Who Is In, Who Is Out, and Who Should Be? A Transatlantic Perspective on Space Cybersecurity Regulation

Anna Blechová[1]

Keywords: *Cybersecurity Regulation; Space Law; Policy; US Law; EU Law.*

Abstract:

Space infrastructure has become an indispensable component of contemporary society, underpinning critical services ranging from communications and navigation to financial systems and defence. This growing reliance, however, has also transformed space assets into increasingly attractive targets for cyberattacks as was demonstrated in 2022 via the VIASAT cyber-attack. The perspective on cybersecurity in the space domain is therefore shifting: what was once considered a niche area is now emerging as a central concern within broader cybersecurity governance. Despite this evolution, the field remains insufficiently defined and continues to require significant conceptual, technical, and regulatory clarification.

The space sector presents distinct cybersecurity challenges, including reliance on legacy systems, complex and globally distributed supply chains, limited implementation of security-by-design principles, and a shortage of specialised expertise. These characteristics, coupled with the increasing number of cyber incidents affecting space infrastructure, underscore the urgency of developing a more coherent and targeted regulatory approach.

At present, however, the regulatory landscape remains highly fragmented, particularly within the European Union and the U.S.A. Relevant provisions are dispersed across multiple instruments, including the NIS2 Directive, the Cyber Resilience Act, the revised EU Cybersecurity Act, the proposed Digital Networks Act, and the proposed EU Space Act. While these frameworks collectively address elements of cybersecurity, they do so in a manner that is often indirect, overlapping, or insufficiently tailored to the specificities of space systems. A similar, though structurally different, fragmentation can be observed in the United States, where the regulatory and standardisation landscape is shaped by instruments such as Space Policy Directive-5, as well as standards developed by NIST and IEEE.

Against this background, this paper asks a fundamental question: who is currently regulated within space cybersecurity frameworks, and who should be? Adopting a transatlantic perspective, the study compares the approaches of the European Union and the United States in defining the scope of regulated entities and activities.

The analysis focuses on nine components (areas) of the space sector: ground stations; CubeSats in Low Earth Orbit (LEO); government satellites in Medium Earth Orbit (MEO) and Geostationary Earth Orbit (GEO); commercial satellites in LEO; LEO megaconstellations; "smart" satellite components (such as refuelling systems or control software); government-owned ground stations; launch facilities; and satellite communications (uplink and downlink). It evaluates both their exposure to cyber threats and the extent to which they are addressed within existing regulatory and policy frameworks.

Methodologically, the paper draws on semi-structured interviews conducted with representatives from academia, industry, and policymaking institutions, complemented by doctrinal and desk-based analysis. By mapping technological vulnerabilities against regulatory coverage, the paper identifies structural gaps, inconsistencies, and blind spots in current frameworks. It ultimately argues for a more clearly defined and systematically structured approach to determining the subjects of space cybersecurity regulation.

[1] Email: Anna.blechova@law.muni.cz, Affiliation: PhD candidate at Masaryk University; Fulbright Visiting Researcher at Cornell University and George Washington University.

1. Introduction

In 2026, humans return to the Moon for the first time since Apollo 17, fifty-four years earlier.[2]The same year finds roughly 17,000 active satellites in Earth orbit[3], more than a hundredfold increase on the 157 satellites operating fifty-eight years ago.[3] The difference is not only one of scale but of ownership: where Neil Armstrong's era of "one small step for man, giant leap for mankind" was defined by state-driven space activity, contemporary space infrastructure is predominantly owned and operated by private entities. SpaceX alone operates approximately 9,400 satellites, [4] a concentration of capability that has shifted the balance of power beyond the Kármán line from states toward private companies.

This shift has coincided with a deepening societal dependence on space infrastructure. Navigation applications, mobile banking, precise time-stamping, and connectivity in remote locations all rely, often invisibly, on satellite systems; contemporary global supply chains are similarly inseparable from satellite networks. That dependence has made space infrastructure an increasingly attractive target for cyberattack. Satellites and their ground segments are exposed to multiple attack vectors capable of producing systemic consequences, and the long-standing assumption that physical distance from terrestrial networks affords protection has been repeatedly disproven, most visibly during the war in Ukraine.

The cyberattack on the KA-SAT network in February 2022[5] is the clearest illustration. Beyond its intended target, the attack disrupted wind turbine monitoring in Germany and cut satellite internet service for roughly 3,900 users in France, with spillover effects across central Europe. It demonstrated that a cyber operation against a satellite system can produce immediate, tangible effects well beyond the theatre of conflict, and it brought cybersecurity in outer space, for the first time, sustained international attention.

That attention has proven durable rather than episodic: a cyberattack on the Polish Space Agency[6], a breach of ESA systems in autumn/winter 2025, and reported cyber activity involving the Russian *Luch*[7] satellites indicate that KA-SAT was not an isolated event but part of a broader, still-accelerating pattern (discussed in Section 2). Cybersecurity in space has consequently moved from a niche technical concern to a central question in cybersecurity governance more broadly.[8]

Yet the field remains conceptually and technically underdefined, and its regulation fragmented. In addition, the question of who should be compliant with space cybersecurity regulation remains unanswered. It is important to note that the legal framework governing outer space activity was built in the 1960s around state actors; it has not been systematically updated to reflect a sector now driven by commercial operators and converging cyber risk.[9] Scholars including Falco[10], Verco[11], Larsen[12], Livingstone[13], and Blount[14] have repeatedly flagged this gap, though (as elaborated in Section 2) the reasons for

---

[2] Tory Shepherd, 'Humans Are En Route to the Moon for the First Time in 54 Years – and Australia's Dish Is Tracking Them' *The Guardian* (2 April 2026) <https://www.theguardian.com/science/2026/apr/02/humans-are-en-route-to-the-moon-for-the-first-time-in-54-years-and-australias-dish-is-tracking-them> accessed 8 July 2026.

[3] 'How Many Satellites Are in Orbit in 2026? — Live Count | Orbital Radar' (19 June 2026) <https://orbitalradar.com/how-many-satellites-in-orbit> accessed 8 July 2026.

[4] https://time.com/article/2026/04/16/space-debris-satellites-growing-risk/

[5] Viasat, 'KA-SAT Network Cyber Attack Overview' (*Viasat.com*, 18 July 2026) <https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/> accessed 18 July 2026; 'Case Study: Viasat Attack' (*Cyber Peace Institute*) <https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat> accessed 31 May 2023; Viasat.

[6] 'Cyberattack Detected at Polish Space Agency, Minister Says' *Reuters* (2 March 2025) <https://www.reuters.com/world/europe/cyberattack-detected-polish-space-agency-minister-says-2025-03-02/> accessed 26 September 2025.

[7] Aleix Nadal Campos, 'How Russia Is Intercepting Communications from European Satellites' (2026) <https://www.rand.org/pubs/commentary/2026/03/how-russia-is-intercepting-communications-from-european.html> accessed 17 August 2026.

[8] M Manulis and others, 'Cyber Security in New Space: Analysis of Threats, Key Enabling Technologies and Challenges' (2021) 20 International Journal of Information Security 287 <https://doi.org/10.1007/s10207-020-00503-w>; Gregory Falco, *The Vacuum of Space Cyber Security* (2018) <https://doi.org/10.2514/6.2018-5275>; Edward Verco, 'Satellites Are Cyber Insecure: We Need Regulation to Avoid a Disaster' (2021) 2 ANU Journal of Law and Technology 57.

