

Justine Dousset

LEGAL QUESTIONS RELATED TO THE EU'S SATELLITES AS TARGETS OR TOOLS IN AN INTERNATIONAL ARMED CONFLICT

INTRODUCTION

The use of satellites in armed conflicts has become increasingly indispensable.¹ Space-based technologies are now integral to modern warfare, providing critical capabilities such as remote sensing, signals intelligence, secure communications, Earth observation and precise navigation and timing. These systems enable commanders to maintain real-time situational awareness and coordinate operations across multiple theatres simultaneously. Since the First Gulf War, military dependence on such capabilities has grown steadily, making satellites not merely useful tools but essential infrastructure, and, inevitably, prime targets for adversaries with diverse and often hostile intentions.² As critical infrastructures, space assets become objects of aggression in armed conflict, targeted to destabilise or weaken an adversary's capabilities. This reality was vividly illustrated by the Russian invasion of Ukraine in February 2022, when one of the first acts of war was a cyberattack on ViaSat's KA-SAT network.³ This incident exposed both the vulnerability of space infrastructures and their critical importance in contemporary warfare.⁴

The growing strategic importance of satellites in armed conflicts raises fundamental legal questions about the characterisation of hostile actions under international humanitarian law. The space environment presents a distinctive legal challenge: determining whether specific actions constitute

¹ As evidenced by the collective contributions presented in this volume.

² BATAILLE-MESSINA 2020.

³ POIRIER 2022.

⁴ Council of the European Union 2022a.

an ‘armed aggression’ under the UN Resolution 3314,⁵ an ‘armed attack’ under Article 51 of the UN Charter⁶ or cross the threshold of prohibited force under Article 2(4)⁷ proves exceptionally difficult. Hostile actions in outer space typically manifest not as conventional kinetic attacks but rather as radio-frequency interference, simulated accidents, directed-energy operations, or unauthorised orbital manoeuvres, actions that require no conventional weaponry and leave limited forensic traces. Consequently, such actions occupy an indeterminate ‘grey zone’ between peacetime competition and armed conflict, the legal characterisation of which remains deeply contested. The extant framework governing international armed conflict appears inadequately equipped, if not obsolete, in addressing this spatial dimension.

The international community has acknowledged this governance gap. The Open-ended Working Group on the Prevention of an Arms Race in Outer Space in all its aspects⁸ (OEWG PAROS) (2025–2028) was established to develop possible norms, rules and principles of responsible behaviour in the space domain, thereby addressing the legal ambiguities inherent in characterising hostile space operations. A significant shift has occurred in legal analysis: rather than attempting to characterise whether a given space action constitutes an “armed attack” or prohibited force, emphasis has increasingly turned towards assessing the intent and behaviour of the acting

⁵ UN Doc. A/Res/3314 (XXIX), Annex Definition of Aggression, Preamble, para. 5.

⁶ As a reminder, Article 51 of the UN Charter states: “Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.”

⁷ Article 2(4) of the UN Charter states: “All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.”

⁸ UN Doc. A/Dec/79/512.

State, recognising that traditional thresholds of armed conflict may prove inadequate as analytical tools. Whilst the present analysis acknowledges this fundamental legal difficulty, the scope of the present chapter does not extend to resolving the question of act characterisation. Instead, the discussion proceeds from a distinctly European perspective,⁹ examining how the Union and its Member States may lawfully employ or protect space assets in contexts where armed conflict is at play.

For decades in Europe, the space domain had been regarded primarily through its societal, economic and scientific dimensions.¹⁰ The European Union (EU) was slow to acknowledge space as a sector of strategic relevance, as it possessed no formal competence in this field before the entry into force of the Treaty of Lisbon.¹¹ A similar situation prevailed within the European Space Agency (ESA), an intergovernmental organisation independent from the Union, whose mandate remains limited to the promotion of exclusively civilian space activities.¹²

However, over the past decade, this perception has been shifting profoundly.¹³ Starting in 2016 with the Space Strategy for Europe, which acknowledged the need to strengthen synergies between civil and security uses of space,¹⁴ this position was reinforced by the 2022 Strategic Compass for Security and Defence, which explicitly identified outer space as a contested domain of strategic significance alongside the high seas, air and cyberspace.¹⁵ These political documents reflect a progressive recognition that Europe's security and defence interests are tied to its space infrastructures.

The adoption in 2023 of the EU Space Strategy for Security and Defence (EUSSSD)¹⁶ represents the culmination of this evolution. The EUSSSD

⁹ For an analysis of the EU's role within the OEWG PAROS see BATAILLE 2025.

¹⁰ DE NEVE 2024.

¹¹ Its competence in the space sector was formally recognised with the Treaty of Lisbon and Article 189 of the Treaty on the Functioning of the European Union.

¹² ESA Convention, Article II.

¹³ ARADI 2024.

¹⁴ European Commission 2016: 10.

¹⁵ Council of the European Union 2022b.

¹⁶ European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2023.

formally enshrines the space and defence nexus, stating that “space is critical for the strategic autonomy of the EU and its Member States”.¹⁷ It affirms, on the one hand, the need to ensure security in space, conceived as the protection of European space assets against hostile acts, and, on the other, the objective of harnessing space for security and defence¹⁸ by enabling the operational use of EU satellites in support of civilian missions and military operations, in accordance with international law.¹⁹ This position was recently reaffirmed in the European Preparedness Union Strategy.²⁰

In view of this evolution, and of the Union’s explicit recognition of both security in space and space for security and defence, EU-owned satellites must now be understood as occupying an inherently ambiguous and increasingly exposed position. As dual-use infrastructures designed to serve civilian needs while simultaneously supporting defence and security objectives, they raise complex legal questions when employed in situations of international armed conflict. Their operational use by the EU and its Member States may qualify them as *tools* of warfare, while at the same time exposing them to being treated as potential *targets* of hostile action due to their perceived military value. These two hypotheses structure the present chapter: the first section examines the legal framework applicable to EU-owned satellites when used as *tools* in an armed conflict, while the second turns to the regime governing their potential qualification and treatment as *targets* in such a conflict.

Although the EUSSSD adopts a broad understanding of the space domain, encompassing not only orbital infrastructures but also ground stations, radio-frequency links, user terminals, and the associated cyber

¹⁷ European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2023: 1.

¹⁸ European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2023: 10–14; DARNIS–VECLANI 2011.

¹⁹ European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2023.

²⁰ European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2023a.

and industrial components that sustain them,²¹ the present chapter adopts a narrower focus. For the purposes of the analysis that follows, attention will be confined to satellites alone,²² and “EU-owned satellites” will be understood as those space systems that form integral components of the EU Space Programme as established by Regulation (EU) 2021/696.²³ This regulatory framework consolidates the Union’s space activities under a unified governance structure. It demonstrates that the EU is the owner of all tangible and intangible assets created or developed under the programme’s components.²⁴ The programme encompasses four primary components: Galileo,²⁵ Copernicus,²⁶ the EU Governmental Satellite Communications (GOVSATCOM),²⁷ and the Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS²),²⁸ and support services such as the European Union Satellite Centre (SatCen) and the EU Space Surveillance and Tracking Partnership (EU SST).

²¹ European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2023: 2.

²² This focus reflects the research framework of the present volume, *Legal and Policy Aspects of the Use of Satellites in Armed Conflicts*, which is specifically concerned with the legal status and uses of satellites, rather than with space infrastructures in a broader sense.

²³ Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU, OJ L 170/69, 12.5.2021.

²⁴ Regulation (EU) 2021/696, Article 9.

²⁵ Galileo is the EU’s global navigation satellite system, providing autonomous positioning, navigation and timing services.

²⁶ Copernicus is the EU’s Earth observation programme, providing environmental and security-related data.

²⁷ GOVSATCOM is a programme that aims to provide secure, resilient and cost-efficient satellite communications for critical missions and governmental operations.

²⁸ IRIS² is the EU’s initiative for secure satellite communication, enhancing connectivity and resilience.

EU-OWNED SATELLITES AS TOOLS
IN AN ARMED CONFLICT

In light of the preceding introduction, it must be concluded that the Union has expressly accepted that its satellite systems may be used for security and defence purposes. The EUSSSD reflects a clear policy choice to enable EU space programmes to support defence-related activities, notwithstanding their formally civilian designation. This is evidenced by the explicit anticipation of special regimes governing the provision of sensitive services and data to defence users, including differentiated access rights, operational safeguards and restrictions on dissemination, particularly in military contexts.²⁹ Such measures are incompatible with the notion that any military use of EU satellite assets would be merely subsidiary or exceptional. On the contrary, the Strategy affirms that defence and security requirements are to be integrated directly into the technical architecture of both future and existing EU space systems, noting that “the Commission will embed military and security user requirements in the design of relevant new EU space systems and the upgrade of relevant existing systems”.³⁰ This promotion of dual-use by design is also advanced in the European Preparedness Union Strategy.³¹ From an institutional perspective, EU space capabilities have now been incorporated into defence planning frameworks, with defence interests represented throughout EU space governance structures. Taken together, these developments demonstrate that the military use of EU space assets is not a contingent by-product of civilian programmes, but a foreseeable, authorised and institutionally prepared use, endorsed at both policy and structural levels of the Union.³²

²⁹ European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2023: 10.

³⁰ European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2023: 10.

³¹ European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2023a: 13.

³² Council of the European Union 2022b: 31–32; European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2023: 5–10.

This dual-use orientation is particularly evident in the Union's flagship constellations, Galileo, Copernicus and the forthcoming IRIS², all of which are explicitly associated with security and defence applications. Galileo offers a Public Regulated Service (PRS) restricted to government-authorised users and intended for sensitive applications requiring a high level of service continuity,³³ a capability described as a "critical enabler for military operations".³⁴ Copernicus, initially conceived under the name GMES (Global Monitoring for Environment and Security),³⁵ was from the outset designed to provide security-related services. Its data have already proved operationally useful to the Ukrainian armed forces.³⁶ However, it was not tailored initially to specific defence requirements, which explains the current efforts to establish an EU Earth Observation Governmental Service (EOGS)³⁷ for government-authorised users to support security and defence decision-making.³⁸ Sensitive geospatial intelligence products derived from Copernicus data are processed and disseminated through the SatCen, whose role has expanded significantly in support of Common Security and Defence Policy (CSDP) missions and the Member States' military operations.³⁹

³³ Decision No 1104/2011/EU of the European Parliament and of the Council of 25 October 2011 on the rules for access to the public regulated service provided by the global navigation satellite system established under the Galileo programme, OJ L 287/1, 4.11.2011.

