Technology and Regulation

special issue: security in the digital age

Space Infrastructure as Critical Infrastructure: Rights Beyond Earth in the Digital Age

Author(s)	Francesco Casaril, Giovanni Tricco
Contact	francesco.casaril@imtlucca.it, giovanni.tricco2@unibo.it
Affiliation(s)	Francesco Casaril - PhD Candidate - IMT School for Advanced Studies Lucca Giovanni Tricco - PhD Candidate - Università di Bologna/ Vrije Universiteit Brussel
Keywords	space; critical infrastructure; disaster response; dual use; cybersecurity; human rights; governance; Earth observation; resilience
Published	Published: 31 Mar 2026
Citation	Francesco Casaril, Giovanni Tricco, Space Infrastructure as Critical Infrastructure: Rights Beyond Earth in the Digital Age, Technology and Regulation, 2026, 116-134 • XXXXX • ISSN: 2666-139X

Abstract

Space-based services have become an indispensable pillar of modern society. Earth Observation technologies are used to map wildfires and mitigate climate disasters, Satellite Communication (SATCOM) bridges the digital divide with connectivity in remote regions, and Position Navigation and Timing (PNT) satellites support agriculture, transport, finance, and many other critical sectors our societies rely on.

The increased use and interconnection of space with terrestrial networks offer significant economic and societal opportunities, but they also introduce new security challenges in the digital era. As critical infrastructure classifications extend to space-based systems, under evolving European Union legal frameworks, the space sector is adapting to broader requirements for resilience and sustainability. This requires space operators to balance economic development with the protection of fundamental rights, including the rights to security, access to essential services, and a healthy environment.

This paper explores the interconnection between terrestrial and orbital infrastructures by examining the emerging threats posed by the digitalisation of space systems. It assesses the mechanisms necessary to ensure their long-term safety and reliability, focusing on how space infrastructure is defined as critical under EU law and mapping the obligations arising for the space industry. Central to this analysis is the role of satellite networks in safeguarding multiple fundamental rights. In considering two use cases, Earth Observation for emergency management and GNSS to enhance several critical services,

this paper explores the impact of cyberattacks on these domains and their repercussions on fundamental rights.

This analysis offers a fresh perspective on how to achieve a robust, secure, and rights-centric framework for space systems, contributing to a broader discussion on security in the digital age.

1. Introduction

With the increasing diffusion of Information and Communication Technologies (ICTs), access to the internet has become essential for society. ICT Networks allow communication between people, governments, and companies located in any corner of the globe. Societies and communities thrive on the opportunities offered by digital connectivity, and businesses and companies can grow by accessing cross-border opportunities. In addition, different aspects of governmental services are being digitalised, requiring citizens to be connected to the web.

The digital world no longer ends at the edge of a fibre-optic cable. Every day, pictures, voice calls, and emergency signals jump from ground networks to satellites and back again. Those satellites guide firefighters towards a spreading blaze, keep field hospitals online after a storm, and give remote communities access to the internet. In other words, space systems have slipped quietly into the category of things we rely on without thinking, much like electricity or clean water.

But the more we lean on these systems, the more we need them to be resilient against hybrid threats such as cyber-attacks. A well-aimed cyberattack on a single satellite link can scramble Global Navigation Satellite Systems receivers, jam rescue radios, or cut broadband to an entire region. If that happens, people's safety, their right to information, and even the health of the environment can be put on the line. In Europe, legislative initiatives such as the NIS 2 Directive and the new Critical Entities Resilience Directive now mention satellites when they talk about "essential services". The big question is whether those rules are strong and specific enough to keep this space-enabled world safe.

This paper aims to reply to the following research questions:

- RQ1: How does the growing reliance on space technologies impact the protection of fundamental rights such as the right to life and health?
- RQ2: What are the risks posed by cyberattacks to space infrastructure, and how might such attacks undermine human security and emergency response operations?
- RQ3: To what extent do existing legal and policy frameworks (e.g., the EU's NIS2 Directive, Critical Entities Resilience Directive) and future ones (the draft EU Space Act) adequately classify and protect space infrastructure as critical digital infrastructure?

To address these research questions, Section 2 presents the methodological framework adopted, grounded in EU fundamental-rights law and focused on the intersection of resilience and human security. Section 3 examines how modern space networks have become essential infrastructure, supporting several critical services on which we rely. Sections 4 analyse two major applications: Earth Observation (EO) and Global Navigation Satellite Systems (GNSS), as enablers of rights protection, illustrating through case studies how these systems support emergency management, food security, and public safety, while also introducing governance and privacy challenges. Section 5 explores the vulnerabilities of these infrastructures to cyber threats and their implications for human rights, linking technical failures to rights impacts. Sections 6 then assess how current and emerging EU legal frameworks, namely the NIS 2 Directive, and the Critical Entities Resilience Directive, address the classification, protection, and governance of space infrastructure as critical digital infrastructure. Section 7 addresses the proposed EU Space Act alongside the challenges

posed by the dual-use nature of contemporary space systems. It examines how civilian-military applications, private operator control, and cybersecurity risks complicate the protection of rights-enabling services, and evaluates emerging EU and international governance responses. The conclusion synthesises the findings, demonstrating that the resilience of space systems is now inseparable from the protection of fundamental rights and proposing policy principles for a secure and rights-based space governance.

For the purposes of this paper, space systems are understood as the combination of space-based and ground-based components that enable the operation of services delivered through space infrastructure. They typically include spacecraft, ground control and mission operations centres, user terminals, and data processing or distribution facilities. This definition is consistent with the one adopted by the International Telecommunication Union, which refers to a space system as "*any group of associated space objects, one or more of which are capable of providing space radiocommunication or other space functions, together with the associated ground segment*".[1]

The term critical infrastructure denotes those assets, systems, and networks, whether physical or virtual, whose disruption would have a significant impact on the security, economy, public health, or safety of a nation or of the Union. Within the European Union legal framework, Article 2(4) of the *Directive (EU) 2022/2557 on the resilience of critical entities (CER Directive)* defines critical infrastructures as those providing "*an essential service, the disruption of which would have significant consequences for vital societal functions, economic activities, public health or safety*".[2]

When this paper refers to space infrastructure as critical infrastructure, it refers to the orbital and terrestrial elements that provide indispensable digital, communication, and environmental services whose failure would endanger essential societal functions and fundamental rights.

2. Methodological Framework

This paper employs a qualitative, cross-sectoral legal-policy analysis that is grounded in the European Union's fundamental-rights framework. It examines how selected space-based services, such as Earth Observation and Global Navigation Satellite Systems, contribute to the realisation of rights whose enjoyment increasingly depends on the continuity of digital and space infrastructure. These two services were chosen as they represent some of the most direct technological interfaces between space systems and human security: EO enables disaster preparedness, environmental protection, and public-health monitoring; GNSS supports emergency response, transport safety, food security, and the timing of critical services.

The analysis focuses on the Directive (EU) 2022/2555 (NIS 2)[3] and the Directive (EU) 2022/2557 (CER)[4] as some of the most recent EU legislative instruments that explicitly recognise space as part of Europe's critical-infrastructure architecture and establish binding cybersecurity and resilience duties for operators. Concerning fundamental rights, the legislative reference is the Charter of Fundamental Rights of the European Union,[5] notably Articles 2 (right to life), 3 (integrity of the person), 6 (liberty and security), 11 (freedom of information), 35 (health care), and 37 (environmental protection), and the right to adequate food and standard of living under Article 11 of the International Covenant on Economic, Social and Cultural Rights.[6] These rights are central but not exhaustive; they illustrate how the resilience of space infrastructure under EU law enhances the protection of fundamental human interests.

