice of military confrontation in outer space –

[21]G.M. RUOTOLO, *Nell'anno delle elezioni hanno tutti ragione. Alcune considerazioni sul ruolo del diritto internazionale ed UE nel contrasto alla disinformazione*, in *SIDIBlog*, 5 aprile 2024, availableat<http://www.sidiblog.org/2024/04/05/nellanno-delle-elezioni-hanno-tutti-ragione-alcune-considerazioni-sul-ruolo-di-diritto-internazionale-ed-ue-nel-contrasto-alla-disinformazione/>.More generally on the topic of fake news from an international law viewpoint, see B. BAADE, *Fake News and International Law*, in *European Journal of International Law*, 2019, p. 1357.

[22]R. PARKES, *The EU's 'hybrid' migration wars: a case of mistaken identity*, in L. LONARDO (ed), *Addressing Hybrid Threats. European Law and Policies*, cit., p. 84. See also S. CABALLERO SANZ, *The concepts and laws applicable to hybrid threats, with a special focus on Europe*, in *Humanities and Social Sciences Communications*, 2023, p. 1.

[23]V. SCHATZ, M. MCCREATH, *EEZ-adjacent distant-water fishing as a global security challenge: An international law perspective*, *Hybrid CoE Working Paper 19*, September 2022, available at <https://www.hybridcoe.fi/wp-content/uploads/2022/09/20220912_Hybrid_CoE_Working_Paper_19_DWF_WEB.pdf>.

[24]On the notion of 'legal resilience', see A. SARI, *Legal Resilience: Just a Warm and Fuzzy Concept?*, in M. REGAN, A. SARI, *Hybrid Threats and Grey Zone Conflict*, cit., p. 533.

[25] NATO, *2022 Strategic Concept. Adopted by the Heads of State and Government at the NATO Summit in Madrid*, cit., para. 7.

as the *Starlink* case aptly epitomizes – calls for a thorough reflection on the implications stemming from those affirmations[26].

3. Outer Space: From 'Black' to 'Grey'

Outer space *in itself* displayscharacteristics that appear well suited for adomain of hybrid warfare. It is possible to outline at least three features: (1) the presence of a variety of non-state actors; (2) the employment of military-sensitive technologies for activities to be conducted in that domain; (3) the usability of non-kinetic and covert means to disrupt or neutralize the enemy's assets.

As per the first feature, outer space is now populated by thousands of private operators (such as SpaceX): in the last decade, what was an area accessible only to a small group of actors (mainly States) has turned into «a vital sphere of commercial and military operations»[27].In addition to owing about 2 out of 3 satellites orbiting around the Earth, private companies will soon engage in a plethora of space activities, such as travelling to other celestial bodies, space tourism, and even placing space stations[28]. This situation will not only fuel confrontation among States (the US, Russia and China, to name only the most active spacefaring countries), but also competition among those private companies. As a common expression goes, outer space is deemed to get evenmore «congested, contested, and competitive»[29] as it is nowadays. Actors operating in outer space are (and will be) driven by the desire to ensure their own freedom of action while striving to restrict others', which is the gist of the very notion of hybrid warfare[30].

The *second* feature that it is appropriate to focus on is the presence of military-sensitive technology, in particular dual-use objects such as satellites and navigation systems. As a matter of fact, contemporary space technology is described as «inherently dual use», serving both civilian and military purposes[31]. SpaceX' Starlink has clearly

[26] As a confirmation, the Hybrid CoE has dedicated an *ad hoc* publication to outer space: see HÖYHTYÄ, UUSIPAAVALNIEMI, *The space domain and the Russo-Ukrainian war: Actors, tools, and impact*, cit.
[27]M. DE ZWART, *Hybrid and Grey Zone Operations in Outer Space*, in M. REGAN, A. SARI, *Hybrid Threats and Grey Zone Conflict*, cit., p. 289, at p. 293.
[28] See J. FOUST, *Commercial space stations go international*, in *Space News*, 3 July 2024, available at <https://spacenews.com/commercial-space-stations-go-international/>.
[29]R. HARRISON, *Unpacking the Three C's: Congested, Competitive and Contested Space*, in *The International Journal of Space Politics & Policy*, 2013, p. 123.
[30]See SARI, *Legal resilience in an era of grey zone conflicts and hybrid threats*, cit., p. 856.
[31]DE ZWART, *Hybrid and Grey Zone Operations in Outer Space*, cit., p. 294.

