Coexisting in Low-Earth Orbit: Large Constellations and Cybersecurity Governance

P. J. Blount* & Laetitia Cesari Zarkan**

Large constellations present unique challenges to space operators in a variety of ways, but due to the increasing interconnection between the satellites within these architectures, cybersecurity is a critical concern. The potential for a massive shutdown of such a system through a network attack could have long-term consequences for the space environment. This article describes the role that legal structures play in managing such risks and asserts that more robust governance should be pursued to mitigate the potential for a catastrophic attack.

Keywords: constellations, telecommunications, cyberspace, satellites, sustainability, space, safety, security, orbit, orbital, responsibility, communications, international law, standards

1 INTRODUCTION

In an interconnected world, it can be easy to only consider the advantages provided by software-driven applications. Not only does the operational capability of satellite systems rely on computers, but space data processing and distribution also depend on cyberspace. Both payload and bus command and control operations are composed of interconnected components. The use of computers and software for space activities makes them fast, efficient and more reliable. Yet, this reliance on information technology networks and systems presents a risk, at each stage of a space operation: a breach could spread within the systems and prevent or disrupt the functioning of space-based assets constituting a constellation.

The cybersecurity of space systems can only be envisaged with clear safety requirements, serving as minimum standards of behaviour for all present stakeholders and access to all future players. The space infrastructure is composed of interconnected elements composing the space segment, the ground segment and the user segment. Most of the elements of this infrastructure are software driven. First, space-based assets need access to specific instructions to be controlled and checked remotely and payloads and spacecraft subsystems collect, process, store and

* (Dr) Lecturer in Law in the School of Law and Politics at Cardiff University. Email: blountpj@cardiff.ac.uk.
** Doctoral researcher at Luxembourg University and a researcher at UNIDIR. Email: laetitia.zarkan@uni.lu.

Blount, P. J. & Cesari Zarkan, Laetitia. 'Coexisting in Low-Earth Orbit: Large Constellations and Cybersecurity Governance'. *Air & Space Law* 48, Special Issue (2023): 1–30.

transmit data that go through cyberspace, using signal transmission. Second, the ground segment is a network of centres, antennas and facilities that rely on computing systems to gather information on space-based assets and coordinate operations from all over the world, based on the reception, processing and implementation of commands and data transmitted from and to the ground. Third, the user segment is managed through the distribution of processed space-related data and relies on software-enabled space applications.

As such, a dedicated regulatory framework applying to the protection of cyberspace, whether voluntary or binding, must be flexible and precise enough to ensure efficient protection of space systems against failure risks and disruption threats. The nature of space activities is rapidly changing and adapting to technological transformations that are resulting from the rise of information technologies. These changes affect both the operations of space systems as well as the services they provide. This can clearly be seen in the context of very large constellations. Such infrastructure is enabled by standardization and digital communications and is designed to disseminate information to users worldwide. Operators are to be believed these constellations present opportunities to advance society through the goods of connection and data as well as opportunities to reap great profits.

Regardless of whether these promises will come to fruition, these systems are indeed being deployed. The architecture of these systems creates unique challenges at both the technical and governance levels. It is important to note that it is specifically the architecture of these systems that drive these challenges. This article seeks to engage with how these architectures create challenges specifically in the realm of cybersecurity. As the future of space applications seems to lie – at least in part – on large constellations of interconnected assets, a massive shutdown is particularly concerning for the sustainability of the low-Earth orbit (LEO).

As described in this article, while legal provisions exist at some national and regional levels, there is currently no harmonization of rules applicable to cybersecurity and even less applicable to space systems.

A legal enterprise in this respect could not develop in silos: the different actors must all be integrated, from the legislator to the in-house lawyer and the lawyer, including technical experts and operational practitioners, but also the end-users. Without all of these stakeholders, sharing best practices, effective governance measures, and digital hygiene measures is often overlooked.

Nowadays, digital technologies and interconnection between systems and access to the World Wide Web are widespread. Albeit virtual, cyberspace has become a significant part of humanity's everyday life, as critical data and information are stored and transmitted through a complex network of systems, equipment and global communication infrastructure.

Therefore, considering the increasing interconnection between space systems, a cyber shutdown of space systems, and particularly large constellations of satellites, would be extremely disruptive for space sustainability. On the one hand, interruption of services or of the controlling signals would render the satellites useless and subsequently create orbital debris. This space junk will contribute to the high concentration of the orbital shell in LEO and potentially congest it. Consequently, from a technical perspective, the increase of uncontrolled objects will not only disrupt astronomy but also coordination between assets in orbit and future launches that will cross the assets, with high risks of collision. From a legal perspective, this situation could cause life reduction of satellites, with an increased use of propellant for collision avoidance manoeuvre, and higher probability of collision, triggering State liability and insurance issues.