³⁴ European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2023: 10.

³⁵ Regulation (EU) 911/2010 of the European Parliament and of the Council of 22 September 2010 on the European Earth monitoring programme (GMES) and its initial operations (2011 to 2013) Text with EEA relevance, OJ L 276, 20.10.2010.

³⁶ European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2023: 11.

³⁷ European Commission 2025a; European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2023: 11.

³⁸ European Commission 2024.

³⁹ European Union Satellite Centre 2025.

In parallel, GOVSATCOM⁴⁰ and IRIS²⁴¹ constellations are being developed with explicit provisions for secure military communications. The security and defence dimension of these assets has been publicly reaffirmed by the High Representative for Foreign Affairs and Security Policy and Vice President (HR/VP), who stated that European satellites “serve our military missions on the ground”, thereby acknowledging that space systems provide operational support to armed forces.⁴² In the same vein, the latest annual report on the implementation of the CSDP highlights the need to further develop the European Space Programme in light of the strong connections between the space and the defence and security sectors when preparing the new Multiannual Financial Framework (MFF).⁴³ This orientation is already reflected in the Commission’s proposal for the next MFF, notably through the European Competitiveness Fund, which enables closer alignment between Union space programmes and defence-related funding.⁴⁴

The fact that EU-owned satellites are now politically envisaged as supporting security and defence does not, by itself, settle the legal framework governing their use in an armed conflict. Instead, the applicable legal questions vary depending on which actor employs these satellites in that context. For the Union, as owner of the assets, the primary issue is not how it may use them, but more fundamentally whether it can itself become a party to an armed conflict at all. By contrast, for the Member States, which can undeniably become parties to an armed conflict by virtue of their status under international law, the focus shifts to the legal framework governing their use of EU-owned satellites and the potential consequences that such use may entail.

⁴⁰ European External Action Service 2017.

⁴¹ Regulation (EU) 2023/588 of the European Parliament and of the Council of 15 March 2023 establishing the Union Secure Connectivity Programme for the period 2023–2027, OJ L 79/1, 17.3.2023.

⁴² KALLAS 2025.

⁴³ European Parliament 2024: Point 150.

⁴⁴ European Commission 2025b.

The use by the EU of its satellites as tools in an armed conflict

The question of whether the EU may use its own satellites as tools in an international armed conflict presupposes, as a preliminary matter, an examination of the international organisation's capability to enter an armed conflict.⁴⁵

International organisations as parties to an armed conflict

In contemporary international law, the possibility that an international organisation may become a party to an armed conflict is no longer excluded in principle. The starting point lies in the International Court of Justice's (ICJ) jurisprudence on the legal personality of international organisations. In its Advisory Opinion of 11 April 1949 concerning *Reparation for Injuries Suffered in the Service of the United Nations*, the Court held that the United Nations "was intended to exercise and enjoy, and is in fact exercising and enjoying, functions and rights, which can only be explained based on the possession of a large measure of international personality and the capacity to operate upon an international plane".⁴⁶ This Advisory Opinion established that international legal personality is fundamentally contingent upon two essential factors: the existence of autonomous, intrinsic competences vested in the organisation, and the formal recognition of sufficient organisational autonomy to enable the effective exercise of such competences in pursuit of its mandated objectives.⁴⁷

⁴⁵ CLAPP 2023: 1. The European Parliament glossary terms bases its definition of armed conflict on the interpretation of the International Committee of the Red Cross: "An armed conflict is said to exist when there is an armed confrontation between the armed forces of States (international armed conflict), or between governmental authorities and organised armed groups or between such groups within a State (non-international armed conflict). Other situations of violence, such as internal disturbances and tensions, are not considered to be armed conflicts."

⁴⁶ International Court of Justice, *Reparation for Injuries Suffered in the Service of the United Nations*, 9.

⁴⁷ KOLB et al. 2005: 121–122.

At the same time, the Court emphasised that international organisations are entities created by their constitutive instruments and enjoy only attributed competences, those expressly conferred or necessarily implied by their mandates.⁴⁸ Their rights and obligations under international law are thus not general but confined to what is required to attain their functions.⁴⁹ This reasoning has been extended in doctrine and by bodies such as the Institute of International Law⁵⁰ to the field of armed conflict. Where an organisation is entrusted with security functions and possesses the material means to conduct military operations, it may acquire the *ratione personae* capacity to be bound by international humanitarian law (IHL), not through formal Treaty adherence but through customary IHL.⁵¹ Crucially, this capacity depends not on the legality of the resort to force (*jus ad bellum*), but on the factual engagement of organised armed violence reaching the threshold of an armed conflict.⁵²

On this basis, an international organisation may, in principle, qualify as a belligerent where its constitutive instruments entrust it with security or defence functions. This will be the case where, in exercising those functions, it commands organised armed forces and disposes of sufficient material means to conduct military operations of the requisite intensity. Only under such circumstances does it become meaningful to speak of the organisation using its assets, including space systems, as tools of warfare.

The EU's capacity to become a party to an armed conflict

Applied to the EU, this framework requires a careful distinction between international legal personality, on the one hand, and belligerent capacity, on the other. Since the entry into force of the Treaty of Lisbon, the Union

⁴⁸ Confirmed by the International Court of Justice in its 1996 Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons.

⁴⁹ KOLB et al. 2005: 123–125.

⁵⁰ Institute of International Law 1999.

⁵¹ FERRARO 2015: 1232.

⁵² International Committee of the Red Cross 2024: 5–7.

has acquired a whole international legal personality, enabling it to conclude treaties, assume international obligations, and act autonomously on the international plane.⁵³ By analogy to the ICJ's reasoning in the 1949 Reparations Opinion, the EU clearly meets the threshold for international legal personality: it possesses autonomous competences enumerated in its founding Treaties, its institutions display a sufficient degree of formal autonomy, and it constitutes a new legal order capable of producing binding effects independently of its Member States.⁵⁴

Possessing international legal personality does not, however, automatically confer upon the Union the capacity to become a belligerent. As developed above, such a personality operates only within the limits of the competences conferred upon the international organisation by the principle of speciality, and within the EU context, is further constrained by the principle of conferral.⁵⁵ The Union's foundational objectives are centred fundamentally on the proper functioning of the internal market, and whilst the Union has acquired specific competences in security and defence matters through the CSDP framework, these remain distinctly circumscribed.⁵⁶

CSDP missions include both military and civilian operations.⁵⁷ Nonetheless, the presence of military operations does not automatically mean that CSDP forces are involved in an armed conflict. Even in regions experiencing armed conflict, the presence of international forces does not inherently make them participants in the conflict.⁵⁸ Peace support troops can operate within a host nation engaged in active armed conflict

⁵³ The EU holds observer status with the General Assembly: UN Doc. A/Res/65/276: Participation of the European Union in the work of the United Nations.

⁵⁴ Judgment of the European Court of Justice, *Van Gend & Loos*, Case 26-62 (5 February 1963), para. 3: "The European Economic Community constitutes a new legal order of international law for the benefit of which the States have limited their sovereign rights, albeit within limited fields."

⁵⁵ The Treaty on European Union, Article 5.

⁵⁶ *FALCO* 2009: 175. It is an accepted opinion that the EU's CSDP will not establish an EU army responsible for the defence of the EU Member States.

⁵⁷ European External Action Service 2025a: 1.

⁵⁸ *BOTHE-DORSCHER* 2001: 501–502.

while avoiding engagement in hostilities, especially when their mandate is strictly limited.⁵⁹ Therefore, military operations led by the EU may avoid being classified as belligerent as long as their mandate limits involvement in active conflicts.

The EU's foundational values reinforce this legal circumscription: respect for human dignity, freedom, democracy, equality, the rule of law and human rights,⁶⁰ which are constitutive of its identity and further constrain the manner in which any use of force may be conceived. These values, embedded in the EU's constitutive Treaties, reflect a structural institutional preference for multilateral, law-centred responses rather than unilateral military action, rendering the notion of the EU as an autonomous belligerent fundamentally at odds with its founding Treaties.

This preference is further evidenced by the CSDP's institutional design. Unlike the United Nations (UN) or the North Atlantic Treaty Organisation (NATO), whose founding instruments explicitly identify the maintenance of international peace and security as central objectives and provide for robust military structures, the EU's CSDP⁶¹ is framed primarily in terms of crisis management, peacekeeping and conflict prevention,⁶² rather than for autonomous military action by the Union itself.⁶³ The empirical record confirms this orientation: an analysis of past and ongoing CSDP missions demonstrates that the Union predominantly engages in civilian operations characterised by low-intensity stabilisation and capacity-building activities, rather than in high-intensity military operations associated with belligerent status.⁶⁴

Beyond these institutional and normative constraints, the Union lacks the material means to conduct military operations, as operational capacity is built from civilian and military assets provided by the Member States, which retain sovereign command and control over the

⁵⁹ MURPHY 2003: 154; NAERT 2010: 470.

⁶⁰ The Treaty on European Union, Article 2.

⁶¹ The Treaty on European Union, Articles 21–46.

⁶² The Treaty on European Union, Article 42; European External Action Service 2025a: 1.

⁶³ SUR 2011: 288.