demonstrated its dual-use nature, being employed both by private persons longing for high-speed Internet connection around the globe and by state actors, such as the already mentioned Ukrainian army in the context of the ongoing armed conflict against the Russian Federation[32]. This makes space objects particularly desirable objectives of hostile activities: neutralizing them can cause substantive damage to civilian infrastructure and military assets.

The *third* feature is that the means through which such neutralization can be sought combine kinetic and non-kinetic force. The practice of ASAT tests, which major spacefaring States have conducted in the last decades (the US, China, India, and the Russian Federation), seems an anticipation of future active engagements of enemy satellites[33]. As far as the November 2021 Russia's test, it has been argued that Russia's ultimate objective was not the direct target that it engaged (its own satellite), but rather Starlink satellites, placed below the *Cosmos-1408*'sorbit: the test was allegedly intended to cause disturbances to the US-based company, few weeks before the full-scale invasion of Ukraine[34]. However, kinetic means are not the sole tools to be employed in the space dominion. In addition to direct-laser weapons, cyberweapons may turn a formidable instrument to target enemy systems and infrastructure*covertly* – something that traditional, kinetic-force tools could hardly ensure[35].Not only is the malicious source of the attack harder to discover, but it is also simpler for the authors to deny their involvement in the operation (i.e. «plausible deniability»), as commonly happens with cyberoperations in terrestrial domains. A scenario recently simulated in the NATO framework concerns the use of a cyberweapon not against on-orbit satellites, but against Space Situational Awareness (SSA) systems[36]. In the context of the Russo-Ukrainian conflict, the Russian Federation conducted a cyberattack against the Viasat satellite network – a ground-based infrastructure –, which resulted in major disruptions of

[32] For a discussion of Ukraine's use of Starlink technology and the anticipated reactions by Russia, seeD. MAURI, *Cose dell'altro mondo: la Russia considera obiettivi militari alcune costellazioni commerciali di satelliti*, in *Quaderni di SIDIBlog*, 2022, p. 145.

[33] On ASAT tests and future employments, see more extensively D. KOPLOW, *ASAT-isfaction: Customary International Law and the Regulation of Anti-Satellite Weapons*, in *Michigan Journal of International Law*, 2009, p. 1188.

[34]As a matter of fact, a few months after the Russian test the debris generated by the destruction of the Soviet-era satellite approached SpaceX's constellation, risking causing extensive damage: see J. FOUST, *Starlink satellites encounter Russian ASAT debris squalls*, in *Space News*, 9 August 2022, available at <https://spacenews.com/starlink-satellites-encounter-russian-asat-debris-squalls/>.

[35]See J. PAVUR, I. MARTINOVIC, *The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space*, in T. MINÁRIK ET AL. (eds), *2019 11th International Conference on Cyber Conflict: Silent Battle*, Tallinn, 2019, p. 1.

[36]See D. MAURI, *Attività di impiego e di* testing *di armi anti-satellite e diritto internazionale*, in *Rivista di diritto della navigazione*, 2022, p. 635, at p. 639.

Ukrainian modems and across European States[37]: incidentally, this demonstrates also the degree of interconnectedness between States, which makes it difficult to contain cyberattacks in a spatially determined area.

As the concept of hybrid warfare implies that of targets' 'vulnerability'[38], the space environment – including ground-based infrastructure, as mentioned above – is renown as being particularly vulnerable to hybrid threats. In current debates, as far as outer space is concerned, this notion is understood mainly in its *technical* sense: some fear that the increasing confrontation in the space domain, between state and non-state actors, will increase risks to human activities, thus pushing those actors to internalize higher costs and discouraging new ones to invest in the space field[39].

