LUISS Guido Carli
LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

Department of International Relations

Chair of Exogeography: Astropolitics and Space Economy

Academic Year 2024-2025

BLACK SWANS IN SPACE: THE ROLE OF INTERNATIONAL FRAMEWORKS AND EMERGING TECHNOLOGIES IN SPACE GOVERNANCE

Supervisor

Prof. Alfonso Giordano

Co-supervisor

Prof. Giuseppe Pascale

Candidate

Davide Salvatore Gallina – 655342

INDEX

ABSTRACT

This dissertation examines the resilience of several fundamental international frameworks for outer space governance against unforeseen, high impact events. These frameworks now face several contemporary risks deriving from developments such as space militarization, the establishment of private actors and new technological threats. Through four macro-indicators and several micro-indicators, the thesis seeks to analyze current weaknesses and propose specific improvements. This effort is complemented by an exploration of the role of emerging technologies (artificial Intelligence, blockchain, and quantum cryptography) both as potential solutions and as risk factors for new strategic vulnerabilities. Findings suggest that updating treaties, formalizing public-private partnerships and integrating new technologies might positively contribute to a more efficient outer space governance system, especially in a context of crisis.

1. INTRODUCTION

Outer space can, as of today, be considered one of the main areas when it comes to maintaining global security and effectively responding to crises. Satellites facilitate daily life on Earth through a remarkably high number of activities which range from enabling navigation to communications, banking and critical infrastructure operations. Military and humanitarian activities, at the same time, depend on space-based systems. In short, space capabilities go hand in hand with day-to-day economic and security functions on a global scale. This exponentially growing reliance on orbiting assets, however, exposes states and societies to new vulnerabilities. If these assets are disrupted or destroyed by accident, deliberate attack, or natural phenomena, the consequences can be severe. As a recent Defence Intelligence Agency assessment (2022) notes, space powers like the United States, China, and Russia consider space essential when it comes to power projection and rapid response in crises.

Yet, the flip side of this strategic value is strategic risk: the same report warns that competitors are developing means to exploit adversaries' dependence on space and potentially "undercut" their advantages (Defence Intelligence Agency, 2022). By all means, space has become yet another domain for geopolitical competition, making future failure or conflict virtually unavoidable, but certainly reducible, if the proper steps are taken. It should be kept in mind that the current geopolitical and technological context has heightened both our dependence on outer space and the vulnerability that accompanies it. Space infrastructure has become critical infrastructure. Yet the rapid changes in space activities have not been fully matched by updates in international governance. This gap between the pace of innovation and the pace of rulemaking is widening the risk of crises in space. The objective of this dissertation is to identify weak links within these frameworks and to propose several improvements that take into consideration multiple perspectives, from cross-integrating public and private actors to treaty adaptation and the implementation of new, world-changing technologies in the diverse spheres of the matter concerned.

The content will be divided into eight chapters, including the present introduction. This introduction's main objective is to, essentially, outline why outer space governance is at what is commonly defined as an inflection point. The vulnerabilities are increasing, but so are the opportunities to address them through cooperation and innovation. Effective prospects, lying ahead, will require the international community to exercise a defined willingness to adapt our perception to new realities. By doing so, we can ensure that humanity can continue to reap the benefits of the space domain, even amidst uncertainty and risk, suggesting pathways forward for the global governance of outer-space activities. This chapter will be followed by a review of the relevant literature, including also, other than relevant books and scientific articles, the legal and theoretical frameworks that currently govern the matter of space cooperation; at the same time, several reports and briefings from specialized agencies have been included.

Chapter 3, which is effectively the first of the five thematic chapter, will focus on the current legislative frameworks that concern space cooperation at the international and supranational levels, examines the current cooperation frameworks governing outer space in detail. Since the dawn of the Space Age, nations have recognized that outer space, much like the high seas or Antarctica, cannot be governed by one state alone, a recognition which gave rise to a web of international treaties and institutions aimed at ensuring space remains a realm of peace and cooperation. The main goal of chapter 3 is to provide an overview of these frameworks and to analyse their structure and "resilience" (by definition, how able they are to adapt and respond under stress), the latter of which is being increasingly called into question by academics and analysts.

The first section of the chapter focuses on providing a precise definition of the term according to specific and quantifiable parameters, according to which the considered institutions will be put to the test through examples of unexpected and high impact crises, ranging from "grey swan" to "black swan" scenarios, with a particular focus on the latter.

Section two of the chapter is dedicated to analysing the role of the United Nations and, more specifically, its Committee on the Peaceful Uses of Outer Space (COPUOS). Established in 1959, COPUOS serves as a multilateral forum where

spacefaring and non-spacefaring nations alike can discuss and develop norms for space. Under UN auspices, a number of non-binding guidelines and principles have been agreed, complementing the legally binding treaties. For example, in 2019, the United Nations' Office for Outer Space Affairs finalized a set of 21 Guidelines for the Long-Term Sustainability of Outer Space Activities (2019), analysing current problems such as debris mitigation, information-sharing, and collision avoidance practices. Although these guidelines are voluntary, they represent international consensus on best practices and enjoy a degree of persuasive weight. COPUOS has also endorsed transparency and confidence-building measures, encouraging states to share information about launches and be careful in avoiding harmful interference and its consequences. The United Nations General Assembly (UNGA) has also been active on contemporary challenges, recently adopting resolutions on norms of responsible behavior in space and aiming to avoid destructive ASAT tests (though these too are practically non-binding). The UN system provides the primary venue for inclusive global cooperation in space governance, aiming to universalize norms and prevent conflict. Given its consensus-based nature, progress can be slow and subject to political obstacles when great powers clash.

Another case study, which will be covered in section 3 of chapter 3, is the European Space Agency (ESA). Founded in 1975, the ESA is a regional agency with 22 European member states that manages resources for space research, satellites and exploration; it has often been described as a "hybrid" organization, serving at the same time as an intergovernmental agency and as a tool for the facilitation of national programs (Beaumier, Couette, & Morin, 2024). Being, arguably, an international organization, a collective space program and an industrial policy instrument at the same time, it serves as a sort of bridge between nations, also helping them to establish partnerships with other institutions and actors. The ESA frequently acts as a negotiator, drafting agreements not only with European Union bodies but also with NASA, Roscosmos and other agencies. This role helps maintaining the space governance system interconnected and reduce fragmentation that might occur in the case of more isolated and national-oriented behavior. For smaller European countries, ESA membership is effectively the only way to be meaningfully involved in space activities (Beaumier, Couette, & Morin, 2024). Thus, the organization serves as an example of how supranational cooperation can

amplify collective capabilities and ensure that even nations without independent launchers or large budgets have a voice in space activities. Non-western centric frameworks, such as the Asia-Pacific Space Cooperation Organization (APSCO) uniting several Asian countries (Yan, 2020), also need to be taken into consideration, though these bodies act, for now, on a more modest scale.

The International Space Station (ISS), which will be further explored in the fourth section, can be considered one of the most historically successful examples of cooperation in outer space. Launched in 1998 and inhabited continuously for over two decades, the ISS is operated by a partnership of five agencies: NASA (United States), Roscosmos (Russia), JAXA (Japan), ESA (Europe), and CSA (Canada). The station is governed by the ISS Intergovernmental Agreement (IGA, 1998) which allocates responsibilities and rights among the partners and, particularly when considering Russia, enables competing and adversarial nations to cooperate. This required both technical coordination and diplomatic effort, given the problems that may stem from the effort to put together different legal jurisdictions (for example, the ISS module ownership defines which nation's laws apply in each part of the station). The ISS partnership has proven itself to be an example of stability and concrete proof when it comes to build mutual trust and interdependence in outer space, managing to resist, although in the short term, even during conflicts such as the 2014 Crimea crisis or the 2022 war in Ukraine, when U.S. and Russian crews have continued working together aboard the ISS, which is by itself a remarkable fact and serves as a precedent for how international agreements might successfully regulate future activities like a lunar base or human missions to Mars, even in cases of on-earth conflict (Farsaris, 2021). It shows that with the right agreements in place, countries with divergent interests can achieve a stable and cooperative presence in space stations and settlements; this is not to say that the ISS has not been impacted by on-earth militarization, as will be seen in the section.

The fifth section focuses on treaties and binding agreements. One of the primary and most important sources is the Outer Space Treaty (OST) of 1967. The OST established foundational principles that still guide space activities today. It declares that the exploration and use of outer space "shall be carried out for the

benefit and in the interests of all countries" and that space is "the province of all mankind," not subject to national appropriation or claims of sovereignty. It further prohibits the placement of nuclear weapons or other weapons of mass destruction in orbit and requires the Moon and other celestial bodies be used exclusively for peaceful purposes. The treaty also makes states internationally liable for damage caused by their space objects and responsible for supervising national space activities, including those of private entities. The idea at the core of the OST is that outer space is a global common to be shared and protected collectively: an area free for exploration by all yet owned by none. This concept will be expanded on in a later chapter. The OST, now with 116 parties, has been remarkably successful in defining "acceptable behavior" and preventing overt territorial competition in space. It represents, overall, the foundation upon which subsequent agreements were built. For instance, the Rescue Agreement (1968) elaborated duties to assist astronauts in emergency situations and the Liability Convention (1972) tried to give a framework for compensating damage caused by space objects. The Registration Convention (1976) requires states to register objects they launch into space in an effort to build transparency. Another notable treaty, the Moon Agreement (1979), attempted to extend the OST's principles by designating the Moon and its resources as the "common heritage of mankind". The Moon Agreement failed to gain support from major space powers and remains ratified by only a few states (Mavroeidi, 2019). This fact arguably is proof of current limits in treaty-based governance when national interests diverge, particularly when pondering the possibility of future resource extraction.

In terms of legal frameworks, beyond the ones already mentioned, new bilateral or plurilateral non-binding agreements and soft-law instruments (which shall be focus of the last section) are emerging to address gaps and improve collaboration. A notable recent development is the Artemis Accords (2020), a U.S.-led set of principles for countries participating in NASA's Artemis program to return to the Moon. The Artemis Accords articulate a shared vision for sustainable and transparent space exploration, explicitly grounded in the Outer Space Treaty's provisions (de Zwart, 2021). Signatories (which now include over 25 nations) commit to guidelines such as: operating with transparency, releasing scientific data publicly, using space resources in accordance with international law, and

deconflicting lunar activities by establishing “safety zones” around sites of operation. While the Accords are not a formal treaty, they represent a political understanding among like-minded states about how future exploration should proceed. They have been praised as a much-needed step forward in updating norms (de Zwart, 2021), particularly regarding resource utilization on the Moon, a topic which was left vague by the OST. However, major spacefaring nations like Russia and China have not signed the Artemis Accords, instead pursuing their own cooperative initiatives (for example, a proposed China-Russia lunar research station). This highlights that, as space activities diversify, governance is becoming competitive in itself: different blocs of countries might adhere to different normative frameworks. Furthermore, a range of informal coordinating mechanisms contribute to managing specific issues. The Inter-Agency Space Debris Coordination Committee (IADC), for example, is a technical consortium of the world’s space agencies that issues guidelines on debris mitigation (IADC, 1993).

International cooperation in space has achieved remarkable successes under this regime: preventing the weaponization of space with WMDs, enabling joint scientific missions (such as Apollo-Soyuz in 1975 and the ISS) and keeping basic order as humanity’s presence in orbit grew from a few satellites to thousands. However, this regime was largely forged in an earlier geopolitical era and under assumptions of a stable strategic environment, and current frameworks face significant limitations and gaps when confronting the kinds of crises and threats now emerging. While existing international frameworks have provided a foundation for peaceful space activities, they exhibit, as will be discussed across all sections, clear shortcomings in coping with rapidly evolving challenges and potential crises. Many of these agreements were crafted decades ago and did not anticipate today’s intense pace of commercialization, the entry of numerous private actors, the resurgence of great-power rivalry in space, or the sophistication of cyber threats. As a result, there are gaps and ambiguities in space governance that become most apparent under stress, which one may argue is precisely when effective and swift diplomatic cooperation is needed the most.

One fundamental limitation is the lack of binding enforcement mechanisms and the reliance on voluntary compliance. The Outer Space Treaty and related

accords set important principles but provide no stringent verification or enforcement body. Compliance, as of today, still lies in the notably unregulated realm of trust, good practices and reciprocity. For instance, if a state were to violate the OST by claiming territory on the Moon, the treaty offers no concrete penalty beyond international condemnation. In routine times, this has not been a critical issue, given that no state has had reason to overtly put into discussion the OST's foundational principles. The absence of enforcement means the system is only as strong as the political will of its adherents, which may constitute a serious problem in a conflictual scenario, as that collective will may fragment and weaken. We saw hints of this when, after Russia's 2022 invasion of Ukraine, technical cooperation in some space projects started to become more uncertain: Europe's ESA, for example, suspended joint missions with Russia (like the ExoMars rover launch) in response to the conflict, and Russia threatened to withdraw from the ISS prematurely. Although the ISS partnership endured, these incidents reveal that geopolitical stress on Earth can cause serious problem to a type of space cooperation which largely still relies on goodwill.

Another gap lies in how military activities and security threats in space are included in the treaty. The OST famously designates space for "peaceful purposes" and bans weapons of mass destruction in orbit. But it does not forbid the use of force in space or the placement in orbit of conventional weapons. During the Cold War, both superpowers went to a certain length to exercise restraint in this domain, and later efforts were made in the Conference on Disarmament to negotiate the Prevention of an Arms Race in Outer Space (PAROS) treaty. These talks had little success, and to date there is no comprehensive legal instrument to put a halt to the development or testing of anti-satellite weapons or other counterspace capabilities. As a result, we have witnessed a series of ASAT weapon tests by various countries in the 21st century. The United States (in 2008), Russia (most recently in 2021), China (famously in 2007), and India (in 2019) have all destroyed satellites in orbit under the banner of demonstration or defence. Each of these tests generated space debris and drew international criticism, but none of them was effectively illegal. The lack of a prohibition or arms control regime for ASATs, as Lauer (2022) also points out, appears to be a defective aspect of space governance. It raises the risk that in a military confrontation, states might actually carry out attacks on satellites,

with potentially disastrous consequences for the orbital environment and escalation dynamics. Even non-destructive military activities, like targeting another nation's satellite with a laser or jamming its communications, still reside within a legal grey area. They could be seen as being in contrast with the principle of non-harmful interference, but even in that case enforcement is not guaranteed. Essentially, the current framework has no clear and explicitly binding rules of engagement for current technologies and potential models for conflict in space, making crisis stability a grave concern.

The governance system also struggles with the challenge posed by dual-use technologies and the rise of private actors. Most space technology (launch vehicles, satellites, robotics) is inherently dual use: the same rocket that carries a commercial satellite can also launch a weapon; a servicing robot capable of refuelling a satellite could also disable one. Treaties like the OST did not foresee the scale at which private companies would operate in space or the degree to which military and civilian capabilities would intertwine. Today, companies like SpaceX, Blue Origin, OneWeb, and others are deploying large constellations that provide services globally, some of which have strategic importance (as seen with Starlink in Ukraine). Yet international law still holds states responsible for supervising their national space companies (United Nations Office for Outer Space Affairs, n.d.). This model is under strain as governments rely more on commercial services rather than operating all satellites themselves. It creates potential accountability gaps: if a private satellite is involved in a collision or is hacked and used to transmit propaganda, for example, it is unclear how international responsibility, and liability would be sorted out in practice. Furthermore, major private actors are not directly party to international agreements – they operate under national regulations, which vary in bindingness. There is a risk of regulatory fragmentation and a "race to the bottom" where companies might seek jurisdictions with the most permissive space laws if standards are not harmonized. The international frameworks have only gingerly begun to address this by, for instance, incorporating industry perspectives in discussions (the UN COPUOS Long-Term Sustainability guidelines encourage engaging private sector best practices). But in a crisis, such as, for example, a private mega constellation satellite that causes interference or a collision, the current governance tools to coordinate a response may need qualitative

improvements. We might be reliant on ad hoc arrangements and the goodwill of the corporation involved, which do not constitute a solid foundation for an effective strategy.