1. International Telecommunication Union (ITU), Radio Regulations, Edition of 2020, Art 1.112, 27.
2. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities [2022] OJ L333/164.
3. 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 [2023] OJ L333/80 (NIS 2 Directive).
4. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities [2022] OJ L333/164 (CER Directive).
5. Charter of Fundamental Rights of the European Union [2012] OJ C 326/391, Arts 2, 3, 6, 11, 35, 37 and 38. (EU CFR)
6. United Nations, *International Covenant on Economic, Social and Cultural Rights* (adopted 16 December 1966, entered into force 3 January 1976) 993 UNTS 3, Art 11 (ICESCR).

The methodological framework adopted aims to trace the connections between governance instruments, critical-infrastructure obligations, and the protection of fundamental rights in the European legal order, providing a basis for comparative and future policy research on space resilience and human security.

3. Space Infrastructure in the Digital Age

Space systems have played an important role from a geopolitical and technology perspective since the Cold War, when the space race between the USSR and the USA pushed a fast development in space technologies. Space systems from that time on have been increasingly used for different aims, from ensuring communications, to distributing TV signals, to observing the earth and to spy on rivalries, and to develop navigation, positioning, and timing (PNT) infrastructures.

In the last century, space systems were mostly launched in geostationary orbit (GEO) to enable near-global coverage with one or a few satellites, particularly for communications and meteorological missions.[7] They were costly, ambitious, and long-term projects. However, while such systems could offer important services, their latency stroke is high, given the distance from the surface of the Earth (roughly 36,000 km); for these reasons, such systems were mostly utilised for specific purposes and could not get to ubiquitous use. Space capabilities have progressed rapidly: although geostationary orbit remains a cornerstone of space operations, attention has now pivoted towards low-Earth-orbit (LEO) constellations.[8]

Four interrelated factors underpin this transition.[9] First, access to orbit has broadened substantially: average launch costs have fallen over the past two decades, while the annual number of launches increased by more than fifty percent per year between 2019 and 2023, a trend destined to increase with the arrival of reusable launchers.[10] Second, advances in component design and software-defined payloads have enabled small satellites to undertake missions that previously required significantly larger payloads, thereby reducing both capital and operating expenditures. Third, the sector has experienced notable financial deepening, with private investors committing more than seventy billion US dollars to space ventures during 2021-2022, expanding the industrial base and accelerating innovation cycles beyond the traditional governmental mission.[11]

Together, these shifts have made space systems economically accessible and deeply entwined with terrestrial value chains, features that the first space era could not deliver.

Indeed, LEO constitutes a unique environment in space that offers proximity to the earth, offering communication channels with low latency, resembling terrestrial connectivity metrics. For example, *SpaceX*'s Starlink mega-constellation of satellites is claimed to offer a connection with a latency of just 20-40ms, similar to typical submarine cables.[12] In terms of capacity, the Starlink constellation provides better capabilities for satellites in GEO, but less so for submarine cables, having a capacity of up to 200 tbps.[13] However, the outlook is promising, with expected capacity increases on the horizon. The Starlink constellation consists of approximately 6,000 satellites, with plans to expand to 42,000 satellites by 2035.[14]

---

7. European Space Agency (ESA), *Orbits and Launches: Understanding Geostationary and Low-Earth Orbits* (ESA, 2023) https://www.esa.int/Enabling_Support/Operations/Orbits_and_launches accessed 29 June 2025; see also J. N. Pelton and S. Madry, *Handbook of Satellite Applications*, 2nd edn (Springer, 2017) 47-49.
8. J Zhang, Y Cai, C Xue, Z Xue and H Cai, 'LEO mega constellations: Review of development, impact, surveillance, and governance' (2022) *Space: Science & Technology* 1-14.
9. Acket-Goemaere *et al*, 'Space: The $1.8 Trillion Opportunity for Global Economic Growth' (McKinsey & Company 2024).
10. N Adilov, P Alexander, B Cunningham, and N Albertson, 'An analysis of launch cost reductions for low earth orbit satellites' (2022) 42(3) *Economics Bulletin*, 1561-1574.
11. W Peeters, 'The paradigm shift of newspace: new business models and growth of the space economy' (2024) 12(3) *New Space*, 202-213.
12. SpaceX, Starlink Legal Documents: DOC-1400-28829-70 https://www.starlink.com/legal/documents/DOC-1400-28829-70 accessed 29 June 2025.
13. C Daehnick, I Klinghoffer, B Maritz and B Wiseman, 'Space Collisions: Will It Be Different This Time?' (McKinsey & Company 2020), 4.
14. T Pultarova, 'Starlink satellites: Facts, tracking and impact on astronomy' (9 January 2025) Space.com https://www.space.com/spacex-starlink-satellites.html accessed 29 June 2025.

Such systems can be deployed to offer connectivity in rural areas and to act as relays for traditional communication services that fail to provide access to the internet. A recent UK program illustrates this logic clearly. In 2024, the UK Space Agency, working with the Department for Science, Innovation and Technology and ESA's telecommunications program, committed £3.5 million to three pilot projects on Rathlin Island (Northern Ireland) and Papa Stour (Shetland).[15] Each pilot will deploy hybrid, multi-orbit terminals that blend low-Earth-orbit links (for low latency) with geostationary capacity (for resilience), feeding local 5G/6G or Wi-Fi cells. The objective is two-fold: first, to bring gigabit-class broadband to communities where fiber or microwave back-haul is uneconomic; second, to create a portable network-of-last-resort that emergency services, farmers, or event organisers can mount on a vehicle when terrestrial infrastructure is damaged or unavailable. The UK case thus demonstrates how modern satellite architectures already underpin rural inclusion and communications resilience, the very roles that first-generation GEO systems could not fulfil at scale.[16] Such projects allow data to be transferred more quickly between ground terminals and satellites, therefore enhancing connectivity with terrestrial infrastructure.[17]

The performance of such systems is only set to improve as communication technologies advance. The upcoming 6G connectivity will bring a new wave of progress, with SATCOM playing an eminent role.[18] In addition, the space industry as a whole is at an inflection point with expectations of becoming the next trillion-dollar industry,[19] hence the rising investment in the development of new space technologies that will lead to a novel era of opportunities and connectivity.

In addition, the many satellites that make up today's mega-constellations deliver global coverage of every point on Earth several times each day, paving the way for ambitious Earth Observation programs. Unlike the large, distant platforms in geostationary orbit, these small low-Earth-orbit spacecraft can be replaced rapidly with newer models carrying very-high-resolution (VHR) sensors. This capacity for continuous, fine-grained monitoring supports humanitarian and social initiatives and improves the prediction of natural hazards, enabling timely intervention and helping to safeguard citizens and their property.

At this stage, it is evident how central satellites have become and how deeply society depends on their continuous operation. Mega-constellations of satellites are an integral and crucial layer of the digital stack that forms our digital societies.[20] An interruption of their functioning brings a breach of different fundamental rights, from access to the internet, protection of private life, to protection of the environment. For these reasons, it is key to secure their adequate protection to ensure the sustainment of a digital society where satellite systems are an integral part of it. The next section examines in detail how these technologies support the protection of these rights and the risks arising from their growing interdependence.

4. Earth Observation and GNSS as a Tool for Rights Protection

The previous section outlined the emerging role of satellite networks, a role set to expand with the projected increase in satellite launches over the next decade. This section focuses on specific use cases illustrating how satellites are employed to safeguard the environment and how Earth Observation systems contribute to the protection of fundamental rights.

15. UK Space Agency, 'Satellite communications to improve connectivity in remote areas' (27 November 2024) https://www.ukspace.org/satellite-communications-to-improve-connectivity-in-remote-areas/ accessed 24 October 2025.
16. Government of the United Kingdom, 'Satellite communications to improve connectivity in remote areas' (Press release, 27 November 2024) https://www.gov.uk/government/news/satellite-communications-to-improve-connectivity-in-remote-areas accessed 29 June 2025.
17. Internet Society, *Perspectives on LEO Satellites for Internet Access* (17 November 2022) https://www.internetsociety.org/wp-content/uploads/2022/11/Perspectives-on-LEO-Satellites.pdf accessed 29 June 2025.
18. L Xingqin, *et al*, 'On the path to 6G: Embracing the next wave of low earth orbit satellite access' (2022) 59.12 *IEEE Communications Magazine* , 36-42.
19. World Economic Forum (WEF), 'Space: The $1.8 Trillion Opportunity for Global Economic Growth' (8 April 2024) https://www.weforum.org/agenda/2024/04/space-the-1-8-trillion-opportunity-for-global-economic-growth/ accessed 29 June 2025.
20. T Bria, M Timmers and A Gernone, *EuroStack – A European Alternative for Strategic Sovereignty* (Bertelsmann Stiftung 2025).