This article will first address the vulnerabilities of large constellations of satellites from a technical perspective. Then, it will consider the legal aspects of the cybersecurity challenges presented by these architectures considering legal structures that seek to prevent breaches and that create consequences for breaches. It will conclude with an analysis that suggests that cybersecurity risks for large constellations must be understood within the larger context of cybersecurity governance and risk management practices.

2 LARGE CONSTELLATIONS

The era of large satellite constellation deployment has already begun. While it corresponds to the growing need for data transfer and interconnection between equipment and applications, it also contributes to an overpopulation of LEO, with increased risks of collision and harmful interference. Building up the safety and security of space systems applies to all segments, whether in outer space or on the ground. This implies protecting the space segment, the ground segment and the user segment from external threats and breaches, for security purposes, and from internal malfunctioning and risks of collisions, with safety measures.[1] This section details the architectures of large constellations that create the potential for adversarial cyber operations that could result in catastrophic damage to the space environment impacting the safety and sustainability of operations. Furthermore, it describes existing multilateral mechanisms for the coordination of orbital slots and radio frequencies and considerations on the registration of this new kind of space infrastructure.

[1] Laetitia Cesari Zarkan, *What's in a Word? Notions of 'Security' and 'Safety' in the Space Context*, UNIDIR (2020), https://unidir.org/commentary/whats-word-notions-security-and-safety-space-context (all websites cited in this article were accessed and verified on 6 Feb. 2023).

Large satellite constellations have the particularity of being composed of a very large number of objects. Therefore, these assets have to be coordinated with each other as well as with other space objects, especially in the context of access to space, with respect to the crossing of lower orbits. Therefore, the coordination and recording procedures in place for space systems and earth stations

A large satellite constellation is a complex system of interconnected assets designed in a similar or complementary manner to operate as a single unit from LEO, composing the space segment.[2] Constellations are space-based infrastructure hosting apps and solutions broadcasted using a user segment. The systems composing this type of space infrastructure are manoeuvred from a ground segment, generally, a satellite operation centre, that enables the Telemetry, Tracking and Command (TT&C).[3] The ground segment consists of stations and antennas located across the world and sending orders from Earth while checking the parameters and good functioning of the assets composing the constellation.[4]

This type of architecture is beneficial to providers aiming to cover customers worldwide by providing services over large geographical areas. However, the number of assets makes it a big concern for space safety and subsequently, the sustainability of LEO. First, each asset has the potential of causing harmful interference with other services. The signals sent to and received by these assets need to constantly be coordinated and controlled in order not to prevent the good functioning of other space objects placed in close vicinity. Second, the presence of thousands of assets implies increasing risks of collisions with other assets launched and crossing this orbit.

In 1959, reacting to the advancement in radio spectrum usage and, particularly, to the need for providing and coordinating frequencies for space communications, the International Telecommunication Union (ITU) incorporated the definition of space service, the Earth-space services and the radio astronomy service into the Radio Regulations and allocated within the Frequency Allocation Table space applications – starting with space research purposes and extending to commercial uses over time.[5] Implemented through a 'first come, first served' procedure, the coordination of the right to use orbital and spectrum resources is based on the assumption that the relevant national administrations acquire this right

AQ1

[2] Jha et al., *Safeguarding the Final Frontier: Analyzing the Legal and Technical Challenges to Mega-constellations*, 9(4) J. Space Safety Eng'g 637 (Dec. 2022).

[3] Madhavendra Richharia & Leslie David Westbrook, *Satellite Systems for Personal Applications: Concepts and Technology* 41 (John Wiley & Sons, Ltd 2010).

[4] *Ibid*.

[5] History of ITU Portal, *Administrative Radio Conference* (Geneva 1959), http://handle.itu.int/11.1004/020.1000/4.85.

through negotiations, based on the orbits needed and the volume of spectrum necessary to national operations.[6]

According to Article 44 of the ITU Convention, orbits are limited natural resources and countries must have equitable access to them.[7] Therefore, protecting access to orbits, whether geosynchronous orbit (GSO) or non-geosynchronous orbit (non-GSO) is critical. The allocation process was organized within three regions, with reserved slots and bandwidth for non-spacefaring nations not to be disadvantaged.[8] This process had to be framed to ensure equitable access to orbital slots for non-spacefaring nations. However, with the fast deployment of constellations, and despite coordination measures, the presence in orbit of thousands of assets, in the same orbital shell, raises concerns for equitable access.