Put short, hostile 'competition' is likely to obfuscate genuine 'cooperation' in the use and exploration of outer space, a phenomenon that, metaphors aside, runs in contravention with the cornerstone principle of international space law, that is the pacific use of outer space, which must be explored and used «for the benefit and in the interests of all countries», as enshrined in the so-called Outer Space Treaty (OST)[40]. From this perspective, it is easy to see how the tactics of hybrid warfare are likely to impact on the respect and the application of existing rules and principles of international law, which is now appropriate to investigate.

4. *International Law Applicable to 'Hybrid' Space Activities*

4.1 *Overview*

As of today, no one doubts that international law applies fully to activities conducted in the space domain[41].In addition to international space law (which flourished in the 1960s and in the 1970s), other branches of international law regulate what state and non-state actors do in outer space.

---

[37]HÖYHTYÄ, UUSIPAAVALNIEMI, *The space domain and the Russo-Ukrainian war: Actors, tools, and impact,* cit., p. 10.
[38] See *supra*, para. 2.
[39]DE ZWART, *Hybrid and Grey Zone Operations in Outer Space*, cit., p. 296.
[40]*Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, adopted on 19 December 1966, Preamble and art. I.
[41]B. CHENG, *The Military Use of Outer Space and International Law*, in B. CHENG (ed), *Studies in International Space Law*, Oxford, 1997, p. 523; C. CEPELKA, J.H.C. GILMOUR, *The Application of General International Law in Outer Space*, in *Journal of Air Law and Commerce*, 1970, p. 30.

The first branch that may come to the fore is international humanitarian law (IHL), that is the law applicable to armed conflicts, both of an international and of an internal nature. IHL regulates what States and other armed groups can do in the battlefield: it is traditionally referred to as *jus in bello*. It is today held that IHL is not limited to armed confrontation on Earth but applies also to military operations in outer space: international legal scholarship anticipating what may come in case of 'space wars' have blossomed in recent years[42]. The future use of ASAT in actual combat scenarios – and not as simple tests – elicited a vivid debate in the international community[43].

The other body of norms that would regulate activities in outer space – and which is even more of interest when discussing hybrid warfare –is the law on the use of force, or *jus ad bellum*, which establishes the conditions meeting which States are allowed to use force in international relations.The bedrock rules of this entire body of law are to be traced in the UN Charter. Article 2(4) establishes as one of the «principles» of the UN the prohibition of the threat and use of force against the territorial integrity or political independence of any State, or in any other manner incompatible with the Charter[44].This rule is universally acknowledged as customary in nature[45], and by some also corresponding as an imperative norm of the international legal system (to the point that this branch of law is sometimes referred to as *jus contra bellum*)[46].

Taking into account this second set of international rules and principles, and other norms of general international law, it seems appropriate to identify specific norms and to apply them to activities that may take place in outer space and that may qualify as instances of hybrid warfare.

---

[42] See D. STEPHENS, C. STEER, *Conflicts in Space: International HumanitarianLaw and its Application to Space Warfare*, in *Annals of Air & Space Law*, 2015, p. 2; M. PEDRAZZI, *Il diritto internazionale dello spazio e le sue prospettive*, in *Quaderni di relazioni internazionali*, 2008, p. 46; S. MARCHISIO, *Gli usi militari dello spazio: scenari internazionali e tavoli negoziali*, in S. MARCHISIO, U. MONTUORO(eds), *Lo spazio* cyber *e cosmico. Risorse* dual use *per il sistema Italia in Europa*, Torino, 2019, p. 145.

[43]For an overview, see MAURI, *Attività di impiego e di* testing *di armi anti-satellite e diritto internazionale*, cit., atp. 646.

[44]*Charter of the United Nations Organization*, adopted on 26 June 1945.

[45]International Court of Justice (ICJ), *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Judgment of 27 June 1986, para. 188.