4.1 The role of Earth Observation in disaster management and emergency response

As climate risks escalate and natural disasters become more frequent, space-based technologies are essential for environmental monitoring and disaster management today. Among these technologies, Earth Observation satellites play a major role by providing comprehensive, high-resolution, and near-real-time data that is vital for understanding and protecting our planet.[21]

EO satellites are equipped with sophisticated optical or radar sensors capable of systematically observing the Earth's surface, atmosphere, and oceans. The continuous number of datasets they provide is critical for tracking climate change indicators such as global temperature variations, glacial retreat, sea level rise, desertification, and shifts in vegetation patterns. Missions like the European Copernicus program and NASA's Earth Observing System expanded our ability to detect and analyse these trends.[22]

Such data is now foundational for climate modelling and data-driven policymaking; scientists can refine forecasts and assess the effectiveness of mitigation strategies by integrating satellite-derived observations with ground-based measurements and artificial intelligence tools. Given the widespread use of EO data and its benefits, especially when publicly funded and used by public authorities, these technologies are moving towards recognition as a global public good that supports international cooperation in environmental protection.[23]

Beyond long-term environmental monitoring, EO satellites are vital for disaster preparedness and response. They enable early detection of phenomena such as wildfires, hurricanes, floods, landslides, and droughts. Real-time imaging and thermal data, for instance, allow authorities to monitor wildfire progression, assess flood impact, and track storm trajectories with high precision.[24]

Following Hurricane Matthew in 2016, Haiti faced devastating losses to homes, infrastructure, and ecosystems. In response, the Haiti Recovery Observatory (RO)[25] was established by CEOS (Committee on Earth Observation Satellites) in collaboration with Haitian authorities and international partners, including UNOSAT, Copernicus, and UNDP. The Observatory provided EO imagery coverage of the affected regions, including high-resolution imagery of damaged urban areas, deforestation in Macaya National Park, and disrupted agricultural zones.

These satellite data were vital for post-disaster needs assessments and for guiding fair andtransparent reconstruction.[26] National and international actors were able to assess damage remotely, prioritise aid based on objective evidence, and monitor the progress of rebuilding efforts over time. EO data in this case enabled a data-informed response; the Observatory contributed to supporting the right to life and security, especially for displaced populations, and supported the construction of new, better housing, infrastructure, and environmental rehabilitation.[27]

This case demonstrates how the integration of EO into disaster management systems enhances situational awareness but also resource allocation and emergency planning. Furthermore, EO data supports post-disaster assessments, informing reconstruction efforts and international humanitarian aid coordination, as in the case of Haiti.

More recently, on February 6, 2023, a powerful earthquake struck southern Turkey and northern Syria. Within hours, the Turkish Disaster and Emergency Authority (AFAD) activated the International Charter "Space and

21. G Schumann *et al*, 'Role of earth observation data in disaster-response applications: Current and future prospects' (2016) Earth Science Satellite Applications 119-146.
22. G Denis *et al*, 'The evolution of Earth Observation satellites in emergency response services' (2016) 127 *Acta Astronautica* 619-633.
23. M Machon, 'Global Public Goods: The Case for the Global System of Systems' (2023) arXiv preprint arXiv:2312.00623.
24. G Schumann *et al*, 'Role of earth observation data in disaster-response applications: Current and future prospects' (2016) 119–146.
25. Global Facility for Disaster Reduction and Recovery (GFDRR), *Understanding Risk: Moving Forward* (World Bank Oct 2019).
26. ibid.
27. ibid.

Major Disasters".[28] The International Charter is a non-binding international agreement established in 1999 by the European Space Agency (ESA) and the French Space Agency (CNES), with the Canadian Space Agency (CSA) joining in 2000. The Charter officially entered operation on 1 November 2000 and serves as a global cooperative mechanism to provide free and coordinated satellite data in support of emergency response operations in the aftermath of natural or technological disasters.[29]

Today, the Charter brings together 17 space agencies and over 270 satellites, including both optical and radar platforms such as Pléiades, TerraSAR-X, and recently Pléiades Neo, which are tasked on demand to supply high-resolution Earth Observation imagery. The Charter operates through a cooperative framework governed by a Board and an Executive Secretariat and may be activated by authorised users or, in certain cases, by affected states in partnership with associated bodies like civil protection authorities. The Charter enhances the effectiveness of humanitarian missions, facilitates life-saving decisions, and supports the protection of fundamental rights, including the right to life, health, and security, during crises.

Among the satellites deployed during the Turkey earthquake was Airbus' Pléiades Neo,[30] a new high-resolution system capable of delivering optical imagery at 30 cm resolution and responding to tasking requests within minutes. Thanks to this rapid satellite tasking, imagery of the disaster zones was delivered to Turkish authorities the very next day, revealing the extent of damage in cities like Antakya and Iskenderun. These maps helped rescue teams navigate collapsed infrastructure, prioritise rescue operations, and identify safe routes, actions directly linked to the protection of life and humanitarian relief.

The use of both optical and radar data ensured visibility even under cloud cover and at night. Combined with AI-driven analysis and automated change detection, EO imagery was transformed into actionable maps used to coordinate local and international efforts. Over 350 crisis images from 17 space agencies were delivered, demonstrating the global solidarity and rapid coordination enabled by the space community.[31]

The two case studies discussed above demonstrate that Earth observation satellites do more than just collect environmental data; they also protect human rights during natural, man-made or climate-related crises. In 2016, in Haiti, these satellites facilitated equitable recovery planning. In 2023, in Turkey and Syria, they empowered first responders to save lives during critical time windows. The evolution of the technology's maturity and usage highlights how rapidly it is advancing and becoming more efficient and operational. In both cases, space-based systems acted as a bridge between technology, governance, and humanitarian operations.

These examples are not isolated: the International Charter "Space and Major Disasters" has been activated over 800 times since its inception,[32] more than 400 times for floods alone, and nearly 130 times for hurricanes and storms. Similarly, the Copernicus Emergency Management Service (EMS) has been operational 24/7 since its inception in 2012, without any service disruptions. Over the years, it has been activated more than 1000 times, encompassing both Rapid Mapping and Risk and Recovery Mapping.[33] Prioritizing rapid mapping and risk assessment tools in response to disasters worldwide. These figures illustrate the growing dependency on EO infrastructure in safeguarding civilian populations, managing risks, and supporting reconstruction.

Given the value of EO data in preventing or mitigating disasters, restricting access to such information, whether for commercial, political, or security reasons, or through the disruption of digital infrastructure

28. Airbus, 'How Earth observation satellites help guide emergency workers during disasters' (23 September 2023) https://www.airbus.com/en/newsroom/stories/2023-09-disasters-how-earth-observation-satellites-help-guide-emergency-workers accessed 29 June 2025.
29. International Charter "Space and Major Disasters", *About the Charter* (ESA, CNES and CSA, 2024) https://disasterscharter.org/web/guest/about-the-charter accessed 29 June 2025.
30. S Cantrell *et al*, *System Characterization Report on the Pléiades Neo Imager* (US Geological Survey 2023).
31. European Space Agency, 'Satellites support impact assessment and monitoring after Türkiye-Syria earthquakes' (13 February 2023) https://www.esa.int/Applications/Observing_the_Earth/Satellites_support_impact_assessment_after_Tuerkiye_Syria_earthquakes .
32. N K Shrivastava, *International Charter: Space and Major Disasters* (ESCAP 2017).
33. Copernicus Emergency Management Service, 'Stats' in *Copernicus Emergency Management Service: European Union* https://mapping.emergency.copernicus.eu/stats/ accessed 18 May 2025.

via cyberattacks, risks undermining both environmental and human security. As many states increasingly acknowledge environmental protection as part of national security, EO data that supports public safety must remain freely accessible, tamper-resistant, and legally protected under a human-rights-centred framework for digital and space infrastructure governance. The next section discusses some of the potential consequences of a cyberattack against space infrastructure when it comes to emergency response and management.