A large constellation is composed of interconnected space objects and subcomponents. Because of the interdependency between the assets, a cybersecurity breach could incapacitate not only one satellite but a part or the entirety of the constellation. As a consequence, because they will fill entire orbital shells in LEO, the assets composing a large satellite constellation will constitute individual assets deployed around the globe.

Considering each asset individually, these systems are constituted of subcomponents essential to the conduct of space operations. These elements rely on software and applications. Therefore, they are vulnerable to cyber failure or hostile cyber operations. The satellites constituting a large constellation are not only interdependent but also similar in their vulnerabilities. On the one hand, they rely on each other to provide a space application, generally the broadcasting of communication services. On the other hand, each asset is produced in series, with the same characteristics, standards and subsequently, potential risks. To estimate the damaging capacity of a cyber hostile activity, it is necessary to first, consider the means and the target of the perpetrating act, and second, the final consequence of this type of disruptive operation.

The main component of an artificial satellite is generally a primary structure called a 'bus', housing sub-components that keep the system functional. These subcomponents generally consist of a power system, a computer executing instructions to ensure the functioning of the satellite and antennas embedded to receive and/or transmit signals to and from ground-based stations.[9] If it is a manoeuvrable satellite – that can be remotely guided – the bus is also composed of a software-

AQ2

[6] *ITU Radio Regulatory Framework for Space Services* 2, https://www.itu.int/en/ITU-R/space/snl/Documents/ITU-Space_reg.pdf.
[7] Article 44 ITU Convention.
[8] Provision No. 5.2 of the ITU Radio Regulations.
[9] Joseph N. Pelton & Scott Madry, *Introduction to the Small Satellite Revolution and Its Many Implications*, in *Handbook of Small Satellites* 9 (Joseph N. Pelton & Scott Madry eds, Springer, Cham 2020).

defined radio used to process the TT&C links that connect the satellite. The decision to move a satellite or change its angle is usually based on information processed by the flight computer that monitors 'vital signs' of the satellite, including its position and stabilization.[10] These subsystems handle the manoeuvre of the satellite to maintain it in its right orbital slot or, in case of an imminent collision with another object, to conduct a collision-avoidance manoeuvre.

Nowadays, large constellations are inherently highly connected and most of the subcomponents onboard satellites are software-driven and reconfigurable.[11] By using a 'computer-based equipment, automated services or communications mechanisms'[12] to disable or disrupt a software-driven component of a system, placed in outer space or located on the ground, a hostile operator can create concrete, tangible consequences. If it is an individual object, the impacts are less problematic than if it is a constellation of thousands of objects orbiting without any means of control in LEO. Cyber disruptions are very threatening in that they can spread from one connected asset to another, using the breaches identified by a hostile operator to overtake a large part or the entirety of a large constellation.

Whether operated as individual objects or not, artificial satellites are always designed as connected assets, relying on ground-based technologies to transmit and/or receive signals. Hence the need for space operators to assess the risks posed to their space systems and set up adequate cyber protection. Besides propagation, operators must beware of delays for geosync, interference activities, and other risks related to the space environment, including collisions. Therefore, the development of national legal mechanisms applying to both public and private operators, enacted by States, is important, especially with regards to registration and monitoring practices.

These concerns raised by the impact of large constellations on the sustainability of space activities resulted in multilateral debates at the Committee on the Peaceful Uses of Outer Space (COPUOS), and the drafting, for submission, of a document containing statistics and information on practices of States relating to the registration of large constellations and megaconstellations,[13] in accordance with the Convention on Registration of Objects Launched into Outer Space or General Assembly resolution 1721 B (XVI).[14] At the multilateral level, States had

[10] Joseph N. Pelton, *Hosted Payload Packages as a Form of Small Satellite System*, in *Handbook of Small Satellites* 379 (Joseph N. Pelton & Scott Madry eds, Springer, Cham 2020).

[11] Joseph N. Pelton & Scott Madry, *Retrofitting and Redesigning of Conventional Launch Systems for Small Satellites*, in *Handbook of Small Satellites* 407 (Joseph N. Pelton & Scott Madry eds, Springer, Cham 2020).

[12] Tari Schreider, *Cybersecurity Law, Standards and Regulations* 18 (2d ed., Brooksfield: Rothstein Associates, Incorporated 2020).