⁶⁴ DARNIS–VECLANI 2011: 3.

deployment, withdrawal and tactical direction of their forces.⁶⁵ This structural dependency on national contributions reveals that the EU lacks the autonomous material capacity to meet the threshold for becoming a party to an armed conflict. Even if EU operations involve a transfer of authority over military contingents, and even if such control is typically regarded under international law as crucial for attribution of conduct,⁶⁶ this principle remains contested.⁶⁷

Furthermore, our analysis must acknowledge a critical caveat. Although EU-led forces have not thus far become engaged in combat as a party to an armed conflict in any of the EU's military operations, the Union does not exclude, where necessary, the use of armed force in the conduct of a mission.⁶⁸ According to the Salamanca Presidency Declaration, "respect for IHL is relevant in EU-led operations when the situation they are operating in constitutes an armed conflict to which the forces are party".⁶⁹ On this reading, the EU accepted that IHL applies when EU-led forces become parties to an armed conflict and thereby acknowledged that those forces can, in principle, acquire such status.⁷⁰ However, even where force is used in self-defence, the law of armed conflict applies only when the force used crosses the threshold of an armed conflict.⁷¹

A related but secondary question merits consideration: might the Union receive authorisation or delegation from the UN Security Council to conduct operations involving the use of force? Whilst theoretically conceivable

⁶⁵ Key decisions for operations under the CSDP are taken by the Council of Ministers of the EU. The Treaty on European Union, Article 42.

⁶⁶ International Law Commission 2011.

⁶⁷ As evidenced by divergent approaches in the International Law Association's final report on the accountability of international organisations of 2004. NAERT 2010: 515–517.

⁶⁸ Council of the European Union 2014: 16.

⁶⁹ A final document of a seminar organised by the Spanish Presidency of the EU, 22–24 April 2002, on the enforcement and application of international law, including IHL, in EU-led operations, in Salamanca, Doc. DIH/Rev.01.Corr1, exposed by NAERT 2011: 233–234.

⁷⁰ NAERT 2011: 233–235; NAERT 2013: 638–641.

⁷¹ NAERT 2010: 472–473.

under Article 53 of the UN Charter,⁷² such delegated authority would not transform the Union into an autonomous belligerent. When the Security Council entrusts the execution of its mandates to regional organisations, such as NATO in the Balkans,⁷³ it grants juridical legitimacy to the use of force whilst retaining primary responsibility for international peace and security. The delegated entity acts as an instrument of the collective security system, not as an independent international subject exercising autonomous belligerent capacity.⁷⁴ Critically, an EU operation conducted pursuant to Security Council authorisation would necessarily be circumscribed by the scope of that mandate. The Union would act not as a *sui generis* belligerent, but as an executive agent implementing a collective decision within parameters defined by the Council. Even where authorisation permits the use of force, the threshold for belligerent status in international humanitarian law remains distinct from mere authorisation to employ military means. Furthermore, to become a belligerent through a Security Council delegation would require a radical departure from the EU's established practice.

Consequently, although the Union's status as a belligerent in armed conflict is not legally precluded in principle, the combination of restrictive legal thresholds and structural safeguards enshrined in the European Treaties makes such a scenario exceptionally unlikely in practice. Should such a situation arise, the range of legal questions that would follow would be significant and would fall outside the scope of the present analysis. However, the use of European satellites in such circumstances should not differ, in principle, from their current use by the Union for security and defence purposes, outside the framework of an armed conflict.

⁷² Article 53 of the UN Charter, which permits the Security Council to utilise regional arrangements for the application of coercive measures under its authority.

⁷³ UN Doc. A/Res/1244 (1999), Resolution 1244 (1999) on the deployment of international civil and security presences in Kosovo.

⁷⁴ BLOKKER 2000.

*The use by the EU of its satellites for
security and defence purposes*

However, the fact that the Union has not yet acquired belligerent status does not preclude it from intervening in security and defence matters, provided that such intervention conforms to international law.⁷⁵ As established above, EU interventions in the security domain have operated primarily through upstream conflict prevention and downstream stabilisation, employing diplomatic engagement, economic measures, security sector reform, civilian missions and limited advisory operations.⁷⁶

Within this operational framework, EU policies have progressively recognised space systems as strategic dual-use infrastructures capable of supporting these security and defence activities. The EU Space Programme now explicitly serves CSDP objectives,⁷⁷ and the Union accordingly utilises its own space systems in support of CSDP missions.⁷⁸ The crisis in Libya in 2011 provides a pertinent illustration of this capacity. Although NATO conducted the primary military intervention, the EU established a parallel military operation, EUFOR Libya, whose mandate was limited to humanitarian stabilisation.⁷⁹ To fulfil this mission, space assets, specifically Copernicus services, were used to provide rapid geospatial intelligence and damage assessment of critical infrastructure, such as airports and seaports.⁸⁰

This practice confirms that whilst the EU itself cannot become a belligerent, it can and does employ its space assets to support broader security and stabilisation activities within its competences. The question that remains is whether, and under what conditions, Member States may themselves rely on these Union space assets in the conduct of their own military operations in armed conflicts.

⁷⁵ European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2023.

⁷⁶ SUR 2011: 286.

⁷⁷ Regulation (EU) 2021/696, Recitals 79 and 100.

⁷⁸ European Parliament 2024: Point 152.

⁷⁹ Council of the European Union 2011.

⁸⁰ DARNIS-VECLANI 2011: 9–10.

*The use by the Member States of the EU-owned
satellites as tools in an armed conflict*

The capacity of the Member States to engage in international armed conflict is beyond question. Notwithstanding their membership of the Union, they retain their status as sovereign States and, consequently, all prerogatives deriving therefrom under public international law, including the right to resort to armed force within the limits established by the UN Charter. The relevant issue is therefore not whether the Member States may enter into an armed conflict, but rather if once engaged in such a conflict, they may lawfully rely on data and services derived from EU-owned satellite systems.

The prospect of using EU-owned space capabilities for the security and defence needs of the Member States is challenging to contest when examined in light of the Union's own legal instruments. The EU Space Programme expressly lists among its general objectives the aim to "enhance the safety and security of the Union and its Member States",⁸¹ thereby anchoring security and defence-related uses within the very rationale of the Programme. In the same vein, IRIS² is designed to deliver added-value services, such as anonymity of use, low latency and enhanced flexibility, to governmental users,⁸² with Member States exercising effective control through mechanisms comparable to those governing access to Galileo's PRS. It should further be noted that the EUSSTD opens its conclusion by stating that "space systems and services in the EU contribute to the strategic autonomy of the EU and its Member States".

In light of these provisions, the European political and legal framework not only permits but structurally organises the use by Member States of EU-owned satellites and derived services for security and defence purposes, including in the specific context of armed conflict. Accordingly, rather than questioning the permissibility of such uses, the more pertinent analysis is to examine the potential legal consequences that may flow from them for the Union, the other Member States and ESA, particularly about their possible qualification as 'co-parties' to an armed conflict. To that end, the

⁸¹ Regulation (EU) 2021/696, Article 4.

⁸² Regulation (EU) 2023/588, Article 3.

following analysis proceeds in two stages: it first examines the threshold of co-belligerency as it applies to satellite-enabled forms of support in contemporary armed conflict, before turning to the question of attribution of participation in hostilities to the Union, the Member States and the ESA.

The co-party threshold and satellite-enabled support

The central question examined here is whether the use by a Member State of data from European satellites gives rise to legal repercussions for the Union and other Member States, and, more specifically, whether such use would render them 'co-parties'⁸³ to an armed conflict. It must be emphasised at the outset that this question arises principally in relation to access to the secure or restricted components of satellite systems, rather than to publicly available data,⁸⁴ which are already routinely used in armed conflicts without raising issues of third-party involvement.

It must first be established that international law does not clearly define the moment at which a State may be considered to have become a party to an armed conflict, nor does it provide definitive criteria for participation in a pre-existing armed conflict.⁸⁵ This doctrinal lacuna is particularly significant: the threshold at which support provided by one or several States to another in its fight against a common enemy renders the supporting State(s) a party to the armed conflict remains ambiguous.⁸⁶

The prevailing approach in contemporary IHL holds that financing, the provision of equipment (including transfers of arms), the furnishing

⁸³ For the purposes of this analysis, the terms "co-belligerency" and "co-party" are used interchangeably, notwithstanding the substantive doctrinal differences between them, as a detailed examination of these distinctions falls outside the scope of the present inquiry. For the same reason, this analysis will also not tackle the difference between international armed conflict (IAC) and non-international armed conflict (NIAC).

⁸⁴ Programme of the European Union, Copernicus Data Access (<https://www.copernicus.eu/en/access-data>).

⁸⁵ International Criminal Tribunal for the Former Yugoslavia, Prosecutor v. Tadić; GRIGNON 2022: 1.

⁸⁶ WENTKER et al. 2024: 8–10.

of intelligence, and the training of armed forces do not, in themselves, confer the status of co-belligerent.⁸⁷ The decisive criterion is the existence of a direct operational connection to hostile acts and engagement in the planning or supervision of specific military operations.⁸⁸ A broad strand of the doctrine agrees that supplying arms, in and of itself, lacks the requisite direct operational nexus to an international armed conflict to qualify as co-belligerency.⁸⁹ Instead, a State would typically acquire co-belligerent status only through: the use of force against the adversary (for instance, through the establishment of prohibited military zones), the provision of intelligence that forms an integral part of concrete military operations and targeting processes, or the provision of territory as a base for the launching of military operations.⁹⁰

Applied to satellite activities, this suggests that the mere provision or availability of EU satellite data, absent operational integration into specific attack plans, falls short of the co-belligerency threshold, a conclusion reinforced by State practice in which extensive space-based support (encrypted GPS signals for allies, Ukrainian use of Copernicus imagery, Galileo navigation and commercial satellite communications) has not led to the supporting entities being treated as parties to the conflict. This legal framework has been validated by recent international developments. The international community formally recognised the Russian Federation's aggression on Ukraine,⁹¹ affirming its right to self-defence under Article 51 of the UN Charter. Within this context, the provision of EU satellite data and related geospatial intelligence to Ukrainian armed forces exemplifies the permissible scope of such support, through which the Union supports Ukraine in the exercise of its legitimate right to self-defence. Therefore, the assistance of this nature remains compatible with the legal constraints on third-state participation in armed conflict.

⁸⁷ International Committee of the Red Cross 1977, Article 43; WENTKER et al. 2024: 17–21.

⁸⁸ MELZER 2009.

⁸⁹ HELLER–TRABUCCO 2022: 263–265.