[9] Neta Palkovitz, *Regulating a Revolution : Small Satellites and the Law of Outer Space* / (Kluwer Law International, 2020).

[10] Falco (n 8).

[11] Verco (n 8).

[12] Paul Larsen, 'Small Satellite Legal Issues' (Social Science Research Network 2017) SSRN Scholarly Paper 3784281 <https://papers.ssrn.com/abstract=3784281> accessed 10 May 2022.

[13] David Livingstone and Patricia Lewis, 'Space, the Final Frontier for Cybersecurity?' (Chatham House 2026) <https://www.chathamhouse.org/2016/09/space-final-frontier-cybersecurity> accessed 19 April 2026.

[14] PJ Blount and Laetitia Cesari Zarkan, 'Coexisting in Low-Earth Orbit: Large Constellations and Cybersecurity Governance' (2023) 48 Air and Space Law <https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\AILA\AILA2023035.pdf> accessed 25 March 2025; PJ Blount, 'Space Security' *Elgar Concise Encyclopedia of Space Law* (Edward Elgar Publishing 2025) <https://www.elgaronline.com/display/book/9781802207361/chapter75.xml> accessed 17 August 2026.

its persistence remain under-examined. Nevertheless, even though the question of why space activity should be regulated remains still open, the more pressing challenge is determining which concrete actors that regulation should address.

Against this background, the paper asks a fundamental question: **who is currently regulated within space cybersecurity frameworks, and who should be?** It adopts a transatlantic perspective, comparing how the European Union and the United States define the scope of regulated entities and activities, structured around nine components of the space sector, from ground stations and CubeSats to megaconstellations and satellite communications links. Section 2 sets out the conceptual and technical background; Section 3 details the methodology; Sections 4 and 5 map the EU and US frameworks respectively; Section 6 compares regulatory coverage against the nine components; and Sections 7 through 9 discuss the findings and propose a more coherent basis for defining the scope of space cybersecurity regulation.

2. Space Cybersecurity: Conceptual and Technical Background

Space cybersecurity sits at the intersection of two governance domains that developed largely in isolation from one another. Space law was framed in the 1960s and 1970s around state responsibility and liability for objects launched into orbit; cybersecurity law developed later, and separately, around terrestrial IT and OT systems. The interconnection between the two domains has been marginalised since the inception of space activity, an omission now the subject of sustained scholarly criticism.[15]

Space cybersecurity can be defined as the protection of space systems, ground infrastructure, and the links between them from malicious interference, treating mission continuity and availability as first-order design and security primitives rather than as secondary operational concerns.[16] This distinguishes it from conventional cybersecurity governance, where availability is one objective among several, rather than the organising principle. Four structural drivers explain why terrestrial security assumptions transfer only partially to this setting. Legacy systems and long asset lifespans mean that satellites launched a decade or more apart fly incompatible authentication protocols and cryptographic algorithms side by side, with many platforms operating years beyond their design life and built without cybersecurity in mind. [17]Cost pressures drive reliance on commercial off-the-shelf components of uncertain provenance and limited security validation, pointing to supply chain assurance that is uneven rather than centrally governed. Security-by-design adoption also remains weak, as cost-constrained developers, particularly smaller firms, prioritise demonstrating mission viability to investors over cybersecurity investment. Finally, the field faces a shortage of specialised expertise, compounded by organisational silos that separate aerospace engineering from cybersecurity practice. [18]

These drivers manifest differently across the ground, space, and link segments that structure the sector. The ground segment, comprising control centres, ground stations, and user terminals, is the most conventionally exposed: the KA-SAT incident illustrated this when compromised ground-segment access, rather than the space segment itself, was used to disable tens of thousands of user terminals. [19] The space segment is comparatively shielded from direct network access but becomes physically unreachable and cryptographically fixed once launched, leaving it unable to adapt to threats that emerge over a mission's lifetime. The link connecting the two, constrained by bandwidth and intermittent visibility, bounds which security functions, such as authentication or key rotation, can practically be executed and when. Section 6 develops this three-part view into the nine-component framework used to map regulatory coverage.

The pattern of incidents since KA-SAT bears this out. A cyberattack on the Polish Space Agency exposed national space institutions to malicious cyber activity. In autumn/winter 2025, a cyberattack on the European Space Agency reportedly resulted in the leakage of space-related data from Europe.[20] Reported cyber activity involving the Russian Luch satellites further suggests that exposure is not confined to ground infrastructure but extends to on-orbit assets themselves.[21] This trajectory is registered in recent policy literature: contributions to A Research Agenda for Cybersecurity Law and Policy[22],

[15] Falco (n 8); Verco (n 8).
[16] Rajiv Thummala, Eric Rice and Gregory Falco, 'Why Is Space Cybersecurity Unique?' *Proceedings 2026 Workshop on the Security of Space and Satellite Systems* (Internet Society 2026) <https://doi.org/10.14722/spacesec.2026.23055> accessed 17 August 2026.
[17] ibid.
[18] ibid.
[19] ibid.
[20] Emma Gatti, 'ESA Confirms Data Breach' (*SpaceNews*, 30 December 2025) <https://spacenews.com/esa-confirms-data-breach/> accessed 17 August 2026.
[21] Nadal Campos (n 7).
[22] 'A Research Agenda for Cybersecurity Law and Policy' <https://www.e-elgar.com/shop/gbp/a-research-agenda-for-cybersecurity-law-and-policy-9781803929187.html> accessed 17 August 2026.

the ENISA Space Threat Landscape 2025[23], and the report Outer Space Cyberattacks: Generating Novel Scenarios to Avoid Surprise[24] all treat the rise of cyberattacks on space infrastructure as a live and growing agenda item.

The scale of what is now exposed compounds the risk. The commercial space sector's valuation currently exceeds USD 447 billion and is projected to reach USD 1 trillion by 2030 and USD 1.8 trillion by 2035 [25] more satellites were launched in 2022 than in any prior year, a trend that continues to accelerate.

The legal literature has registered this shift but has focused mainly on describing the absence of regulation rather than explaining it. Larsen suggests that, because negotiating binding international rules is too slow relative to the sector's pace of change (illustrated by the proliferation of small satellites), soft-law instruments are filling the gap; a parallel dynamic recurs elsewhere in commercial space law.[26]

3. Methodology

This paper adopts a mixed-methods design, combining doctrinal, desk-based legal analysis with primary qualitative research. The study employs semi-structured interviews with representatives from academia, industry, and policymaking institutions, thereby grounding the comparative mapping exercise in empirical evidence rather than in text analysis alone.

The desk-based component consists of a doctrinal review of the primary legal and policy instruments governing cybersecurity in the space sector on both sides of the Atlantic. On the EU side this includes the NIS2 Directive, the Cyber Resilience Act, the revised Cybersecurity Act, the proposed Digital Networks Act, and the proposed EU Space Act; on the US side it includes Space Policy Directive 5 and relevant NIST and IEEE standards. Because the Digital Networks Act and the EU Space Act remain at the proposal stage at the time of writing, their treatment here is necessarily provisional and is flagged as a limitation below. As a subsidiary question, the analysis also asks whether the United States favours a soft-law approach in this domain relative to the EU's more hard-law orientation, a divergence observed in AI and data-protection regulation but not yet tested for space cybersecurity.