[13] General Assembly resolution A/AC.105/1243, annex I, 2022, para. 14.

[14] Convention on Registration of Objects Launched into Outer Space (the 'Registration Convention'), adopted by the General Assembly in its resolution 3235 (XXIX), opened for signature on 14 Jan. 1975, entered into force on 15 Sep. 1976.

discussions pertaining to the registration of large constellations of satellites to find a common understanding of how to allocate 'jurisdiction and control' over space objects and eventually, personnel, to foster responsibility and transparency when carrying out space operations, in line with the principles contained in the Guidelines on Long-term sustainability of outer space activities.[15] With the new momentum caused by the deployment of large satellite constellations, States are considering adjusting the regime applicable to the registration of space objects in order to ensure better clarity and transparency of current and future space operations. It includes information about constellations and the communication of a clear point of contact for all questions about emergency and collision avoidance. This is particularly true in case of disruption or malfunctioning.[16] The next section will describe the legal aspects arising from the emergence of large constellations of satellites, from different perspectives, including Space Law, Telecommunication Law, and Cybersecurity Law.

3 LEGAL ASPECTS

As detailed in the previous section, the technical architectures that underlie very-large constellations create the potential for adversarial cyber operations that could result in catastrophic damage to the space environment impacting the safety and sustainability of operations. Many of the solutions to this problem will need to emerge from within the technical architects themselves, but law plays a role in incentivizing operators to implement these architectures through traditional carrot and stick mechanisms. This section will evaluate current legal frameworks that serve the particular function of regulating cyberattacks against very-large constellations. Of course, there is no law specific to this particular aspect of space activities. As a result, this section will deal broadly with three areas of law that have impact in this area, namely, Space Law, Telecommunication Law, and Cybersecurity Law. The analysis itself will be two-pronged to address the two primary ways in which the law addresses such attacks. First, this section will discuss law that is intended to prevent these attacks – i.e., preventative law – and second, it will address the law that is applicable in the wake of such an attack – i.e., consequential law. This section will not endeavour to do deep analysis in each of these areas as such legal

[15] Guidelines for the Long-term Sustainability of Outer Space Activities of the Committee on the Peaceful Uses of Outer Space were adopted (A/74/20, para. 163 and Annex II), Jun. 2019.

[16] Committee on the Peaceful Uses of Outer Space Legal Subcommittee Sixty-first session Vienna, Item 6 of the provisional agenda, Status and application of the five United Nations treaties on outer space, Discussion paper by the Chair of the Working Group on the Status and Application of the Five United Nations Treaties on Outer Space on the topic of registration of large constellations and megaconstellations, Paper submitted by the Chair of the Working Group, 30 Mar. 2022, A/AC.105/C.2/2022/CRP.20.

analyses are well-trod areas in the literature. Rather this section will attempt to raise a number of substantive legal areas and their limitations in order to set the stage for the substantive analysis below.

3.1 Preventative legal mechanisms

Within the space domain, accidents and intentional acts can have significant long-term effects for all actors. An example of this can be seen in the recent history of kinetic Anti-satellite weapons (ASAT) tests, some of which have left significant amounts of debris in the orbital environment creating a challenge for a diversity of space actors. To this end, legal frameworks are often designed with the goal of preventing future incidents that can result in interference with operations and damage to the space environment. As will be seen, these legal frameworks are limited in what they are able to accomplish in this regard.

3.1[a] *Preventative Space Law*

The body of international space law does seek to prevent conflict and interference in the space domain as one of its core goals, but it has been vested with limited prescriptive power to accomplish this task and leaves much of the substantive process to the good faith effort of States and their domestic regulations.

In general, the Outer Space Treaty and the subsequent treaties[17] that emerged after the opening of the space age seek to foster a cooperative and communicative international environment in space. To this end, the Outer Space Treaty places significant emphasis on international cooperation[18] and communication among space actors.[19] Article IX is indicative. It emphasizes the notion of international cooperation and seeks to operationalize this notion through the undefined principle of 'due regard'.[20] Due regard seemingly consists of taking note of the activities of other States activities and performing one's own activities in such a way as to not impinge the other's operations and possibly their international rights. In Article IX, States are also given the duty to request 'international consultations' if the State believes that it may cause another State 'harmful interference' or be the victim of such interference. What is notable here is that Article IX, though a critically important part of the Outer Space Treaty, does little more than encourage cooperation and information sharing.