In the area of crisis management, there is a noticeable absence of clear protocols and communication channels specific to space emergencies. Unlike aviation, where mechanisms exist for search and rescue or emergency landings, space incidents often rely on improvisation. If an astronaut were in peril on board a spacecraft, the Rescue Agreement obliges other states to assist (Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space, 1968), which can be considered a positive obligation that nations have planned for. However, consider a different emergency: a large piece of space debris is found to be on a collision course with an active satellite that provides critical services to multiple countries. Who coordinates the warning and possible mitigation (e.g., ordering a satellite to move or, in extreme cases, shooting down the debris)? Currently, notifications about such conjunction threats are handled through informal channels, such as the U.S. Space Surveillance Network alerting satellite operators. There is no single international "space traffic management" authority, though calls for one have grown louder (Martinez, 2021; Migaud et al., 2020). During a crisis, this gap could prove costly. Similarly, if a cyberattack took down a satellite network, affected nations might scramble to figure out who should respond and how to share information, with no established international cyber emergency team for space systems. The first hours or days of a space crisis could thus be mired in confusion due to the lack of predefined cooperative procedures. This stands in contrast to other global domains (e.g., maritime distress signals or the International Health Regulations for disease outbreaks) where at least some crisis protocols exist. Space governance has not yet matured to that level of preparedness.

Moreover, underlying many of these specific gaps is a broader issue: major power rivalry can paralyze consensus-based institutions. The UN COPUOS and other bodies operate largely on consensus. When U.S.-China or U.S.-Russia relations are strained on Earth, it often spills into difficulty reaching agreements in COPUOS or the UN General Assembly. For example, attempts to negotiate even

voluntary “rules of the road” for military behavior in space were, until recently, stymied by political disagreements, with some states favouring legally binding arms control, others preferring non-binding norms, and mutual suspicions blocking progress (Martinez, 2021). During crises between great powers, relying on those same actors to cooperate smoothly in space may be optimistic. There is a trust deficit that the current governance mechanisms have not fully overcome. Theresa Hitchens (2010) observed that from the start, space activities have been a push-pull between competition and cooperation. Presently, the pendulum has swung toward competition in many respects, as evidenced by the formation of military space commands and the pursuit of exclusive partnerships (like Artemis vs. parallel Sino-Russian efforts). This competitive undercurrent can undermine existing cooperative frameworks just when they are needed most. For instance, if an incident happens involving a U.S. and a Chinese satellite, there is no established bilateral forum dedicated to space crisis communication between those nations (though general diplomatic channels exist). The risk of misunderstanding or attribution error (confusing an accident with an attack, for example) looms, and the governance regime offers few reassurances.

It is also clear how new domains and technologies influence the current limits of current treaties. The OST and Moon Agreement did not clearly resolve the status of space resources (mining water or minerals on the Moon and asteroids). This legal ambiguity is already a point of tension: some countries enact national laws granting companies rights to space resources, while others call for a global regime to ensure sharing of benefits. In future scenarios (say, were a private entity’s actions in extracting lunar resources to lead to international disputes), the lack of a legal framework may be bound to lead to conflict. Likewise, emerging concepts like mega-constellations, active debris removal (which could be misconstrued as anti-satellite activity), or the deployment of thousands of small satellites raise questions not fully answered by existing rules. The speed of technological innovation, as is often the case, tends to be faster than the speed of lawmaking. For example, when the OST was written, cyber warfare and AI-driven satellite constellations constituted nothing more than science fiction; now they are reality, and it is important for our governance system to catch up to this fact.

It is increasingly the case, then, that current international and supranational frameworks, while foundational and certainly not to disregard in their entirety, could show significant stress points. Reliance on voluntary adherence without enforcement leaves considerable grey zones pertaining security matters, as does the fact that they have not fully adapted to new actors and technologies. During routine operations these weaknesses might be manageable, but under the intense pressure of a crisis or "black swan" event, they could result in inadequate or uncoordinated responses, with disastrous consequences. This dissertation maintains that strengthening this aspect is a central challenge for the future of space governance. Chapter 3 assesses the strengths of the existing mechanisms as well as their weaknesses in managing crises or enforcing compliance. This sets the stage for evaluating how well these frameworks can handle the challenges outlined in the introduction.

Chapter 4, which is the second thematic chapter of this dissertation, introduces the concept of unforeseen "black swan" events in the space domain, examine the existing cooperation frameworks meant to manage space affairs, and identify their limitations in circumstances characterized by geopolitical tension (be it financial, diplomatic or outright military) and cybersecurity threats.

Nassim Nicholas Taleb (2007) popularized the term "black swan" to describe extremely rare and unexpected events that have massive consequences. Black swans lie outside ordinary expectations; they surprise observers and are only rationalized in hindsight. The space domain, despite its highly technical and monitored nature, is not immune to such events, and the complexity of space systems and the environment's intrinsic harshness create the potential for sudden crises that can make established plans of no relevance or utility. In this context, a "black swan" could be any low-probability and high-impact incident that threatens one or more sectors when it comes to space activities.

The chapter further discusses crisis management using specific case studies and the analysis of real-life scenarios. It takes into consideration historical incidents such as the 2009 Iridium–Cosmos collision and the series of ASAT tests by various countries, as well as ongoing issues like the increasing militarization of space, the growing role of private actors in security crises (e.g. the use of commercial satellites

in the Russia–Ukraine war), and the emergence of cyber warfare targeting satellites. Through these cases, Chapter 4 explores how different types of space-related crises develop and how the existing governance frameworks have responded (or failed to respond) in practice. It identifies common patterns, such as delays in international coordination, ambiguities in the law, and ad hoc industry measures that will inform the subsequent discussion of resilience and reforms. Two interrelated trends need to be observed: the increasing militarization of outer space and the rise of cybersecurity threats to space systems. Since the early space age, military uses of space have been a reality, but direct weaponization was heavily limited. In recent years, however, multiple states have exerted somewhat of a more assertive posture in space. China's emergence as a major space power and Russia's renewed investment in space capabilities have contributed to what some call a new space arms competition (Defence Intelligence Agency, 2022). Both countries (as well as the United States) view dominance in the space domain as crucial to overall military power. The establishment of specialized military space units reflects this shift. Russia's November 2021 direct-ascent ASAT missile test underscored that the norms against creating debris or threatening space assets are fragile. The United States has declared a self-imposed moratorium on debris-causing ASAT tests as of 2022, and a number of other countries joined in that pledge. Apart from kinetic ASATs, nations are developing non-kinetic counterspace weapons. Space is becoming "militarized and some nations have tested and deployed counterspace weapons" (Lauer, 2022). This recognition of space as an increasingly militarized zone was made evident, for example, by NATO's identification of space as an "operational domain" (Defence Intelligence Agency, 2022).

One often cited example of problems resulting by an increasingly trafficked orbit is the possibility of a catastrophic satellite collision or cascade of collisions. Until 2009, no two intact satellites had ever accidentally hit each other at high velocity. That year, however, an active Iridium communications satellite and an obsolete Russian military satellite did collide at 27000 mph, producing over 2000 pieces of debris (Secure World Foundation, 2010). This was the first hypervelocity collision between satellites on record, and it occurred with no prior warning. Fortunately, the impact did not immediately set off a chain reaction, but it served as a wake-up call about what might happen in an even denser orbital environment.

A future incident involving, say, a large space station or a cluster of navigation satellites could have far more severe repercussions, potentially disabling critical services on Earth and polluting orbits with debris fields. Such a scenario would qualify as a black swan: unprecedented in scope and impact, and largely unanticipated by operators accustomed to routine "conjunction warnings" and minor debris avoidance manoeuvres.

Another potential black swan event is a severe space weather incident. The Sun occasionally produces extreme solar flares and coronal mass ejections that can disrupt satellite electronics and power grids on Earth (Cliver et al, 2022). The most infamous case, the Carrington Event of 1859, occurred before the space age but electrified telegraph lines on the ground. A similar event today could knock out dozens of satellites simultaneously or force operators to shut down systems to avoid damage. While scientists monitor solar activity and have models for space weather, an extreme geomagnetic storm hitting Earth's orbital infrastructure could outstrip prior experience, a natural black swan with global technological consequences.

A near-Earth object (NEO) impact is yet another low-probability, high-consequence event. Large asteroids or comets striking the Earth (or exploding in the atmosphere, as with the 2013 Chelyabinsk meteor) are exceedingly rare. But they represent one of the greatest natural threats to human civilization and, unlike many other disasters, they originate from outer space. The international community currently has no fully realized global response strategy for a detected NEO on collision course. Dixon (2016) refers to the risk of an asteroid impact as a "black swan event" for which the United States and the world lack a coordinated mitigation plan. Efforts are underway through, for example, the UN-endorsed International Asteroid Warning Network and Space Mission Planning Advisory Group, to improve global coordination on planetary defence. Yet until these efforts mature into operational capabilities, an incoming asteroid of significant size would present a crisis of unprecedented scale, testing international cooperation under extreme time pressure. Beyond accidents of nature or random chance, geopolitical conflicts spilling into space might also qualify as black swan-type events from the perspective of those who assume space will remain a peaceful sanctuary. The 2022 Russian invasion of Ukraine has already given a glimpse of how space assets

become entangled in terrestrial conflicts. In the hours before the invasion, a major cyber-attack disrupted the Viasat KA-SAT satellite network, knocking out satellite internet service for thousands of European users (including Ukraine's military communications) (ESPI, 2022). Subsequently, Ukraine's use of SpaceX's Starlink satellite constellation to maintain connectivity prompted attempts at jamming and even hints at more direct attacks on these satellites. Some analysts have described the conflict in Ukraine as the first "space war" insofar as both sides leveraged space systems (for reconnaissance, communication, or targeting) and took aim at the other's space-based capabilities (ESPI, 2022). If a regional war were to escalate into intentional destruction of satellites, it would most certainly represent a dangerous precedent and likely catch many off guard in terms of crisis management and legal response.

In essence, outer space is fertile ground for black swans because our collective experience with severe space crises, which represent a remarkably new field, is limited. The following work seeks to give the reader an overview and analytical evaluation of current cooperation frameworks when it comes to managing outer-space related crises; particular attention will be placed on geopolitical tensions and threats concerning space cyber-security. An element of focus will be the concept of the "theory of black swan events" (Taleb, 2007), which highlights the unpredictable, rare, and high-impact nature of certain crises and the role of preparedness and adaptive response mechanisms; outer space governance, a relatively new domain, can be characterized by uncertainty in that regard, and thus frameworks that ensure prepared response when it comes to crises must be effective and well-envisioned.

Chapter 5 explores the relevance of emerging technologies and their implications for space security and governance. It evaluates the opportunities and risks presented by AI, blockchain and quantum communication in the context of outer space. These three technologies will be the focus of the analysis. The chapter aims to discuss concrete examples and case studies: for instance, AI's role in high-precision collision avoidance, or plans for quantum-encrypted satellite networks (Carrasco-Casado et al, 2016), to illustrate how these tools could enhance security, especially given the potential dangers and fragility of satellites when targeted by informatic attacks (Lauer, 2022). It also considers how, on the other hand, hostile

actors might exploit AI or other technologies and what new strategic vulnerabilities could arise (Wendt, 2023; Raska & Davis, 2024). Through careful examination of technological trends, its goal is to provide a basis for understanding how innovation can be incorporated into governance strategies to improve crisis response, as well as what policy foresight may be needed to prevent instabilities that could even be mostly technologically driven. Artificial Intelligence and Machine Learning can improve satellite orbit predictions (Wendt, 2023) and assist in space situational awareness (SSA). Blockchain technology has applications for data integrity and transparency, potentially ensuring space object registrations without the possibility of tampering or interference or facilitating outer space traffic management. Quantum key distribution (QKD) offers what can theoretically be considered un-hackable encryption for satellite communications (Carrasco-Casado et al, 2016). Emerging technologies can, arguably, help preserve the notion of space as a global commons, but they must be accompanied by effective policy agreements.

Chapter 6 then proposes potential improvements to the cooperation framework for space crisis management. Building on the analysis of previous chapters, it considers lessons from how other global domains handle crises, building, of course, on the most notable example of global crisis in the last years, which was the COVID-19 global pandemic (Lamm et al, 2022). For example, analysing how international health regulations manage pandemics, or how financial authorities coordinate during banking crises to suggest how space governance might adopt similar resilience measures. The chapter explores ideas such as developing rapid coordination protocols (analogous to disaster response frameworks), creating joint military–civilian communication channels for space incidents (and, naturally, improving existing ones), and institutionalizing public–private partnerships for space safety (reflecting the reality of the private sector's role). Chapter 6 also aims to understand how stronger integration between public institutions and commercial operators could be effectively implemented: examples may be possible updates to treaties or the drafting of new international norms to fill urgent gaps. Additionally, the chapter outlines how specific emerging technologies discussed in the previous chapter could be implemented in practice to reinforce cooperation among States and improve decision-making speed during emergencies.

Chapter 7 discusses the future of space governance as human activities in space proceed to exponentially increase. It examines the rise of new, national space powers and the evolving ambitions of countries like China, India and others, making the case that their growing involvement might alter multilateral dynamics and power relations in space. The chapter also summarizes and tries to contribute to the fundamental debate on whether outer space should be treated as a "global commons" or as a domain of competition shaped by national interests, considering the implications of each point of view (Pic et al., 2023; Wang, 2013; Wesel & Lambach, 2021). Scenarios for the evolution of norms and institutions over the coming decades need to be explored and discussed, ranging from a fragmented order of competing blocs and private fiefdoms to a more organized and unified system. The question of what each scenario would mean for issues like crisis management, sustainability and the balance between security and commerce will be of remarkable relevance. The thesis findings will, in this chapter, be further contextualized, given that governance must adapt not just to current conditions but to future developments, which will probably include activities such as lunar mining, space tourism and the rise of Space Forces (something that has already been seen in the United States). Finally, the conclusion aims to give the reader a concise summary and evaluation of the effectiveness and overall resiliency of current frameworks considering the evidence discussed, and of how emerging technologies can (or, in certain cases, cannot) help address their shortcomings. The chapter offers final thoughts on the road ahead for space governance as humanity's dependence on space undoubtedly grow and aims to describe how updated norms, better crisis coordination and management of new actors and technologies can favor international cooperation in outer space.

2. LITERATURE REVIEW

The relevant literature chosen consists mainly of peer-reviewed scientific articles and books. Analytical reports and strategic assessments published by specialized agencies and research institutes are also used for real world case studies and global analyses. Additionally, legal instruments and policy frameworks by governmental bodies and international organizations constitute a necessary component. These resources seek to provide an interdisciplinary basis for analyzing contemporary practices and vulnerabilities as well as future opportunities.

This chapter aims to categorize these sources in a systematic manner, according to thematic contributions, and to describe the "state of the art" in contemporary academic discourse, specifically on governance of outer space activities, the management of crises and unexpected disruptions, the implementation of emerging technologies and the potential opportunities for improving international and supranational cooperative frameworks.

The OST is, naturally, one of the most important legal document to analyze, given that it lays the foundational legal framework for international space law, establishing and defining space activities as endeavors that must be conducted for the benefit of all countries; complementarily to the Outer Space Treaty, the Moon Agreement (1979) extends the "global commons" principles of peaceful use and non-appropriation to the Moon and other celestial bodies, defining them as the common heritage of mankind and calling for international cooperative efforts to govern them and prevent resource exploitation.