The empirical component consists of at least 24 semi-structured interviews with academics, policymakers, and industry representatives, consistent with recognised sample-size thresholds for qualitative elite-interview research.[27] Industry participants were drawn primarily from the New Space sector; policymaking and standard-setting perspectives were sought from bodies including think tanks, NIST, NATO, DOD and IEEE. Participants were approached individually by email and invited to a 30-minute interview, online or in person, with a one-page project summary provided in advance. Interviews probed familiarity with applicable regulation, its perceived necessity and adequacy, and views on regulatory gaps and appropriate remedies. All interviews were anonymised in accordance with research ethics requirements and GDPR. Interview data were analysed through grounded theory[28] with axial and selective, and read alongside the doctrinal analysis described above.

The nine components mapped in Section 6, ground stations, CubeSats in LEO, government satellites in MEO/GEO, commercial satellites in LEO, LEO megaconstellations, smart satellite components, government-owned ground stations, launch facilities, and satellite communications links, extend the ground/space/link segmentation set out in Section 2 into categories that vary by ownership, orbital regime, and scale, the dimensions along which regulatory obligations most plausibly diverge.

Limitations include the evolving, in places draft, status of key instruments, notably the EU Space Act and the Digital Networks Act, meaning the comparative mapping in Section 6 reflects a regulatory landscape still in motion. The interview

---

[23] 'ENISA Space Threat Landscape 2025 | ENISA' (6 November 2025) <https://www.enisa.europa.eu/publications/enisa-space-threat-landscape-2025> accessed 17 August 2026.

[24] Patrick Lin and others, 'Outer Space Cyberattacks: Generating Novel Scenarios to Avoid Surprise' (arXiv, 17 June 2024) <https://doi.org/10.48550/arXiv.2406.12041> accessed 17 August 2026.

[25] 'Space: The $1.8 Trillion Opportunity for Global Economic Growth | McKinsey' <https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/space-the-1-point-8-trillion-dollar-opportunity-for-global-economic-growth> accessed 10 February 2025.

[26] Lesley Jane Smith, 'Constitutionalisation of Space by the European Union: A Perspective' (2025) 50 Air and Space Law <https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\AILA\AILA2025049.pdf> accessed 8 December 2025.

[27] Tom Clark and others, *Bryman's Social Research Methods* (New Edition, Seventh Edition, New Edition, Seventh Edition, Oxford University Press 2026); Kasper Trolle Elmholdt, Michael Gill and Jeppe Agger Nielsen, '"How Many Interviews Do I Need?" An Examination of Interview Numbers and Sampling Moves in Qualitative Research' [2026] Organizational Research Methods 10944281261424516 <https://doi.org/10.1177/10944281261424516>.

[28] '(PDF) The Discovery of Grounded Theory (Glaser and Strauss, 1967)', *ResearchGate* <https://www.researchgate.net/publication/273261126_The_Discovery_of_Grounded_Theory_Glaser_and_Strauss_1967> accessed 17 August 2026; Barney Glaser and Anselm Strauss, *Discovery of Grounded Theory: Strategies for Qualitative Research* (Routledge 2017) <https://doi.org/10.4324/9780203793206>.

sample, while within recognised thresholds for qualitative legal research, remains modest relative to the full population of relevant stakeholders, and findings should be read as indicative rather than statistically representative.

4. The EU Regulatory Landscape

4.1 The European Union as a Regional Actor

As a regional actor the EU presents the most interesting example as a unique regional actor in space. Whereas other regional frameworks attempt to create space cooperation sui generis, the EU's space cooperation is firmly nested in within mature institutional frameworks.[29] In particular, this allows for the EU to act significantly more like a state when adopting law and regulation related to space cybersecurity. Significantly, this has meant that the regulation of space cybersecurity has emerged from a rapidly maturing regulatory regime for cybersecurity more generally.

Space cybersecurity was first directly addressed as part of the NIS 2 Directive, which addresses EU wide network and information security. This directive only offers a partial framework for cybersecurity regulation in the space sector. One of its main aims is to identify sectors of high criticality and regulate them with regards to cybersecurity due to the societal risk of a successful cyberattack. Such an approach increases legal risk, based on the type of system being operated, by imposing liability on the operator. In this context, the directive adopts space as a sector of high criticality, but it limits this category to "operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks."[30] The regulation's focus on ground infrastructure targets the ground-space interface as the critical link in the use of space, but future directives could expand this category. As an EU directive, member states retain discretion in transposition of the regulation to their national regulation, and could, in theory, expand their national legislation to include space assets located in orbit. This hypothetical scenario would create an intriguing dynamic, as widespread national initiatives of this kind could weaken the perceived need for an EU level space law. However, given that only thirteen Member states currently possess a national space policy and only Latvia broadened the scope of NIS 2 directive[31] in that regard, such considerations remain largely theoretical.

Another reason for the limitation to ground stations could have been connected to the characterization of space as a shared competence under Art. 189[32] of the Treaty on the Functioning of the EU (TFEU). This limits the EU from harmonizing space law across the member states. Article 4(3) TFEU confers upon the Union competence to carry out activities in space, in particular to define and implement programmes, while expressly preserving Member States' capacity to exercise their own competence in parallel. Article 189 TFEU operationalises this shared competence by empowering the Union to establish measures, potentially in the form of a European space programme, expressly "without harmonising the laws and regulations of Member States." Read together, and in light of the principle of conferral, these provisions suggest that the Union's regulatory activity here is better understood as coordinating rather than displacing national competence; the instruments examined below are, accordingly, best characterised as a general cybersecurity regime extended incrementally into the space sector, rather than a self-standing body of space law.

Nevertheless, the EU is currently pursuing some level of synchronization of member state space laws as seen in the publication of the proposal for an EU Space Act in June 2025, which has now gone through a number of drafts.[33] This regulation seeks to standardize requirements for market access to the single market of the EU - rather than adopt space law in a more traditional sense – by requiring operators to get an EUSA certification for both launch vehicles and

---

[29] Other regional organizations like APSCO, APSRAF, SCO, among others, revealed no significant activity with regards to building space governance frameworks.

[30] Annex 1, 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) (Text with EEA relevance) 2022 (OJ L).

[31] Art. 20, 'Nacionālās kiberdrošības likums' (*LIKUMI.LV*) <https://likumi.lv/doc.php?id=353390> accessed 12 August 2026.

[32] Article 189 TFEU

1. To promote scientific and technical progress, industrial competitiveness and the implementation of its policies, the Union shall draw up a European space policy. To this end, it may promote joint initiatives, support research and technological development and coordinate the efforts needed for the exploration and exploitation of space.
2. To contribute to attaining the objectives referred to in paragraph 1, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall establish the necessary measures, which may take the form of a European space programme, excluding any harmonisation of the laws and regulations of the Member States.
3. The Union shall establish any appropriate relations with the European Space Agency.
4. This Article shall be without prejudice to the other provisions of this Title.