4.2 GNSS as a Human-Rights Enabler

Just as Earth Observation data directly supports humanitarian relief and public-health monitoring, GNSS-based Positioning, Navigation, and Timing services underwrite several fundamental rights protected under EU law, including the right to life, the right to health, the right to access essential services, and the right to an adequate standard of living.

In Europe, the 112 emergency-call system relies on GNSS, specifically Galileo, to determine caller location with metre-level accuracy. Since March 2022, the majority of the smartphones sold in the EU integrate Galileo for automatic location transmission to emergency dispatchers.[34]

This has reduced average response times and demonstrably saved lives, reinforcing the right to life under Article 2 of the Charter of Fundamental Rights of the European Union.[35]

The integration of Galileo with Europe's 112 emergency number demonstrates this life-saving potential. The 112 service, operational across all EU Member States for over three decades, connects citizens free of charge to Public Safety Answering Points (PSAPs) for police, ambulance, and fire-brigade assistance. Thanks to Galileo-enabled Enhanced 112 (E112) and Advanced Mobile Location (AML) technologies, responders can pinpoint a caller's position within just a few metres instead of kilometres. This system, installed in new vehicles, has cut emergency response times by up to half and significantly reduced fatalities and severe injuries in road accidents.[36]

Galileo also contributes to the COSPAS-SARSAT search-and-rescue system: distress beacons are detected globally within minutes, and Galileo's return-link message reassures victims that help is on the way.[37] These mechanisms make operational Member States' duty to protect life and security by ensuring rapid assistance wherever disasters strike.

GNSS is also crucial in the domain of agriculture and food security, where GNSS signals, augmented by the EU's EGNOS service, enable centimetric guidance for tractors and drones, allowing variable-rate seeding, irrigation, and fertilisation.

Such precision agriculture can increase yields by ≈ 10 % and reduce inputs by 20 %, supporting sustainability and the right to adequate food under Article 11 of the International Covenant on Economic, Social, and Cultural Rights[38]. The European Space Programme reports that GNSS-based farm management tools enhance climate resilience and reduce food loss, proving a "*powerful ally against food insecurity*"[39].

London Economics[40] conservatively values the UK's reliance on GNSS at approximately £10.2 billion per year, roughly 75 percent of total GNSS benefits, showing how deeply GNSS is integrated into both public services and commercial value chains. Considering the emergency services use case; automatic caller-

34. European Union Agency for the Space Programme (EUSPA), *Galileo: Making a Difference for Public Safety* (2023) https://www.euspa.europa.eu/newsroom/news/galileo-e112-saving-lives-every-day accessed 10 October 2025.
35. EU CFR (n 5), Art 2.
36. European Union Agency for the Space Programme (EUSPA), *112 and Galileo: Answering the Call and Saving Lives* (9 February 2024 https://www.euspa.europa.eu/newsroom-events/news/112-and-galileo-answering-call-and-saving-lives accessed 11 October 2025.
37. European Commission, *Galileo Search and Rescue Service: Saving Lives Worldwide* (2024) https://www.gsc-europa.eu/galileo/services/search-and-rescue-sar-galileo-service accessed 10 October 2025.
38. ICESCR (n 6) Art 11.
39. European Union Agency for the Space Programme (EUSPA), How Space Services Help Farmers Grow Smarter (2024) https://www.euspa.europa.eu/newsroom/news/how-space-services-help-farmers-grow-smarter accessed 29 June 2025.
40. London Economics, *The Economic Impact on the UK of a Disruption to Satellite Services* (Report for the UK Space Agency and Innovate UK, August2021).

location via GNSS-enabled Public-Safety Answering Points (PSAPs) accelerates dispatch decisions, reducing response times by an average of 20 percent and saving an estimated £5.4 billion annually in lives preserved, downstream health-care costs, and operational efficiencies. Simultaneously, road-transport operators exploit turn-by-turn navigation and fleet telematics cut journey times by up to 15 percent, saving some £4.0 billion per annum in fuel, labour and emissions costs. Even precision farming, which accounts for over £0.5 billion in yield-optimisation and input savings, hinges on sub-metre GNSS accuracy for variable-rate applications across Europe's arable lands.[41]

These figures, however, conceal GNSS's latent vulnerabilities. Under a seven-day "Reasonable Worst-Case Scenario" outage, London Economics projects an aggregate UK loss of £7.6 billion, with emergency services (-£3.5 billion), road transport (-£1.7 billion) and maritime logistics (-£1.5 billion) bearing the toll of a GNSS disruption. Even a single-day disruption would cost roughly £1.4 billion, illustrating how rapidly modern societies bleed value when PNT signals vanish.[42]

GNSS is also behind several other essential services, such as electricity grids, telecommunications networks, and financial systems. Power grids use GNSS time to balance generation and demand in real time, while banks and stock exchanges employ it for legally mandated transaction timestamping under MiFID II.[43]

These functions sustain the right to health by ensuring hospitals and emergency systems remain powered, and the rights to security and property by maintaining reliable communications and economic stability.[44]

A full technical discussion of GNSS architectures and sector-specific dependencies falls outside the scope of this paper, but it is nonetheless important to recognise that satellite navigation services constitute a hidden backbone of critical infrastructure resilience. They support the sectors discussed here but also logistics, water management, and digital communications domains, where continuity is directly tied to the enjoyment of fundamental rights and the functioning of modern societies.

The examples described above demonstrate that GNSS functions as a human-rights enabler: by locating people in emergencies, feeding populations, and synchronising critical services, satellite navigation systems support fundamental rights and ensure they are guaranteed.

4.3 Balancing Human Rights and Privacy in Space-Enabled Services

EO and GNSS clearly enable the protection of life, health, and security, but a complete assessment must also acknowledge their ethical and governance trade-offs. The expansion of Earth-observation constellations and near-real-time data analytics amplified concerns about privacy, surveillance, and proportionality.[45] Scholars note that high-resolution imagery can reveal sensitive details of private property or individuals without consent, blurring the line between legitimate use observation and intrusive monitoring.[46]

The dissemination of satellite data across jurisdictions and private platforms can occur without clear data-protection safeguards or retention limits, creating a risk that information collected might later be repurposed for surveillance or commercial use.[47]

A parallel concern applies to GNSS-based services. The continuous tracking of an individual's or vehicle's position can reveal detailed personal patterns and associations and raise privacy risks under the EU data-

41. ibid.
42. ibid.
43. European Securities and Markets Authority (ESMA), Guidelines on Synchronisation under MiFID II (ESMA70-872942901-63, 2021).
44. EU CFR (n 5), Arts 6 and 17.
45. M Pedram, S Chandler and E Georgiades, 'When open-source information backfires: Satellite imagery and privacy breaches' (2025) 58 *Vand. J. Transnationall L.*, 119.
46. T Lawal *et al*, 'Privacy in the Age of Remote Sensing During Natural Disasters in Australia and Indonesia' (2023) 4(2) Digital Law Journal 15-39.
47. S Shufelt, 'Remote-Sensing Satellites and Privacy: Why Current Regulations Will Ultimately Fail' (2020) 9(3)American University Business Law Review 487-523.

protection regime. For instance, a recent decision by the European Data Protection Board (EDPB)[48] noted that the use of GPS tracking in a fleet-management setting must be justified by a legitimate interest, time-limited, and transparent; otherwise, it may infringe individuals' rights under the General Data Protection Regulation (GDPR). Although GNSS enables life-saving services, without proper safeguards, the same positioning signals can become tools of pervasive surveillance rather than empowerment.