[46] M. E. O'CONNELL, *The Prohibition on the Use of Force*, in N. WHITE, C. HENDERSON (eds), *Research Handbook on International Conflict & Security Law,* Cheltenham-Northampton, 2013, p. 89; O. CORTEN, *The Law Against War*, Oxford, 2010, p. 55; R. KOLB, *Ius contra bellum. Le droit international relatif au maintien de la paix: précis*, Bruxelles, 2009, p. 247.

4.2 *Violations of Sovereignty and The Principle of Non-Intervention*

One of the core rules of the Westphalian international community is thatas States possess equal rights and duties, they are obliged to respect other States' sovereignty, that is to refrain from interfering in their internal and external affairs. This principle is so pivotal in the modern and contemporary international legal system, that its actual meaning and content changes constantly, depending on the historical and political context in which it operates[47]. The duty to respect other States' sovereignty has generated another crucial rule as 'corollary', namely the prohibition of intervention in the domestic sphere of other States[48]. The relationship between those two norms – as well as their constitutive elements – is heavily contested and debated in academia.

As regards the principle of non-intervention, States are prohibited from intervening in the so-called «domaineréservé» of other States, that is those matters in which States are free to decide their actions[49], without constraints from the international legal system (to name one, the formulation of foreign policy)[50].In order to qualify as such, forms of intervention must be coercive in nature, that is they must involve the use of «economic, political or any other type of measures […] in order to obtain [from the coerced State] the subordination of the exercise of it sovereign rights and to secure from it advantages of any kind»[51].It is held that, while coercion may take a multitude of forms, it must in all cases result in the targeted State's impossibility to reasonably resist the pressure[52].Such a traditionally high bar would render mere 'interference' – that is,

[47] S. BESSON, *Sovereignty*, in R. WOLFRUM (ed), *Max Planck Encyclopedia of Public International Law*, April 2011, para. 3.
[48] See M. JAMNEJAD, M. WOOD, *The Principle of Non-Intervention*, in *Leiden Journal of International Law*, 2009, p. 345; R. SAPIENZA, *Il principio del non interventonegliaffariinterni. Contributo allo studio della tutela giuridica internazionale della potestà di governo*, Milano, 1990, and more recently M. ROSCINI, *International Law and the Principle of Non-Intervention. History, Theory, and Interactions with Other Principles*, Oxford, 2024.
[49] ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, cit., para. 205.
[50] Scholarship and adjudicatory bodies are divided as regards the methodology to identify which choices pertain to the «domaineréservé». See F. KRIENER, *Intervention, Prohibition of*, in A. PETERS (ed), *Max Planck Encyclopedia of Public International Law*, August 2023, para. 4 ff.
[51] United Nations General Assembly (UNGA), *Declaration 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), 15 December 1970, Annex, para.1, Principle c).
[52]JAMNEJAD, WOOD, *The Principle of Non-Intervention*, cit., p. 348. See also A. TZANAKOPOULOS, *The Right to be Free from Economic Coercion*, in *Cambridge International& Comparative Law*, 2015, p. 616, at p. 620 (arguing that coercion is the element distinguished prohibited intervention from lawful interference).

intervention short of the element of coercion – in line with the principle, and absent any other primary rule prohibiting or regulating it, lawful under existing international law[53].

The rapidly evolving technology in the cyberspace has challenged the content and the limits of these ancient rules of international law.Many functions that States exercise in the cyber domain – such as the delivery of social services, the conduct of elections, the collection of taxes, and national defense – are at risk of being interfered with through covert operations that may not amount to 'intervention' as defined above:one of the clearest examples in this regard is cyber espionage[54]. This is why recent state practice has pushed itself to admit that in some cases violations of sovereignty through cyber means, which do not amount as prohibited 'intervention', may nonetheless run in contravention of existing law[55]. It is unsettled, however, whether the same would go for cyber operations resulting in neither physical damage nor loss of functionality[56]. Put differently, it seems that a minimum threshold of gravity, to be demonstrated with regard to the actual harm inflicted, must be met in order for such mere violations of sovereignty to be qualified as unlawful under international law.