---

17 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (entered into force 10 Oct. 1967) [hereinafter Outer Space Treaty].

18 *Ibid.*, Preamble, Arts I, III, IX, X, & XI.

19 *Ibid.*, Arts I, V, VIII, IX, X, XI, & XII.

20 *Ibid.*, Art. IX.

States 'shall' use due regard, but actual harmful interference is not banned. Instead, the Treaty seeks to encourage States to engage in bilateral communication in hopes of preventing harmful interference. Even the nature of the bilateral talks, the consultations, is undefined leaving States to structure these interactions and in no way the Treaty ensures resolution to disputes. In the context of very-large constellations, this means that the Outer Space Treaty and the connected body of international space law encourage States to communicate their plans to other actors and engage in discussions to facilitate coordination of activities. The core preventative measure then is built on an ad hoc, self-organizing principle, through which States must work together to ensure that their activities do not cause conflict. Unfortunately, while such a system gives some indication of how States might resolve potential conflicts among planned systems, this system does not tell us much about the cybersecurity aspects of these systems. The underlying cybersecurity plans would likely not be considered as a matter of potential interference open for discussion in consultations.

International space law also seeks to ensure that States are accountable for the space activities that occur within their purview. Issues of responsibility and liability will be covered in the next subsection, but here it is important to note a State's Article VI duty to authorize and continually supervise the activities of its non-governmental actors. This duty is most often fulfilled by licensing regimes through which the State creates obligations for its non-governmental space actors and implements oversight conditions. This is clearly applicable to the authorization of very-large constellations. Specific to cybersecurity, while most space laws do not directly address the notion of cybersecurity, it is likely that some administrations are including cybersecurity aspects within the licensing regimes that have been implemented. Private actors that wish to engage in space activities, including very-large constellations, will likely be required to make disclosure about the security stance of that system, and the licensor will need to make a determination as to the adequacy of the cybersecurity plan in light of the operators planned space activities. Cybersecurity plans will be dealt with in more detail below.

3.1[b] *Preventative Telecommunications Law*

Telecommunications law is addressed at the use of the radiofrequency spectrum and the prevention of harmful interference within that spectrum. The underlying premise is that radiofrequency spectrum is a limited resource and that multiple users on the same frequency reduce the utility of the frequency for all users due to interference. Thus, telecommunication law at the international and domestic levels seeks to maintain interference-free use of the radiofrequency spectrum and maximize efficiency and equity in such uses. Telecommunications law is directed at space activities to the

extent that these activities use frequency, and the location in orbital space of these activities is of significance to reducing the likelihood of interference. As such, it is through the mechanisms of telecommunication law that we are often able to gain information about planned satellite systems including very-large constellations.

At the international level, telecommunication is regulated and coordinated through the auspices of the ITU. The ITU has a system for the filing of planned uses of space systems that allows for the pre-coordination of these uses before the system is developed. Though the ITU only serves as a forum through which States can coordinate their activities, these filings in a sense become reservations for future uses that allow for capital expenditures on the development, construction, and deployment of a satellite system. These filings for coordination of frequency usage are made by national telecommunication administrations on behalf of the operators and included information on the frequencies intended to be used as well as the orbital positions of the planned system. As a result, one of the best sources for planned very-large constellations is the ITU. This system is intended to reduce the potential for future harmful interference, but it is important to understand that harmful interference in this context means, explicitly, interference with regard to the radiofrequency spectrum and not other types of potential interference between and among actors. So, while operators do give information about planned orbital locations, the ITU system only protects indirectly against physical interference. Further, though the ITU has begun work on cybersecurity standards,[21] non-interference rules would only reach to addressing electronic attacks such as spoofing or jamming and not reach as far as cyber exploits that involve code injection onto satellites.[22]

Domestic telecommunication law will also impact operators. The authorization or licensing processes within domestic rules may involve review of the cybersecurity protections employed by the operator much in the same way that it is required for authorization of space activities. This will, however, be on a State-by-State basis as to whether such review is required.

3.1[c] *Preventative Cybersecurity Law*

Cybersecurity law is a less cohesive body of law compared to space law and telecommunications law. It is fractured across numerous legal frameworks that

[21] International Telecommunication Union, Telecommunication Standardization Sector of ITU (04/2008) Series X: Data Networks, Open System Communications and Security, Telecommunication security, Overview of cybersecurity, Recommendation ITU-T, X.1205, Series X: Data Networks, Open System Communications and Security.