Space-based services operate within a tension between utility and oversight. The challenge for EU governance is to ensure that space capabilities are deployed under privacy-by-design standards, robust cybersecurity requirements, and transparent data-sharing rules. There is a need to embed such safeguards, through instruments such as the forthcoming EU Space Act,[49] that would enable the Union to take advantage of the humanitarian potential of space technologies without eroding other fundamental rights. Here an effective governance can bridge technological resilience and fundamental-rights resilience. Before examining the legal framework governing the protection of space infrastructure, the next section explores the cyber risks to which these systems are exposed.

5. The Vulnerability of Space Infrastructure: Cybersecurity Risks and Humanitarian Consequences

The case studies of Haiti and Turkey-Syria have shown how Earth Observation supports disaster response and post-crisis recovery. Space technology can provide critical, time-sensitive data that helps rescue teams locate survivors, assess infrastructure damage, monitor displaced populations, and plan long-term reconstruction. EO systems, therefore, operate not merely as scientific instruments but as lifelines, upholding fundamental rights, including the right to life, health, and access to essential services. Yet, the very digital infrastructure that enables this life-saving functionality is increasingly exposed to cyber threats.

Space operations depend on intricate digital systems, ground control stations, data reception facilities, and cloud-based processing platforms. They are often part of a vast and sophisticated supply chain, which increases their vulnerability to cyberattacks. The growing use of space technology, added to its increasing integration with other terrestrial applications, has led to a rise in the number of attacks.[50] Even a relatively simple cyberattack could have significant consequences, especially if it occurs during a large-scale humanitarian emergency. To showcase how such attacks can affect space infrastructure, we use some fictional scenarios.

The following scenarios introduced in this section are fictional constructs; their purpose is to demonstrate how a cyber incident affecting orbital and terrestrial components of space infrastructure could affect other critical sectors and impact fundamental rights. They are used to trace causal and regulatory relationships under existing EU resilience frameworks. This qualitative scenario method is useful to visualise interdependence and legal responsibility; however, it carries inherent limitations. Fictional cases cannot be empirically validated, their assumptions may not generalise across technologies or jurisdictions, and they simplify the complexity of cascading effects. The scenarios are presented as illustrative thought experiments whose purpose is to test whether current governance instruments, particularly NIS 2 and CER, are adequate to prevent or mitigate comparable real-world incidents.

In the first case, we examine a ransomware attack on Earth Observation ground infrastructure. This highlights that space, despite being a complex and unique critical infrastructure, is not immune to other

48. European Data Protection Board (EDPB), 'Safety of Property Can Be a Legitimate Interest for GPS Tracking, but the Measure Must Be Proportionate' (National News, 4 March 2022) https://edpb.europa.eu/news/national-news/2022/safety-property-can-be-legitimate-interest-gps-tracking-measure-must-be_en accessed 18 October 2025.

49. European Commission, *Proposal for a Regulation on the safety, resilience and sustainability of space activities in the Union* COM(2025) 335 final (25 June 2025). [EU Space Act]

50. A Carlo and K Obergfaell, 'Cyber attacks on critical infrastructure: Lessons from recent events' (2024) 46 *Journal of Critical Infrastructure Protection* 46 100701.

types of attacks that affect other "*legacy*" sectors. Particularly when we consider the ground network, it resembles similar IT infrastructures such as those of telecommunication networks.

Let's consider that in the immediate aftermath of a major natural disaster, such as a cyclone or earthquake, the International Charter "*Space and Major Disasters*" is activated. Dozens of satellites are tasked to collect imagery of the affected areas, and rapid mapping services are mobilised to guide emergency responders. However, just as data from satellites begins to stream towards national authorities, a ransomware attack disables a key ground station responsible for processing and distributing the imagery.

Within minutes, emergency mapping systems go offline. Rescue teams lose access to geospatial data identifying collapsed buildings, blocked roads, or isolated communities. Vital hours are lost, not because of a lack of satellite coverage, but because the digital pipeline that delivers the data is compromised.

In this scenario, a cyberattack does not merely interrupt a technical process, but also directly endangers lives. The denial of access to EO data means a denial of essential information for delivering medical care, evacuating vulnerable populations, or distributing food and water.

Moving towards GNSS technologies, a targeted cyber-attack on GNSS, whether by jamming or spoofing, would immediately erode the capabilities described in Section 4.2. In a jamming scenario, first-responders would revert to manual location-finding techniques, adding an estimated 2-3 minutes per dispatch and potentially increasing preventable mortality in mass-casualty events. Loss of continuous AIS tracking during a spoofing attack would force search-and-rescue teams to rely on slow radar sweeps, delaying aid to mariners in distress. In the context of agriculture, GNSS signal manipulation would disrupt precision-farming equipment, such as seeding, fertilisation, and irrigation, leading to crop failures, resource waste, and volatile food prices that disproportionately harm vulnerable communities.

These scenarios highlight a pressing challenge: satellite systems must be recognised and protected as critical digital infrastructure. The security of the ecosystem is not only a matter of national interest or technological resilience; it is a matter of global solidarity and human rights protection.

Securing these systems involves multiple layers: reinforcing the cybersecurity of ground stations, ensuring the integrity of space data throughout the processing chain, building redundancy protocols for crisis operations, and fostering transparency in how information is collected and used. This also requires stronger legal and institutional frameworks to ensure that space capabilities can withstand cyber threats and continue to serve their humanitarian mission.

While fictional, the scenarios reflect documented patterns of real cyber incidents targeting space-based systems and their terrestrial interfaces. For example, the Viasat KA-SAT attack (February 2022) disabled tens of thousands of satellite modems and caused connectivity loss for Ukrainian institutions and thousands of European energy assets, showing how a single supply-chain breach can cascade into critical-infrastructure disruption.[51] A similar incident affected the Dozor-Teleport (June 2023),[52] which was temporarily paralysed, hindering Russian governmental communications. These events illustrate the strategic consequences of attacking commercial SATCOM providers.

Attacks on Earth-observation systems, include the 2014 NOAA (National Oceanic and Atmospheric Administration) intrusion.[53] The breach forced NOAA to shut down certain data services for emergency

51. Carlo Antonio, and Kim Obergfaell, 'Cyber attacks on critical infrastructures and satellite communications' (2024) 46 *International Journal of Critical Infrastructure Protection* 100701. See also: F Casaril and L Galletta, 'Securing SatCom user segment: A study on cybersecurity challenges in view of IRIS2' (2024)140 *Computers & Security* 103799.

52. J Willbold, *et al*, 'Vsaster: Uncovering inherent security issues in current vsat system practices' (2024) *Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks*.

53. L Nakashima, 'Chinese Hackers Breach NOAA Satellite Systems' *The Washington Post* (12 November 2014) https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-noaa-satellite-systems/2014/11/12/4e7a81d0-6a3d-11e4-a31c-77759fc1eacc_story.html accessed 18 October 2025.

maintenance, cutting off data vital to disaster planning, aviation, shipping and other crucial uses. For about two days, satellite data distribution was offline, which skewed weather forecasts slightly and impeded the flow of environmental information until systems were restored. Had the outage persisted, it could have seriously hampered storm tracking, hazard warnings, and climate monitoring, exactly the kind of disruption the fictional scenario envisions for disaster-response data.

GNSS spoofing incidents are amongst the most reported in recent times; data from the Baltic Sea and Nordic region illustrate a growing pattern of GNSS interference attributed to Russian jamming and spoofing, which has directly impacted commercial aviation, marine navigation and timing-dependent functions. According to Swedish aviation authorities, spoofing and jamming over eastern airspace have affected both air and sea traffic[54]. The impacts of spoofing in the region are exponentially increasing; nearly 123,000 flights were disrupted in early 2025 due to GPS signal interference.[55]

All these examples reinforce the scenario modelling in this section and call for governance frameworks that link space-system resilience with the protection of fundamental rights. Given the real-world scenarios, the fictional cases discussed in this paper are plausible representations of existing threat patterns and thereby reinforce the legal and policy analysis that follows.