[33] European Commission (ed), *EU Space Act: The EU's Ambition for a Cleaner, Safer and More Competitive Space Sector* (Publications Office 2025); European Commission, 'PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the Safety, Resilience and Sustainability of Space Activities in the Union'

spacecraft, which is issued by a "qualified technical body."[34] Within this context the draft law adopts the notion of resilience as one of its pillars, which is predominantly concerned with cybersecurity of space assets.[35] Under this pillar regulated entities are required to "shall take appropriate technical, operational and organisational measures to manage the risks posed to the security of network and information systems."[36] Specifically, the act requires a risk mitigation process built on an "all hazards approach" and includes a list of items to be addressed in this process, which will be further elaborated in an implementing act from the European Commission.[37] Finally the draft act includes a reporting requirement for cybersecurity incidents.[38]

4.2 EU and Cybersecurity – NIS 2, CER, and EU Space Act Matrix

The relationship between the proposed EU Space Act and the broader body of Union cybersecurity legislation remains in development. The interaction between the EU Space Act and NIS2 illustrates this evolution. In its original form, the EU Space Act operated as a *lex specialis* in relation to NIS2. The December 2025 proposal, however, departed from this approach. Article 75 and the revised recital 72 explicitly emphasize that cybersecurity requirements under NIS2 and the proposed EU Space Act must be synchronized and coordinated so that the obligations remain identical for all relevant categories of entities. This marks a deliberate shift away (but in good direction) from the earlier model of regulatory hierarchy.

In principle, the original *lex specialis* approach was defensible. Yet the implementation of NIS2 through a directive allowed Member States to extend its scope beyond the minimum requirements established by Union law. Member States could have in fact done so by adopting broader definitions of space services. Latvia, for example, expanded the scope of space activities subject to national cybersecurity regulation.[39] This creates the possibility of conflict between the EU Space Act and national legislation transposing NIS2. In such cases, however, the principle of primacy ensures that Union law prevails.[40] The EU Space Act would therefore supersede any national cybersecurity provisions adopted under NIS2 that are inconsistent with its requirements.

In view of the research objectives of this contribution, it appears increasingly clear that the first version of the proposed EU Space Act did not provide the comprehensive, coherent cybersecurity framework that the sector requires. The reason for this is straightforward. The Union already possesses a cybersecurity framework that applies, at least in part, to the space sector. This existing framework, however, did not align seamlessly with the initial legislative proposal. Instead of promoting coherence, the proposal risked introducing additional fragmentation. This concern was widely echoed by stakeholders such as U.S. Department of State[41], CSSMA[42], EARSC[43], Iridium[44] and AIPAS[45], all of which warned against overlapping competences and regulatory inconsistency.

It is essential to recall that the NIS2 Directive, which constitutes the general regulatory framework for cybersecurity within the internal market, has already been transposed into the national law of most Member States.[46] NIS2 expressly identifies

---

[34] Draft Regulation on the safety, resilience and sustainability of space activities in the Union (EU Space Act) (30 March 2026), Art. 7-8.
[35] Draft EU Space Act, Arts.75, 75a, 93. *See also,* Corinna Visser, 'Space Act: ESA Warns against Duplicate Structures' (*Table.Briefings*, 7 November 2025) <https://table.media/en/europe/news/space-act-esa-warns-against-duplicate-structures> accessed 11 August 2026.
[36] Draft EU Space Act, Arts. 75a(3).
[37] Draft EU Space Act, Arts. 75a(4)-(5).
[38] Draft EU Space Act, Arts. 93.
[39] Para. 20, Nacionālās kiberdrošības likums (2024) <https://likumi.lv/ta/id/353390-nacionalas-kiberdrosibas-likums>
[40] *Primacy of EU Law (Precedence, Supremacy) - EUR-Lex*, https://eur-lex.europa.eu/EN/legal-content/glossary/primacy-of-eu-law-precedence-supremacy.html (last visited Sept. 26, 2025).
[41] 'Feedback from: U.S. Department of State' (*European Commission - Have your say*) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13971-EU-Space-Act-new-rules-for-safe-resilient-and-sustainable-space-activities/F33113182_en> accessed 17 December 2025.
[42] 'Feedback from: Commercial Smallsat Spectrum Management Association (CSSMA)' (*European Commission - Have your say*) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13971-EU-Space-Act-new-rules-for-safe-resilient-and-sustainable-space-activities/F33114180_en> accessed 17 December 2025.
[43] 'European Association of Remote Sensing Companies (EARSC)' (*European Commission - Have your say*) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13971-EU-Space-Act-new-rules-for-safe-resilient-and-sustainable-space-activities/F33113682_en> accessed 17 December 2025.
[44] 'Feedback from: Iridium Communications Inc.' (*European Commission - Have your say*) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13971-EU-Space-Act-new-rules-for-safe-resilient-and-sustainable-space-activities/F33106604_en> accessed 17 December 2025.
[45] 'Feedback from: AIPAS - Associazione Delle Imprese Per Le Attività Spaziali' (*European Commission - Have your say*) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13971-EU-Space-Act-new-rules-for-safe-resilient-and-sustainable-space-activities/F33114221_en> accessed 17 December 2025.
[46] 18 Member States, 'NIS2 Directive Transposition Tracker' (*ECSO*) <https://ecs-org.eu/activities/nis2-directive-transposition-tracker/> accessed 17 December 2025.

the relevance of the space sector, particularly ground based infrastructure such as ground stations.[47] Nevertheless, as is characteristic of directives, Member States retained discretion to broaden its scope.

This expansion generates tension with the EU Space Act, which, as clarified in its initial provisions, was intended to operate as *lex specialis* vis a vis the broader cybersecurity acquis. Although *lex specialis* ordinarily prevails, established case law of the Court of Justice requires national legislation to be interpreted in conformity with Union law. In practice, this means that national provisions exceeding the scope of the EU Space Act could become redundant. While this issue requires clarification, it is ultimately secondary to a more fundamental structural problem.

A more significant difficulty lies in the lack of alignment between the EU Space Act and the existing cybersecurity framework. This issue was raised repeatedly during the public consultation.[48] Stakeholders supported the development of cybersecurity rules tailored to space assets but emphasized the necessity of full consistency with the existing acquis. The consistency, especially in the first published version of the proposal, was, however, lacking.

The starting point for assessing the Union's space cybersecurity acquis is the NIS2 Directive, which addresses network and information security across the internal market and constitutes, at present, the principal, if partial, framework applicable to the sector. NIS2 identifies sectors of high criticality and subjects entities operating within them to a regulatory model that increases legal exposure according to the system operated, chiefly through risk-management and reporting obligations resembling a form of operator liability. Space is designated as a sector of high criticality, but the Directive confines this narrowly, to "operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks." This formulation privileges the ground segment as the critical interface through which space services reach the internal market, leaving spacecraft, Earth observation and space situational awareness satellites, micro-operators, third-country launch services, and Union-owned constellations outside its scope entirely. As a directive, NIS2 further affords Member States discretion in transposition, a discretion that could, in principle, extend national obligations to assets in orbit; in practice, however, only thirteen Member States currently possess a national space policy, and only Latvia has used this discretion to broaden its transposing legislation. NIS2 additionally excludes, under Article 2, entities whose activities are predominantly national security, defence, public security, or law enforcement related, a carve-out of particular significance in space, where dual-use civil-military assets are the norm and the Directive offers no clear criterion for distinguishing covered from exempt activity.