⁹⁰ GRIGNON 2022: 2.

⁹¹ UN Doc. A/Res/ES-11/1, Aggression against Ukraine.

*Attribution of conflict participation to
the EU, Member States and ESA*

Against this background, the next step is to assess whether, and under what conditions, the Union, other Member States or ESA might nonetheless incur legal consequences, particularly co-belligerent status, through a Member State's use of EU-operated satellite systems in an armed conflict.

Turning first to the EU itself, before examining whether the provision of satellite data could render the Union a co-party to an armed conflict, it is necessary to recall that, as demonstrated above, the question of whether the EU can itself enter into an armed conflict remains legally unsettled. The prevailing view, however, is that it most certainly will not itself be regarded as a belligerent in the sense of the law of armed conflict, and mere ownership or operation of dual-use infrastructure such as satellite systems does not, in and of itself, amount to participation in an armed conflict. In this respect, the Union's position is closely analogous to that of States hosting undersea communication cables: even though such neutral infrastructure may be intensively used or targeted by belligerents, this does not, in and of itself, render the coastal or territorial State a party to the conflict,⁹² and by the same token the fact that military operations rely on EU satellites does not, by itself, turn the Union into a co-belligerent.

As Member States retain their full sovereignty and status as independent subjects of international law, the threshold articulated above must be applied. Co-belligerency, in the context of international armed conflict, requires both a direct connection to hostilities and a significant degree of operational cooperation with a belligerent State. In this regard, the relevant conduct is the act of the individual State employing satellite-derived data in support of its military operations. That act must be assessed as the act of a State under general international law, not as the act of a "Member State" in its

⁹² HEINTSCHEL VON HEINEGG 2017.

institutional capacity within the Union.⁹³ The sole link to the Union lies in the fact that the data originates from an EU satellite. Still, this technical provenance does not alter the legal classification of the conduct as that of the using State. The provision of satellite data by the Union, particularly when accessed by a Member State through established institutional frameworks with the agreement of all Member States, represents an attenuated form of support that lacks the operational directness required by IHL. In light of these considerations, the prospect that non-participating Member States could incur legal consequences under the law of armed conflict as a result of such indirect involvement appears far-fetched.⁹⁴

A further question arises regarding ESA, which plays an active operational role in the functioning of the Union's satellite systems. However, the practical difficulties of attributing co-belligerent status to ESA are even more pronounced than in the case of the Member States. Not only would there be no rational interest for an adversary State in characterising a technical and scientific organisation as a co-party to a conflict, but such a characterisation would appear conceptually incoherent under the law of armed conflict. ESA possesses neither the legal capacity to wage war nor the political authority to direct military operations; it functions solely as the technical operator of the infrastructure.⁹⁵ Therefore, to attribute belligerent status to such an entity would appear even more far-fetched.

In conclusion, the legal consequences of a Member State's use of EU-operated satellite systems in an armed conflict appear either minimal or non-existent for the Union, the other Member States and ESA, provided such use is consistent with the Member State's obligations under international law. The links connecting these entities to the Member State utilising

⁹³ NAERT 2010: 526. As to the question of the legal consequences for EU Member States engaged in an EU-led operation when that operation becomes a party to a conflict, the prevailing view holds that the Member States do not thereby acquire the status of parties to the conflict. By extension, the utilisation of satellites by the Union or by individual Member States would not, in itself, constitute participation in an armed conflict by the other Member States.

⁹⁴ NAERT 2010: 526.

⁹⁵ ESA Convention, Article II.

satellite data are considerably more attenuated than in other empirical examples that have not, in practice, led to the characterisation of third parties as co-belligerents.

EU-OWNED SATELLITES AS TARGETS IN ARMED CONFLICT

The preceding section established that EU space systems are explicitly designed and operationally employed as military tools. This military use may lead adversaries to regard them as potential targets. The question, therefore, arises: What legal framework governs the EU's and its Member States' response to attacks against EU-owned satellites?

The EU has become acutely conscious of this vulnerability. While the EUSSSD explicitly acknowledges that space assets face diverse and evolving threats,⁹⁶ the Strategic Compass emphasises the greater urgency in addressing hostile acts originating in or directed against outer space.⁹⁷ This recognition reflects the acknowledgement that space is no longer conceived as a sanctuary immune from conflict, but as a contested operational domain where European assets face significant risks.

Whilst the Union does not pursue aggressive or offensive space capabilities, it seeks to prepare itself to defend against attacks, as space systems are essential to European economies and societies.⁹⁸ The EUSSSD stresses that contemporary European societies depend fundamentally upon space services for financial systems, transportation networks, energy grids and military operations. Loss or degradation of these services would produce cascading effects, justifying space infrastructure protection as a core security priority. The Union's approach, therefore, emphasises resilience rather than offensive posturing.

⁹⁶ European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2023.

⁹⁷ Council of the European Union 2022b.

⁹⁸ European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2023: 3.

To address these challenges, the Union has established political coordination and governance processes designed to respond more effectively to space threats and attacks. While the overall model broadly mirrors the approach used for non-space-related threats, its application is considerably more complex due to the specific technical characteristics and cross-domain dependencies of space systems. As with other types of hostile activity, the first step is to detect, characterise and attribute the threat, to enable a timely, proportionate, and coherent response at both national and EU levels.⁹⁹ It is therefore necessary to begin by examining the mechanisms for detection and characterisation that enable attribution, before turning to the question of response.

*From technical detection and
characterisation to legal attribution*

The detection and characterisation of space threats do not primarily raise legal questions, but rather technical, operational and governance challenges involving the Union, its various specialised entities, and the Member States. These mechanisms are nonetheless essential to addressing one of the most complex legal issues in the context of space attacks, namely the attribution of responsibility.

Technical detection and characterisation of space attacks

One of the main technical challenges in the space domain is achieving near-real-time awareness of activities in orbit, which is the function of the Space Domain Awareness (SDA). It consists of detecting, identifying and characterising space objects of interest in near real time, understanding their behaviours, and linking this information to underlying doctrines

⁹⁹ European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2023: 7.

and associated space systems.¹⁰⁰ This situational picture is nourished by intelligence from Member States, with the EU cooperating closely with national space commands that provide regular updates on threats in orbit.¹⁰¹

The Union's SDA architecture rests on several complementary components that collectively support both operational protection and legal attribution. The EU SST Partnership provides collision and fragmentation detection based on Member States sensors,¹⁰² and, the SatCen delivers geospatial intelligence that supports attribution by detecting adversary activities and assessing damage to space and ground infrastructure. In parallel, the Single Intelligence Analysis Capacity (SIAC) produces classified analyses of the space threat landscape by synthesising Member States intelligence and open-source information, thereby contextualising detected activities within broader strategic assessments. At the same time, the Cybersecurity Service for the Union Institutions, Bodies, Offices and Agencies (CERT-EU) and national cyber authorities conduct forensic analysis of cyber-based threats targeting space systems and their ground segments.¹⁰³

To reinforce this ecosystem, the Union is developing the European Space Shield initiative. This project is intended to strengthen Member States' defence capabilities and enhance the resilience and protection of space assets and services in an increasingly hostile threat environment.¹⁰⁴ The overarching objective is to establish and safeguard a coherent European system of space capabilities serving defence purposes, building on both EU space systems and existing national capacities, and thereby providing a more robust basis for credible attribution and response.

¹⁰⁰ European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2023: 8.

¹⁰¹ KALLAS 2025.

¹⁰² Regulation (EU) 2021/696, Article 4.

¹⁰³ FIOTT 2022: 25.

¹⁰⁴ European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2025b: 8.

Legal attribution of space attacks

Attribution is one of the central legal challenges raised by space attacks, since any meaningful response presupposes that the conduct can be linked to a responsible State or, at least, to identifiable non-State actors. The mechanisms for detecting and characterising space activities are therefore not merely operational tools, but indispensable preconditions for legally and politically credible attribution. The EUSSSD explicitly underlines that SDA is “key for attributing space threats in orbit and triggering a potential EU response” and calls on Member States that own and develop the relevant capabilities to provide SDA services to the Union to ensure its strategic autonomy in the space domain.¹⁰⁵

However, in practice, even robust SDA capabilities do not eliminate the inherent difficulties of attribution. It remains particularly challenging for non-kinetic operations where technical forensics are ambiguous, for in-orbit activities carried out by satellites with opaque ownership or control structures, and for dual-use behaviours that may mask hostile reconnaissance or weapons testing behind ostensibly civilian or commercial operations.¹⁰⁶ Indeed, the non-physical nature, cross-domain effects and anonymity that characterise cyber operations against space infrastructure further complicate the identification of perpetrators and the legal qualification of their acts under the existing international framework. These features hinder both the assessment of whether an operation reaches the threshold of use of force and the ability to attribute that operation to a State with the standard of proof required by the law on State responsibility.¹⁰⁷

In sum, resolving the most acute attribution difficulties will depend not only on the progressive clarification of applicable legal standards, but also, perhaps primarily, on strengthening the protection of space systems to reduce the scope for successful attacks in the first place, and on continuously

¹⁰⁵ European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2023: 8.

¹⁰⁶ CESARI et al. 2020.

¹⁰⁷ SU-JIANG 2025.

improving the technical mechanisms for detecting and characterising hostile activities in orbit.

Legal framework governing responses to space attacks

Once a space attack has been technically characterised and legally attributed, the question of how to respond becomes central. The notion of retaliation, understood here in a broad sense encompassing restrictive measures, diplomatic action and other non-forcible responses, remains relatively novel in the space context.¹⁰⁸ Depending on the gravity of the incident, the nature and extent of its effects, and the degree of political consensus, responses may be undertaken at the EU level or by Member States acting collectively.

Institutional EU response: Council Decision 2021/698

Mindful of the threats facing its critical space systems,¹⁰⁹ the Union has, through Council Decision (CFSP) 2021/698, established a framework that enables it not only to safeguard the continuity and integrity of its space infrastructure, but also to attribute and respond to threats that affect, or may affect, the security of the Union and its Member States.¹¹⁰

In the event of such a threat, the Decision provides that the Member States, the Commission, the European Union Agency for the Space Programme, or any security monitoring structure designated, are under an obligation to inform the HR/VP without delay of all relevant elements at their disposal.¹¹¹ The HR/VP, in turn, must immediately notify the Council of the threat and

¹⁰⁸ KALLAS 2025.