COPUOS, on the other hand, serves as a central platform for developing space law and guidelines, particularly relevant in the formulation of key treaties and principles that govern space activities. Martinez, P. (2021), in reviewing the guidelines, tries to put into focus their role in preserving space as a global commons, a concept that will come up often during this dissertation: Goehring (2021) questions why outer space isn't considered a global commons, analyzing legal and political factors. Martinez, L. (2021) explores international cooperation and competition in outer space and global commons governance. Wang (2013) went as far as taking into consideration the paradigm of the "tragedy of the commons": space, traditionally considered a commons, lacks boundaries when it comes to state

usage rights, with space debris as an example of clear negative externalities resulting from unregulated space activities; space debris, Wang argues, must be reframed in the optic of property rights theory and of limited and structured forms of privatization as a pragmatic measure to lessen the overuse of this shared resource. Wesel and Lambach (2021), on the other hand, approach the space debris problem from a global commons perspective and argue for international cooperation in debris mitigation. Other relevant articles on the topic come from Migaud et al. (2020), Pic, Evoy, and Morin (2023) and Toyoma (2021).

Committees have also been created for specific subjects of interest: the Inter-Agency Space Debris Coordination Committee Guidelines (IADC, 1993), which developed guidelines to mitigate space debris and focused in particular on minimization of debris released during normal operations through post-mission disposal of potential sources of debris and preventive measures in order to avoid on-orbit "break-ups". In that sense, Yaniz (2022) highlights the emergence of private actors and the commercialization of space, noting that liability for space debris needs complex legal frameworks to properly overcome them. This dissertation also considered the relevance of the International Space Station Intergovernmental Agreement (1998), which constitutes the legal framework at the roots of the International Space Station's design and practical utilization: Farsaris (2021) discusses the IGA as a virtuous example and a precedent for future human settlements on celestial bodies like Mars. The IGA shows how legal frameworks can be successfully structured for the effective management of space cooperative activities, although issues may arise and have done so, especially since the 2022 Russian invasion of Ukraine. When it comes to the moon, it is relevant to also understand what lies at the basis of the Artemis Accords (2020), which set forth principles for cooperation in the civil exploration and use of the Moon, Mars, comets, and asteroids, focusing mainly on principles such as peaceful exploration, transparency, interoperability, emergency assistance and sustainability concerning the use of space resources. De Zwart (2021) examines the Artemis Accords, essentially arguing that although they represent a step towards updating space governance, concerns may arise regarding potential conflicts with existing international treaties and focusing on the potential for creating parallel legal frameworks.

Several strategic partnerships (bilateral as well as multilateral) and security policies have been taken into consideration as well. Case studies include mainly the strategic partnership agreements that Japan signed both with the United States (1960) and the European Union (2019), as well as its National Security Strategy (2022) and that of the United States (2022), all of which contain an explicit focus on outer space security and cooperation. The European Union's Space Strategy for Security and Defence (2023) tries to focus as well on its own need to protect European space assets and disincentivize hostile activities, aiming for as much strategic autonomy as convenient. NATO's Space Policy (2019), at the same time, appears to distinctly recognize space as a new aspect to consider for present and future scenarios as well as an important asset for deterrence and defense.

A portion of the literature also references other models of governance, such as that of the European Space Agency (ESA). Beaumier, Couette, and Morin (2024) analyze it as a hybrid organization with a unique structure that effectively mediates national and supranational interests in space governance, combining intergovernmental and supranational elements that allow it to mitigate fragmentation within the space governance system. By examining the ESA's role, the authors share their view that hybrid organizations can serve as helpful instruments for coordination between national actors with separate goals. Brandenburg and Lieberman (2022), at the same time, provide a comparative study of European and U.S. institutions involved in outer space activities through the framework of historical institutionalism; they explore how different policy choices have influenced arrangements in Europe and the United States, discussing their implications for international cooperation and competition in space and the need to understand institutional contexts for a more effective analysis of outer space policy-making.

Yan (2020) examines yet another space governance organization, which is the Asia-Pacific Space Cooperation Organization (APSCO), as a case study in regional space cooperation and capability building. The study, which will be referenced in comparing APSCO with its European counterpart, focuses on how it facilitates the development of space capabilities among its member states through methods such as collaborative projects, training programs and transparent sharing of information. Yan argues that such organizations are important in promoting

access to space technologies, especially to developing countries, and allow cooperative approaches to their future growth in space exploration and utilization. Cross and Pekkanen (2023) introduce the concept of space diplomacy, along with its theoretical foundations and the practical applications that derive from it. Space, they argue, has become increasingly integral to national interests, and diplomacy must take this evolution into consideration and adapt to it. The authors discuss how space diplomacy encompasses not only state-to-state interactions but also involves growing non-state actors, commercial entities and international organizations, which increasingly contribute to the governance of activities in outer space. Hodgkins and Routh (2021) also discuss the evolution of space diplomacy and propose perspectives for a new paradigm which could take into account the increasing involvement of private sector actors and the growing importance of space in national security considerations. The authors suggest that future space diplomacy will require more inclusive and flexible frameworks to "make room" for all actors. When it comes to governance analysis, Del Canto Viterale (2024)'s multilevel governance (MLG) framework appears to be a useful tool to analyze the global space system: the study identifies various actors operating and interacting among themselves at various levels of governance. The paper analyzes the complexity of the current space framework and essentially argues for increased multi-level coordination in the perspective of being prepared for emerging challenges.

The militarization of space, which has intensified as major powers developed counterspace capabilities, is also widely studied within contemporary literature: the Defense Intelligence Agency (2022) gives an overview of the advancements of China and Russia in space and counterspace programs and of the challenges they could pose to U.S. and allied interests. Cybersecurity threats have become prominent, as evidenced by the European Space Policy Institute analysis (2022) of the KA-SAT cyberattack during the Ukraine conflict, identifying the potential for vulnerabilities in commercial space infrastructure. A relevant OECD (2022) report also analyzes how the war in Ukraine has affected space activities. In that regard, Liu (2024) explores China–Russia cooperation in outer space arms control, giving a perspective on other powers' frameworks in their creation and adoption of space policies. Hammack (2021) discusses the risks of miscalculation

and the weaponization of space and analyzes how security pertaining to space matters is significantly impacted by diplomatic relations on earth. This can be linked to Hitchens (2010)'s advocacy for multilateralism on earth to achieve stability in outer space relations and Meyer (2016)'s warning against the resurgence of "dark forces", a term intended for the rise of international tensions and distrust, which could reverse progress and make collaboration more difficult. The Institute for International Affairs (IAI, 2023), based in Italy, examines the cyber threats to space systems and the unavoidable co-dependence of cyber-security and space. Lauer (2022) analyzes the motivations behind states testing anti-satellite weapons and criticizes the absence of binding agreements in that domain. Unal (2019) addresses the cybersecurity of NATO's space-based strategic assets and makes the point for these assets needing renewed and stronger protective measures. Naturally, human-made emergencies do not include all possible events requiring political and legal frameworks to be prepared; black swans, unpredictable events with unforeseen consequences, are generally discussed at length in Taleb's widely known work, The Black Swan: The Impact of the Highly Improbable (2007). Kipping (2021) explores the occurrence of black swans in astronomical data and how difficult the prediction of rare events can be. Cliver et al. (2022) make the case for a non-human type of emergency, which consists of extreme solar events on space systems and their impact on a global scale. Dixon (2016) explicitly talks about avoiding "black swan" events in examining the U.S. response to Near-Earth Objects (NEOs). Lamm et al. (2022) consider the SARS-CoV-2 pandemic as a crisis offering lessons that, with some contextual revision, can be applied to space-related crises. Coordination at the international level on matters of global security in the space context is analyzed by Kofler et al. (2018), who focus on the work of IAWN (International Asteroid Warning Network) and SMPAG (Space Mission Planning Advisory Group) in adequately responding to and mitigating asteroid-related threats.

The Secure World Foundation reports have been of great importance in identifying several aspects of space policy, mainly when it comes to security purposes: their fact sheet on the 2009 Iridium-Cosmos collision, which constituted an example of the consequences of space debris, gives an accurate picture of an important and contemporary real case study (Secure World Foundation, 2010). The

juridical and political nature of space as either a global commons or not is, as well, analyzed in another report (Secure World Foundation, 2022). Another report concerned the development of counterspace capabilities by 12 countries; the study considered, most importantly, the proliferation of non-destructive counterspace activities (2024).

Technology and its application to space are of fundamental importance in the context of this dissertation. Wendt's (2023) comprehensive overview examines contemporary threats to state security, which range from and encompass artificial intelligence, cyberspace and space; the main point is how interconnected these domains currently are, a link that will only increase in the future, giving reason to argue that subsequent measures must address and keep into consideration these threats in a single, elaborate framework. The topic is also discussed at length in the book The New Laws of Outer Space (Pagallo, 2024), which focuses on the role of Artificial Intelligence in outer space-related affairs, pondering the question of how autonomous systems and smart robots have the potential to influence, in that context, human society and legal systems. These arguments are further reinforced by authors such as Graham (2024).

Though not strictly related to technical and technological matters in nature as much as it is to their social application, this dissertation draws from existing technical literature. Peng and Bai (2019), for example, propose a machine learning approach to improve satellite orbit prediction accuracy; Carrasco-Casado et al. (2016) explore the role of quantum key distribution (QKD) over free-space optical channels, with considerable potential for securing space-based communications through satellites, in order for the latter to be more reliantly resistant to cyber-attacks; blockchain technology is introduced by referencing the effective and accessible description laid out by Abdi et al (2020).

3. ANALYSIS OF CURRENT COOPERATION FRAMEWORKS

3.1. Defining and Measuring Institutional Resilience

Resilience is generally defined as “the ability of a system, community or society exposed to hazards to resist, absorb, accommodate, adapt to, transform and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions through risk management” (United Nations General Assembly, 2016). In the context of outer space crisis management, to "stress-test" space governance frameworks against black swan events both effectively and measurably, a generic definition of resilience, and more specifically of institutional resilience, is insufficient.

In evaluating a framework’s ability to endure unexpected crises, optimal indicators should aim to measure effectiveness standards across all three dimensions of international cooperation: the technical dimension, mainly related to the setting of international operational standards and best practices, which allow for successful and efficient collaborative activities; the normative dimension, which relates to international actors’ ability to adhere to existing legal instruments, either binding or not binding, and to produce new ones in accordance with global developments; the diplomatic dimension, which takes into account inter-state consensus building, conflict-avoidance and negotiation processes.

As shown by the experience of the recent COVID-19 pandemic, entire institutional frameworks can be disrupted by a real-world crisis of considerable speed, suddenness and scale (Lamm et al., 2022). To meaningfully evaluate space governance frameworks, it is thus necessary to establish precise and measurable parameters against which institutional resilience can be judged, and respective frameworks can be compared; this section’s aim is to lay the former out.

The two main dimensions that are generally identified in defining this characteristic are awareness (how proficient is an institution in understanding and successfully interpreting its surrounding environment) and “adaptive capacity” (the ability to respond and adapt subsequently) (Rahi, 2019). Gherghina et al. (2023)

also distinguish between three phases: preparedness (pre-crisis awareness), agility (during-crisis adaptability), and robustness (post-crisis effective recovery). In this sense, institutional resilience appears to be multi-dimensional and characterized by a dynamic aspect. The argument that concrete assessment also needs measurable and quantitative indicators is substantiated by Huber et al. (2023), who link factors related to organizational resilience directly to the recovery time of "key performance indicators" (KPI) after a disruptive process. The specific set of measurable parameters which will be employed is designed to measure the three aspects underlined by Gherghina et al (2023). It must be noted that ESA, COPUOS and the ISS, given their organizational nature, are more prone to this type of analysis, which will nonetheless encompass the framework treated in sections 5 and 6 as well as possible.

To measure Preparedness, it will be examined whether crisis protocols which aim to answer to both specific threats (satellite collisions, cyberattacks, space debris) and less predictable black swan events are present, and to what degree they are. Another clear metric that can be employed, especially when it comes to institutions and agencies, is quantitative and consists in evaluating what fraction of the total budget of an organization or normative cooperation framework is used for activities related to surveillance and crisis prevention. The three sub-indicators described are: crisis protocols, which checks for the existence (yes/no) of general response procedures and, if present, for their general applicability against unpredictable, black-swan events (low, medium, high); resource allocation (low, medium, high, taking into consideration the percentage share of the organization's budget which is used for monitoring and crisis prevention).

Agility might be evaluated in quantifying the time that occurs between the identification of an ongoing crisis and subsequent reactive measures or operations, offering a indication of institutional responsiveness through observing how fast (which might be quantitatively measured in hours, days or weeks) financial and technical resources can be used or reallocated to address an urgent crisis and the ability on the part of the decision-making structure to do so as rapidly as possible, which builds upon the consideration that centralized systems generally make decisions faster than consensus-based ones. The two sub-indicators can thus be understood as reaction speed, slow to fast, and institutional centralization

(classifying a framework as centralized, decentralized or consensus-based), low to high.

Recovery measures the amount of time (once again, measurable in hours, days or weeks) within which these frameworks manage to return to pre-crisis levels and its capacity to involve public, private, and third relevant actors in the recovery and adaptation process, coordinate a comprehensive response and rapidly formalize improvements. In this sense, the two sub-indicators, ranging from low to high, are KPI recovery speed, as illustrated by Huber et al (2022), and post-crisis improvement ability, both of which comprehend an institution's ability to mobilize third actors and external resources.

In order to more organically include treaties and soft-law instruments in the analysis, another indicator will be normative resiliency, which tries to measure how much a framework's legal structure to manage and resist under crises, with particular regard to the normative dimension of international cooperation, related to the difference between binding treaties and soft law instruments; the binding treaties which were negotiated within the context of COPUOS and have been analyzed in section 3.5, along with the UN COPUOS Guidelines, will be organically evaluated in the context of COPUOS itself in section 3.2. The three sub-indicators will be the enforceability of the legal framework (which is binary, as the evaluation will consist of whether the framework's provisions are or are not binding), the existence of dispute settlement mechanisms (which is also binary, but will also evaluate the real-world strength and utility of the mechanism under crisis-related pressure) and endurance of core principles, a more qualitative analysis of whether a framework's underlying principles hold up against contemporary developments, ranging from weak to strong.

In the context of the analysis: in the case all sub-indicators of either one of the macro-indicators are evaluated most negatively, the latter would be considered "very low"; if, on the other hand, all sub-indicators are assessed most favorably, a macro-indicator would score "very high".

3.2. United Nations and Committee on the Peaceful Uses of Outer Space (COPUOS)

The United Nations, through COPUOS and the UN Office for Outer Space Affairs (UNOOSA), constitutes the main global forum when it comes to governing space activities at international level. The UN's central role, in this domain as in others, is that of providing States with a political space in which they can develop shared norms in the common interests of humanity.

COPUOS, short for "Committee on the Peaceful Uses of Outer Space" (1959), is the oldest legal framework to be analyzed within this dissertation, being established with the mandate to coordinate space activities in the clear direction of the "use of space for the benefit of all humanity: for peace, security and development". These general principles, which to this day remain at the core of outer space law, were foundational for the making of subsequent treaties such as the Outer Space Treaty (1967). In fact, "the five treaties and five principles of outer space" (Yaniz, 2022), consisting, namely, in the aforementioned OST, the Rescue Agreement (1968), the Liability Convention (1972), the Registration Convention (1975) and the Moon Agreement (1979), were all negotiated with the United Nations' guidance and contribution; with the notable exception of the Moon Agreement, they were rapidly and widely ratified by spacefaring nations, which indicated substantial agreement on rules of principle.

The Committee has the main function of being an international forum in which to conduct research, analyze the constant evolution of space technology and subsequent activity and debate issues; most of its activities concern the normative and diplomatic dimensions of international cooperation, respectively when it comes to helping producing normative instruments and conducting negotiation procedures. This function is important in the context of addressing black swan events such as large-scale satellite collisions (one example being the Iridium-Cosmos 2009 collision, which will be addressed in the fourth chapter) through the establishment of relevant guidelines for debris mitigation and emergency response procedures. In fact, COPUOS has most recently produced non-binding guidelines on emerging challenges; some examples are the Space Debris Mitigation Guidelines (endorsed by the UN in 2007) and, more recently, the 2019 Guidelines

for the Long-Term Sustainability of Outer Space Activities (21 "best-practice" guidelines that address various topics of concern and aim to increase safety in the context of outer space).