The Cyber Resilience Act, Regulation (EU) 2024/2847, approaches the problem from a different vantage point: rather than regulating operators, it imposes product-level cybersecurity obligations on manufacturers of hardware and software "with digital elements" placed on the Union market wherever the product's intended use entails a logical or physical connection to a device or network. This horizontal scope is broad enough to capture satellite ground equipment, such as modems, routers, and gateway terminals, by default. The Regulation classifies products into a tiered structure of risk: the default category, comprising the majority of covered products, is subject to self-assessment against the essential requirements in Annex I, while products designated "important" or "critical" under Annexes III and IV require third-party conformity assessment or mandatory certification respectively. Vulnerability and incident reporting obligations enter into force on 11 September 2026, with the remaining requirements, conformity assessment, and CE-marking obligations fully applicable from 11 December 2027, a timeline that will substantially precede the Space Act's anticipated entry into force. Article 2 CRA nonetheless permits the Commission to limit or exclude, by delegated act, products already covered by sector-specific Union rules achieving equivalent protection. Whether this mechanism will be used to exclude spacecraft or satellite components once the Space Act's resilience pillar applies remains, at the time of writing, unresolved, leaving open which instrument a given piece of space hardware is actually required to satisfy.

The Commission's January 2026 proposal to revise the Cybersecurity Act, Regulation (EU) 2019/881, expands ENISA's mandate in preparing certification schemes, extending certification beyond discrete ICT products, services, and processes to an organisation's broader "cybersecurity posture." Certification remains, and would remain, voluntary, with each scheme specifying an assurance level, basic, substantial, or high, calibrated to risk. To date, only the EUCC scheme, covering ICT products and modelled on the Common Criteria framework, has been formally adopted; a cloud-services scheme, EUCS, remains under development, alongside nascent schemes for 5G and managed security services. None of the schemes adopted or under active development is specific to space products, and the revised proposal does not introduce one. Satellite manufacturers seeking certification would, accordingly, have to fit within generic ICT schemes not designed with

[47] 'NIS2 and Earth Stations - 10 Statements' (*SpaceFinland*) <https://spacefinland.fi/en/-/nis2-and-earth-stations-10-statements> accessed 17 December 2025.

[48] 'Feedback from: U.S. Department of State' (n 41).

orbital dynamics, link-segment bandwidth constraints, or hardware immutability in mind. The revised Cybersecurity Act's engagement with the space sector is thus better described as latent than active.

The proposed Digital Networks Act, adopted by the Commission on 21 January 2026, is the instrument most directly concerned with regulating satellite connectivity itself, intended, together with the accompanying cybersecurity package, to repeal and replace substantial portions of the existing telecommunications acquis, including significant elements of the European Electronic Communications Code. It would replace the current patchwork of national telecoms authorisations with a single, EU-level authorisation for satellite communications networks and services, coupled with a harmonised mechanism for spectrum access informed by a new European Table of Allocation of Satellite Frequencies. Access to spectrum is expressly conditional on compliance with cybersecurity requirements, including the ICT supply-chain security obligations under the revised Cybersecurity Act, linking market access directly to cybersecurity compliance in a manner the Space Act does not replicate. The proposal further introduces a Union Preparedness Plan for Digital Infrastructures, extending the resilience framework explicitly to non-terrestrial networks and recognising satellite connectivity as a resilience layer for terrestrial infrastructure. The DNA's contribution to space cybersecurity governance is thus genuine but circumscribed: it governs market access and spectrum for the link connecting ground and space segments, not the cybersecurity of the spacecraft or ground segment as such.

The proposed EU Space Act, published in June 2025 and substantially revised since, is the first Union instrument to name space cybersecurity directly rather than by implication. It regulates market access to the internal market rather than space activity as such, conditioning access on an EUSA certification, issued by a qualified technical body, for both launch vehicles and spacecraft. Because it regulates access to the market itself, its scope, unlike NIS2's, extends to third-country operators, a design choice that follows directly from its market-access rather than operator-liability orientation. Among its several pillars, resilience is the one predominantly concerned with cybersecurity: regulated entities must take "appropriate technical, operational and organisational measures to manage the risks posed to the security of network and information systems," operationalised through a risk-mitigation process built on an "all hazards" approach, its substantive content to be further elaborated by a Commission implementing act. The draft further imposes a dedicated incident-reporting obligation, discharged not to the national authorities designated under NIS2 but to newly established National Space Bodies, a parallel channel that stakeholders including the U.S. Department of State, CSSMA, EARSC, Iridium, and AIPAS flagged during the public consultation as a source of inconsistency with the existing acquis. The Act's relationship to NIS2 has evolved materially: whereas the original proposal positioned it as lex specialis, the December 2025 text, at Article 75 and revised recital 72, instead requires the two regimes to be synchronised such that obligations remain identical across relevant entity categories, a shift from hierarchy to coordination.

Read together, these five instruments overlap substantially in coverage without corresponding alignment in scope or mechanism, a pattern that is structural rather than incidental. NIS2 and the CER Directive secure the ground segment but, by design, exclude spacecraft, EO/SSA satellites, micro-operators, and Union-owned constellations, precisely the gap the Space Act was conceived to close. Yet it remains unclear which measures an entity within scope of both regimes must actually apply, NIS2's Article 21 obligations or the Space Act's resilience chapter, since the synchronisation clause resolves the question of hierarchy without resolving which body of requirements governs day-to-day compliance. The CRA adds a parallel, product-based layer whose boundary with the Space Act's resilience pillar depends on a Commission exclusion decision not yet taken. The revised Cybersecurity Act's certification track and the DNA's spectrum-conditioned resilience requirements each touch space infrastructure without squarely regulating it. Entity thresholds compound this fragmentation: none of the five instruments defines "space operator" consistently, so a given actor's obligations depend on which instrument's threshold, sectoral classification, or market-access gate happens to capture it. National-security-sensitive assets sit precariously within this landscape, since NIS2's defence and public-security carve-out has no clear counterpart in the Space Act, leaving dual-use satellites potentially regulated by neither regime, or by both, depending on how individual Member States exercise their retained discretion. It is this structural fragmentation, rather than any single instrument's deficiency, that constitutes the principal obstacle to a coherent Union framework for space cybersecurity.

5. The US Regulatory Landscape

The first substantive U.S. policy response to space cybersecurity is Space Policy Directive-5 (SPD-5), Cybersecurity Principles for Space Systems, issued in September 2020. SPD-5 states that *"it is the policy of the United States that executive departments and agencies . . . will foster practices within Government space operations and across the commercial space industry that protect space assets and their supporting infrastructure from cyber threats and ensure continuity of operations."* Rather than imposing binding obligations, SPD-5 sets out principles agencies should pursue *"through rules, regulations, and guidance . . . and adoption, where*

appropriate, of cybersecurity best practices and norms of behavior."[49] As a presidential policy directive rather than legislation or regulation, SPD-5 carries no independent legal force; it operates aspirationally, directing agencies to translate its principles into binding requirements only where they choose to exercise existing statutory authority, such as FCC licensing or DoD procurement, discussed below. Five years on, SPD-5 remains the only cross-agency articulation of U.S. space cybersecurity policy, a striking contrast to the EU's growing body of hard-law instruments.