¹⁰⁹ Council Decision (CFSP) 2021/698 of 30 April 2021 on the security of systems and services deployed, operated and used under the Union Space Programme which may affect the security of the Union, and repealing Decision 2014/496/CFSP, OJ L 170/178, 12.5.2021, Recital 5.

¹¹⁰ Council Decision (CFSP) 2021/698, Article 1.

¹¹¹ Council Decision (CSFP) 2021/698, Article 2.

its potential implications for the security of the Union or of one or more Member States, accompanied by proposed instructions on the course of action to be taken. The Council, acting unanimously on a proposal from the HR/VP, then adopts the necessary instructions.¹¹² Where, however, the urgency of the situation does not allow for a prior Council decision, the HR/VP is authorised to adopt the provisional measures required, which the Council is subsequently called upon to confirm, amend or revoke as soon as circumstances permit.¹¹³

Although the Union asserts ownership over its space assets, the power to determine the substance of the response remains vested in the Council acting unanimously, with the HR/VP's autonomous role strictly circumscribed and confined to provisional action in situations of urgency. This unanimity requirement ensures that Member States retain decisive control: no response measure may proceed without the collective consent of Member States. Though structured by a Council Decision, the decision-making process remains fundamentally intergovernmental, with the HR/VP serving as coordinator of Member States will rather than as an independent institutional actor.

The EUSSSD clarifies that this mechanism is intended to serve as a dedicated “space toolbox”, complementary to the Union's cyber diplomacy and hybrid toolboxes.¹¹⁴ The range of responses contemplated includes, at the technical level, the activation of specific operational response modes embedded in the security design of space systems; at the diplomatic level, discussions, engagement in multilateral fora and public statements by the Union and the Member States aimed at preventing and responding to irresponsible behaviour in the space domain; and, at the economic level, the use of restrictive measures, including sanctions. The EU Military Staff is, furthermore, tasked with preparing any potential military contribution to the

¹¹² Council Decision (CSFP) 2021/698, Article 3.

¹¹³ Council Decision (CSFP) 2021/698, Article 4.

¹¹⁴ European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2023: 8–9.

Union's response in the space domain, thereby connecting this framework to the Union's broader security and defence posture.¹¹⁵

Notably, the EUSSSD explicitly envisages that Article 42(7) TEU on mutual defence could be invoked "should a space threat or incident amount to an armed attack on its territory".¹¹⁶ However, from a legal perspective, recourse to this Treaty provision in the context of space satellites is not as straightforward as it may appear. Careful analysis of this question is therefore required.

Collective Member States response: Article 42(7) TEU

Article 42(7) TEU provides that if a Member State is the victim of armed aggression on its territory, the other Member States shall have an obligation of aid and assistance by all the means at its disposal, in accordance with Article 51 of the Charter of the UN.¹¹⁷ The incorporation of this mutual defence commitment into EU primary law¹¹⁸ marked a significant step in the emergence of a European defence architecture, anchoring collective defence within the EU's own legal order rather than relying solely on NATO structures or bilateral arrangements.

It is now necessary to examine the impact of the distinctive characteristics of the space domain on the activation of this article and subsequently on the nature and implementation of the obligation of aid and assistance.

¹¹⁵ European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2023: 9.

¹¹⁶ European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2023: 9.

¹¹⁷ The Treaty on European Union, Article 42(7).

¹¹⁸ Introduced with the Lisbon Treaty and therefore terminating the Modified Brussels Treaty.

Challenges to activating Article 42(7) in the space domain

The legal threshold for triggering the Article is 1. an act of armed aggression 2. occurring on the territory of a Member State. However, in the event of an attack against a European satellite, satisfying these two criteria appears problematic. The potential activation of the mutual defence clause in response to such an attack faces two primary obstacles: the definition of what constitutes an ‘armed aggression’ within the space domain and the requirement of territoriality.

*The terminology of “armed aggression”
through the prism of space*

It is first necessary to examine the terminology the Union selected for its mutual defence clause. Unlike Article 5 of the North Atlantic Treaty or Article 51 of the UN Charter, which reference an “armed attack”,¹¹⁹ Article 42(7) TEU employs the term “armed aggression”.¹²⁰ The ICJ defines an armed attack as “the most grave forms of the use of force”,¹²¹ whereas the notion of aggression is understood to be “the most serious and dangerous form of the illegal use of force”.¹²² Even though Article 3 of the Definition of Aggression lists serious uses of force that often amount to an armed attack, the concepts are not interchangeable;¹²³ consequently, it is always necessary to analyse whether a particular act meets the gravity threshold of an armed attack.¹²⁴ The choice of the term ‘armed aggression’ therefore has the consequence of lowering the threshold for triggering the mutual defence clause.¹²⁵

¹¹⁹ The terminology diverges between the English and French versions.

¹²⁰ FAZIO 2025.

¹²¹ International Court of Justice, *Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua v. United States of America*), 101.

¹²² UN Doc. A/Res/3314 (XXIX), Annex Definition of Aggression, Preamble, para. 5.

¹²³ UN Doc. A/Res/3314 (XXIX), Annex Definition of Aggression, Article 3.

¹²⁴ FAZIO 2024.

¹²⁵ BODDENS HOSANG – DUCHEINE 2023; CLAPP–VERHELST 2022; MARTIN 2024: 269–270.

This lower threshold raises the question of whether the clause could be triggered by a cyberattack that remains below the threshold of a conventional military attack but inflicts significant damage on an EU Member State.¹²⁶ This question is essential for our analysis: while one cannot exclude the possibility of a satellite collision or an anti-satellite (ASAT) strike, the primary risks threatening satellites remain cyberattacks, as demonstrated by the Russian attack on the ViaSat network.

In general, applying international law to cyberspace is complex. Although the UN General Assembly has recognised that international law is fully applicable to cyberspace, just as it is to traditional conflict areas on land, at sea and in the air, the international community continues to grapple with this issue.¹²⁷

The Union has not provided a concrete answer as to whether a cyberattack would entail the potential activation of the mutual defence clause.¹²⁸ However, it must be highlighted that it has already organised scenario-based exercises on the activation and implementation of the mutual assistance clause following large-scale cyberattacks.¹²⁹

Nevertheless, the interpretation governing the legal threshold for activating the article appears sufficiently expansive, when analysing the unique activation of the article by France in November 2015, following the terrorist attacks in Paris.¹³⁰ This precedent is particularly instructive, as the clause was activated in response to terrorism, despite the initial understanding that armed aggression must originate from an external State actor.¹³¹ This expansive interpretation of 'armed aggression' that emerged from that unique

¹²⁶ FAZIO 2025.

¹²⁷ UN Doc. A/Res/73/266: Advancing responsible state behaviour in cyberspace in the context of international security. The Tallinn Manual 2.0, widely regarded as authoritative in this field, establishes that a cyber operation resulting in serious injury or death or causing significant damage to or destruction of property would meet the threshold and effects of an actual armed attack.

¹²⁸ European Commission 2020.

¹²⁹ Council of the European Union 2022b.

¹³⁰ ANGHEL-CIRLIG 2016; MARTIN 2024.

¹³¹ Although France justified this by stating that the attacks had been planned in Syria. MARTIN 2024: 270–271.

activation to date suggests that a similarly expansive interpretation could equally apply in the present context of cyberattacks and space operations.

Therefore, it falls to the victim Member State to determine, in its sole discretion, whether that specific cyberattack constitutes an “armed aggression” within the meaning of Article 42(7) and thus warrants its invocation, and secondly, whether the aggression occurred on its territory, the second critical legal threshold for activation.

The territorial requirement challenged by space specificity

It is now necessary to examine the second legal threshold of Article 42(7) TEU: the requirement that the aggression must occur on the territory of a Member State. Regarding the space domain, this question arises on at least two levels: first, concerning an attack¹³² on the ground segment of a space system located on Member State territory; and second, regarding armed aggression against the space segment.

At first glance, the first scenario does not raise significant territoriality issues, as the ground segment is physically located within the territory of a Member State. By contrast, the second scenario is more complex. Since satellites operate in outer space, an international realm,¹³³ one might assume that armed aggression against them would not occur on the territory of a Member State. Thus, the conditions for activating the clause would not be met.

However, from a technical perspective, the ground segment cannot function without the satellite segment, and *vice versa*. Given this interdependence, it is difficult to envisage how an attack on one component would not affect the other. Consequently, it would be logical to argue that if the space segment were to suffer armed aggression, this could be interpreted as an attack on the space system as a whole, and, by extension, on the ground segment located on Member State territory.

¹³² The terms “(armed) aggression” and “attack” are used interchangeably herein for stylistic purposes to avoid repetition and should not be confused with the legal concept of “armed attack” under international law.

¹³³ FIOTT 2022: 26–27.

If this interpretation remains unconfirmed, an analysis of European legislation suggests that the Union has not adopted the logic of treating space systems as unified wholes. Indeed, the NIS2 Directive,¹³⁴ (which concerns the cybersecurity of sectors designated as highly critical, including the space sector) confines its *ratione materiae* scope to “ground-based infrastructure [...] that support[s] the provision of space-based services”,¹³⁵ thereby explicitly excluding the space segment of the system. This approach clearly establishes a distinction in status and applicable legal regime between the space and ground components of a space system. Even if this choice likely stems from pragmatic considerations regarding the implementation and verification of the Directive’s provisions, by analogy, one might be compelled to conclude that this distinction would also apply to the interpretation of Article 42(7). This would prevent armed aggression against satellites from being encompassed within the scenarios for activation, as they do not fulfil the article’s territoriality condition.