The Committee counts over 90 member States, including almost every spacefaring nation, with some exceptions such as North Korea, Turkmenistan, Serbia and other powers that have limited resources and thus play a minor role in the outer space domain. It is also useful to note that COPUOS membership includes many States that, although not currently being considered "spacefaring", have the ambition to play a part in the future, such as Djibouti and Latvia, which are the Committee's two most recent members as of 2024. The inclusive nature of COPUOS also ensures that space governance discussions are not limited to a few superpowers but involve developing countries as well. The structural multilateralism through which the Committee operates may, by itself, be considered an achievement worthy of note.

The United Nations framework's strengths, at their core, are those of a universalist mandate and an approach based on the consensus of State powers with diverging interests. Thus, when decisions are approved, they are widely understood as politically legitimate. Fundamental international organizations such as the European Space Agency (ESA) have also formally declared their adherence to rights and obligations under the core treaties (Friedl, 2023). It may be argued that the core principles that went on to be enshrined in the OST through UN involvement could have historically helped to prevent unilateralism in outer space and to encourage cooperative behavior among powers. The underlying principles that guided COPUOS have, arguably and as of now, largely kept outer space free of territorial claims and weapons of mass destruction (this aspect will be further analyzed in the fifth section of this chapter). The absence of major military conflicts between superpowers, complemented by the relative stability which characterized the Cold War, may have also by itself encouraged the creation of a framework of shared rules. By the 1990s, negotiations on new treaties had become more difficult because of geopolitical and commercial divergences. Thus, during the post-1989 political framework, as formal treaties became less feasible, COPUOS has apparently transitioned from treaty-making to the development of "soft-law guidelines" on topics such as debris, traffic management, resource utilization and

the long-term sustainability of space activities. Hodgkins and Routh (2021) point out how difficult of a task it has been to produce new agreements within COPUOS when taking the last four decades into consideration.

The COPUOS framework's limitations, especially concerning its direct effectiveness in responding to unexpected crises, come from the consensus-based decision process. All COPUOS decisions, by nature of its own structure, need to be agreed upon by all member states. This rule encounters the issue of having progress obstructed through vetoes, even when it comes from a small minority of member states. Martinez (2021) observes that even reaching agreement on basic "rules of the road" for military behavior in space have historically observed political obstacles; States have been divided between proponents of legally binding arms control and those who preferred to endorse non-binding norms, with mutual suspicions effectively blocking further progress. Within COPUOS, such differences have protracted negotiations even for the redaction of simple guidelines. For instance, the LTS guidelines (2019) took nearly eight years of work and effort on the part of both technical experts and the entirety of the committee to reach a final consensus. It must be noted that in the context of outer space time is particularly of the essence, given the impressive progress of related technologies. During that same eight-year period space technology and commercial activities evolved quickly, and the concern that governance is not catching up to the real-world scenario might be a legitimate one. The slow pace is inherent when it comes to the need for unanimity: States often prefer to procrastinate decisions rather than accepting steps that they see as against their interests, especially when further margins for negotiations are perceived. This dynamic has prevented COPUOS from addressing urgent issues in a timely manner. It is a fact that after the 1979 Moon Agreement no new binding treaties have been negotiated in COPUOS; this was largely because major powers could not agree on what may constitute the future "rules of the game" when it comes to space resources or on arms control. The consensus-based nature of COPUOS represents a critical vulnerability in the context of black swan governance, limiting the ability to globally respond to a sudden and severe crisis.

Another limitation lies in the lack of enforcement power. COPUOS, as a U.N. body, has no power to enforce compliance; that power is left to States (through

national laws or voluntary adherence) or the U.N. Security Council in extreme cases of peace threats, which in space have, for the time being, never occurred. This means that if a country or entity chooses to ignore COPUOS guidelines (i.e., an anti-satellite missile test creating debris and contrary to related mitigation guidelines) COPUOS can do virtually nothing in response, other than applying diplomatic pressure. Recent events have shown the limits of voluntary measures: destructive ASAT tests were carried out by several nations in the 2000s and 2010s, for example, constituting events that happened despite guidelines. Normative pressure, sometimes, is simply not enough to avoid such behavior on the part of space powers. In a "black swan" scenario, such as a sudden cascade of collisions (Kessler Syndrome) or hostile acts in space, COPUOS's tools would necessarily be limited to non-binding measures such as recommendations, possibly relying on those very actors that were involved in the crisis. This reactive and diplomatic nature, which is typical in international systems where actors should enforce the rules to which they themselves are bound, may prove of little use, if not counter-productive, in the context of urgent crises.

COPUOS effectively lacks general and effective crisis management protocols, especially in the context of unpredicted "black swan" events: COPUOS' existing protocols are non-binding (e.g., the previously referenced 2007 and 2019 guidelines), often covering just specific issues and failing to capture or anticipate unexpected crises. The only treaty obligation relevant to crisis management lies in the 1968 Astronaut Rescue Agreement, although, given that it only applies to aiding astronauts in distress, it has a very narrow range of applications. Therefore, Crisis Protocols scores "low". Resource Allocation also scores "low", as COPUOS' funding is entirely dependent on national member states and agencies and COPUOS itself does not contribute; COPUOS's entire budget, managed by UNOOSA and financed through Programme 5 "Peaceful uses of outer space", is funded from the regular UN budget and does not exceed single digits if measured by million dollars, amounting to approximately 5 million USD in 2024, including extra-budgetary contributions (UNOOSA, 2024). In that context, the UN-SPIDER program, which focuses on collection and distribution of satellite data during catastrophes, only received approximately $339000, roughly 6% of the entire budget. Preparedness,

overall, scores “low” and not “very low” because of the existence, to some degree, of protocols, although largely not binding and specialized.

Because of its own fundamental structure and unanimity requirements, as previously referenced through making the case that no binding treaty has been approved since 1979, COPUOS needs years of negotiations to make decisions, operating through a consensus-based model. Reaction Speed is evaluated as “slow” and, naturally, Institutional Centralization’s assessment is “consensus-based”. UN COPUOS’s Agility score is “very low”.

Evaluating the recovery speed of the UN COPUOS’s key functions is difficult: “recovery of key functions” can be described as restoring the normative dimension of international cooperation or its own guidelines after some sort of crisis-determined shock. An example might be represented by the sequence of destructive ASAT tests which took place between the 2000s and 2010s, and which are described in more depth in Chapter 4. In that context, COPUOS did not play any particularly immediate role other than issuing condemnations, and there is little to no evidence that it alone could effectively and rapidly mark a recovery of normative international cooperation after an international crisis or involve external actors in doing so (as will be shown when analyzing how COPUOS fares under the next indicator, a quantitative assessment would have to be measured in years, which is consistent with COPUOS’s structure and shows its limitations). KPI Recovery Speed scores “low”.

The ability of COPUOS to learn from crises and formalize improvements is also somewhat limited by its own structure, with regulatory progress only coming through negotiations. For example, although the 2007 Chinese ASAT test showcased the role of these weapons in the creation of debris, there is no direct trace of the topic in the COPUOS Debris Mitigation Guidelines, even though they came three years later and do not possess binding force; at the same time, it can be argued that the framework possesses a higher ability for normative post-crisis improvements than for autonomously recovering its key functions. Although slowly, COPUOS did indirectly address the topic of ASAT tests with its LTS Guidelines (2019). This illustrates delayed but real post-crisis normative recovery and the overall presence of a forum to discuss multilateral solutions after a

disruptive event. Post-Crisis Improvement Ability thus scores “medium-low”. Recovery, overall, scores “low”; the UN COPUOS framework is unable to autonomously recover its KPIs but can somewhat improve itself after a crisis, although such objective requires previous negotiation efforts that often produce non-binding instruments.

Putting aside the body of treaties that COPUOS helped negotiate in the 1970s, it must be noted that the framework’s decisions are non-binding by design. Its recent output exclusively consists in soft law, thus relying on voluntary compliance with no enforcement mechanism and no impartial dispute settlement body: as it was previously noted, tensions on earth tend to have a spillover effect COPUOS discussions. On the other hand, the foundational principles promoted by COPUOS and its derived treaties (peaceful use, non-appropriation, benefits for all humanity) have remained relevant to this day, although increasingly under stress; notably, to this day no weapon of mass destruction was placed in outer space, consistently with OST provisions. However, the framework did not anticipate contemporary issues such as ASAT tests and mega-constellations and appears to struggle in adapting to them. Enforceability of the COPUOS framework is evaluated as “not binding”, and Dispute Settlement Mechanisms are considered “weak”, given that there are none. Endurance of Core Principles, however, scores “medium”. Normative Resiliency scores “medium-low” overall due to the UN COPUOS framework and its derived treaties’ fundamental legal structure.

Macro-Indicator	Sub-Indicator	Assessment
Preparedness	Crisis Protocols	Low
	Resource Allocation	Low
	Preparedness (aggregate)	Low
Agility	Reaction Speed	Slow
	Institutional Centralization	Consensus-based

	Agility (aggregate)	Very Low
Recovery	Recovery Speed	Low
	Post-Crisis Improvement Ability	Medium-Low
	Recovery (aggregate)	Low
Normative Resiliency	Enforceability	Not Binding
	Dispute Settlement Mechanisms	Weak
	Endurance of Core Principles	Medium
	Normative Resiliency (aggregate)	Medium-Low

Table 1. Evaluation of macro and sub-indicators performance, UN COPUOS.

3.3. European Space Agency (ESA)

The European Space Agency (ESA) is another important regional framework for normative cooperation in the pursuit of outer space-related goals. The agency was established through the 1975 Convention and, as of today, it is composed of 22 European member states and additional, external members such as Canada. ESA has steadily expanded from 10 founding members in 1975 to its current number, effectively doubling it.

The ESA is the result of the merger undertaken by the European Space Research Organization (ESRO) and the European Launcher Development Organization (ELDO), which were themselves products of 1960s European collaboration. Membership increased especially after the end of the cold war, with eastern European countries such as Romania (2011) and Poland (2012) and, much more recently, as associate members, Lithuania (2021) and Slovakia (2022), ensuring a broader range for cooperative activities and serving as an example for other regional organizations such as the recent African Space Agency (2022) and the Latin-Caribbean Space Agency (2021), and, as an additional example, the Asia-Pacific Regional Space Agency Forum, established in 1993. (Del Canto Viterale, 2024).

The ESA Convention entered into force in 1980 and provided its Member States with a legal framework with common objectives and governance structures regarding European space activities. Thus, an organization with its own legal personality, organs and programs was born for European and adjacent States to speak with one voice, when it was needed, in matters related to outer space. The European Space Agency was not born because of national objectives and reasons and purposes mainly dictated by a need for national security, an element which distinguishes it from NASA (Brandenburg & Lieberman, 2022), which is nonetheless an important partner for several operations and activities, as this section will show. Article II of the ESA Convention (1975) explicitly states the purposes of the ESA as “to provide for and to promote, for exclusively peaceful purposes, cooperation among European States in space research and technology and their space applications”.

An important aspect in that regard is that ESA membership is not identical to that of the European Union: the ESA, as a matter of fact, is also composed of non-EU countries (Canada has already been mentioned, but other States include the UK, Switzerland and Norway) and the EU includes a few countries that have not taken part to the agency's membership, though most EU states participate in ESA programs. This aspect allowed the ESA to establish a semi-autonomous autonomy and thus cooperate with a wider range of partners at the European and global levels, as pointed out by Beaumier et al (2024), who also argue that the agency's nature of an hybrid organization enables it to internally "act as a bridge" between less developed spacefaring powers and the international community, improving overall authority and standing of its member states through a structure that helps maintaining a flexible (but cohesive) model for decision-making. Hybrid organization, in that context, is used to describe the ESA's role as "an international organization, a space agency, and an industrial policy actor" (Beaumier et al, 2024, p. 2). The authors also point out how, for example by being a signatory of the International Space Station in the same fashion as many National Space Agencies, the ESA enjoys what is often seen as "having a 'peer-to-peer' or 'horizontal' relationship with national space agencies" (Beaumier et al, 2024, p. 14), also noting the fact that its particular membership status enjoyed the benefit of having "created bridges between European and non-European companies by allowing them to become contractors or subcontractors" (Beaumier et al, 2024, p. 20). The ESA's governance structure itself is designed to balance national interests with cooperative decision-making. ESA leadership at the executive level lies in the Director General, who is voted within the context of the ESA Council (Brandenburg & Lieberman, 2022). The Council, where all member states are represented, acts as the executive body and is of primary importance when it comes to major decisions: each member has one vote in the Council and decisions on important matters often require either unanimity or a qualified majority, with an effort to balance representativeness of all members and at the same time ensure that the States which contribute the most have a say that is proportional to the volume of their national investments; this is also shown, as also pointed out by Brandenburg and Lieberman (2022) by the arguably unique structure behind the agency's programs, which are divided between mandatory and optional activities: while mandatory programs (basic science, general budget, technology research) are financed by all Members according to

their respective GDPs, there is also the option for single members of participating in optional activities that operate under a rationale of proportionality. with the ESA itself assuring that "tenders and contracts will be assigned as far as possible to match inputted funds" (Brandenburg & Lieberman, 2022, p. 100), with single countries deciding the level to which they want to contribute to a specific activity. This rule has arguably maintained a high level of political commitment, given its capacity for guaranteeing that all members see the economic benefits that come from their contributions; at the same time, though, it may also lead to higher costs for activities, given the fact that, under this framework, related contracts need to be distributed across several countries.

ESA member states, while collaborating internationally, have also adopted their own, separate national regulations. Some examples might be, respectively: the *Loi no 2008-518*, a french law related to authorization procedures for space operations and appliable outside French territory when it comes to activities initiated by French nationals; the *Satellitendatensicherheitsgesetz (SatDSiG)*, which is specific German legislation related to the regulation of remote sensing data; Italy's *Legge 23/1998* and *153/2005*, pertaining respectively to liability and registration of space objects; The United Kingdom's *Outer Space Act*, which ensures compliance with the UK's international obligations through the UK Secretary of State's responsibility (Jakhu & Pelton, 2017).

There is little doubt that the ESA has enjoyed the benefits that came from its operations: one example is the 2021 launch of the James Webb telescope, which came from its virtuous collaboration with NASA and was possibly the most important step toward a more effective observation of space (and subsequent data collection) in several decades, ever since the launch of its predecessor, the Hubble Telescope; (Del Canto Viterale, 2024). As a reward, the agency enjoys approximately 15% of the telescope's observation time. The ESA's contribution to international missions, coming from instruments or modules, has time and time again secured flight and scientific data sharing opportunities for European astronauts.

ESA activities and subsequent successes, for example, in space exploration have been many, over the decades, as effectively outlined by Del Canto Viterale

(2024, pp. 28-29): “Cassini-Huygens became the first spacecraft to orbit Saturn (2004); the Columbus science laboratory was attached to the ISS (2008); Rosetta made the first soft landing on a comet (2014); the launch of the ExoMars program (2016); the launch of the BepiColombo mission to Mercury in partnership with JAXA (2018).”

Brandenburg & Lieberman (2022) also note how the European Union and the ESA collaborate on several important projects despite structural differences in approaches and leadership style, given the nature of the former as a supranational organization and of the latter as an intergovernmental one. Such collaboration is also a necessity for the realization of costly and high-complexity projects. Important success in that regard was obtained in satellite navigation, with the development of Galileo, Europe’s own GPS equivalent which was also co-funded by the European Union; the collaboration with the EU was also instrumental to the Copernicus project, which aimed, through the use of satellites, at ensuring strategic autonomy at the european level when it comes to environmental and security purposes. Although the projects were not enough for the European space technical cooperation framework to be considered on par with China or the United States (Brandenburg & Lieberman, 2022), they nonetheless served as fundamental steps in a positive direction.