The incidents and scenarios discussed above demonstrate that satellite networks are now integral to the broader digital-infrastructure ecosystems. Their disruption, whether through cyberattack, interference, or cascading failure, produces effects similar to those of terrestrial digital assets. Space infrastructure forms a subset of critical digital infrastructure, extending the surface of risk and the scope of resilience obligations addressed by instruments such as NIS 2 and CER. Safeguarding this ecosystem is not solely a technical or national-security concern: it is directly tied to the continuity of rights-relevant services, such as navigation for rescue operations, connectivity for hospitals, and data for environmental protection, whose interruption endangers the rights to life, health, and security. Protecting space infrastructure, therefore, advances resilience, but also human-rights protection through the continuity of essential services.

The following section discusses the classification of space as a critical infrastructure sector under EU Law, what it entails, and whether this classification is enough to guarantee the resilience of space and the services it provides.

6. Towards a Secure and Rights-Based Space Governance

6.1 Space Infrastructure as a Critical Infrastructure

The relevance of space technologies lies in their widespread use and variety of applications in several critical or less critical domains, but especially when it comes to strategic use of EO or SATCOM or GNSS technologies, stricter and more efficient security requirements are needed to preserve vital functions of space. For this reason, space is now widely recognised, at least in the European Union, as a critical infrastructure domain.

It is important, however, to clarify that space as a physical domain, like land, sea, air, and cyberspace, cannot itself be classified as critical infrastructure, since it constitutes an operational environment rather than an asset or service. What can be considered as critical are the space-based systems and infrastructures, including satellite constellations, ground segments, and data-distribution networks, that provide essential functions to society. These systems are recognised as part of the European Union's critical infrastructure framework under the NIS 2 Directive and the Critical Entities Resilience (CER) Directive.[56]

54. 'Sweden Accuses Russia of Widespread GPS Jamming Over Baltic Sea', The Moscow Times (4 September 2025) https://www.themoscowtimes.com/2025/09/04/sweden-accuses-russia-of-widespread-gps-jamming-over-baltic-sea-a90427 accessed 18 October 2025

55. 'VT: GPS disruption has affected 123,000 flights in the Baltic region', ERR News (23 July 2025) https://news.err.ee/1609792437/gps-disruption-has-affected-123-000-flights-in-the-baltic-region accessed 18 October 2025

56. NIS 2 Directive (n 3); CER Directive (n 4).

As recent literature shows, the European legal and policy landscape mostly treats space infrastructure as a critical sector, extending to cybersecurity and resilience obligations for satellite operators and data providers.[57]

By contrast, in the United States, this recognition remains under discussion. Several federal documents (e.g., the 2020 Space Policy Directive-5[58] and the 2023 National Cybersecurity Strategy Implementation Plan[59]) acknowledge the criticality of space-based services. Still, the space sector has not yet been designated as a formal Critical Infrastructure Sector under Presidential Policy Directive 21 (PPD-21).[60] NATO, on the other hand, recognises space as a fifth operational domain, alongside air, land, maritime, and cyberspace, and considers an attack against space infrastructure as a possible cause to activate Article 5, emphasising its strategic and security importance.[61]

Space is, therefore, a domain of operations. In contrast, space infrastructure, composed of orbital and terrestrial assets that sustain critical services, is part of a critical infrastructure in both legal and practical terms. This paper supports the view that space infrastructure should be treated as critical infrastructure, and that the space domain, as NATO affirms, is a critical strategic domain whose protection underpins societal and humanitarian resilience.

The EU's 2022 NIS 2 Directive explicitly names the space sector, putting operators of SATCOM, GNSS, and EO services on the same footing as energy grids and hospitals. As *"essential entities"*, operators must implement a series of practices such as risk-based cybersecurity, incident-reporting within 24-h, multi-factor authentication, supply-chain assurance, and board-level oversight, with fines of up to €10 million for non-compliance. Complementing NIS 2, the CER Directive obliges every Member State to draw up national strategies that also cover space systems, carry out stress tests and guarantee business-continuity plans for "*functions vital to society*".

Yet even the European legal frameworks remain essentially technocentric: they list controls to be installed and reports to be filed, but do not explain to operators why these precautions matter in humanitarian terms, nor do they guide decision makers once a crisis escalates from cyber incident to armed conflict. A report from the International Committee of the Red Cross (ICRC) offers a missing normative layer, at least with regard to international conflicts and international humanitarian law. Having analysed the civilian consequences of counter-space operations, the ICRC urges states to always do five things:[62]

- Refrain from disabling satellites that underpin essential services;
- Segment military functions from civilian ones whenever feasible;
- Positively identify and mark satellites that must be spared;
- Desist from weapons or tests that create debris;
- Cooperate to ensure that first responders retain multi-system access to satellite links during emergencies.

Read alongside NIS 2 and CER, these recommendations support the idea of reframing compliance checklists as duties rooted in human rights protection. For example, the NIS 2 Directive's requirement that operators adopt risk-based security[63] gains clear substance when risk is understood to include not only loss of revenue but the knock-on effects on hospitals or power grids if GNSS timing fails. The ICRC's call for physical

57. Francesco Casaril and Letterio Galletta, 'Space Cybersecurity Governance: Assessing Policies and Frameworks in View of the Future European Space Legislation' (2025) 11(1) Journal of Cybersecurity 013.
58. ibid.
59. White House, National cybersecurity strategy (Washington, DC 2023).
60. Executive Office of the President, Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience (2013); The White House, Space Policy Directive-5: Cybersecurity Principles for Space Systems (4 September 2020).
61. NATO, Brussels Summit Communiqué (14 June 2021), para. 33; see also NATO, Space Policy (2023).
62. International Committee of the Red Cross, *ICRC Observations on Protection from Disruption by Military Space Operations* (June 2024).
63. NIS 2 Directive (n 3), Art 21(1).

or logical segmentation that can complement the Commission's Space Act proposal[64] to make a single, renewable licence conditional on demonstrable traffic separation and rapid rerouting capacity.

In this light, the Commission's EU Space Act[65] proposal can link the rights-centred rationale to enforceable governance levers. As an internal-market regulation, it conditions market access on demonstrable safety, resilience, and sustainability by space operators, translating continuity of rights-relevant services (e.g., GNSS timing, emergency communications) into licensing obligations.

Read together with NIS 2 and CER, the Act should operate as *lex specialis* for space, filling the gap for Union-owned assets and aligning space-specific risk-management with the general EU cybersecurity framework. The Act also harmonises incident handling through sectoral significant-incident reporting and empowers the Commission to set uniform reporting templates and, where needed, technical rules for orbital traffic and trackability, which together support rapid, proportional responses that minimise civilian harm during disruptions.

While the proposal does not explicitly create the connection between space technologies and their role in supporting human rights, its architecture is rights-relevant in effect, it makes resilience a precondition for authorisation, standardising how outages are prevented, flagged and handled, and creating coordination rails across Member States, such implementation would therefore reduce the likelihood and duration of service loss in the space-enabled functions on which life, health, security and other fundamental rights now depend.

Integrating this human-rights check into the EU framework requires only incremental legal work but represents a qualitative policy shift. Additionally, specifically concerning international conflicts, national cyber-security agencies would certify that satellite operators have aligned their architectures with the ICRC's least-harm logic. Stress-tests already mandated by the CER Directive could be expanded to rehearse constellation-level fail-overs and to verify that protected satellites are correctly flagged in space-traffic-management registries. The forthcoming licence regime could bind operators to publish annual "*humanitarian resilience statements*" that attest to segmentation, spare-capacity agreements, and debris-avoidance compliance.

7. The EU Space Act: Space Infrastructure Protection and Fundamental Rights

The European Commission's proposal for a Regulation on the safety, resilience, and sustainability of space activities in the Union (the "Space Act"), published in June 2025,[66] addresses many of the vulnerabilities identified throughout this paper. This section analyses how the Space Act puts together protection for the rights-enabling services discussed in Sections 4.1 and 4.2, identifying limitations that could constrain its effectiveness as a rights-protective framework.