[22] Simona Spassova, *Disruptions of Satellite Communication: Comparing Cyber Attacks and Harmful Interference for the Purposes of Legal Regulation*, in *Space Law in a Networked World* 131–142 (P. J. Blount & Mahulena Hofmann, Brill, forthcoming 2023).

AQ3

require security for different types of systems and data that impact different operators. There are few laws that impose specific cybersecurity requirements on space actors.[23] Most often, cybersecurity law is part of an organization's internal governance and implicates the legal function of compliance as well as private law ordering with contract partners.

From an organizational perspective, cybersecurity law is about fulfilling obligations the organization owes to keep its data and systems secure. These obligations can be found in laws, regulations, and contracts to which the organization is subject. At its core, cybersecurity is a risk management process through which an organization assesses its risks and takes steps to adequately mitigate those risks to acceptable levels. This is an evidentiary process through which the organization seeks to build up an internal body of evidence through documentation that it is taking proper steps to manage the risk that it is subjected to through cyberspace. Organizations turn to technical standards that guide them through this process from both a technical and legal perspective and assist in creating the necessary body of evidence in case an incident leads to a future dispute.

With regard to very-large constellations, the question that the operator must engage with are what unique risks my particular architecture creates and what constitutes adequate mitigation of those risks. As discussed above, the architecture of very-large constellations creates potential for massive effects to result from a breach in cybersecurity. Operators of these systems will need to evaluate this within the context of their specific systems. Although there are likely some steps that all operators of these systems will need to take, cybersecurity plans must be customized for each enterprise because it is not a one-size-fits-all process. At this time there are no specific cybersecurity laws or standards for these types of systems, but as noted above, through the national licensing regimes many States will exert at least some oversight of cybersecurity for these systems.

Finally, it should be noted that the very-large constellations have almost exclusively been suggested as architectures for telecommunications. This means that it would be possible for them to fall under the purview of laws and regulations that require heightened cybersecurity for 'critical infrastructure'[24] or 'essential services'.[25] This will, again, be a State-to-State decision based on domestic regulation and how the system is integrated into the national system.

---

[23] For example, Australia's Space (Launches and Returns) (General) Rules 2019, ss 22, 56, & 97 and Space (Launches and Returns) (High Power Rocket) Rules 2019, s. 29.

[24] For example, White House, *Executive Order: Improving Critical Infrastructure Cybersecurity* (12 Feb. 2013).

[25] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 Dec. 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).

3.2 Consequential law

To a large extent, law that imposes consequences is intended to be preventative in the sense that it makes actors aware of sanctions that result from non-compliance. Imposed sanctions require actors to engage in a cost-benefit analysis that takes into account the burden of non-compliance. If sanctions are significant enough, then at least theoretically, actors will avoid breaches to avoid the resulting costs. However, though there is a preventative underpinning to law imposing consequences, this law for the most part is backward facing in that it only operates after an incident that gives rise to a dispute occurs. Its outcome is to punish bad actors and/or to compensate damaged actors for their damages. This subsection will also explore this type of law by looking at space law, telecommunication law, and cybersecurity law.

3.2[a] *Consequential Space Law*

International space law adopts two significant consequences for States: responsibility and liability. These are related concepts but flow from different breaches. Responsibility is the result of a breach of international law,[26] and via Article VI of the Outer Space Treaty, a State has responsibility for the breaches of its non-governmental actors. Liability, on the other hand, results when an actor breaches a duty of care owed to other actors. Article VII of the Outer Space Treaty in conjunction with the Liability Convention imposes liability on the Launching State of a space object that causes damage regardless of whether the space object is government or commercially operated. Depending on where this damage is done it can either be a strict liability standard or a fault-based liability standard.[27] These general rules will apply to very-large constellations because of the way in which they implicate a State's duty to compensate has become important in influencing how States implement their duty to authorize space activities, and States wishing to minimize their exposure will impose more stringent obligations on their licensees. It also means that States will have to evaluate these activities based on the potential for future liabilities to be incurred.

The position on international law on responsibility and liability for non-governmental activities, means that States will need to take into account the nature of each space activity and ensure that the activity complies with minimum standards set by the State based on its interests and its interpretation of international

[26] UN General Assembly, Responsibility of States for internationally wrongful acts: resolution / adopted by the General Assembly, 8 Jan. 2008, A/RES/62/61, Art. 2.