The ESA actively supports international norms and standards and has, to some degree, contributed to their evolution during the last several decades, having internally accepted the rights and obligations of the U.N. space treaties at the time of their founding (Convention for the Establishment of a European Space Agency, 1975) and actively collaborates with UN agencies, providing inputs and helping to produce guidelines and normative instruments. Its commitment to, for example, non-appropriation and peaceful use of outer space as a collective entity has also had a role in the reinforcement of those same principles.

While the European Space Agency (ESA) represents a successful model of regional normative cooperation among technologically advanced nations, its structure and priorities differ significantly from frameworks designed for developing countries. For example, as Yan (2020) notes, unlike ESA, the Asia-Pacific Space Cooperation Organization (APSCO) focused more narrowly and

explicitly on the issue of capacity building; this is mostly explained by the fact that many APSCO member states lack comprehensive national space laws and are very resource-constrained when it comes to independently manufacture their own satellite on an industrial scale. Therefore, APSCO's primary goals, procedures are instruments are well distinct from the ESA's focus on scientific research and exploration (Yan, 2020).

For all its strengths, the ESA framework appears to have inherent limitations that arise, as they often do, from issues related to its internal functioning and the competing national interests within the agency. The “geographical return” principle might be politically useful, but can also, as mentioned previously, reduce efficiency, given the fact that projects run the risk to be distributed across countries not because their technical merit but to satisfy “return quotas” for its contributors, generating otherwise unnecessary problems. Also, it is the case that individual member states have different priorities according to their objectives: some want to focus on scientific exploration, others may be more interested on their applications or the commercial aspects that the former may generate. Satisfying all agents through the establishment of a common agenda might lead to obstructionism (it must be remembered that all Member States, even those that are not particularly developed when it comes to resources or spacefaring power, have significant capacity for obstruction under the current framework), which can in turn lead to middle of the road, “lowest common denominator” decisions and protracted debates, particularly when it comes to funding levels. From a black swan governance perspective, the ESA's decentralized governance model and its principle of “geographical return” could slow down action during a crisis that requires immediate and centralized allocation of resources. A related issue is also budgetary constraint: the agency's budget is significantly modest compared to NASA’s funding and reflects the hesitancy that pertains to what member governments are willing to contribute. Ambitious projects sometimes put this budget (which has continuously been in the order of less than 10 billion dollars overall) under stress, effectively forcing the agency to either need external partners or necessarily limiting the scope of its more costly operations. Thus, the overall ability on the part of the actors involved to undertake multiple important projects at the same time is limited, forcing tough choices that can disappoint some members or scientific communities. Increasing

spending and ensuring a more effective coordination, especially when it comes to contracts, may arguably be necessary in order to improve aspects related to strategic autonomy and expand the range of possible future operations at the European level.

Other problems, especially in the future, could reside in the dual governance model that effectively characterizes European outer space activities; there is a clear space governance overlap with the European Union's roles, which has started to create its own bodies, such as the European Union Agency for the Space Programme (EUASP), which was created in the context of the new EU Space Program (2021-27) through a 2021 resolution adopted by the Council and the European Parliament (Del Canto Viterale, 2024). While the agency maintains a substantial degree of independence from the EU as itself, the EUASP reports directly to the Commission and the Council; as it often is when it comes to overlap in functions, there may be room for concern in considering potential coordination and bureaucratic issues as well as a sub-optimal utilization of resources.

One of the most relevant limits to this dissertation appears to be what was already referenced when discussing the differences between ESA and NASA: namely, article II of the 1975 ESA Convention, or rather its traditional interpretation, which leads to the exclusion of military or defense-related space activities. For decades, the ESA remained distant from involvement in any security or military space projects. On one hand, its attitude was instrumental in maintaining diplomatic cooperation civil and open with many other actors; on the other, it also meant that, at its core, Europe had no collective mechanism for military collaboration in outer space (those efforts either proceeded inter-governmentally or were carried through other organizations such as NATO). As of today, security issues like space situational awareness for internal regional security or satellite communications for defense have become more prominent, and real case studies are starting to emerge. ESA's exclusively peaceful mandate could severely limit its capacity to act in response to a security-related black swan event, which may constitute a problem for its governance structure.

One example, as thoroughly analyzed by a report from the European Space Policy Institute (2022), is the Russian cyber-attack on the ViaSat's KA-SAT satellite network, which the Ukrainian army used for communications. The report

found that “the cybersecurity of space systems is rather overlooked in EU policies and regulations”. The lack of an ESA role and its absence of influence in that sphere could be considered a problem worth looking at. The European Union has begun addressing space security through other means such as the EU Space Strategy for Security and Defence (2023), yet ESA mandate and structure may need to be adjusted to employ its potential when it comes to security needs. The absence of a defence dimension within the ESA framework can be a limitation when considering “black swan” scenarios such as a conflict extending to space: the agency itself, as of now, could not directly participate in any coordinated European response, nor could it assist in planning related to military space assets, since those areas currently lie outside its powers. Member states’ national space agencies and EU defense bodies could theoretically be equipped to handle such crises, but a strong disadvantage could be represented by fragmentation in response. The ESA is, at its core, an alliance of states and represents, as already described, an intergovernmental framework of government with no military applications: this can, arguably, represent a weakness in times of crisis. In a more extreme “black swan” scenario, an example being a broad conflict or a major accident affecting Europe or, nonetheless, several of its member states, the agency’s projects could suffer under two perspectives.

Internally, the internal absence of readiness in consensus-based decision-making: thus far, ESA members have maintained unity, but it is not hard to imagine potential scenarios in the future in which member states’ political differences might put the European Space Agency in a difficult position. Externally, the ESA could pay the consequences that stem from the arguably “peace time” framework and inclination by which it is characterized, both in responding to its own security threats and participating to a coordinated international response to global outer space-related crises.

ESA effectively lacks general and effective crisis management protocols, an element that is only reinforced when considered under the context of unpredicted “black swan” events: ESA’s existing protocols (one example is the ESA Space Safety Program) are technical and specific also due to the previously referenced absence of a defence dimension within ESA, which is an important limit when it comes to the agency’s ability to respond to space security crises by itself, without

consulting national or EU authorities. Therefore, Crisis Protocols scores “low”. Resource Allocation also scores “low”, given that ESA dedicates only a modest fraction of its also modest budget (especially when compared to agencies such as NASA) to space safety and surveillance: a large portion of those functions are not carried out by the ESA itself. When considering the entire ESA 2024 budget (7,88 billion dollars, in contrast to NASA’s 24 billions), it can be seen that the item “Space Safety” received 277 million dollars, approximately 3.5% of the overall budget, much less than its American counterpart. Preparedness, overall, scores “low”, not “very low”, due to the existence of protocols, although they are technical, specialized, limited in their range and mostly not applicable to “black swans”.

Given its governance model and the requirement for broad support among its 22 member states for major decisions reactive speed could be slow when referring to major political and budgetary decisions, although ESA proved itself able to act relatively swiftly when it came to technical anomalies, one example being the 2019 Aeolus-Starlink collision-avoidance maneuver (Klein & Boensch, 2024): the predicted conjunction was on September 1st 2019, exceeding the threshold required for intervention on 29 August. Relevant commands were sent on September 2nd, respectively at 10:14, 10:17, and 10:18, 50 minutes before the predicted conjunction. In this case, the time required puts reaction speed at 4 days, with the agency planning to use new technologies to automate related processes to further reduce reaction time. ESA does not possess centralized budgetary authority, with each member state choosing which optional program to invest in. Institutional Centralization’s assessment is “Decentralized”; ESA’s comprehensive Agility score can be evaluated as “medium”.

When it comes to the ESA, “recovery of key functions” can be described as restoring ESA’s mission infrastructure and timeline after an important disruption. Historical cases, such as the ViaSat cyber-attack discussed in Chapter 4, shows once again the limit represented by ESA’s absence of focus on defence purposes, as immediate recovery efforts were mostly managed through EU channels and were not coordinated by the Agency. ESA’s KPI Recovery Speed thus scores “low”.

ESA does possess the ability to learn from crises and formalize improvements, although it is limited. Although ESA has begun acknowledging gaps

such as cybersecurity vulnerabilities, especially after the 2022 ViaSat attack, consistent reforms require treaty changes which are able to incorporate a defence dimension. Without such reforms, ESA's institutional-level post-crisis adaptation remains slow, although more adaptive than KPI autonomous recovery, resulting in a Post-Crisis Improvement Ability score of "medium-low". Recovery, overall, scores "low"; ESA lacks the ability to rapidly recover its KPI functions independently, and while it can implement minor technical improvements after crises, significant normative reforms appear to be needed.

The ESA's framework, unlike others such as COPUOS, is legally binding under the 1975 Convention, obliging national member states to commit financially to some commitments that are backed by treaty; at the same time, the ESA Convention includes arbitration clauses and thus a mechanism for dispute settlement, although it remains largely untested in the context of important and unexpected crises, making it difficult to evaluate comprehensively. Thus, "enforceability" is accounted for as "yes". Dispute settlement mechanisms are evaluated as "medium", given they are present but untested.

ESA's core principles of peaceful cooperation among European states (both diplomatic and technical) have proved stable since the adoption of the Convention 1975 and have largely succeeded in maintaining unity or, at least, preventing notable outer-space related intra-european tensions. However, as noted, the militarization of space accelerates, making its mandate to renounce defence-related purposes considerably less solid. Additionally, the severing of the partnership with Roscosmos in 2022 after the Russian invasion of Ukraine appeared to show a degree of vulnerability of its normatively cooperative principles. Thus, Endurance of Core Principles scores "medium". Normative Resiliency, overall, scores "medium" due to ESA's otherwise stable legal structure, which is nonetheless negatively impacted from considerable pressure on its exclusively peaceful mandate and limitations in a rapidly evolving geopolitical environment.

Macro-Indicator	Sub-Indicator	Assessment
Preparedness	Crisis Protocols	Low
	Resource Allocation	Low
	Preparedness (aggregate)	Low
Agility	Reaction Speed	Medium

	Institutional Centralization	Decentralized
	Agility (aggregate)	Medium
Recovery	Recovery Speed	Low
	Post-Crisis Improvement Ability	Medium-Low
	Recovery (aggregate)	Low
Normative Resiliency	Enforceability	Yes
	Dispute Settlement Mechanisms	Medium
	Endurance of Core Principles	Medium
	Normative Resiliency (aggregate)	Medium

Table 2. Evaluation of macro and sub-indicators performance, ESA.

3.4. International Space Station (ISS)

The International Space Station is a large, floating space station located in low earth-orbit. It was established through a comprehensive collaborative accord, the Space Station Agreement (1998), also known as the Intergovernmental Agreement, currently signed by five national and regional space agencies: the ESA, as already referenced, the Canada Space Agency (CSA), the Japan Aerospace Exploration Agency (JAXA) and Roscosmos, the Russian State Corporation for Space Activities. The agreement has also been signed and ratified by fifteen partner states. The five agencies mentioned, as of today, also contribute to its ordinary and extraordinary maintenance.

Although the five agencies referenced constitute the actual membership of the Station, it is important to mention that Roscosmos was not a founding member of the ISS, only taking part to it in 1998, seven years after the collapse of its legal predecessor, the Soviet Space Program (1951-91), and the dissolution of the USSR. In fact, the ISS was born out of US-based initiative through President Reagan's call for the establishment of an inhabited space station in earth's orbit and the subsequent signing of the Intergovernmental Agreement of 1988 (Farsaris, 2021), which, in time, gave way to the ISS framework as we know it today. Remarkably, the United States and Russia, after decades of Cold War competition, became partners when it comes to this undertaking, mutually accepting a degree of mutual interdependence between their respective astronauts; arguably, the International Space Station historically stands out as one of, if not the most, effective examples of the possibility of withstanding tensions and establishing effective technical cooperation between rival space powers while upholding the founding principles of all important outer space legislation. This was evident after Russia's annexation of Crimea, when tensions perceivably increased on earth but did not significantly disrupt NASA and Roscosmos's continuous work on orbit. Farsaris (2021) also notes how some of the limits of the 1988 agreements were virtuously overcome and helped create a more cooperative political environment: the 1988 version of the IGA effectively contained provisions that gave the United States an "extra-ordinary jurisdictional grant", providing it with jurisdiction for any given offense on the station. This was no longer the case when the 1998 IGA granted equal jurisdictional

authority of all partners over their resources, a change that is widely considered to be a valuable precedent.

Del Canto Viterale (2024) interestingly points out how, political rivalry notwithstanding, in more than two decades of activity Russia and the United States have successfully worked together in ISS-related matters; the Station itself, he notes, has boarded more than 200 astronauts from almost 20 different nations and allowed more than 3000 scientific experiments to be conducted. The ISS's most important function is, in fact, that of serving as a research laboratory, taking advantage of the microgravity environment resulting from the ISS's orbital positioning (Farsaris, 2021).

The main strengths of the ISS framework are effectively listed by Farsaris (2021), who argues that they mostly lie in correctly addressing issues related to jurisdiction, control and, very importantly, liability. This fact was, arguably, a necessary condition for allowing space agencies (and the respective member states) in reciprocal competition to coordinate their operations while maintaining certain sovereign rights and collaborating without the obligation of creating a supranational authority. A direct example of this approach is the jurisdictional model employed in controlling the different areas of the ISS. Each partner effectively "owns" their modules and personnel. This principle proved itself useful in controlling constitutional conflicts (especially for the more powerful member States, which are also notably more sensitive to limitations of sovereignty) and maintained legal clarity in operations, a very important factor given the coexistence of very different actors within the ISS framework: each partner can contribute according to both resources, capabilities and specific interest if it is able to, at the same time, adhere to the operational standards and procedures for dispute resolution described in the agreement.

Both Del Canto Viterale (2024) and Farsaris (2021) pointed out one of the most useful applications of the ISS for current and future purposes, which is its role in cooperative exploration that goes well beyond Earth orbit. The legal-institutional coordination mechanisms that characterize ISS may prove themselves to be of fundamental importance for missions to the Moon and Mars. Farsaris (2021), in his paper, mainly analyzes how ISS's intergovernmental framework could be

replicated or evolved in upcoming projects such as the Lunar Gateway or Martian bases. It is also argued how the ISS is in a unique position, because of its equipment and testing facilities, to be central for further, continued exploration of the moon and mars (Del Canto Viterale, 2024).

The ISS framework, its merits notwithstanding, is not without flaws. One of the most notable ones is that it is not a truly global framework, its members being mostly western-aligned agencies and States (with the clear exception of Roscosmos). Such criticism is only strengthened by NASA being the ISS's largest contributor and the absence of both China and India from membership. This international but not all-inclusive framework is also shown by China's decision to pursue its own space station (Tiangong, with the latest modular station completed in 2022) and invite other countries to cooperate there (Yaniz, 2022). India has also announced its intention to build a modular space station, the Bharatiya Antariksh Station, making it operational by 2028 through Indian Space Research Office oversight. These parallel efforts may reduce the chance for truly global standards or collaboration, and potentially even introduce competition (e.g., which station gets certain experiments from third-party countries).

Internal ISS cooperation, although able to withstand significant geopolitical crises, has been increasingly strained in recent years. Recent developments, as can and will be seen in the fourth chapter, are marked by an increasing shift of Russian outer space policy toward China and the global east, further weakening the ISS framework. The most defining event, especially when it comes to Russia's relation with other ISS parties, has arguably been the Ukrainian war. In response to sanctions over the war, Roscosmos' head Dmitry Rogozin publicly threatened to end shared work on the ISS and let the station fall to Earth if Russia could not operate it, although space diplomacy appeared to prevent the worst from happening despite the circumstances (Cross & Pekkanen, 2023). in July 2022, Russia announced its withdrawal from the station (effective from 2028), attributing it to other States' economic countermeasures (Liu, 2024). Had Russia unilaterally pulled out in a more decisive fashion, that development would have constituted a very serious "black swan" event, with a terrestrial conflict abruptly ending decades of space teamwork. The remaining partners would have faced enormous challenges in maintaining ISS operations (a portion of which are handled by Roscosmos), at least

in the short term. ISS, in that regard, may lack a conflict-resolution mechanism that goes beyond intra-agency diplomacy and may also rely too much on members remaining cooperative (or at least not actively hostile) among themselves. The partners, as previously stated, do have legal agreements in force, but those tend not to properly account for crisis scenarios in which they could break down. In that context, because of the ISS's own structure, no higher authority exists to incentivize technical cooperation.