This challenge that the EU faces reflects a broader interpretive problem affecting collective defence frameworks. NATO faces a similar predicament under its mutual defence clause.¹³⁶ Article 6 of the North Atlantic Treaty defines ‘armed attack’ as occurring either on the territory of the parties [similar to Article 42(7)] or “on the forces, vessels, or aircraft of any of the Parties”.¹³⁷ It would thus appear that satellites do not fall within the direct scope of NATO’s mutual defence clause.¹³⁸ However, NATO leaders have recently agreed that “attacks to, from, or within space present a clear challenge to the security of the Alliance, the impact of which could threaten national and Euro-Atlantic prosperity, security and stability, and could be as harmful to modern societies as a conventional attack. Such attacks could lead to the

¹³⁴ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333/80, 27.12.2022.

¹³⁵ Directive (EU) 2022/2555, Article 2 and Annex I.

¹³⁶ See the chapter authored by Endre Miszori in this book.

¹³⁷ North Atlantic Treaty, Article 6.

¹³⁸ North Atlantic Treaty, Article 5.

invocation of Article 5”.¹³⁹ This precedent demonstrates that where political will converges with strategic necessity, mutual defence clauses can evolve beyond their textual scope to encompass space-based threats.

Therefore, it seems that where political will exists, as has been the case with NATO, the interpretation of these provisions can evolve alongside technological and societal advancements. A similar development could occur with respect to the Union and Article 42(7). Whilst the EUSSSD stated that Member States can invoke the mutual assistance clause “should a space threat or incident amount to an armed attack on its territory”,¹⁴⁰ this formulation remains ambiguous regarding the territoriality of the incident: it could still refer exclusively to the ground segment rather than encompassing attacks on satellites in orbit.

In January 2025, the HR/VP affirmed that Member States may resort to Article 42(7) if “an attack in space or against space infrastructure” were to occur.¹⁴¹ The formulation ‘attack in space’ suggests an attack against the space segment of the system, thereby potentially extending the territorial threshold. Unlike NATO’s explicit political commitment, the Union’s stance remains comparatively ambiguous and less categorical, leaving open the question of whether the mutual defence clause can be invoked for armed aggression directed solely against satellites in orbit.

However, a more expansive interpretation could bring the legal conditions into line with the political ambition to apply Article 42(7) to a space attack, through what is known as an effects-based analysis.¹⁴² Initially developed in the context of cyberattacks, this approach focuses not on where an attack originates, but on its direct and significant consequences within Member State territory. An operation occurring outside physical territory can constitute armed aggression “on” that territory if it produces

¹³⁹ North Atlantic Treaty Organization 2021. A position confirmed by NATO’s updated policy on “Collective Defence and Article 5” on its website last updated in November 2025.

¹⁴⁰ European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2023: 9. Confirmed by the Council Conclusions on the EUSSSD.

¹⁴¹ KALLAS 2025.

¹⁴² MARTIN 2024: 267–268.

direct material effects on critical infrastructure. This framework could be applied to space systems, as EU space infrastructure constitutes critical infrastructure of sovereignty:¹⁴³ attacks disabling these systems produce cascading consequences on terrestrial territory, affecting financial systems, power grids, transportation networks and emergency services.¹⁴⁴ The HR/VP's statement that "when we defend space, we are defending our economies [...] [t]he security of our satellites is the security of our societies"¹⁴⁵ captures this logic: space system security directly determines territorial security and functionality, thereby satisfying Article 42(7)'s territorial requirement through demonstrated effects rather than physical location. However, this effects-based doctrine carries a significant interpretive risk: the framework relies on causality chains that may be difficult to establish with legal certainty, distinguishing between a space attack producing direct armed aggression consequences versus collateral economic damage remains contested, potentially lowering the threshold for what constitutes actionable armed aggression under the mutual defence clause.

In sum, the territorial condition is undermined in the context of space-based aggression. Traditionally rooted in a physical and geographical conception of territory, this requirement struggles to apply to attacks on orbiting satellites. However, the Union's political will and broad legal interpretations, notably the effects-based approach, enable the legal thresholds to be met and Article 42(7) activation to be possible.

However, another critical question remains: Article 42(7) stipulates that the victim of armed aggression must be a Member State. Yet, since the Union is the owner of European satellites, if an attack were to occur against them, the victim would not be a Member State but the EU itself. An attack against a European system targeting its ground segment does not raise this question acutely, as that component is physically located on the territory of a Member State; thus, that State would have suffered aggression on its territory even though the assets concerned belong to the Union. The question becomes more delicate for satellites operating in

¹⁴³ Council of the European Union 2022b; DEEN et al. 2022: 16.

¹⁴⁴ FAZIO 2024: 10.

¹⁴⁵ KALLAS 2025.

outer space. In such circumstances, is a Member State the “victim”? If the Union is the victim of an attack against a European satellite, and since these services serve all Member States collectively, then all Member States are simultaneously victims. But who, then, must assist whom? It would appear that in such cases, all Member States would be required to assist the Union itself. This would require yet another expansive interpretation of Article 42(7), prompting questions about its actual relevance and coherence. Even as EU documents and political declarations persistently reference Article 42(7) as the response mechanism to space attacks,¹⁴⁶ the entirety of the legal thresholds associated with its activation appears undermined by spatial specificity, or at a minimum, by the specificity of attacks against EU-owned satellites. This illustrates that where political will exists, legal safeguards are interpreted and reconfigured to such an extent that one must question the very pertinence of such juridical barriers. This question hangs unresolved.

We must now turn to the duty of aid and assistance that flows from the activation of this article, to determine what substantive obligations actually weigh upon Member States once this clause is invoked.

Consequences of the space domain for aid and assistance obligations

Once activated, Article 42(7) creates a legally binding obligation on all Member States to assist the attacked State. However, the article prescribes neither a formal procedure for invoking it nor any requirements for the assistance provided thereafter. Understanding how this framework applies to space requires examining both its flexibility in practice and its articulation with complementary legal mechanisms.

¹⁴⁶ Council of the European Union 2022b; European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2023: 9; KALLAS 2025.

Great flexibility in invocation and Member States response

When France invoked Article 42(7) following the 2015 terrorist attacks, it did so only by way of a political declaration, since neither detailed procedural requirements nor prior authorisation by an EU institution are required. Although the Council discussed the French invocation, it did not adopt a formal decision. Instead, it confirmed that the Member States unanimously considered that the support provided to France satisfied their legal duty of assistance, that no formal Council decision or Council Conclusions are needed for Article 42(7) to be triggered, and that the assistance takes the form of bilateral aid rather than a single unified EU operation.¹⁴⁷ This practice illustrates the mechanism's fundamentally intergovernmental nature and the continuing centrality of Member States sovereignty.

In contrast to the flexibility of invocation, the response obligation for other Member States is exceptionally demanding. Unlike NATO's Article 5, which assists "as it deems necessary", Article 42(7) imposes that Member States have "an obligation" to provide "all aid and assistance by all the means in their power". This formulation creates a legally more compelling duty than NATO's mutual defence clause, yet it does not specify how this obligation must be discharged, as it does not create an integrated command structure or an automatic military response. On the contrary, assistance can range from diplomatic support and technical or medical help to civilian or military aid. For the unique precedent, assistance took a bilateral form. France requested increased contributions to the international fight against terrorism, and each responding State independently determined the form of support to provide. Therefore, Article 42(7) creates a unique legal architecture: a firm obligation (more compelling than NATO) discharged through extraordinarily flexible mechanisms (no formal procedures, bilateral arrangements, case-by-case determination).

However, some Member States called for its "operationalisation", stating that "another lesson [they] collectively identified is the importance of European solidarity to act and react to crises. A key work, in that regard, will

¹⁴⁷ Council of the European Union 2015: 6–7.

be the operationalisation of the Article 42(7) TEU”.¹⁴⁸ The EU subsequently committed to test the framework through structured exercises. This signals institutional determination to transform Article 42(7) from a dormant Treaty provision to a practical response mechanism.

The great flexibility of both the invocation and response processes makes Article 42(7) surprisingly well-suited to space incidents. Once a Member State invoking the clause considers activation conditions met and other Member States do not contest this decision, a threshold exemplified by the French case, the article may be applied to satellite aggression. Other Member States may assist in multiple forms: military support, diplomatic backing, economic measures, or technical assistance. However, the main technical challenge remains: attribution. Determining the attack’s origin is necessary for a credible invocation and for tailoring aid appropriately. However, the absence of strict procedural requirements provides unexpected flexibility for the EU-owned satellite scenario. Since no formal procedure exists, the Union itself could invoke Article 42(7), or any Member State could do so on behalf of collective European interests. This flexibility circumvents the “victim question” that would otherwise paralyse response.

*Complementary mechanisms: Article 222
and coordination architecture*

Article 42(7) can be operated simultaneously with other assistance mechanisms, most notably Article 222 TFEU. It establishes a solidarity clause obliging the Union and Member States to act jointly if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster.¹⁴⁹ Unlike Article 42(7) TEU, Article 222 is institutionally elaborated through Council Decision 2014/415/EU,¹⁵⁰ which specifies activation procedures, institutional responsibilities, and coordination mechanisms amongst EU

¹⁴⁸ Ministers of Defence of France, Germany, Spain and Italy 2020.

¹⁴⁹ Treaty on the Functioning of the European Union, Article 222.

¹⁵⁰ Council Decision 2014/415/EU on the arrangements for the implementation by the Union of the solidarity clause, OJ L 192, 1.7.2014.

agencies and Member State authorities. This dual-mechanism approach reflects a strategic logic, while Article 42(7) addresses armed response and military dimensions, Article 222 mobilises civil protection and institutional crisis management.¹⁵¹ Both may apply simultaneously to complex space incidents.¹⁵² However, since Article 222 is not explicitly referenced in the EUSSSD, the present chapter will not develop its analysis.

As the solidarity clause's purpose is crisis management for terrorist attacks, natural disasters, or technological disasters within Union territory, its scope expressly encompasses terrorist attacks committed through cyber means or interference with critical infrastructure, which could include space systems. Therefore, Article 222 may be activated if a space-related incident constitutes either a terrorist attack employing or targeting space infrastructure, or a man-made disaster producing severe consequences affecting Member States' populations, critical infrastructure, or territorial integrity.