At the crossroads of the fourth and the fifth domains, those rules must be applied carefully. As already noted, satellite systems play a crucial role in the everyday life of millions – if not billions – of people: targeting them via cyberattacks may impact on entire populations, which renders them the perfect objective of hybrid tactics. Jamming, spoofing, and other means of disturbance of satellite activities could thus be qualified as intervention in internal or external affairs (proscribed also in space law)[57], and also as forms of interference of sovereignty that, in light of the emerging understanding of

[53]KRIENER, *Intervention, Prohibition of*, cit., para. 46 ff.
[54] See more extensively R. BUCHAN, *Cyber Espionage and International Law*, London, 2021.
[55]See for instance *Italian Position Paper on 'International Law and Cyberspace'*, p. 4.See for instance Ministry of Foreign Affairs of the Italian Republic,*Italian Position Paper on 'International Law and Cyberspace'*, 2021, available at <https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf>,p. 4.*Contra* see UK's reservation to the 2020 NATO Allied Joint Doctrine for Cyberspace Operations: NATO, Allied Joint Doctrine for Cyberspace Operations, Allied Joined Publication-3.20, January 2020, available at <https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf>. For a discussion of this practice, see H. MOYNIHAN, *The Application of International Law to State Cyberattacks*, Chatham House, December 2019, p. 1.
[56]M.N. SCHMITT (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*, Cambridge, 2017, Rule 5, p. 21.
[57] See R.S. JAKHU, S. FREELAND (eds),*McGill Manual on International Law Applicable to Military Uses of Outer Space: Volume I- Rules*, Montreal, 2022,Rule 117 («Space activities, including military space activities, shall be carried out in conformity with the principle of non-intervention under international law»).

international norms applicable in the cyberspace, may constitute an internationally wrongful act.

More to this, it must be kept in mind that international space law already addresses certain forms of interference: for instance, according to Article IX of the OST, any State Party having reason to believe that an activity or experiment planned by it or its nationals in outer space would cause «potentially harmful interference» with activities of other States has a duty to consult with those other States (which in turn have a right to request such consultation)[58]. This rule is also reflected in non-binding instruments[59]. At this point, one may object that, in keeping with the understanding of hybrid warfare proposed above, activities *willfully*aiming to destabilize opponents in outer space are inherently *covert*: there would be no interest, on the part of a State preparing to launch a hybrid attack against another, to notify its intended activity in advance.The fact that States will not abide by a rule… confirms the existence of such rule; more importantly, it confirms that in outer space explicit rules are in place prohibiting even lower forms of interference in international relations. More specific rules are set by other international instruments, both legally binding and non-legally binding: for instance, in additional to a overarching prohibition on generic «intentional harmful interference»[60], the Constitution of the International Union of Telecommunications provides the Union with the power to act to avoid «harmful interference between radio stations» of different States, and imposes Member States a duty to refrain from causing it (as a *negative* obligation) and to prevent it (as a *positive* one)[61].This applies undoubtedly also to outer space activities[62].

While those rules are believed to leave considerable scope for discretion to States[63], it must be kept in mind that the reasons behind these rules must be traced back to the fundamental principles regulating States' behavior in outer space, namely the

[58]*Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, cit., Art. IX. For a commentary on this prohibition, namely on the notion of «potentially harmful», see S. MARCHISIO, *Article IX*, in S.HOBE ET AL. (eds), *Cologne Commentary on Space Law. Volume I*, Koln, 2009, p. 556.
[59]JAKHU, FREELAND (eds), *McGill Manual on International Law Applicable to Military Uses of Outer Space: Volume I- Rules*, cit., Rule 121.
[60]JAKHU, FREELAND (eds), *McGill Manual on International Law Applicable to Military Uses of Outer Space: Volume I- Rules*, cit., Rule 139.
[61] See *Constitution and Convention of the International Telecommunication Union (with annexes and optional protocol)*, adopted on 22 December 1992, arts. 2, 6, and 45.
[62]JAKHU, FREELAND (eds), *McGill Manual on International Law Applicable to Military Uses of Outer Space: Volume I- Rules*, cit., Rules 140-144 (for more detailed rules).
[63] H. NASU, *Targeting a Satellite: Contrasting Considerations between the Jus ad Bellum and the Jus in Bello*, in *International Law Studies*, 2022, p. 142; M.N. SCHMITT, *International Law and Military Operations in Space*, in A. VON BOGDANDY, R. WOLFRUM (eds), *Max Planck Yearbook of United Nations Law*, 2006, p. 89, at p. 105.