[27] Convention on International Liability for Damage Caused by Space Objects (entered into force 1972), Arts II–III.

legal standards. As noted above this likely implicates cybersecurity planning by operators. If these licensing provisions are breached by the operator, the operator may be subject to either administrative or criminal sanction within the domestic legal system.[28] Further, if actual damage occurs as the result of an incident, then the operator may be subject to civil action based on tort or contract. If such actions occur due to a cybersecurity incident, it will be up to the operator to prove that it was adequately mitigating its cybersecurity risks.

3.2[b] *Consequential Telecommunications Law*

Since ITU law is focused on harmful interference with the usage of radiofrequency spectrum, the ITU dispute resolution process will likely not be relevant for a cybersecurity incident. The extent to which such incidents will be subject to an enforcement action by a national telecommunication administration will depend a great deal on the State in question and its adopted legal regime.

3.2[c] *Consequential Cybersecurity Law*

As discussed above, while the establishment of a cybersecurity plan within an organization is intended to prevent future incidents, the technical standards used for this process will also create a pathway for building up evidence of cybersecurity for usage post-incident. Therefore, for instance, if a cybersecurity incident were to cause an accident in the space environment with its fault-based liability regime, then the operator would want to show that it was employing reasonable and prudent cybersecurity measures to prevent such an incident in order to show that it had not breached the requisite duty of care.

Some States may require some types of organizations to report cybersecurity incidents to national authorities after they occur. It is not unreasonable that this could be included as part of a state's licensing regime for space activities. Such reporting is not about attributing fault but is rather about ensuring that there is proper response and recovery at both the organizational and national levels.

4 ANALYSIS

Three interrelated conclusions can be drawn from the preceding parts of this article. First, there are potentially catastrophic consequences of a cyberattack on a very-large constellation. Second, no system is ever completely 'cybersecure' and

[28] *See* for instance, the case of Swarm Technologies. David Shepardson, *FCC Fines Swarm $900,000 for Unauthorized Satellite Launch*, Reuters (20 Dec. 2018).

as a result, this means that operators will need to be vigilant to maintain resilience from potential cyberattacks. Finally, legal frameworks do provide carrots and sticks for very-large constellations to maintain cybersecurity, but these are limited and generally not substantively different from the general law applicable to all space activities. Indeed, to some extent, the architecture of a very-large constellation changes very little from a cybersecurity perspective as to the applicable law. Whilst the substance of the law does not vary for very-large constellations, the nature of the risk assessment is that an operator must engage to ensure safe, secure, and sustainable operations. The density of operations and the potential impact of these operations require special care for system-wide risk assessment in both the realm of cybersecurity and physical operations.

Within this realm, there is potential for new legal paradigms to address the issues created by very-large constellations. For instance, the ITU is currently considering the problems associated with filings for these systems.[29] At the same time, with only the initial activities happening with deployment of these systems, there are significant questions as to *how* these systems should be regulated, and there is potential that the law is not always going to be the best solution for the problems presented by these systems. Indeed, this holds particular truth in the realm of cybersecurity. While a general legal rule that requires an organization to maintain cybersecurity of its systems has significant differences from a law that requires specific implementations of cybersecurity, the latter has the potential to enshrine as hard law technical solutions that may not be appropriate for all operators and may not maintain their value into the future. Such technical problems are better addressed through sub-statutory governance mechanisms that have more flexibility, and this will most certainly be true when it comes to the particular problem of cybersecurity for very-large constellations. Of course, some governance mechanisms have the potential to ossify into law, but not all should or necessarily need to. Rather, much of governance is about the capability to maintain assured operations through adaptable frameworks.

Governance consists of a variety of mechanisms that have the ability to influence an actor's behaviour and push it towards the notion of 'responsible' within a certain context. These mechanisms include law and regulation, but also include accepted standards, guidelines, policies, good practices, and a number of similar mechanisms. Taken together these mechanisms help form the contours around what constitutes responsible behaviour within the context they address. This is particularly important in disputes that arise from tort or contract as the

AQ4

[29] Elina Morozova, *Non-geostationary Satellite Systems: New Rules of Bringing Them into Use and Phasing Their Deployment*, in *Space Law in a Networked World* 143–161 (P. J. Blount & Mahulena Hofmann eds, Brill, forthcoming 2023).

concern in such disputes is not whether there was a breach of the law but whether the actor in question behaved reasonably and responsibly. This is not unique to space and is a phenomenon that is visible in most complex systems.