While Article 222 offers advantages over Article 42(7) as EU institutions coordinate response more directly and specialised technical capacities mobilise rapidly, it suffers a few limitations: no military response authority, potential reluctance to invoke solidarity, and the requirement under Decision 2014/415 that affected Member States demonstrate exhaustion of national capabilities before requesting EU assistance. For space incidents, Article 222's most significant utility lies in hybrid scenarios in which hostile actions trigger cascading civilian consequences requiring a coordinated EU-level response beyond the capacity of a single Member State.

In this regard, the EU has established the Space Threat Response Architecture (STRA), a framework coordinating political, diplomatic, technical, and intelligence responses to security incidents affecting EU space systems. To test and refine this coordination architecture in practice, the Union has conducted a series of Space Threat Response Architecture exercises (STRA-X).¹⁵³ These exercises engage Member States in scenario-based simulations of attacks targeting EU space assets, demonstrating institutional

¹⁵¹ FIOTT 2022: 26–27; DEEN et al. 2022: 10–11.

¹⁵² FIOTT 2021: 6.

¹⁵³ European External Action Service 2025b: 9–10.

commitment and operational readiness.¹⁵⁴ STRA-X-24 addressed both the technical and higher-level policy aspects of the detection, attribution and response to space threats. This discussion also touched upon the potential invocation of Article 42(7), recognising the persistent challenges around attribution and the legal threshold for activation.¹⁵⁵

It is hoped, and the ongoing exercises and workshops suggest, that the various legal difficulties concerning utilisation of Article 42(7) and its articulation with complementary mechanisms, such as Council Decision 2021/698 and Article 222 TFEU, will continue to be progressively addressed. Only through continued practical operationalisation can the Union develop the legal and institutional clarity necessary for credible collective space defence.

CONCLUSION

Regarding the use of European satellites as *tools* in armed conflict, it is essential to emphasise that the use of these space systems for security and defence purposes is already explicitly established and operationalised within the context of CSDP missions. However, the conditions that would permit the Union itself to become a party to an armed conflict are so restrictive that such a scenario is virtually impossible and would arguably conflict with principles of international public law. Nevertheless, given the Union's strategy of permitting Member States to utilise these satellites in armed conflict, it is reasonable to assume that the Union would do likewise should it find itself in such circumstances. In any event, EU-owned satellites can legally serve within the framework of armed conflict, with relatively limited implications for third-party actors. The use of European space infrastructure for defence purposes operates within established legal parameters and does not fundamentally alter the international law obligations of the Union or its Member States.

¹⁵⁴ For more information on the relevance of wargames for space see FRANCIS 2025.

¹⁵⁵ European External Action Service 2024.

Regarding the legal framework governing EU-owned satellites as potential *targets* in armed conflict, it must be read in light of the Union's growing awareness of the critical role these infrastructures play. The EU has begun implementing procedures to mitigate these risks as far as possible, alongside technical and governance arrangements for detection, characterisation and attribution, even though these processes are particularly complex in the space domain. In parallel, the Union has developed two main avenues for response and retaliation: one based on unanimously adopted Council decisions, and the other grounded in the mutual defence clause in Article 42(7) TEU, even though this analysis has highlighted the significant difficulties involved in activating that clause for a space attack, especially when it comes to meeting its legal conditions. In any event, it is natural to conclude that recognising the need to strengthen the security of space systems is essential, and that the ambition to increase the use of European satellites for security and defence purposes has become unavoidable in light of mounting geopolitical tensions.

Making EU satellite data available for security and defence and ensuring the protection of the underlying infrastructure, can no longer be seriously questioned. The task now is to align the relevant legal frameworks with these political ambitions, while remembering that the Union remains an international organisation without a general defence vocation; nevertheless, it can serve as a central framework for intergovernmental coordination among all its Member States.

REFERENCES

- ARADI, Norbert (2024): The EU's Space Policy Framework from a Defence and Security Policy Approach: A Belated Rush or an Elaborated Trial? In BARTÓKI-GÖNCZY, Balázs – SÜLYÖK, Gábor (eds.): *The New Space Age. Legal and Policy Perspectives*. Budapest: Ludovika University Press, 55–76.
- ANGHEL, Suzana Elena – CIRLIG, Carmen-Cristina (2016): Activation of Article 42(7) TEU. France's Request for Assistance and Member States' Responses. *European Council Briefing*, July 2016. Online: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/581408/EPRS_BRI\(2016\)581408_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/581408/EPRS_BRI(2016)581408_EN.pdf)

- BATAILLE, Mathieu (2025): The EU as a Key Player in Multilateral Forums on Space Security: Perspectives for the OEWG 2025–2028. *Stockholm International Peace Research Institute*, April 2025. Online: <https://www.sipri.org/publications/2025/eu-non-proliferation-and-disarmament-papers/eu-key-player-multilateral-forums-space-security-perspectives-oewg-2025-28>
- BATAILLE, Mathieu – MESSINA, Valentine (2020): Europe, Space and Defence. From ‘Space for Defence’ to ‘Defence of Space’. *European Space Policy Institute*, February 2020. Online: <https://www.espi.or.at/wp-content/uploads/2022/06/ESPI-Public-Report-72-Europe-Space-and-Defence-Executive-Summary.pdf>
- BLOKKER, Niels (2000): Is the Authorization Authorized? Powers and Practice of the UN Security Council to Authorize the Use of Force by ‘Coalitions of the Able and Willing’. *European Journal of International Law*, 11(3), 541–568. Online: <https://doi.org/10.1093/ejil/11.3.541>
- BODDENS HOSANG, Hans – DUCHEINE, Paul (2023): Implementing Article 42.7 of the Treaty on European Union: Legal Foundations for Mutual Defence in the Face of Modern Threats. In MARQUARDT, Stephan – BLOCKMANS, Steven (eds.): *The European Union’s Contribution to International Peace and Security. Liber Amicorum in Honour of Gert-Jan van Hegelsom*. Leiden: Brill–Nijhoff, 214–242.
- BOTHE, Michael – DORSCHER, Thomas (2001): The UN Peacekeeping Experience. In FLECK, Dieter (ed.): *The Handbook of the Law of Visiting Forces*. Oxford: Oxford University Press, 487–506.
- CESARI, Laetitia – LACROIX, Lisa – CARLO, Antonio (2020): *The Challenge of Protecting Space-based Assets against Cyber Threats*. International Astronautical Congress. Online: <https://hal.science/hal-04491327/document>
- CLAPP, Sebastian (2023): Armed Conflict: A Glossary of Terms. *European Parliamentary Research Service*, December 2023. Online: [https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/757582/EPRS_ATA\(2023\)757582_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/757582/EPRS_ATA(2023)757582_EN.pdf)
- CLAPP, Sebastian – VERHELST, Anne (2022): A Comparative Analysis of Article 5 Washington Treaty (NATO) and Article 42(7) TEU (EU). *European Parliamentary Research Service*, December 2022. Online: [https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/739250/EPRS_ATA\(2022\)739250_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/739250/EPRS_ATA(2022)739250_EN.pdf)
- Council of the European Union (2011): *Council Decides on EU Military Operations in Support of Humanitarian Assistance Operations in Libya*, PRESSE 91, 8589/11, 1.04.11. Online: <https://data.consilium.europa.eu/doc/document/ST-8589-2011-INIT/en/pdf>
- Council of the European Union (2014): *European Union Concept for EU-led Military Operations and Missions*, CSDP/PSDC 750, 17107/14, 19.12.2014. Online: <https://data.consilium.europa.eu/doc/document/ST-17107-2014-INIT/en/pdf>
- Council of the European Union (2015): *Outcome of the Council Meeting of 16 and 17 November 2015*. 14120/15. Online: <https://data.consilium.europa.eu/doc/document/ST-14120-2015-INIT/en/pdf>

- Council of the European Union (2022a): Russian Cyber Operations against Ukraine: Declaration by the High Representative on Behalf of the European Union. *Press Release*, 10 May 2022. Online: <https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/>
- Council of the European Union (2022b): *A Strategic Compass for Security and Defence. For a European Union that Protects Its Citizens, Values and Interests and Contributes to International Peace and Security*. Online: <https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf>
- DARNIS, Jean-Pierre – VECLANI, Anna (2011): *Space and Security: The Use of Space in the Context of CSDP*. Online: [https://www.europarl.europa.eu/RegData/etudes/etudes/join/2011/433834/IPOL-SEDE_ET\(2011\)433834_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/etudes/join/2011/433834/IPOL-SEDE_ET(2011)433834_EN.pdf)
- DEEN, Bob – ZANDEE, Dick – STOETMAN, Adája (2022): Uncharted and Uncomfortable in European Defence. The EU's Mutual Assistance Clause of Article 42(7). *Clingendael Report*, January 2022. Online: <https://www.clingendael.org/sites/default/files/2022-01/uncharted-and-uncomfortable.pdf>
- DENEVE, Alain (2024): Article 189 TFUE. La politique spatiale européenne. In BERNARD, Elsa – LOIEZ, Quentin – RODRIGUES, Stéphane (eds.): *L'Union européenne de la défense. Commentaire article par article*. Belgium: Bruylant, 693–719.
- European Commission (2016): Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. COM(2016) 705 final. *Space Strategy for Europe*. Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016DC0705>
- European Commission (2020): Joint Communication to the European Parliament and the Council. JOIN(2020) 18 final. *The EU's Cybersecurity Strategy for the Digital Decade*. Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020JC0018>
- European Commission (2024): *Developing Reconnaissance Capabilities at an EU Level*. Online: https://defence-industry-space.ec.europa.eu/developing-reconnaissance-capabilities-eu-level-2024-01-23_en
- European Commission (2025a): *A Secure Europe*. Online: https://defence-industry-space.ec.europa.eu/secure-europe_en
- European Commission (2025b): Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. COM(2025) 570 final. *A Dynamic EU Budget for the Priorities of the Future – The Multiannual Financial Framework 2028–2034*. Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0570>
- European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2023): Joint Communication to the European Parliament and the Council. JOIN(2023) 9 final. *European Union Space Strategy for Security and Defence*. Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023JC0009>