The intergovernmental approach in defining jurisdiction and procedure which was discussed earlier in this section may also constitute a limit in the case of miscommunication, given member states' differing standard operating procedures; although some mitigation mechanisms and procedural integrations are in place (Farsaris, 2021). Still, an unexpected, not-accounted-for crisis would most likely be a challenge for emergency responses; for example, determining whether a partner might prioritize its own hardware, employees or resources in a way that conflicts with others. The Rescue Agreement of 1968 would apply if an emergency evacuation and rescue were needed, but only covers such issues at a broad level, without room for specific arrangements and emergency procedures.

The ISS appears to be a remarkable case study from which two conclusions can be drawn: firstly, that adequate frameworks can encourage cooperative behavior even among rival space powers; secondly, that both rapid change in political circumstances and the emergence of crises can severely affect even virtuous agreements and long-standing mechanisms related to outer space collaboration, with all the risks involved, making the capacity of these mechanisms to adapt to said circumstances a necessary condition.

While the ISS partnership framework enjoys strong and detailed technical procedures for emergencies onboard (evacuation procedures are one example), it mostly lacks a framework in the context of international diplomatic crises, especially when it comes to intra-partner disagreements. The absence of a predetermined protocol for scenarios such as partner withdrawal or conflict-induced rupture, as considered when describing the 2022 Russia crisis, severely limits the framework's readiness for black swan events. Given these important limits, Crisis Protocols scores "medium-low".

Resource Allocation scores “medium-strong”, given that the ISS program dedicates a 25% share of its budget (which comprehends the lion’s share of US fundings amounting to 4.4 billions, 16% of NASA’s 2024 budget, aiming at sustaining human presence in low-earth orbit) to operational monitoring and safety of operations, more than a billion dollars (NASA Office of Inspector General, 2024), although investments in broader, unexpected crisis prevention, especially in the context of “black swans” is not as thorough. Preparedness, overall, scores “medium” as the ISS possesses very thorough crisis procedures for specific missions but appears to be somewhat lacking when considering comprehensive plans for “black swans”, especially in the context of diplomacy.

The ISS can largely be described as a consensus-based model among equal partners, without a supranational authority capable of unilateral action during a crisis. While it can react in a matter of hours to technical challenges (e.g., the 2021 Pegasus rocket and 2022 Cosmos 1408 avoidance maneuvers), effectiveness in diplomatic crises is severely limited by the need for multilateral agreement and, consequently, diplomatic negotiation, which, as seen with Roscosmos in 2022 and Russia’s intentions to withdraw from ISS partnership, might take months to years. Arguably, crisis management should not assume rational or cooperative behavior to persist, and a framework that takes into consideration the possibility of prior diplomatic arrangements being dissolved could be more effective. This scenario shows that the ISS framework, although being able to maintain operational stability during times of peace, is critically vulnerable to these particular kinds of black swan events, in which its fundamental assumption of a partner’s “bona fide” action is proven as non-appliable. Reaction Speed is therefore assessed as “medium-low” because of limitations in political responses, while Institutional Centralization is evaluated as “consensus-based”. ISS Agility’s score could be rounded to “low” and constitutes its worst-performing macro-indicator.

The ISS partnership, as of today. has shown a consistent ability to recover from minor-to-medium disruptions and continue its mission, as seen in 2022; it must be noted, at the same time, that the ISS never had to recover fully from a sudden partner withdrawal. The ISS’s modular design ensures that, in the case if one system fails, often another partner can assist. On the other hand, certain failures would be hard to recover quickly if a partner abruptly leaves the framework: if

Russia suddenly pulled its own modules, the remaining partners would face, as previously referenced, severe difficulties in maintaining operations. In this sense, the planned 2028 withdrawal of Russia is a predictable challenge; an unscheduled and hostile departure, because of the very fact that the ISS governance framework has no effective contingency plans, could more effectively represent an event that is both sudden and not accounted for. It's taking NASA several years to develop a new propulsion module to ensure ISS orbit maintenance post-Roscosmos. So, ISS recovery speed would be evaluated as "medium", given that up-to-date setbacks have been handled effectively, but political crises could exercise more strain on the current system.

The ISS framework has implemented a degree of procedural improvements after technical incidents, and legal adaptations, one example being the revision of jurisdictional arrangements in the IGA (1998). On the other hand, no significant formal improvements were implemented because of diplomatic crises, such as during the 2014 Russian annexation of Crimea or the war in Ukraine. Post-Crisis Improvement Ability scores "medium-low".

Recovery, overall, would score between "medium" and "medium-low"; given the focus of this dissertation on black swan events, it can be argued that the lack of prevention mechanisms for recovering from large scale diplomatic crises would place it in the latter category.

ISS agreements, such as IGA (1998), are legally binding agreements from which stem obligations related to funding, crew and modules. Enforceability therefore scores as "binding".

Dispute Settlement Mechanisms are evaluated as "present" and have functioned effectively in cases of jurisdictional (as previously mentioned) and operational disagreements; nonetheless, these mechanisms are still reliant on partner cooperation, indicating weakened practical strength in the cases described. These mechanisms are evaluated as "medium".

The ISS's core principles of interdependence and reliance on the technical dimension of international cooperation, even when among former rivals, have been perhaps between the most endurable and, as facts stand, have withstood the diplomatic tensions of 2022. Although endurance of core principles is very solid as

of today and arguably deserving to be evaluated as “high”, Russia’s planned 2028 withdrawal indicates that its stability is far from permanently guaranteed, especially in the 2025-28 timeframe. Normative Resiliency scores a cautious “medium-high” overall, with relative weakness when it comes to the potential management of diplomatic crises in future years.

Macro-Indicator	Sub-Indicator	Assessment
Preparedness	Crisis Protocols	Medium-Low
	Resource Allocation	Medium-Strong
	Preparedness (aggregate)	Medium
Agility	Reaction Speed	Medium-Low
	Institutional Centralization	Consensus-based
	Agility (aggregate)	Low
Recovery	Recovery Speed	Medium
	Post-Crisis Improvement Ability	Medium-Low
	Recovery (aggregate)	Medium-Low
Normative Resiliency	Enforceability	Binding
	Dispute Settlement Mechanisms	Medium
	Endurance of Core Principles	High
	Normative Resiliency (aggregate)	Medium-High

Table 3. Evaluation of macro and sub-indicators performance, ISS.

3.5. Binding Agreements and Legal Frameworks

The first part of this section will mainly focus on the five foundational space treaties that have characterized international cooperation on the diplomatic level in outer space during the last decades and the related legal frameworks, as long as they are characterized by some degree of bindingness, illustrating their content and analyzing strengths and weaknesses. These treaties, which were already briefly mentioned in section 2 as they were negotiated primarily through the United Nations COPUOS between the 1960s and 1970s, have been part of the earliest political initiative aimed at establishing forms of space governance.

The first subject of analysis is the "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies" (1967), more commonly referenced as the Outer Space Treaty. The OST, which is broadly considered to be "the Magna Carta of space law" (Friedl, 2023, p. 52), was drafted and approved in the Cold War period, which was notably characterized by the rivalry between, arguably, the only two spacefaring powers of that time. The initial space activities of the United States and the Soviet Union were military and competitive in nature, but both parties came to understand the need for an international legal framework to regulate outer space and thus establish some shared foundational principles. That consensus *de facto* allowed the United Nations General Assembly, most notably through Resolutions 1721 (XVI), 1884 (XVIII), and 1962 (XVIII), to formalize the core principles later incorporated into the OST (Aoki, 2024). The author also observes that, though many of these principles might have crystallized into customary international law even before the Treaty's entry into force, the OST's function has been that of providing them with additional clarity and legitimacy, especially given the very limited number of influential spacefaring actors.

The three most important principles (laid out, respectively, in articles I, II and IV) laid out within the OST can be listed as the principle of freedom of exploration and use, the non-appropriation principle and the peaceful use of outer space.

Article I states that activities in outer space should be undertaken "for the benefit and in the interests of all countries, irrespective of their degree of economic

or scientific development". In the second part the article also emphasizes the right on the part of States to explore outer space without incurring discrimination and to freely conduct scientific research "in outer space, including the moon and other celestial bodies", with a duty on the part of other States to encourage and facilitate the process.

Article II formally excludes "claim of sovereignty" in outer space. This factor, at least formally, had an equalizing function: it considered all states, regardless of power and resources, at the same level when it comes to outer space claims (given that appropriation is generally prohibited, Gabon enjoys the same right as the United States to potentially explore the Moon).

Article IV goes more into detail regarding the principle of peaceful use, prohibiting in-orbit placement of weapons of mass destruction. The article defines these weapons in a general sense that is not limited to nuclear weapons, arguably accounting for the development of possible future technologies. In the second part, the article aims to prevent the "militarization of space" (explicitly talking about military base installations, research aimed at non-peaceful purposes and testing of weapons).

Other relevant articles are VI (national responsibility for State activity), VIII (sovereignty over State property launched in outer space) and IX (the duty on the part of the States to implement measures to avoid "harmful contamination" and interference with the activities of other States): these provisions creates national obligations for States not only to themselves but also to supervise activities from private companies. In this context, UNGA has actively asked States to approve national laws to better enact supervisory duties (Jakhu & Pelton, 2017). It can be argued that the Treaty's assumptions, given the increasing number of actors and the complexity of their activities, could be put under stress by a single black swan event that it was never designed to predict, one example being a massive international accident caused exclusively by the actions of a private company, such as a autonomous collision avoidance failure on the part of a software of a private mega-constellation (e.g., Starlink), an event which could, as a consequence of numerous collisions, generate tens of thousands of undesirable debris objects. Under the Outer Space Treaty, the launching state (the U.S.) would be internationally liable for the

damage. However, the Treaty lacks a real-time crisis management mechanism and protocols which could coordinate an immediate response, if required, at the international level. Essentially, the OST's foundational principles need to be supplemented by additional procedures needed to govern technological black swan events initiated by a powerful non-state actor, phenomena which, differently from today, were not cause for immediate concern when the treaty was written.

The binding treaties that follow the OST essentially make an effort to expand its existing provisions. The Agreement on the Rescue of Astronauts, the Return of Astronauts, and the Return of Objects Launched into Outer Space (1968), for example, extends Article V of the OST on rescuing "envoys of mankind" from dangerous situations. States have a duty to assist astronauts during emergencies and return them safely to their nation of origin (along with space hardware, whenever the latter reaches their territory). Remarkably, the Rescue Agreement has to this day never been used in a real case scenario when it comes to astronauts, though there have been returns of fallen space objects. The Convention on International Liability for Damage Caused by Space Objects (1972) complements the Rescue Agreement by establishing a legal framework for liability and subsequent compensation.

It attributes very strict liability for space objects to launching States: in the case of on-earth or vehicle damage by a crashed object that is the property of another State, launching States have liability even in cases where fault is not found. For damage that occurs in space, on the other hand, the State can only be liable if there is an element of fault. This Convention was only at risk of being applied in one case: during the Cosmos 954 incident in 1978, when a Soviet satellite crashed in Canada (Moltz, 2024). In the end, Canada receiving compensation through diplomatic means, with no formal liability being pursued. Despite its lack of historical applications, some States have been somewhat responsive in terms of national implementation: South Korea, for instance, has approved a compensation regime for possible damages caused by their space activities (Jakhu & Pelton, 2017).

The Convention on Registration of Objects Launched into Outer Space (1974) complements the Liability Convention and OST Article VIII by establishing who is responsible for each object through the latters' identification and registration

within both respective national registries and a central UN database. Although most States largely comply and thousands of satellites have already been registered, there have been cases of military or intelligence-related launches with delayed registration or vague, if not at times misleading, information attached (Moltz, 2024). Though not perfectly applied, it can be said that the Convention is largely useful and can help technical and diplomatic cooperation through, for example, allowing for more precise notification of conjunction warnings and claims of ownership for lost or fallen objects.

The Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (1979), which was largely built on existing OST provisions with the aim of providing a specific framework for the moon and celestial bodies, declared the Moon and its natural resources the "common heritage of mankind", to be governed through international cooperation and with a prohibition on ownership of lunar resources by single States or entities. It is important to note that no nation with significant space capabilities ratified the Moon Agreement (De Zwart, 2021), making it the main UN space treaty that effectively failed to be broadly implemented, with only 17 parties (most of which are effectively non-space faring) and 11 signatories as of 2025. For example, Saudi Arabia, which has been increasingly investing in space capabilities during recent years (Paikowski, 2024), left the Moon Agreement in 2023. The lack of major players has arguably made the Moon Agreement *de facto* irrelevant, given its binding effect only on its parties and its failure in creating an international regime. In a 2020 executive order closely related to the Artemis Accords, the United States Government also explicitly rejected the concept behind the Agreement, stating that it was not effective with regard to "the promotion of commercial participation in the long-term exploration, scientific discovery, and use of the Moon, Mars, or other celestial bodies" (De Zwart, 2021, p. 5). The main point of disagreement with major space powers consisted in the "common heritage" principle: with spacefaring nations developing better infrastructure and capabilities for future commercial development (space mining, which necessarily requires resource utilization, is an example), restraints toward measures of supranational limitations increase, as it is often seen. This may also be one of the broader limitations of the frameworks discussed in this section. Major countries are already regulating their own activities and providing an

example for other national powers: once the United States, for example, passed national laws on space mining in 2015, Luxembourg and the United Arab Emirates declared that they would soon follow suit, and effectively did. Luxembourg's subsequent Draft Law on the Exploration and Use of Space Resources was explicit in ensuring ownership of space resources to companies who extract them (Jakhu & Pelton, 2017), as was the UAE's 2019 provision. As De Zwart (2021, p. 2) also observes, the five treaties' sequential readability is identical "in both date order and descending number of ratifications". At the time of the OST's drafting, the reality of mass commercial use of space was not considered to be an immediate one; it may be the case that this perception encouraged national governments' willingness to be subject to supranational constraints: when state interests are different and capabilities for concrete and profitable actions develop, multilateral discussion might become difficult, disturbing the effectiveness of consensus-based frameworks in creating binding norms, as pointed out in section 2 of this chapter. In this circumstance, there can be a degree of risk: nations might only negotiate broadly shared treaties only when caught by surprise in the case of a large-scale global crisis. As chapter 4 will further analyze, historical examples appear to indicate that regulatory change follows disruptive crises rather than preceding them.

Given that multilateral treaties represent only a part of binding legislation, which is complemented by bilateral outer space agreements between States, the second part of this section will briefly focus on the latter, with the historical and legal relationship between the United States and Japan as a case study.

As Moltz (2024) notes, that Japan's advanced launch capabilities were developed in direct partnership with the U.S ever since their economic recovery in the post-WW2 context, especially during the 50s and 60s. Economic prosperity encouraged Japan to start to invest in the development of its own space capabilities and to initiate a lasting and successful partnership with the United States, especially when it came to technological assistance for launch systems and rockets.

To these efforts corresponded the Treaty of Mutual Cooperation and Security (1960), more widely known as "Anpo", a more general legal security bilateral framework that provided mutual defense advantages, for example through Japan allowing the construction of U.S. military bases in its national territory. This

treaty substantially changed the relationship between the two countries and effectively made Japan one of the most important western allies in the Asian region (Pekkanen, 2024).