NIST has translated SPD-5's principles into technical guidance rather than binding standards, consistent with the voluntary-adoption model that characterises most NIST output. NIST Interagency Report (IR) 8270, Introduction to Cybersecurity for Commercial Satellite Operations[50], applies the NIST Cybersecurity Framework to commercial satellite operators not owned, operated, controlled, or leased by the federal government, offering an example set of desired security outcomes and suggested controls rather than mandatory requirements. NIST IR 8323 rev.1[51] extends this work with a Foundational Profile for the user segment of the space ecosystem. Neither document constitutes a standard in the formal sense; adoption is voluntary unless incorporated by reference into a contract or licence condition, at which point the underlying guidance acquires binding force indirectly, through the mechanisms discussed below, rather than through NIST's own authority.

Industry standards bodies have moved somewhat further toward space-specific technical detail. IEEE 3536-2026, Standard for Space System Cybersecurity Design[52], sets out cybersecurity design requirements aimed specifically at satellite and ground segment architectures, complementing the more general-purpose ISO/IEC 27001 and NIST Risk Management Framework that space operators have historically had to adapt themselves. As with NIST guidance, IEEE standards remain voluntary in themselves; their normative force in practice depends on incorporation into procurement contracts or licence conditions.

Where binding obligations do exist, they arise not from a general space-cybersecurity statute but from sector-specific licensing and procurement authority. The FCC's satellite licensing rules, most recently overhauled in a rulemaking effective February 2026, now require applicants to certify that they have created, and will implement and update, a cybersecurity and physical-security risk management plan; the same rulemaking bars licences to entities identified on the Commission's national-security "Covered List" or otherwise subject to control by a foreign adversary. Congress has moved further still with the proposed Satellite Cybersecurity Act[53], which would establish a dedicated cybersecurity clearinghouse for the commercial satellite sector,[54] a step toward the kind of cross-sectoral obligation the EU has already adopted through NIS2. On the government-satellite side, the Department of Defense layers additional, more prescriptive requirements onto its own supply chain: the Space Force's Infrastructure Asset Pre-Approval (IA-Pre) programme requires commercial satcom operators seeking to sell bandwidth to the military to comply with a defined subset of NIST controls, verified by third-party audit, while the Committee on National Security Systems' CNSSP-12 sets baseline requirements for national security space systems specifically.[55] Both overlays reach only the slice of commercial activity that intersects with government contracts or licensed spectrum use; a commercial operator with no FCC licence and no government customer faces no binding federal cybersecurity requirement at all, civilian or otherwise.[56]

Taken together, the U.S. landscape inverts the EU's structure rather than mirroring its gaps. Where the EU has produced multiple binding instruments whose coverage is fragmented and overlapping, the U.S. has produced a single coherent policy statement, SPD-5, whose implementation is almost entirely voluntary, becoming binding only where it is pulled into licensing or procurement relationships that were not designed with space cybersecurity specifically in mind. The result is a coverage gap that is functionally comparable to the EU's: an operator with no FCC licence, no DoD contract, and no

---

[49] 'Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems – The White House' <https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/> accessed 17 August 2026.

[50] Matthew Scholl and Theresa Suloway, 'Introduction to Cybersecurity for Commercial Satellite Operations' (National Institute of Standards and Technology 2023) NIST Internal or Interagency Report (NISTIR) 8270 <https://doi.org/10.6028/NIST.IR.8270> accessed 17 August 2026.

[51] Michael Bartock and others, 'Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services' (National Institute of Standards and Technology 2023) NIST Internal or Interagency Report (NISTIR) 8323 Rev. 1 <https://doi.org/10.6028/NIST.IR.8323r1> accessed 17 August 2026.

[52] 'IEEE SA - Standards Store | IEEE 3536-2026' <https://store.accuristech.com/standards/ieee-3536-2026?vendor_id=11916&product_id=3031956> accessed 17 August 2026.

[53] Gary C [D-MI Sen. Peters, 'Text - S.3404 - 119th Congress (2025-2026): Satellite Cybersecurity Act of 2025' (14 April 2026) <https://www.congress.gov/bill/119th-congress/senate-bill/3404/text> accessed 17 August 2026.

[54] 'Senate Commerce Advances Satellite Cybersecurity Act and Secure Space Act' <https://communicationsdaily.com/news/2026/04/15/Senate-Commerce-Advances-Satellite-Cybersecurity-Act-and-Secure-Space-Act-2604140068> accessed 17 August 2026.

[55] Philip Harlow, 'Resolving the Disconnect between Industry and the DOD's Space Strategy' (*C4ISRNet*, 19 April 2024) <https://www.c4isrnet.com/battlefield-tech/2024/04/19/resolving-the-disconnect-between-industry-and-the-dods-space-strategy/> accessed 17 August 2026.

[56] Amy McCullough, 'Space Force Finally Rolls Out Cyber Standards for Commercial SATCOM Providers' (*Air & Space Forces Magazine*, 31 May 2022) <https://www.airandspaceforces.com/space-force-finally-rolls-out-cyber-standards-for-commercial-satcom-providers/> accessed 17 August 2026.

state-level oversight is regulated by neither regime. But the underlying cause is the opposite of the EU's, not competing hard-law instruments producing overlap, but the absence of any general-purpose one producing a residual space that no voluntary standard, however well designed, can fill on its own.

6. Comparative Mapping, Discussion, and Scope

6.1 Comparative Mapping: Nine Components of Space Infrastructure

This section operationalises the ground, space, and link segmentation introduced in Section 2 into the nine components used to map cyber exposure against regulatory coverage in the European Union and the United States: ground stations, CubeSats in LEO, government satellites in MEO/GEO, commercial satellites in LEO, LEO megaconstellations, "smart" satellite components, government-owned ground stations, launch facilities, and satellite communications links. Exposure is coded qualitatively as low, medium, or high, based on network-facing attack surface, dependence on legacy or commercial off-the-shelf components with weak security-by-design, and the systemic consequences of compromise, cascading failure, supply-chain propagation, or state-level targeting. Regulatory coverage is coded as full, partial, indirect, or absent for each jurisdiction, depending on whether a binding instrument names the component explicitly, captures it incidentally through a broader category, or excludes it altogether.

Ground stations present a paradox borne out in the interview data: seven respondents identified the ground segment as the weakest link in space cybersecurity, network-facing, often built on legacy IT/OT, and the most straightforward entry point for an attacker, yet it is also the component with the most developed regulatory coverage on both sides of the Atlantic. In the EU, ground stations are the only space-related component NIS2 names explicitly, as high-criticality operators of ground-based infrastructure; in the US, coverage remains indirect, resting on voluntary NIST frameworks rather than a binding mandate. Respondents attributed the EU's comparative maturity here to the fact that ground-segment cybersecurity requirements closely resemble terrestrial IT/OT obligations, making the component more approachable for regulators than the orbital or launch segments discussed below.