pacific use of it inasmuch as «province of mankind»[64]: legally speaking, basing on rules and principles that were established at the very beginning of space exploration (and that continue to be binding today) the logic of 'genuine cooperation' must prevail over the logic of 'hostile confrontation'.

4.3 *Threat and Use of Force and Aggression (and Self-Defense)*

As stated at the beginning of the present section, the prohibition on the threat and the use of force is one of the bedrock rules of post-1945 international legal order: in addition to being formulated in written, it also stems from the principle of non-intervention, as no one fails to see that using or threatening military force is one of the most intense forms of intervention in other States' internal or external affairs[65].

As far as general international law on the use of force is concerned, the apparently crystal-clear rule enshrined in Article 2(4) of the UN Charter has inspired a multifarious practice of States and international organizations. In particular, the exact content of the prohibition and its boundaries have made the object of heated debates[66]. The ICJ has famously stated that various degrees of force can be identified: it is possible to distinguish «the most grave forms of the use of force (those constituting an armed attack)from other less grave forms»[67].

As a matter of fact, the rule has been held to apply also to threats or uses of force *minoris generis*, that is not only in cases of direct uses of force on the part of one State against another, but also in cases of participation in other state and non-state actors' uses of force[68]. A convincing argument has been put forward that also those cases of minimal (or reduced) use or threat of force be included in the rule, so as tocurb States' attempts at finding a justification to their conducts[69]. However, it must be noted that practice so far tends to include in the prohibition under Article 2(4) only military forms of physical force between States; non-military forms, such as massive influx of

---

[64] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, cit., Art. I.
[65] KRIENER, *Intervention, Prohibition of*, cit., paras. 22 ff.
[66] O. DÖRR, *Use of Force, Prohibition of*, in R. WOLFRUM, *Max Planck Encyclopedia of Public International Law*, cit.
[67] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, cit., para. 191. See also ICJ, *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)*, Judgment of 19 December 2005, paras. 163-165.
[68] In addition to the jurisprudence of the ICJ quoted above, see UNGA, *Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations*, cit.
[69] T. RUYS, *The Meaning of «Force» and the Boundaries of the jus ad bellum: Are «Minimal» Uses of Force Excluded from UN Charter Article 2(4)?*, in *American Journal of International Law*, 2014, p. 159.

refugees or economic coercion, or cross-frontier employment of natural forces, do not amount as 'threats or uses' of force, but rather they qualify as violations of the principle of non-intervention or the rule of sovereignty[70].A partially divergent trend can be registered in the field of cyberattacks, where some commentators (and, importantly, States) are more willing to accept that attacks intended to cause physical damage to property or injury to persons, as well as disrupting essential infrastructures of a State, may amount to threats or uses of force, even if short of 'armed' force in the traditional sense[71].

Looking at the other side of the spectrum, gravest uses of force may amount to 'armed attack' or 'aggression'. As regards the consequences of such qualification, it is worth recalling at the outset that while violations of the prohibition of the threat and use of force constitute unlawful acts, allowing victim States to adopt countermeasures in accordance with international law, armed attacks allow targeted States to react in individual or collective self-defense pursuant to Article 51 of the UN Charter.Again, qualification of acts as armed attacks is a challenging operation. In the decades following the adoption of the UN Charter, opposite tendencies have emerged: on the one hand, States have strived to interpret the notion extensively, to legitimize armed reactions under the umbrella of self-defense[72]; on the other hand, adjudicatory bodies – the ICJ in the first place – have sponsored a more cautious approach, setting a high bar for a use of force to be considered as 'armed attack' (e.g., in addition to a criterion linked to the gravity of the act, also a specific intention on the part of the alleged attacker)[73]. Reference is often made to the 'scale' and 'effects' of a given conduct[74].