Anpo's relevance for this dissertation is related to the fact that, over the decades, its contents have organically included activities such as joint missile defense in 2003 and, more recently, in January 2023, when the United States extended Article V protections by explicitly referencing the possibility of attacks in outer space and adapting it to new contexts; Pekkanen (2024) also notes how there is still a degree of ambiguity that remains, noting it's important to possibly better define "what circumstances or cases in the space nexus would 'constitute an armed attack for the purposes of Article V of the US-Japan Security Treaty'" (p. 17).

Japan's role within this bilateral framework is only possible because of relevant changes to its domestic laws and constitutional approach: the two examples pointed out by Pekkanen (2024) are Japan's 2008 Basic Space law, redefining its outer space technology and asset placement approach as non-aggressive rather than outright "non-military", and the 2014 Cabinet Decision on Self-Defense, which recognized Japan's right to collective self-defense, enabling it to defend an attacked ally and providing justification for the application of Anpo's article V.

3.6. Soft Law Instruments and Governance Initiatives

As the latter section pointed out, increasing difficulty has been observed when it comes to concluding binding agreements at the international level. Current diplomatic and non-binding frameworks like the UNOOSA guidelines (2019) and the Artemis Accords (2020) can be regarded as "soft law" attempts to fill gaps without necessarily waiting for formal treaties. Because of current constraints, soft law has essentially become the main object of space-related lawmaking during the last thirty years: Moltz (2024), in his book *Crowded Orbits*, goes as far as stating how, ever since the 1970s, the only area with remarkable international progress leading to improved space governance has been the issue of orbital debris control, the legal instruments implicitly referenced being, respectively, the Inter-Agency Space Debris Coordination Committee (1993), a non-binding, intergovernmental forum established to improve monitoring efforts and coordinated action with regard to orbital debris, and the interlinked Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space (2007), approved fourteen years later and aimed at minimizing debris through more efficient disposal of waste, more transparent communication and overall reduction in the release of objects during normal operations (Wesel & Lambach, 2021). The guidelines were developed through the collaboration of COPUOS and the IADC, with successive UNGA approval.

It should be remarked that, given the Guidelines' non-binding nature, some of its provisions are not enforced globally (for example, a consistent percentage of satellites have not still been properly deorbited), a factor that, as Wesel and Lambach (2021) argue, caused fragmentation, creating "a multitude of individual sets of rules by states and private organizations (such as the ISO) and ambiguity within the space community" (p. 2).

Soft law instruments also include the UN COPUOS Guidelines for the Long-term Sustainability (LTS) of Outer Space Activities (2019), 21 guidelines that aim to illustrate the best practices regarding space sustainability, focusing mainly on risk mitigation and cooperative sharing of information with regard to space debris, satellite collisions and reciprocal interference between spacefaring actors (Martinez, 2021). The 21 Guidelines are broadly considered to be a remarkable

milestone when it comes to outer space normative cooperation; although they are (naturally) voluntary, there appears to be some political pressure to adhere, considering that virtually all major spacefaring nations have done so and are effectively in the process of working on respective national implementation. One limitation is that a few issues, most importantly mechanisms for space traffic management, were left for future discussion because of the lack of internal consensus among parties (Martinez, 2021).

The last soft law framework that this section is going to analyze are the Artemis Accords, a cooperative initiative of governance started by the United States Government in the context of their Artemis program, which aims to return astronauts on the moon for the first time since 1972 and, at the same time, establishing a continuous and sustained human presence on the celestial body (De Zwart, 2021). The Accords have currently been ratified by 55 countries across all continents, including most ESA members as well as India, Brazil, Japan, South Korea and Saudi Arabia among others.

The Artemis Accords are not a set of treaties and, thus, cannot be considered binding in accordance with international law. Nonetheless, they represent a political commitment on the part of their members. Concretely, the Accords explicitly reinforce and expand already existing obligations, mainly tied to issues of standard-setting and accountability, especially when it comes to public sharing of data and information. A new element, not taken into consideration by previous agreement, is the protection of what are called “heritage sites” of historical human activity in space and on celestial bodies (e.g., the Apollo landing sites); the Moon agreement is also practically rejected through the Accords’ stance on the extraction and utilization of space resources, considered both legitimate and consistent with the OST “with specific emphasis on Articles II, VI, and XI” (Artemis Accords, 2020), though they should be done with an intent to benefit all. Establishing safety zones to avoid harmful interference is also part of the Artemis Accords framework. The general significance of the Accords, which have attracted a certainly universal but somewhat broad coalition of States, for cooperation frameworks comes from a model that essentially rejects universal consensus in establishing norms for space activity (even beyond the exploration of the moon) in favor of a membership-based model. This may also constitute a weakness, according to different perspectives:

although Russia and China, who are not members and have failed to establish an alternative multi-member framework, working mainly through bilateral agreements (Cross & Pekkanen, 2023), their absence from the Artemis Agreements means not recognizing the safe zones already described. There is also disagreement on the idea of regulating space resource extraction and utilization: Russia has stated a need for utilizing space resources for strengthening State sovereignty (Liu, 2024). The Secure World Foundation (2022) on the nature of space as global commons (a theme that will be further explored in Chapter 7) also explores this issue: actors have disagreements on whether space should be governed as a shared resource or not; this discussion affects the implementation of soft law instruments on a global level. One weakness of soft-law frameworks is thus their potential for "regionalization" and fragmentation, with a consequence: several juxtapositional and unharmonized models might make it more difficult for a State (or otherwise actor) to decide which standards or model to prioritize or join. Soft-law initiatives like the Artemis Accords could arguably even constitute a limit to the management of a global-scale "black swan" event: competing and fragmented governance models could be ill-equipped to act and even raise issues related to miscalculation.

Accounting for unexpected crises, soft law instruments and guidelines arguably enjoy at least one strength: they can adapt more quickly to fast changes through more flexible updates of their respective contents. Weaknesses appear to come mainly from the absence of mandatory response mechanisms, which during a crisis could product national security-oriented behavior and in this context do not possess enforceability, and a difficulty in constraining rule-breaking actors if not by isolation mechanisms and diplomatic reactions, both non-preemptive methods. The idea that peer pressure is enough to ensure compliance appears to be relatively unfounded: one example is the ASAT test moratoria, which prohibited destructive tests being carried on satellites and has been broken by the United States in 2008 (Lauer, 2022). The current trajectory suggests soft law will continue to be one of the main instruments of reliance, possibly in combination with very specific and targeted binding agreements: as chapter 4 will point out in greater detail, this approach might contain several challenges.

4. CRISIS MANAGEMENT AND BLACK SWAN EVENTS IN SPACE

4.1. Preliminary Considerations

The analysis of relevant framework done thus far has observed that, although having proved themselves to be considerably useful in avoiding disruptive conflicts and maintaining cooperative behavior in outer space activities, they seem to show fragility and limitations: most founding treaties have been established in a very different era, both technologically and politically.

This chapter has the function of more concretely analyzing several of these perceived weaknesses by trying to understand how effectively they would respond to a sudden and high impact event. To define such an event, this dissertation takes into consideration the idea of the "black swan", used by Nassim Taleb (2007) to describe events that respond to three defining characteristics, namely: being unexpected (in the sense of "unaccounted for" if one is limited by the analysis of past events); having a disruptive, transformative impact of considerable dimension; lastly, being explainable in hindsight, after they have occurred. It is an event that effectively defies regular expectations, with the potential of rendering almost useless past data and experience. Therefore, analyzing governance through this lens makes it necessary to move beyond predictable risks. In defining "black swans" when talking about outer space crisis prevention policies, this dissertation tries to make a necessary distinction: most threats are more correctly identifiable as "grey swans", namely events that, while sharing the last two attributes of "black swans", possess some degree of conceivability, being "rare and consequential, but somewhat predictable, particularly to those who are prepared for them and have the tools to understand them" (Taleb, 2007, p. 37). At the same time, gray swans, while somewhat predictable, are characteristically underestimated in their probability of occurrence or its potential consequences. Several possible "grey swan" events include natural phenomena (for which real-world case studies, for example, the Carrington Storm of 1856, exist) or accidents of human origin such as the 2009 Iridium-Cosmos collision which served as an example of the dangers that may derive from space debris (Secure World Foundation, 2010). One of the clearest

examples of a potential black swan event in the space domain is a Near-Earth Object impact. As Dixon (2016) argues in her comprehensive post-graduate dissertation, a significant NEO impact fits all three criteria of Taleb's black swan theory: it is both statistically rare, potentially carries extreme consequences and would be explainable only in hindsight. Dixon (2016) also notes that while the international community has taken some steps, as of 2016, there was no coordinated response strategy in place, neither within the US nor at the international level. This chapter will try to identify and categorize different related factors and agents that might play a role in black or grey swan events in outer space, with some focus on the potential response of current mechanisms.

It is important to note why the issue of potential contact with extraterrestrial life or its discovery, although by any means categorizable as a black swan event, is effectively not referenced during the dissertation: any scientific analysis is grounded in empirical evidence, observable trends and data. While black swans are unpredictable, the conditions that might produce most of them (such as the militarization of space, the rise of private actors and the development of ASAT weapons and cyber-warfare) are often visible and referenceable in hindsight. On the other hand, there is no empirical, verifiable data on the existence, much less the potential nature and intentions of extraterrestrial life.

Currently, the one potential source for crisis that remains mostly manageable through political frameworks appears to be potentially human-made, and to be the increasing militarization of space and the rise of cyber-threats, especially satellite related; the most remarkable recent example lies in Russia's cyber-attacks on the KA-SAT GEO satellite network, providing, as the European Space Policy Institute observes, "concrete example of the use of cyber operations in complementarity with conventional military operations on land, sea, and air" (ESPI, 2022, p. 1). This aspect will be discussed in section 2 and, with specific reference to satellite and cyber-attacks, section 4.

Section 3, on the other hand, aims to analyze the role of emerging non-governmental actors from the private sectors and their role in crisis prevention (or escalation). Another ESPI report (2017) examines how space has been transformed and, at times, disrupted by the emergence of non-governmental actors in what has

historically always been a State-driven sector due to the lowering of historically high entry barriers for private companies. The recent tendencies toward more feasible commercial uses in this area has been commonly referenced to as "Newspace", defined as a mix of elements that come with the entry of these new actors and encompass, but are not limited to, increasing private investment, the rise of new space markets, the introduction of innovative industrial approaches in the sector, which might lead the way for disruption of existing systems (ESPI, 2017). This Chapter will, at the same time, make an effort to consider every element discussed within a comprehensive context and analyze how single emerging factors may interact with each other during crises. In particular, the following sections will analyze the primary domains through which such black swans might emerge, namely the unchecked militarization of space, the rise of private actors and the potential subsequent disruption and the weaponization of cyberspace.

4.2. The Militarization of Space

Some degree of military use of space has always been a reality, although excessive weaponization, as seen in Chapter 3, was initially limited by superpower restraint and legal provisions such as the ban of weapons of mass destruction in orbit (OST, 1967); that provision did not, on the other hand, prohibit the use of conventional weapons in space. In practice, States did not really take advantage of this possibility within the last decades; but it remained a possibility. The term "peaceful purposes", for example, was not strictly defined within the OST's text and left room for it to be practically interpreted as "non-aggressive" activities rather than an overall strict prohibition when it comes to prohibiting military assets in space (Aoki, 2024). As we will observe in section 4, this factor includes ramifications related to the use of antisatellite weapons (Lauer, 2022). By the late 20th century, military space systems had become essential for national security as an increasing number of national actors began to build counter-space capabilities for self-defense without adequate "catching up" from legal frameworks. The lack of explicit and clear legal limitations has, subsequently, generated an acceleration that only appeared to increase in more recent years.

Hammack (2021) also notes how international law, especially because of the absence of related binding agreements, has failed to put objective and universal limits on space weaponization, with absence of regulation or through not binding soft law instruments, leaving states unchecked in their pursue of military advantage in outer space. The result is a growing absence of equilibrium between the rapidity of strategic outer space developments and legal framework that was established decades ago, oftentimes not changed and appears to be dangerously static. Miscalculation, defined as "an incorrect assessment which, when applied to political and military affairs, can result in disproportionate acts of force or diplomacy out of defense and/or retaliation" (Hammack, 2021, p. 2), can have more severe consequences in the context of a weakly regulated legal framework.

As the Secure World Foundation (2024) highlights, space capabilities are becoming increasingly more instrumental in supporting and complementing conventional warfare; in earlier decades outer space capabilities have been important when it came to national security, but only more recently as a direct,

active support system for military operations. The Cold War's context mostly framed those as tools of relative deterrence: although counterspace systems were developed, they exercised restraint because of the fear of escalation, strictly interlinked with the respective nuclear arsenals of the two superpowers.

In the past three decades, however, the political context of outer space started to shift; as Del Canto Viterale (2023) put it, the bipolar framework that characterized space activities for the entirety of the Cold War has now evolved into a multipolar one involving, other than emerging national actors that develop their capabilities, "corporations, international organizations, higher-education institutions, and space hubs" (p. 18).

Space-based tools currently support a very important fraction of the logistics and technology behind military operations, in particular when considering high-precision targeting, communications and surveillance and navigation. As the Defence Intelligence Agency (2022) states in a report on space security, the United States have been used space systems in military operations for more than 30 years, allowing for more efficient conduct of activities but also making actors very dependent on potentially vulnerable assets. Rising space powers are also catching up on developing those same systems to "extend their capabilities and deny the US a space-based advantage" (p. IV).

Although satellite-related interference and related hostile activities will be analyzed more in depth in section 4, it is important to note that they do not encompass the entirety of the military and security aspect of space activities. In that regard, The United States formally recognized outer space as a potential conflict area and established a dedicated military branch, the U.S. Space Force, in 2019 (Toyoma, 2021).

China and Russia have also dramatically expanded their military space activities, creating specialized space forces of their own and including space operations into their respective national security strategies: in 2015, Russia re-created the Space Forces and China established the Strategic Support Force, a dedicated structure within the People's Liberation Army that encompasses, among others, both space and cyber warfare activities (Aoki, 2024). The two countries also grew their operational satellites by approximately 70% between 2019 and 2021

alone and drastically increased space investment in later years, with the perspective of considerable part of it being used for military purposes (Defense Intelligence Agency, 2022).

This trend can be observed as countries' defense concerns gradually become more linked with their respective space policies: one example is Japan's National Security Strategy (2022), with outer space being described as a central domain for defense purposes, being placed at the same level of cyber and maritime security. At the same time, the U.S. National Security Strategy (2022) reaffirmed space as critical infrastructure and defense territory, more deeply integrating space-security in technical cooperation with Japan itself as an established ally, also focusing on active threat recognitions and response. At the same time, the non-binding EU-Japan Strategic Partnership Agreement (2019) explicitly included cybersecurity and the protection of outer space assets in its contents. This was further substantiated by a European Parliament (2024) resolution which encouraged further EU-Japan collaboration on related themes.

Even regional governance frameworks which were established for peaceful and cooperative purposes are impacted to some degree by outer space militarization trends. APSCO is an example: Yan (2020) argues that the Organization's structure is "imbued with the notion of hierarchy under the leadership of China", and that "too much dependence on China has given rise to a concern that the independent role of APSCO might have been eroded" (p. 605). The ability of major powers in creating dependencies that could limit the autonomy of other members, from which the outer space sector is not excluded, might both allow for coercive measures and weaken unified responses to global crises.