CubeSats in LEO combine medium-high exposure, arising from minimal security-by-design and a base of academic and early-stage commercial operators with limited compliance capacity, with almost no regulatory coverage in either jurisdiction. Neither NIS2 nor SPD-5 was drafted with a low-cost, short-lifespan satellite class in mind: NIS2's entity thresholds and SPD-5's aspirational, non-binding character both effectively exclude this population by default. The EU Space Act may eventually capture CubeSats through its EUSA certification requirement, but even the current draft leaves open whether smaller missions will qualify for a lighter-touch tier or fall out of scope on cost grounds.

Government satellites in MEO and GEO present the inverse profile: high exposure as state-level, high-value targets, but comparatively well-addressed coverage, precisely because their governmental ownership routes them into defence and national-security frameworks operating outside the general civilian regimes mapped in Sections 4 and 5. In the EU, this occurs through NIS2's carve-out for entities engaged predominantly in national security or defence, which removes these assets from the Directive rather than subjecting them to it. In the US, DoD- and IC-specific frameworks apply outside NIST's civilian scope, addressing the same population through a parallel, classified or semi-classified track.

Commercial satellites in LEO are high exposure by virtue of their dual-use character and rapidly growing numbers, and partially covered in both jurisdictions, though by different mechanisms. In the EU, coverage turns on unresolved scope questions under NIS2 and on the Cyber Resilience Act's product-level reach into onboard hardware and software. In the US, coverage rests on voluntary adoption of NIST SP 800-53 controls and on FCC licensing conditions that, as of the February 2026 rulemaking, are only beginning to attach cybersecurity certification requirements to commercial licences.

LEO megaconstellations raise exposure to a systemic level: compromise of a shared ground architecture, common software baseline, or supply-chain component can propagate across hundreds or thousands of satellites simultaneously, a risk qualitatively different from the compromise of a single asset. Regulatory coverage has not caught up. The EU Space Act proposal is the first instrument to engage with constellation-scale risk explicitly, but its treatment remains unsettled pending the implementing act referenced in Section 4. In the US, SPD-5's principles are broad enough to be read as applicable, but no binding rule addresses megaconstellations as a distinct category.

"Smart" satellite components, including autonomous refuelling systems and onboard control software, represent a novel attack surface created by increasing on-orbit autonomy. Neither jurisdiction addresses this component specifically. In the EU, the Cyber Resilience Act may apply to embedded software with digital elements, but whether it does so depends on an exclusion decision the Commission has not yet taken. In the US, IEEE 3536-2026 and NIST guidance are available but

voluntary, leaving the most autonomous, and arguably highest-consequence, components of modern spacecraft governed by no binding rule in either jurisdiction.

Government-owned ground stations are high exposure, critical infrastructure nodes at the interface between orbital assets and terrestrial command authority, yet, like their government-satellite counterparts, are substantially exempted from the general regimes mapped above. National-security exemptions largely remove them from NIS2's scope in the EU; in the US, federal systems are instead governed under FISMA and associated NIST controls, a track running parallel to, and separate from, the commercial rules discussed elsewhere in this section.

Launch facilities produced the sharpest disagreement in the interview data. A majority of respondents identified launch facilities as under-regulated relative to their exposure, but the underlying reasoning split: some respondents argued there was little to protect, on the view that a facility has "nothing to hack" in the same sense as a networked satellite, while others argued the opposite, that space assets are physically present and integrated at launch facilities immediately before flight, creating a discrete window in which malware could be injected into onboard systems before they ever reach orbit. Neither the EU nor the US space-cyber instruments address launch facilities specifically; in the US, FAA oversight remains focused on flight safety, with cybersecurity a secondary concern at best.

Satellite communications links were the component identified most consistently across the interview sample: respondents agreed, irrespective of country of origin, that the uplink/downlink link remains one of the most vulnerable segments of the sector, a perception the KA-SAT incident discussed in Section 2 substantiates directly. Regulatory coverage, however, remains only glancing. In the EU, the link is touched indirectly through NIS2's coverage of telecoms providers, and more directly, though still prospectively, by the Digital Networks Act's spectrum-conditioned resilience requirements. In the US, the FCC has clear licensing authority over the link but has only recently begun attaching a cybersecurity mandate to it.

Component	Cyber exposure (illustrative)	EU coverage	US coverage
Ground stations (private/commercial)	High — network-facing, often legacy IT/OT	Indirect (NIS2 if 'essential/important entity'; CRA for products)	Indirect (NIST voluntary frameworks; sector-specific gaps)
CubeSats in LEO	Medium-high — low security-by-design, academic/startup operators	Largely unaddressed (below thresholds; EU Space Act may capture)	Largely unaddressed (SPD-5 aspirational, non-binding)
Government satellites (MEO/GEO)	High-value target; state-level threat actors	Member State competence; NIS2 carve-outs for defence/national security	Addressed via DoD/IC-specific frameworks, outside NIST civilian scope
Commercial satellites in LEO	High — dual-use, growing market	Partial (NIS2 scope ambiguity; CRA for onboard software/hardware)	Partial (NIST SP 800-53 adoption voluntary; FCC licensing conditions emerging)
LEO megaconstellations	Systemic — cascading/supply-chain risk	Emerging focus of EU Space Act proposal; not yet settled	SPD-5 principles referenced; no binding constellation-level rule
"Smart" satellite components (refuelling, control software)	High — novel attack surface, autonomy	Not specifically addressed; CRA may apply to embedded software	Not specifically addressed; NIST/IEEE standards voluntary
Government-owned ground stations	High — critical infrastructure node	National security exemptions largely remove from NIS2 scope	Federal systems under FISMA/NIST, separate track from commercial rules
Launch facilities	Medium — physical/cyber-physical convergence	Not specifically addressed in space-cyber instruments	Not specifically addressed; FAA safety focus, cybersecurity secondary

Satellite communications (uplink/downlink)	High — demonstrated in Viasat 2022	Touched by EECC/NIS2 for telecom; DNA proposal relevant	FCC authority exists but cybersecurity mandate limited

Read across all nine components, currently covered are mostly government or military actors, and, on the private side, ground segment operators, a pattern holding on both sides of the Atlantic even though the underlying mechanism differs sharply, mandatory NIS2 obligations in the EU against a largely voluntary compliance model in the US. The starkest gaps are three. CubeSats and other small-satellite missions fall below the entity thresholds or aspirational language of every instrument examined, regardless of the medium-high exposure their weak security-by-design creates. Launch facilities and "smart" on-orbit components are absent from the space-cyber acquis on both sides of the Atlantic, not merely under-covered but effectively unaddressed. And satellite communications links, the component practitioners across jurisdictions rank among the most vulnerable, remain governed only incidentally, through telecoms or spectrum instruments not designed with cybersecurity as a primary objective.

6.2 Discussion: Who Is In, Who Is Out

The comparative mapping above reveals two recurring patterns that cut across all nine components rather than being specific to any one of them.

The first is a small/new-entrant gap. CubeSats, smart on-orbit components, and, to a lesser extent, launch facilities share a structural feature: none was designed into the regulatory instruments examined in Sections 4 and 5, whose entity thresholds and criticality designations were built around large, established operators. This is not confined to a single jurisdiction or regulatory philosophy; NIS2's essential/important entity thresholds and SPD-5's aspirational language achieve functionally the same exclusion by different routes, hard thresholds in one case, the absence of any binding mechanism in the other.