Again, in times of increasing confrontation between States through hybrid tactics, a different understanding of the concept of armed attack – in line with the one outlined above vis-à-vis threats and uses of force – has been advanced.As regards the Tallinn Manual, it is argued that in order for a cyber operation to amount as 'armed attack' the «critical factor» is whether the *effects* of such operation are «analogous to those that

[70]See DÖRR, *Use of Force, Prohibition of*, cit., para. 12.
[71]ROSCINI, *World Wide Warfare* – Jus ad bellum *and the Use of Cyber Force*, cit., at p. 102 ff.
[72]See the famous analysis conducted by T. FRANCK, *Who Killed Article 2(4)? or: Changing Norms Governing the Use of Force by States*, in *American Journal of International Law*, 1970, p. 809. This article was replied to by another international lawyer: L. HENKIN, *The Reports of the Death of Article 2(4) Are Greatly Exaggerated*, in *American Journal of International Law*, 1971, p. 544.
[73]*Oil Platforms (Islamic Republic of Iran v. United States of America*, Judgment of 6 November 2003, para. 64.
[74] ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, cit., para. 195.

would result from an action otherwise qualifying as a kinetic armed attack»[75]. Such theory imposing a comparison between kinetic and non-kinetic (or cybernetic) effects has found its way also in NATO official documents. To name one, in 2021 NATO Member States held that «the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack», thus leading to the invocation of the collective defense clause contained in Article 5 of the Treaty[76].

Importantly, the same logic has been recently extended to the fourth domain. In the 2022 Strategic Concept, it is expressly argued that «[a] single or cumulative set of malicious cyber activities; or hostile operations to, from, or within space; could reach the level of armed attack»[77].In other words, different acts that *per se* do not amount to armed attack, if performed within a specific hostile pattern, can be equated to full-scale armed attack justifying self-defense: this theory, referred to as 'accumulation of events theory' or *Nadelsticktaktik*, is gaining traction in the international discourse on contemporary forms of self-defense against armed attacks, interestingly not just those of a hybrid nature[78].

The argument that this paper advances is that this trend is not just particularly dangerous with regard to space activities (as military confrontation up to armed attacks and self-defense actions in that domain risks producing significant and irreparable harm to human activities), but even more troubling from a *legal* standpoint, on the basis of international space norms as they are today. As is known, not only does *jus ad bellum* apply also to outer space, but the OST contains an explicit *renvoi* to that branch of international law[79]. In other words, forms of threats and uses of force – from the less grave to the gravest – that are unlawful on Earth are equally so in outer space.

If applied *telle quelle* to the space domain, the 'accumulation of events theory' as described above may bring about a nightmarish escalation of military confrontation between States. Repeated disturbances to space activities (e.g., via jamming or spoofing, or through kinetic or non-kinetic ASAT), if of a sufficient gravity, may easily escalate from

---

[75] SCHMITT (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*, cit., Rule 71, at p. 340, 341.

[76] *Brussels Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels*, 14 June 2021, para. 32.

[77] NATO, *2022 Strategic Concept. Adopted by the Heads of State and Government at the NATO Summit in Madrid*, cit., para. 25.

[78] In support of the application of this doctrine, see Y. DINSTEIN, *War, Aggression, and Self-Defence*, Cambridge, 2005, at p. 230; N. FEDER, *Reading the U.N. Charter Connotatively: Toward a New Definition of Armed Attack*, in *New York University Journal of International Law and Politics*, 1987, p. 414.

[79] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, cit., art. III.

mere violations of sovereignty or of the principle of non-intervention, to violations to the principle of the non-use of force in international relations and even 'armed attack'. This approach risks *de facto* nullifying the cornerstone prohibition contained in Article 2(4) of the UN Charter, the core principles of international space law (primarily, the principle of pacific use of space) and even jeopardizing space activities for years to come.