Governance structures rather than law alone set the bounds of responsible behaviour, and space is not different. Indeed, the field has already seen such developments in the realms of debris mitigation[30] and nuclear power sources.[31] Governance mechanisms serve as a critical link between the concept of responsible behaviour and what that entails from the perspectives of safety, security, and sustainability. Governance can help entail how operators need to behave to ensure that there is not an inadvertent breach of international peace and security; it can detail how present operations maintain safety through non-interference and it can detail how operations should take into account sustainability through regard for future operations. In highly technical areas such as space, the governance framework allows for the development and innovation within the field whilst still detailing expectations of responsible actors.

Turning back to cybersecurity, governance is a critical concept. The rapid change within the digitized world of cyberspace means that law is often a poor tool for ensuring the security of operations. The bespoke process of cybersecurity risk assessment and mitigation is more often managed through non-legally binding documentation, such as standards, that guide behaviour. For example, the information security plans that are pursued by standards such as ISO/IEC 27001 or the NIST Risk Management Framework, take into account legal provisions, but go well beyond these provisions to establish a responsible method of pursuing cybersecurity. Very-large constellations' operators can use these standards to establish cybersecurity plans that are applicable to their specific systems and to do so they must take into account the risks associated with the density of operations, the replicability of vulnerabilities across individual satellites, and the unique connectivity of the system.

Of course, there is a gap that likely leaves the lawyer surveying the scene ill at ease. This system of governance is based on actors pursuing adequate cybersecurity through their own internal processes rather than compliance with the law. This means that more often than not, it will only be after an incident that there is an evaluation of whether the actor in question was indeed behaving in a responsible manner. This is particularly problematic in the very-large constellation context, as the potential for catastrophic results makes *post facto* evaluations of responsible behaviour an inadequate way to build our knowledge of governance. At the

[30] For example, UNOOSA, *Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space* (2010).

[31] For example, UNCOPUOS & IAEA, *Safety Framework for Nuclear Power Source Applications in Outer Space* (2009).

same time, this is not so different from the legal processes in space. For instance, until such time as there is an incident and a claims commission of court makes a ruling on the matter, it will be quite difficult to legally define the parameters of 'fault' as understood in the space context.

To mitigate against risk of *post facto* understandings of responsibility, there are two extant legal mechanisms that can be employed to bolster cybersecurity. The first is that States take cybersecurity into account within their authorization and supervision regimes and use these regimes as a mechanism to evaluate whether operators are properly engaging in the risk assessment required for their space systems. The second is the reinforcement of information sharing, which is a significant practice found in space law, telecommunications law, and cybersecurity law. Operators need to have a better understanding of the threats and vulnerabilities that create risk and the methods and practices that prevent risks. This is better achieved when there is collective action through which actors can share information that may be relevant to all operators.

Finally, it should be noted that there have been significant discussions about norms of behaviour with regard to cyber operations by States[32] and in the context of space operations.[33] While these are important discussions at the international level, they have borne little fruit, especially in the context of cyber operations. This means that States may continue to be the biggest threat to safe, secure, and sustainable operation of very-large constellations. Until there is movement in this particular realm, the maintenance of cybersecurity will remain a significant challenge in the face of well-funded, so-called Advanced Persistent Threats (APT). This means that activity in developing responsible behaviour with regard to cybersecurity will most likely occur at the regional, national, and industry levels instead of the global level.

5 CONCLUSION

The rise of large constellations presents an array of opportunities to change how space is used, but it also creates a significant number of risks. The nature of these architectures means that cybersecurity will be a persistent issue that operators must manage not only to ensure the safety of their own on-orbit assets but also the impacts that a breach could have on other operators and the space environment itself. Managing these risks is a complex technical problem that sits within a

[32] *See* Dan Efrony, *The UN Cyber Groups, GGE and OEWG – A Consensus Is Optimal, But Time Is of the Essence*, Just Security (blog) (16 Jul. 2021), https://www.justsecurity.org/77480/the-un-cyber-groups-gge-and-oewg-a-consensus-is-optimal-but-time-is-of-the-essence/.

[33] UN General Assembly Resolution 76/231, Reducing space threats through norms, rules and principles of responsible behaviours (30 Dec. 2021).

broader law and policy framework. The development of robust governance for cybersecurity in this field is necessary to ensure the sustainability of these operations. Legal structures can play a significant role in this but cannot be relied on as the only tool. The concept of governance implicates a wide range of measures that are implemented to ensure outcomes. This is already understood in the wider field of cybersecurity, but there is a need to adapt and develop governance structures for space operations and specifically large constellations. Managing the cybersecurity risk presented by these architectures is a critical step towards managing the overall risk presented by such systems and effectively balancing it with the potential benefits they present.