The second is a national-security carve-out gap. Government satellites and government-owned ground stations are high-exposure, high-value components that both jurisdictions remove from their general civilian regimes rather than regulate directly. In the EU this occurs through NIS2's Article 2 exemption; in the US it occurs through the DoD/IC track running parallel to, and separate from, NIST's civilian guidance. The effect in both cases is the same: the most attractive state-level targets are governed by classified or semi-classified mechanisms invisible to this paper's doctrinal review, a limitation acknowledged in Section 3.

These two gaps sit atop a deeper structural contrast between the two jurisdictions' regulatory philosophies. The EU's approach is binding but fragmented: NIS2, the CRA, the revised Cybersecurity Act, the DNA, and the Space Act each impose enforceable obligations, but, as Section 4's synthesis showed, rarely on the same entities, through the same mechanism, or against the same threshold. The US approach is the mirror image, voluntary but coherent: SPD-5 articulates a single set of principles, but almost nothing under it is enforceable absent a licensing or procurement relationship that pulls the guidance into binding form. The practical consequence is a trade-off between enforceability and adaptability. The EU's binding instruments are enforceable against the entities they cover, but slow to update and, as the Space Act's drafting history illustrates, prone to internal inconsistency as new instruments are layered onto old ones. The US's voluntary framework adapts quickly, NIST guidance and IEEE standards can be revised without legislative process, but has no mechanism to compel adoption by an operator with no government contract or FCC licence.

The mapping also speaks to a more conceptual question: whether space cybersecurity is better organised around the ground/space/link segmentation introduced in Section 2, or around a risk-based or functional logic that groups components by exposure and consequence rather than physical location. The evidence favours the latter. Segment location alone does not predict regulatory coverage: government-owned and commercial ground stations sit in the same segment but are regulated through entirely different mechanisms, while CubeSats and megaconstellations, both space-segment assets, diverge sharply in the systemic risk they present. The interview data suggest instead that exposure clusters along functional lines: components whose risk profile resembles terrestrial IT/OT, ground stations chief among them, attract regulation more readily than components, such as launch facilities or smart on-orbit systems, whose risk profile has no close terrestrial analogue and is, accordingly, harder for regulators to conceptualise using existing tools. Practitioners captured this dynamic directly: the seven respondents who named the ground segment the weakest link nonetheless agreed it was the most regulated, attributing this to the familiarity of ground-segment risk to regulators versed in conventional network security, while launch facilities produced open disagreement among respondents as to whether there was anything

to regulate at all, with some maintaining there was "nothing to hack" and others pointing to the physical proximity of assets and ground equipment during integration as a distinct, and currently unaddressed, injection risk.

6.3 Towards a Coherent Scope: Who Should Be Regulated?

If segment location is a poor predictor of regulatory need, as the discussion above suggests, then scope should be defined functionally rather than structurally. Four criteria, drawn from the patterns identified above, offer a starting point. Criticality of function asks whether a component's compromise disrupts a service society has come to depend on, per the dependencies traced in Section 2, rather than whether the component itself is large or well-resourced. Systemic or cascading risk asks whether compromise of one instance propagates to others, the criterion that most clearly distinguishes megaconstellations from a single CubeSat even though both currently fall outside binding coverage. Dual-use status asks whether an asset serves both civilian and military or state functions, since it is precisely this status that presently removes government satellites and ground stations from general regimes on both sides of the Atlantic, arguably the wrong result given that dual-use assets are, on the interview evidence, among the most attractive targets rather than the least. Market maturity and entrant size asks whether an operator has the compliance capacity entity-threshold models like NIS2 implicitly assume, the criterion whose absence currently excludes CubeSat and early-stage commercial operators regardless of exposure.

Applied to the three gaps identified above, this framework would change coverage materially. CubeSats would be captured not by an entity-size threshold, which currently excludes them, but by a function-and-risk test applied irrespective of operator size, addressing the small/new-entrant gap directly while avoiding a compliance burden calibrated to large operators. Smart on-orbit components would be captured through the criticality and cascading-risk criteria even absent a dedicated instrument, closing the gap between the pace of on-orbit autonomy and the pace of the CRA's or NIST's engagement with it. Government and dual-use assets would remain distinct from purely civilian ones but would no longer be exempted wholesale; a dual-use test could instead calibrate obligations to an asset's actual function rather than its ownership, narrowing, without eliminating, the national-security carve-out gap.

NIS2's essential/important entity tiering offers a template worth adapting rather than replicating. Its core insight, that obligations should scale with the consequence of compromise rather than apply uniformly, is sound, but its reliance on sector and size thresholds is precisely what produces the CubeSat and launch-facility gaps mapped above. A function-based tiering, keyed to the four criteria above rather than to entity size or sector label, would preserve the proportionality NIS2 aims for while closing the gaps its current thresholds create.

Institutional feasibility differs sharply across the Atlantic. In the EU, the appetite for further legislative layering is questionable given the fragmentation Section 4 already documents; the more realistic path is convergence, using the Space Act's implementing acts and the NIS2 synchronisation clause to embed functional criteria into instruments that already exist, rather than legislating a new one. In the US, the constraint is less legislative appetite than agency capacity and the voluntary character of the underlying model; converting SPD-5's principles into enforceable obligations would require Congress to act, as the pending Satellite Cybersecurity Act attempts to do for one component, rather than NIST or the FCC alone. In both jurisdictions, industry burden is likely to be the binding practical constraint on any reform, particularly for the small operators a function-based scope is designed to bring in from outside current thresholds

7. Conclusion

This paper set out to answer a question the existing literature has largely assumed rather than examined: who is currently regulated within space cybersecurity frameworks, and who should be? The comparative mapping in Section 6 shows the EU's binding-but-fragmented approach and the US's voluntary-but-coherent approach converge on strikingly similar gaps by opposite routes. Small and new-entrant operators, CubeSats chief among them, fall outside every instrument examined regardless of exposure, while the most attractive state-level targets, government satellites and government-owned ground stations, are removed from general civilian regimes through national-security carve-outs in both jurisdictions. The ground segment illustrates the inverse problem: the most heavily regulated component in both jurisdictions, yet the one practitioners most consistently rank the weakest link, regulated readily precisely because its risk resembles terrestrial IT/OT that regulators already know how to address.

The paper's central contribution is the four-criteria framework proposed in Section 6.3, criticality of function, systemic or cascading risk, dual-use status, and market maturity, offered as a functional alternative to the segment-based and entity-threshold models currently in use, and as a template for closing the gaps identified above.

Two limitations qualify these findings. The EU Space Act and Digital Networks Act remained draft instruments at the time of writing, so their treatment here is necessarily provisional. The interview sample, while within recognised thresholds for qualitative legal research, remains modest relative to the full stakeholder population, and its findings should be read as indicative of practitioner perception rather than statistically representative. Future research should track the finalised EU instruments against the framework proposed here and extend the comparative method to a third jurisdiction not systematically mapped in this paper. Nevertheless, even with these limitations, we should not stop asking: who is in, who is out, and who should be in?