7.1 Cybersecurity and Resilience

The Space Act's safety framework (Title IV, Chapter I, Articles 58-74) ensures the long-term sustainability of orbital environments upon which space infrastructure depends. The debris mitigation requirements in Articles 61 and 70 mandate limitation of planned debris generation, prevention of accidental fragmentation, and completion of end-of-life disposal within specified timeframes. From a rights perspective, these requirements protect future generations' access to the space-based services that enable rights realisation.

Article 64(1)[67] requires all Union spacecraft operators to subscribe to an authorised collision-avoidance service, ensuring coordinated tracking and protection of satellites that provide essential services.

64. European Commission, *Proposal for a Regulation on the safety, resilience and sustainability of space activities in the Union*, COM(2025) 335 final (25 June 2025).
65. ibid, Arts 6-8 (licensing conditions), Art 22 (resilience obligations), and Recital 31 (link to NIS 2 and CER Directives as *lex specialis*).
66. EU Space Act
67. ibid, Art 64.

Article 73[68] defines constellation-specific requirements that are particularly significant because many rights-enabling services depend on constellation architectures. The enhanced requirements for mega-constellations and giga-constellations implement a precautionary approach to systemic risk. However, these requirements could raise concerns about misaligned priorities. Constellation size triggers enhanced obligations, but service criticality does not. A single Earth Observation satellite providing irreplaceable disaster monitoring capabilities faces less stringent requirements than individual satellites within a large commercial constellation, despite potentially equal or greater importance for rights protection. This represents a gap where technical criteria (constellation size) receive more regulatory attention than functional criteria (service criticality for rights realisation).

The Act's cybersecurity framework (Title IV, Chapter II, Articles 75-95) is designed to protect rights-enabling functions of space infrastructure. Article 76 introduces comprehensive risk management "throughout the lifecycle of space missions". From conception and design through manufacturing, operations, and decommissioning, it addresses vulnerabilities at all stages. This lifecycle approach responds to the threat scenarios explored in Section 5: cyber threats can manifest from supply chain compromises during manufacturing to operational interference during disaster response activation.

In terms of risk reduction, Article 78's[69] requirement for continuous risk assessment, identifying and assessing "*continuously, all sources of risks*", regularly reviewing identified risks, and establishing "*dedicated risk treatment plans for all the cybersecurity vulnerabilities identified*", creates the dynamic, adaptive approach necessary given evolving threat landscapes.

Article 80's[70] requirements for categorizing and managing critical assets set up the protection of rights-enabling infrastructure. In the Earth Observation context analysed in Section 4.1, critical assets include observation satellites, ground processing stations, and mission control centres coordinating disaster response. For GNSS applications discussed in Section 4.2, critical assets encompass satellite constellations, ground control segments, and timing infrastructure. The requirement that categorisation be based on "*the need to ensure the confidentiality, integrity, authenticity and availability of information*" and "*the level of criticality required by the security level of the respective space mission*" creates a framework linking asset protection to mission criticality.

Continuous monitoring requirements are defined in Article 83,[71] which require space operators to use appropriate detection systems, with ground stations required to meet minimum standards and spacecraft required to generate security events transmitted to logically segregated monitoring subsystems. Operators are also required to implement defence-in-depth principles, ensuring that monitoring capabilities remain functional even if operational systems are compromised. In the GNSS context, continuous monitoring enables rapid detection of signal manipulation attempts. In Earth observation contexts, monitoring detects unauthorised access, data manipulation, or distribution disruptions that could compromise disaster response.

Article 87[72] defines business continuity and response/recovery requirements, making operational the resilience necessary to protect rights-relevant services during disruptions. The mandate for plans addressing "*disruptions in the supply of utilities*", "*loss of physical assets at the ground segment*", "*interferences on the ground-to-space, space-to-ground and the space-to-space radio frequency links*", and "*altered or compromised parts of the ground segment*" maps directly to documented attack vectors, including the Viasat incident discussed in Section 5.

Article 85[73] defines cryptographic requirements to address unauthorised command and control threats. The requirements for end-to-end authentication between satellite control centres and spacecraft and encryption

68. ibid, Art 73.
69. ibid, Art 78.
70. ibid, Art 80.
71. ibid, Art 83.
72. ibid, Art 87.
73. ibid, Art 85.

of telecommands address documented vulnerabilities in unencrypted telecommand links. Article 92[74] deals with supply chain risk management requirements and extends security obligations throughout supplier ecosystems, addressing the supply chain compromises that enabled cascading disruptions in incidents like the Viasat attack.

7.2 Environmental Sustainability: Transparency Without Substantive Limits

The Space Act's environmental framework (Title IV, Chapter III, Articles 96-100) requires Union space operators to "*calculate the environmental footprint (EF) of the space activities they carry out*".

Article 96(6)[75] requires Environmental Footprint Declarations accompanied by certificates, supporting studies, while Article 99 establishes the Union Environmental Footprint Database with publicly available aggregated datasets, creating transparency that supports civil society oversight. However, the focus on measuring and reporting impacts does not establish limits on environmental damage or require minimisation of ecological harm. The framework does not mandate that environmental considerations limit space activities or establish environmental standards operators must meet.

7.3 The Defence and National Security Exclusion

Article 2(3)'s[76] exclusion of "*space objects exclusively used for defence or national security purposes*" from the Regulation's scope creates the most significant limitation for comprehensive rights protection. This exclusion is legally necessary given Member State competences under Article 4 TEU,[77] but creates protection gaps given that dual-use assets and services are so widespread in modern space infrastructure.

Many space assets serve both civilian and military functions. Article 2(3)(b)'s provision excluding "*space objects that have been temporarily placed for defence purposes under a military operation and control, for the duration of the respective space mission*" acknowledges dual-use reality but creates uncertainty about protection continuity. When dual-use assets transition to military control, the Space Act's safety, resilience, and environmental requirements no longer apply.

7.4 Progress Towards Rights-Protective Space Governance

The Space Act represents significant progress towards the rights-protective framework this paper advocates. Its safety, resilience, and sustainability requirements ensure that many needs identified as necessary throughout our analysis are met.

However, the defence and national security exclusion creates gaps precisely where dual-use infrastructure serving both military and civilian rights-enabling functions operates. The environmental framework provides transparency without substantive protection standards. The simplified risk management regime prioritises orbital safety over service continuity protection for smaller operators.

The Act's technical focus on safety, resilience, and sustainability does not explicitly articulate the connection between these requirements and the fundamental rights they serve to protect. The Space Act requirements support rights realisation, but the Regulation itself does not frame its objectives in rights terms or require that implementation prioritises continuity of rights-enabling services. A rights-protective framework would require explicit recognition of space infrastructure's role in enabling fundamental rights, prioritisation mechanisms ensuring that rights-enabling services receive enhanced protection regardless of operator size or asset classification. The Space Act provides essential building blocks but not yet the complete architecture necessary for comprehensive rights protection in the space domain.

74. ibid, Art 92.
75. ibid, Art 96.
76. EU Space Act, Art 2.
77. Consolidated Version of the Treaty on European Union [2008] OJ C115/13, Art 4.

7.4.1 Dual use, the solution or the problem?

The space sector experienced the convergence of commercial and military requirements in orbit.[78] This means that most of the new constellations, whether for broadband, Earth observation, or SATCOM, have at least a defence application. This dual-use nature has long been a defining feature of the space sector, offering efficiency, innovation, economies of scale, but also generating security, legal, and humanitarian dilemmas.

From the perspective of international humanitarian law (IHL) and civilian protection, dual-use assets challenge traditional distinctions between civilian and military objects. Satellites and ground stations today often serve multiple clients and purposes at once: a single beam or transponder can relay telemedicine data for an NGO, broadband access for a rural school, and encrypted tactical communications for a defence actor. The targeting or disabling of such systems in conflict times, therefore, risks disproportionate harm to civilians.