- European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2025a): Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. JOIN(2025) 130 final. *European Preparedness Union Strategy*. Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025JC0130>
- European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2025b): Joint Communication to the European Parliament, the European Council and the Council: Preserving Peace. JOIN(2025) 27 final. *Defence Readiness Roadmap 2030*. Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025JC0027>
- European External Action Service (2017): *High Level Civil–Military User Needs for Governmental Satellite Communications* (GOVSATCOM). EEAS(2017) 359. Online: <https://data.consilium.europa.eu/doc/document/ST-7550-2017-INIT/en/pdf%5D>
- European External Action Service (2024): *Space: EU Carries Out Space Threat Response Architecture 2024 Exercise* (STRA-X-24). Online: https://www.eeas.europa.eu/eeas/space-eu-carries-out-space-threat-response-architecture-2024-exercise-stra-x-24_en
- European External Action Service (2025a): *EU Common Security and Defence Policy* (CSDP) *Missions and Operations*. Online: https://www.eeas.europa.eu/sites/default/files/documents/2025/EU-mission-and-operation_2025.pdf
- European External Action Service (2025b): Report of the High Representative of the Union for Foreign Affairs and Security Policy to the Council. HR(2025)73. *Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence*.
- European Parliament (2024): *Resolution on the Implementation of the Common Security and Defence Policy – Annual Report 2024* [2024/2082(INI)]. P10_TA (2025)0058. 02.04.2025. Online: <https://eur-lex.europa.eu/eli/C/2025/4389/oj/eng>
- European Space Agency (1975): *Convention on the Establishment of a European Space Agency*. Online: https://www.esa.int/About_Us/Law_at_ESA/ESA_Convention
- European Union Satellite Centre (2025): *An Overview of SatCen Activity. Annual Report 2024*. Online: <https://www.satcen.europa.eu/keydocuments/Satcen%20Annual%20Report%202024%20web6863fb6508d771430foe581.pdf>
- FALCO, Valentina (2009): The Internal Legal Order of the European Union as a Complementary Framework for its Obligations Under IHL. *Israel Law Review*, 42(1), 168–205. Online: <https://doi.org/10.1017/S0021223700000492>
- FAZIO, Frederica (2024): Collective Defence in NATO: A Legal and Strategic Analysis of Article 5 in Light of the War in Ukraine. *Dublin European Law Institute*, (2).
- FAZIO, Federica (2025): The EU’s Mutual Defence Clause: Legal and Strategic Considerations on Article 42(7) TEU in an Age of Renewed Military Threats. *Nordic Journal of European Law*, 8(3), 1–30. Online: <https://doi.org/10.36969/njel.v8i3.28035>
- FERRARO, Tristan (2015): The ICRC’s Legal Position on the Notion of Armed Conflict Involving Foreign Intervention and on Determining the IHL Applicable to this Type of Conflict. *International Review of the Red Cross*, 97(900), 1227–1252. Online: <https://doi.org/10.1017/S1816383116000448>

- FIOTT, Daniel (2021): Securing the Heavens. How Can Space Support the EU's Strategic Compass? *European Union Institute for Security Studies Brief*, (9). Online: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_9_2021_o.pdf
- FIOTT, Daniel (2022): *The Strategic Compass and EU Space-based Defence Capabilities*. In Depth Analysis of the European Parliament, November 2022. Online: [https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702569/EXPO_IDA\(2022\)702569_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702569/EXPO_IDA(2022)702569_EN.pdf)
- FRANCIS, James (2025): Simulating the Future of European Security: Wargaming for Space Operations. *European Space Policy Institute Brief*, (73). Online: <https://www.espi.eu/wp-content/uploads/2025/04/ESPI-Policy-Brief-73.pdf>
- GRIGNON, Julia (2022): "Co-belligerency" or When Does a State Become a Party to an Armed Conflict? *Strategic Brief of IRSEM*, (39). Online: https://www.irsem.fr/storage/file_manager_files/2025/03/sb-39-grignon-cobelligerency.pdf
- HEINTSCHEL VON HEINEGG, Wolff (2017): Neutrality and Outer Space. *U.S. Naval War College International Law Studies*, 93, 525–547.
- HELLER, Kevin Jon – TRABUCCO, Lena (2022): The Legality of Weapons Transfers to Ukraine Under International Law. *Journal of International Humanitarian Legal Studies*, 13(2), 251–274. Online: <https://doi.org/10.1163/18781527-bja10053>
- Institute of International Law (1999): *Yearbook of the Institute of Internal Law Berlin Session*, 68(II). Online: https://www.idi-iil.org/en/sessions/berlin-1999/?post_type=publication
- International Committee of the Red Cross (1977): *Commentary on Additional Protocol I, Article 43*. Online: https://tile.loc.gov/storage-services/service/l1/llmlp/Commentary_GC_Protocols/Commentary_GC_Protocols.pdf
- International Committee of the Red Cross (2024): *How Is the Term "Armed Conflict" Defined in International Humanitarian Law?* Opinion Paper ICRC. Online: https://www.icrc.org/sites/default/files/document_new/file_list/armed_conflict_defined_in_ihl.pdf
- International Court of Justice (1949): *Reparation for Injuries Suffered in the Service of the United Nations*. Advisory Opinion, 11 April 1949, I.C.J. Reports 1949, 174.
- International Court of Justice (1986): *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States)*, Merits, Judgment, 27 June 1986, ICJ Reports 1986, 14.
- International Court of Justice (1996): *Legality of the Threat or Use of Nuclear Weapons*. Advisory Opinion. I.C.J. Reports 1996, 226.
- International Law Association (2004): *Accountability of International Organisations*. Online: <https://www.ila-hq.org/en/committees/accountability-of-international-organisations>
- International Law Commission (2011): *Draft Articles on the Responsibility of International Organizations*. Online: https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_11_2011.pdf
- KALLAS, Kajas (2025): *Speech by EU High Representative/Vice-President Kaja Kallas at the 17th European Space Conference*. Online: https://www.eeas.europa.eu/eeas/speech-eu-high-representativevice-president-kaja-kallas-17th-european-space-conference_en

- KOLB, Robert – PORRETTO, Gabriele – VITE, Sylvain eds. (2005): *L'application du droit international humanitaire et des droits de l'homme aux organisations internationales: Forces de paix et administrations civiles transitoires*. Brussels: Bruylant.
- MARTIN, Jean-Christophe (2024): Article 42, §7, Alinéa 1^{er}. La clause de défense mutuelle. La politique spatiale européenne. In BERNARD, Elsa – LOIEZ, Quentin – RODRIGUES, Stéphane (eds.): *L'Union européenne de la défense. Commentaire article par article*. Belgium: Bruylant, 263–282.
- MELZER, Nils (2009): *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*. International Committee of the Red Cross. Online: <https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc-002-0990.pdf>
- Ministers of Defence of France, Germany, Spain and Italy (2020): *Letter to Josep Borrell*. Online: <https://www.bmvg.de/resource/blob/261184/4f63d2a54ee7f96476156796f00874ed/20200528-download-brief-pesco-englisch-data.pdf>
- MURPHY, Ray (2003): United Nations Military Operations and International Humanitarian Law: What Rules Apply to Peacekeepers? *Criminal Law Forum*, 14(2), 153–194. Online: <https://doi.org/10.1023/A:1026369302641>
- NAERT, Frederik (2010): *International Law Aspects of the EU's Security and Defence Policy, with a Particular Focus on the Law of Armed Conflict and Human Rights*. Oxford: Intersentia.
- NAERT, Frederik (2011): Legal Aspects of EU Military Operations. *Journal of International Peacekeeping*, 15, 218–242. Online: <https://doi.org/10.1163/18754110X540599>
- NAERT, Frederik (2013): Observance of International Humanitarian Law by Forces under the Command of the European Union. *International Review of the Red Cross*, 95(891–892), 637–643. Online: <https://doi.org/10.1017/S1816383114000058>
- North Atlantic Treaty Organization (2021): *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*. Online: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/06/14/brussels-summit-communique>
- POIRIER, Clémence (2022): The War in Ukraine from a Space Cybersecurity Perspective. *European Space Policy Institute*, October 2022. Online: <https://www.espi.or.at/wp-content/uploads/2022/10/ESPI-Report-84.pdf>
- SU, Yuting – JIANG, Shengli (2025): International Legal Framework for Cyber Attacks in Outer Space: The Issue of “Use of Force”. *US–China Law Review*, 22(2), 79–88. Online: <https://doi.org/10.17265/1548-6605/2025.02.003>
- SUR, Serge (2011): L'Union européenne dans les crises internationales: les conflits armés. In BLUMANN, Claude – PICOD, Fabrice (eds.): *L'Union européenne et les crises*. Brussels: Bruylant, 283–291.
- United Nations General Assembly (1974): Resolution A/Res/3314 (XXIX): *Definition of Aggression*, GAOR 29th Session Supp 31.

- United Nations General Assembly (2011): Resolution A/Res/65/276: *Participation of the European Union in the Work of the United Nations*, GAOR, 65th Session Suppl. 49.
- United Nations General Assembly (2019): Resolution A/Res/73/266: *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, GAOR, 73rd Session Suppl. 49.
- United Nations General Assembly (2022): Resolution A/Res/ES-11/1: *Aggression against Ukraine*, GAOR, 11th Emergency Special Session Suppl. 1.
- United Nations General Assembly (2024): Decision A/Dec/79/512: *Open-ended Working Group on the Prevention of an Arms Race in Outer Space in all its Aspects*, GAOR, 79th Session Suppl. 49.
- United Nations Security Council (1999): Resolution S/Res/1244 (1999): *Resolution 1244 (1999) on the Deployment of International Civil and Security Presences in Kosovo*, SCOR, 54th year.
- WENTKER, Alexander – JACKSON, Miles – HILL-CAWTHORNE, Lawrence (2024): Identifying Co-parties to Armed Conflict in International Law. How States, International Organizations and Armed Groups Become Parties to War. *Research Paper of Chatham House*, March 2024. Online: <https://www.chathamhouse.org/sites/default/files/2024-03/2024-03-06-identifying-co-parties-armed-conflict-international-law-wentker.pdf>