5. *Paths to Take, Paths to Avoid*

The choice of considering outer space as a domain of hybrid warfare seems irrevocable today, in a period characterized by a troubling escalation between resuscitated 'blocs' of States. ASAT tests, the use of private constellation of satellitesby States engaged in armed conflict, the cruciality of space systems for States' economic, social, and military activities have rendered outer space a veritable 'grey area'[80], in which (spacefaring) States may exploit not only technological advances to their own benefit, but also legal loopholes to boost hostile confrontation between them.

It seems interesting, for the purposes of the present contribution, to expand on this latter point. The specific sector of international space law is composed of treaty rules that date back more than sixties years ago: most of them are wide in scope and vague in content, andthey all lack jurisdictional or quasi-jurisdictional mechanisms of control. Such structural characteristics, coupled with the historical period of renewed hostilities between the many 'poles' the World is divided into nowadays, are *de facto* making it implausible to reach a sufficient degree of agreement to adopt new binding law[81]. Hence, 'blocs' of States are seeking refuge in soft law and other political declarations void of binding effect, as well as proposals of new treaties that will likely lack sufficient participation[82]. For instance, it is worth mentioning that the last Joint Declaration adopted by Russia and China contains a strong condemnation of the

[80] SARI, *Legal Resilience: Just a Warm and Fuzzy Concept?*, cit.; DE ZWART, *Hybrid and Grey Zone Operations in Outer Space*, cit.

[81]This point hasbeendiscussed vis-à-vis ASAT: MAURI, *Attività di impiego e di* testing *di armi anti-satellite e diritto internazionale*, cit. Interestingly enough, as far as ASAT are concerned, what is happening is that, given the impossibility to adopt an *ad hoc* binding instrument, some States have begun to issue unilateral declarations renouncing or limiting ASAT testing, with a view to inspiring the formation of new customary law. See also E. CARPANELLI, *Towards a Ban of Anti-Satellite (ASAT) Weapons Tests? Exploring Possible Pathways in Light of Recent Developments*, in *Hiroshima Hogaku*, 2023, p. 178.

[82]See for instance the Russian and Chinese *Draft Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects*, 12 June 2014.

transformation of outer space into a «combat domain»[83]. On their part, Western States have labelled Russia's ASAT test of November 2021 as a «irresponsible behaviour in outer space» – and not, interestingly, an «unlawful» one – and called for the adoption of non-binding rules, norms and principles within the UNCOPUOS framework[84].

Such blossoming of soft law and political declarations in the realm of hybrid warfare in outer space seems particularly indicative of the posture of the international community as a whole vis-à-vis the future – or more correctly the *present* – of space activities. States wish to maintain this state of affairs,in which they are relatively free to take action in a perceived 'grey area', as thismeets their interests more properly in these times.However, from a strictly legal standpoint, one must not lose sight of the fact that States operate within an international legal order, that is in a system made up of rules and principles. Instead of insisting on the need to develop new law(something that, as stated above, sounds more like a pious declaration of intent), as many commentators tend to do, it seems more useful to stick to old and well-founded principles such as those that animated the formation of the very first core of international space law (namely the principle of pacific use of outer space as «province of mankind») as well as rules of general international law (the respect of sovereignty and the principle of non-intervention) and *jus ad bellum*. And to argue that those rules fail to define key notions and concept, or lack sufficient clarity, does notlegally justify any form of hostile confrontation in outer space. This may not be the ultimate antidote to neutralize the escalation risks posed by the rhetoric of hybrid warfare, but at least it helps stay on course in turbulent times.

[83] See *Joint statement between the People's Republic of China and the Russian Federation on deepening the comprehensive strategic partnership of coordination for a new era on the occasion of the 75th anniversary of the establishment of diplomatic relations between the two countries*, 16 May 2024, available in English at <https://geopoliticaleconomy.com/2024/05/24/china-russia-joint-statement-new-era-75th-anniversary/>.

[84] *Statement by the High Representative of the Union for Foreign Affairs and Security Policy on behalf of the EU on the Russian Anti-Satellite Test on 15 November 2021*, cit.