The International Committee of the Red Cross (ICRC) warns that "*the widespread dual use of space systems and the resulting entanglement of civilian and military operators magnify the risk of civilian harm*" and calls for "*special precautions*" before the use of force against any satellite supporting essential services on Earth.[79] This entanglement complicates proportionality assessments and challenges the implementation of IHL principles such as distinction and necessity.

A second dimension of the problem concerns governance and accountability. The control of dual-use systems is most of the time exercised by private corporations whose commercial logic does not always align with states' legal obligations under international law.

The experience of Starlink in the Ukraine War is a useful example:[80] the same commercial network enabling humanitarian coordination also carried sensitive military data. When SpaceX unilaterally restricted access in certain combat zones, both military and humanitarian operations were disrupted, demonstrating the absence of clear escalation channels and accountability mechanisms.[81]

This episode illustrates the privatisation of strategic decision-making in space. When commercial providers can throttle, re-route, or prioritise traffic at will, they effectively exercise powers with direct humanitarian and geopolitical consequences. Yet few frameworks clarify whether such actions fall under state responsibility, corporate due diligence, or contractual discretion. This grey zone of accountability can undermine transparency and predictability in crises.

The technical architecture of modern constellations is also influenced by this dual-use paradigm, which can also increase the attack surface and affect cyber vulnerability. Software-defined payloads and shared ground infrastructure mean that a cyber-attack or kinetic strike intended for a single (military) node could cascade across civilian networks. The humanitarian implications of such spill-over effects, loss of emergency communications, disruption of navigation, and interference with disaster-response satellites are, as analysed in this paper, profound.

Recognising these risks, European institutions and international organisations are developing governance and technological mechanisms to manage, rather than eliminate, dual-use interdependence. The European IRIS² Secure Connectivity Programme, established by Regulation (EU) 2023/588, can be seen as an attempt to separate governmental from commercial traffic. The programme aims to build a European SATCOM

78. D Paikowsky, 'Dual Use of Space Technology: A Challenge or an Opportunity? Space Commercialization in the US After the Cold War'. In: Brian C. Odom (ed) *The Rise of the Commercial Space Industry: Early Space Age to the Present* (Springer International Publishing 2024), 291-306.

79. S Berrang, 'How Would IHL Apply to Hostilities in Outer Space?' (2 November 2023) ICRC Blog https://blogs.icrc.org/law-and-policy/2023/11/02/how-would-ihl-apply-to-hostilities-in-outer-space/ accessed 29 June 2025.

80. A Horton, S Korolchuk and E Dou, 'Russia's Illicit Procurement Networks and Its Advance in Ukraine' The Washington Post (12 October 2024) https://www.washingtonpost.com/world/2024/10/12/starlink-russia-ukraine-elon-musk/ accessed 19 October 2025.

81. J M Rickli and F Mantellassi, *The war in Ukraine: Reality check for emerging technologies and the future of warfare* (GCSP, Geneva Centre for Security Policy, 2024).

multi-orbit constellation; it is structured as a public–private partnership combining commercial broadband services with a "HardGov" layer dedicated to governmental and security communications. The Regulation explicitly requires that the constellation be multi-orbital and modular, with two distinct segments: one financed by the Union for governmental use, and one privately funded for commercial services.[82]

This design entails the principle of segmentation proposed by the ICRC, which shall reduce the risk that the disruption of one service could endanger others and ensure that humanitarian communications remain online in crisis conditions.

The European Commission's Space Act proposal foresees resilience drills simulating cyber, kinetic, and spectrum attacks to verify that re-routing, fail-over, and notice procedures work under stress. These exercises would involve not only satellite operators but also national CERTs and humanitarian agencies, thus integrating humanitarian considerations into routine security certification.

At the international level, several scholars and states have proposed establishing a "*Digital Non-Interference Corridor*" under the United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS).[83] The corridor would assign frequency bands and orbital slots reserved for life-saving services where intentional interference would carry a presumption of unlawfulness. Transparency could be ensured by operator reports on the percentage of governmental versus commercial payload use; such a mechanism could help belligerents make informed proportionality assessments and give humanitarian actors confidence that fallback capacity exists.

The inclusion of the space sector in the EU's NIS 2 Directive and CER Directive is an important step, but complementary norm-building efforts are still needed to define how operators must segment, authenticate, and protect dual-use services. The forthcoming EU Space Law should, therefore, codify the obligations of private operators concerning transparency, data-sharing, and continuity of humanitarian services during crises.

The ethical dimension must not be overlooked. Dual use is not inherently negative; it reflects the shared dependence of civilian and defence communities on the same technologies. The challenge lies in ensuring that the governance of dual-use infrastructure aligns with humanitarian needs. This can be ensured by technical segregation, contractual obligations, and independent oversight mechanisms.

8. Conclusion

This paper discusses how space-based systems are a fundamental layer of Europe's digital infrastructure and key enablers of the protection of fundamental rights. The analysis of Earth Observation and Global Navigation Satellite Systems has shown that these technologies are critical infrastructures on which the realisation of rights such as life, health, food, and access to essential services now depends. Their continuous operation sustains emergency response, environmental monitoring, and the functioning of vital services, meaning that the resilience of space infrastructure has become inseparable from the protection of human security.

To address RQ1, the paper examined how the growing reliance on space technologies affects the protection of fundamental rights. The case studies of Haiti's post-hurricane recovery and the Turkey–Syria earthquake response demonstrated that EO data have become essential for emergency management and response. Similarly, GNSS integration into Europe's emergency communications and critical service delivery systems

82. Regulation (EU) 2023/588 of the European Parliament and of the Council of 15 March 2023 Establishing the Union Secure Connectivity Programme 2023–2027 [2023] OJ L79/1.

83. United States Delegation to the United Nations Committee on the Peaceful Uses of Outer Space (COPUOS), Statement to the Scientific and Technical Sub-Committee (15 February 2024);International Civil Aviation Organization (ICAO), Resolution A41-8 'Protection of Radio Navigation Satellite Service (RNSS) Signals Used for Safety-of-Life Applications' (Assembly 41st Session, Montréal, 2022) para. 3.

shows that satellite navigation now safeguards life and welfare daily. The continuity of these systems ensures the effective exercise of rights guaranteed under the Charter of Fundamental Rights of the European Union and international law.

In response to RQ2, the paper investigated the risks posed by cyberattacks to space infrastructure and how disruptions can undermine human security and emergency operations. The analysis demonstrated that cyber threats to space systems can immediately disrupt life-saving services on Earth. Interference with space systems can cascade into terrestrial crises, interrupting emergency communications, undermining disaster management, and endangering lives. Cybersecurity for space is, therefore, a direct component of human-rights protection.

Addressing RQ3, the paper assessed the adequacy of current European governance frameworks: the NIS 2 Directive, the Critical Entities Resilience Directive, and the proposed EU Space Act, in protecting space infrastructure as critical digital infrastructure. These instruments successfully recognise the space sector's strategic and societal role. Yet they focus on compliance and control rather than articulating the humanitarian rationale underlying resilience. Gaps persist regarding dual-use governance, cross-border enforcement, and the integration of humanitarian and security considerations into operational rules.

Building upon these findings, the paper argues that a next-generation space security regime must rest on five plain obligations. First, links that keep people alive must never go dark. Second, defence traffic and civilian traffic should run on separate circuits. Third, space assets that carry vital services must be clearly flagged in space-traffic systems so operators can spare them in a crisis. Fourth, constellations must include built-in failover mechanisms so that rescue teams and essential services remain connected even if one network is lost. These principles translate humanitarian protection into operational standards, bridging the gap between legal frameworks and technical governance.

In conclusion, this research shows that safeguarding space infrastructure is a prerequisite for protecting fundamental rights in the digital age. The path forward demands the inclusion of humanitarian considerations into technical governance, ensuring that resilience frameworks serve the protection of human life, safety, and welfare.