Regional powers, India being one of the most important examples, also play a role: having mostly encouraged and defended the peaceful uses of outer space earlier on, India started to review its strategy, arguably because, at least in part, of other powers' activities and behavior. China's controversial ASAT test in 2007 might have been one of the reasons for which India felt compelled to show its own ASAT capability in a 2019 test (Secure World Foundation, 2024): Indian officials openly defined the test as an act of deterrence and argued that India risked finding itself unprepared for what was considered to be the inevitability of some form of

future military confrontation in outer space, seen as a direct consequence of the development of these weapons. This logic is emblematic of the classic concept of a security dilemma and shows how one state's securitarian measures may have the counterproductive effect of creating pressure, thus accelerating militarization and potentially increasing the risk for an escalation. As Townsend (2020, p. 18) notes, "lacking any independent external enforcement mechanism, nations often find themselves living in a state of mutual distrust" which appears to make spacefaring powers to be confronted by the choice of falling to "the temptation to adopt competitive security policies in space": Even as India continues, in principle, to be opposed to the "weaponization" of space it has clearly determined that not developing counterspace tools would, as a choice, maximize its vulnerability (Secure World Foundation, 2024).

According to Cross and Pekkanen (2023), the "dual-use" nature of most space technology, which can be defined as the ability of many space objects adopted for civilian purposes to be reused for military ones, creates greater ambiguity when it comes to peaceful use and behavior that can constitute a security challenge. In "Crowded Orbits", Moltz (2024) makes a point of addressing this same phenomenon by referring to the case of the Aegis BMD system, which, while not primarily constructed for military purposes, was employed to destroy an out-of-use satellite in 2008. Another one, laid out by a Secure World Foundation report (2024) on counter-space capabilities, is that of satellites capable of performing Rendezvous and Proximity Operations (RPO): these abilities are essential also when it comes to peaceful purposes such as debris removal, but possess considerable potential for intelligence operation and military attacks. One case examined is that of the United States' Geosynchronous Space Situational Awareness Program (GSSAP), an operational inspection system. Between 2016 and 2022, GSSAP observed more than a dozen operational satellites, which also included military ones belonging to Russia and China: China's TJS-1 and Russia's Luch satellite were approached respectively within 10 and 15 km (Secure World Foundation, 2024). Russia, in turn, has made a point of showing its own RPO capabilities. After the launch in 2019 of its Cosmos 2543 satellite, it appeared to be strategically positioned in a synchronized orbit that allowed it to periodically observe another satellite, USA 245, at between 150 to 300 km exactly from the satellite while it is under sunlight.

Another example is the Russia's Luch (Olymp) satellite, which was continuously placed near the orbit of several other satellites, both military and commercial, and whose behavior was consistent with intelligence collection (Secure World Foundation, 2024).

The increasing militarization of space is also a manifestation of more complex dynamics related to international competition. Aliberti, Cappella, and Hrozensky (2019) provide a useful framework for understanding this phenomenon through their concept of "space power", which they divide in two categories: capacity (ability to actively plan and enact space strategies) and autonomy (the ability to act without external constraints). From this perspective, the development of counter-space capabilities can be seen as a State's attempt to both ensure and reinforce defense capabilities and projecting its status as a spacefaring nation (Aliberti et al., 2019)

This great power focus on space has effectively launched what some analysts already consider to be a new space race characterized by the intersection of rule-making efforts and technological competition (Cross & Pekkanen, 2023). The main example of rule-making efforts is represented by the UN framework, previously referenced in chapter 3: since 1985 the United Nations Conference on Disarmament (CD) has had on its agenda an item titled Prevention of an Arms Race in Outer Space (PAROS), but negotiations have thus far led to nowhere (Hitchens, 2010). The result is that, as of today, there is no universally recognized legal instrument that prohibits the development, testing or use of weapons as a general category in space. China and Russia have also tried to push a draft treaty: the PPWT (Proposed Treaty on the Prevention of the Placement of Weapons in Outer Space). The proposed treaty would, if enforced, effectively ban weapons placement in outer space and the general use of military force toward space objects. They formally introduced a version of this treaty in 2008; Russia, especially, has argued that only binding prohibitions and enforceable provisions that explicitly limit the outer space arms race could be successful in ensuring national security at a global scale (Hitchens, 2010).

The U.S, as of now, together with other several countries, disagrees with several treaty provisions: namely, the fact that it does not account for some ground-

launched objects and, most importantly, that it is very difficult to nearly impossible to consistently define or verify what a ban on "space weapons" would constitute, preferring not to be bound to new legal norms and effectively blocking arms control provisions in the CD forum (Meyer, 2016).

Efforts aimed at voluntary demilitarization have also struggled. The European Union drafted an international Code of Conduct for Outer Space Activities in the 2010s, aiming to get states to voluntarily adopt rules of responsible behavior which included conducting tests with the potential of generating debris. But the Code effectively failed because of its lack of broad approval, mostly given the concerns from major powers about its overall implications (Meyer, 2016). The failure of these initiatives, which included a notion of "no first placement" of space weapons, represents a step back in cooperative space security diplomacy and, arguably, another toward a zero-sum, securitarian framework.

This arguably constitutes an inversion of tendency after a briefly hopeful period earlier in the 2010s decade: in 2013, a UN Group of Governmental Experts (GGE) had produced a report in which it recommended Transparency and Confidence-Building Measures (TCBMs) for space, widely seen as a step for threat reduction which leaned on a more cooperative framework (Meyer, 2016). Unfortunately, the implementation of those measures appeared to be blocked by international tensions, most importantly the deteriorating relations between the United States and both Russia and China: the 2014 annexation of Crimea by Russia, which was followed by western sanctions, led to Russia's decreased engagement within space-related forums (Meyer, 2016). US-Russia strain was only intensified after the invasion of Ukraine, which escalated the conflict to another level and, as pointed out in Chapter 3 when referencing Russia's involvement in the ISS, further complicated the issue. Russia also blocked a U.S.–Japan resolution (USUN, 2024) which, not in contrast with existing provisions, asked a ban on WMD in space; Russia justified its decision by accusing the resolution of being a "politically motivated" tactic by the U.S. At the same time, the competition between the United States and China intensified over trade imbalances, the Taiwan issue, cyber-espionage allegations and military and commercial clashes of interests. The institutional mechanisms appear unable to properly adapt to current developments, an issue that is not only limited to nuclear weapons and ASAT tests: COPUOS

remains focused on civil and scientific technical cooperation and avoids military and security issues; the International Telecommunication Union (ITU) regulates the technical aspects but not the competitive ones that arise from the former.

NATO has started to comprehensively take into consideration space security in the elaboration of its policies through its "Overarching Space Policy", declaring outer space as an "operational domain" in 2019 and coordinating the Alliance's own use of it (NATO, 2019). The European Union also released its Space Strategy for Security and Defence (European Parliament, 2023), confronting the perspectives of future threats. These developments show that although major powers and the corresponding regional alliances are reacting to a changed context, global governance remains a step behind. As things stand, outer space actors are pursuing non-universal interests and developing advanced military capabilities through existing law largely permitting it, possibly under the hope that mutual deterrence will be enough to pre-emptively negate disastrous outcomes.

Those hopes notwithstanding, it is difficult to deny how space militarization could carry potential severe risks: one consists in the increasing probability of miscalculation or accidental conflict within a more crowded outer space. Earth is orbited, as it is known, not only by active satellites but also by debris pieces that move at high speeds: if one of the latter collides with one of the former, especially if it is a critical satellite, it could be misinterpreted for hostile action; the lack of clear communication channels and transparency in space operations today leaves room for dangerous misperceptions, momentarily transforming what was in fact a random technical malfunction or a micrometeoroid strike into an enemy strike (Hammack, 2021). The orbital security dilemma posed by Townsend (2020) could play the role of a risk multiplier for black swan events: a misinterpreted but otherwise not relevant accident could turn into conflict if a governance framework lacks pre-agreed de-escalation mechanisms for these events. The 2009 collision between an out-of-function Russian satellite and a commercial Iridium satellite constitutes a real case scenario: the hypervelocity impact (the satellites were traveling at approximately 27000 km/h of combined speed) between the Iridium 33 communications satellite and the Russian military one Cosmos 2251 happened approximately 789 kilometers above Siberia and was effectively the first accidental collision between two intact satellites in earth's orbit (Secure World Foundation,

2010). The two satellites were destroyed and generated an enormous cloud of orbital debris. Iridium 33, 560 kilograms, was part of the active Iridium constellation. Cosmos 2251, a Strela-class military satellite which was launched by the Russian Federation in 1993, stopped functioning around 1995 and its position and movements were not precisely monitored.

Initial tracking networks catalogued more than 1800 objects larger than ten centimeters (Secure World Foundation, 2010). The U.S. Space Surveillance Network recorded approximately 1632 traceable fragments by the end of that year, an estimate that increased to 2000 in later years. A part of Cosmos 2251's debris fragments arrived at higher orbits during the explosion and thus persisted much longer than expected (Secure World Foundation, 2010). 15 years after the accident more than a thousand pieces of debris continue to endanger other satellites, and many of these are expected to orbit the Earth for several decades.

One important takeaway is that space situational awareness (SSA) systems for interpreting related data and making forecasts were not reliable and did not prevent the collision: neither the U.S. nor Russian military issued pre-collision alerts, despite both having accurate orbital tracking data (Secure World Foundation, 2010). The omission was effectively caused by not prioritizing the event: the U.S. Joint Space Operations Center had been warning Iridium since 2007 but had later stopped doing so because of the burden associated with those operations burden. Iridium 33 and Cosmos 2251 were also not included in periodical safety assessments that estimate collision probability between objects in outer space. These assessments, as the report notes, are based on analysis that rely on statistical models. In critical situations that involve active satellites, they might rely on "a collision avoidance maneuver (...) which could shorten its useable lifespan and result in a financial cost (...) conducting the maneuver could disrupt service to users" (Secure World Foundation, 2010, p. 3). It can be argued that the very consequences of these maneuvers could constitute a disincentive for fast reactions.

Because of the Iridium-Cosmos collision, the U.S. military subsequently expanded its screenings to the entire Iridium constellation and eventually all active satellites in orbit; if two objects are at risk of collision, warnings are now provided with 72 hours of advance "within 1 km for LEO and 5 km for Geostationary Earth

Orbit (GEO)". (Secure World Foundation, 2010, p. 3). Complementarily, the Space Situational Awareness Sharing initiative, under U.S. Strategic Command, was launched for more effective data exchange at the international level.

The Iridium-Cosmos collision also remains "trapped" inside a legally uncertain zone in international space law. The Outer Space Treaty (1967) and the Liability Convention (1972)'s definitions of "fault" and "responsibility" in space appear to be lacking: Russia was the launching State for Cosmos 2251, but at the same time Iridium 33's status was unclear as the satellite was not registered, which was not in compliance with the Registration Convention (1974), a situation which made it difficult to identify its own launching State. The Liability Convention, in the end, did not have a role as the incident was solved, like all other similar instances, through diplomatic channels; this aspect might strengthen the critical claim that the Convention is virtually unaccounted for when real cases occur and has little to no utility. The 2009 Iridium-Cosmos collision could overall be classified as a "grey swan". Nonetheless, the inability to prevent a predictable collision arguably leaves space assets even more vulnerable to a black swan-level attack or disruption.

The prospect of a war of massive proportions in space has the potential of disrupting orbit use for all parties, whether involved or not, and could arguably represent and be framed as a "black swan" scenario to be avoided at all costs. Another risk is the strategic instability that comes from offense-defense asymmetry in space, one example being that, as of now, protecting a satellite comes at a far greater economic cost of destroying one: offensive technologies are becoming more effective and economical at a faster pace than defensive ones (Secure World Foundation, 2022). This asymmetry might also reinforce arms races as outer space powers start to fear for their space infrastructure in the prospect of future conflicts: distrust and assumptions of bad faith could unnecessarily make an otherwise resolvable situation escalate into a crisis.

It can be concluded from previous observations that the militarization of space outpaces universal managing mechanisms as countries incorporate outer space into their defensive plans and, most importantly, increase their related investments. Existing outer space law is not preventing weaponization; many

experts argue that the international community should develop de-escalation measures to prevent a military confrontation (Hammack, 2021; Meyer, 2016). The main existing issues concern mainly the creation of a balance between national sovereignty and security and, on the other hand, the collective responsibility of the international community toward avoiding the shift from strategic competition into active conflicts and crises; such a balance might also benefit from cooperation and reinforced communication between the diplomatic, normative and technical actors and spheres. As Kofler et al (2018) point out through the examples of planetary defence mechanisms such as the IAWN (International Asteroid Warning Network) and SMPAG (Space Mission Planning Advisory Group), which are coordinated under UN COPUOS to prevent and manage potential asteroid threats, and are in fact characterized by multi-disciplinary cooperation, not all security responses and policies in the outer space context necessarily involve militarization. Rather than assuming the superiority of one mechanism over another, it can be argued that the coexistence of both military and, if effective, non-military crisis response strategies is necessary for the establishment of a more comprehensive framework which could further compartmentalizing defence related assets as instruments of last resort.

4.3. The Role of Private Actors

In the traditional Cold War era framework, states were effectively a monopolistic power when it came to space activities, exercising their control through centralized space agencies and negotiating among themselves through formal and informal legal and diplomatic instruments. Especially in recent years, this has changed: private and commercial actors have become important players in outer space, with an increasing ability to shape outer space governance and operations. Private actors' role in outer space is another potential source for black swan events: as will be seen in this Chapter, technical or commercial failures on the part of a private entity can have mass-scale consequences for regional or global services, especially in war-time context. Government-centric systems that do not take into account contemporary developments would be essentially limited in their management of crises. Some experts have discussed the topic at length: Del Canto Viterale (2023), for example, argues that the 21st century represents a new phase that is characterized by a "New Space" paradigm, with an important role on the part of commercial enterprises assuming relevance in domains that up until recently were exclusively managed by governments. The "NewSpace" concept has also been discussed within the European Space Policy Institute (2017) report on the rise of private space actors in the space sector. Beaumier et al. (2024), which were referenced when analyzing the ESA framework, observe that governance systems tend to grow in complexity and heterogeneity when new actors, including private firms, acquire relevance and challenge the traditional models of state-centric diplomatic cooperation. Martinez, L. (2021) argues how technological advancements in outer space are transforming systemic power relations among more and more heterogeneous actors, trying to establish a framework to assess whether international behavior in space is shaped more by top-down systemic power structures or bottom-up agency. Current developments, overall, suggest that any analysis of space crisis management must take into much greater consideration than before the influence and interests of private entities along with those of States.

Quantitatively, the impact of private actors on the space domain is at an all-time high. The global space economy, as Lauer (2022) reports, has grown to over $350 billion USD, with the prospect of reaching $1 trillion or more by 2040. Private

investment in space enterprises amounted to 10 billion in 2021 alone (Del Canto Viterale, 2023). At the same time, according to Fleck (2022), space startups have received investments of approximately $265 billion dollars between 2014 and 2022, 80% of which divided exclusively between companies from the United States (50%) and China (30%), with the remainder being distributed across Europe, India and Japan. Other than in investments, the United States currently holds a distinct quantitative lead in number of space enterprises: over 5500 private space companies operate within their jurisdiction, almost 10 times those of the second country, the United Kingdom, which is home to less than 700 (Del Canto Viterale, 2023). Much of this private growth is thus being driven by commercial investments and activities; as of today, many space sector markets appear to be in the hands of very few actors. One example is that of private satellites. In 2022, "the satellites from only two commercial operators, SpaceX and OneWeb, accounted for almost half of all operational satellites in orbit" (OECD, 2022, p. 2). The report also notes how Starlink, a satellite mega-constellation owned by SpaceX, came to effectively dominate broadband services. ESPI (2017) does not put these developments in an entirely positive light: it describes NewSpace as a "disruptive, commercially-driven, approach to space" (p. 1) in which private actors are able to pursue space business with decreasing oversight or authority on the part of governments.

While being the two most important hubs for the private space industry, China and the United States certainly use two different approaches when it comes to outer space technological and security innovation, a notion that carries considerable implications for their future respective development and, more generally, competition between the two, as Tai and Fukushima (2024) point out.

According to the two authors, the United States has increasingly adopted what define a "bottom-up" approach that views private actors as primarily important when it comes to innovating and raising capital for technological development in the outer space domain: in encouraging start-ups and cooperating with those actors, the Department of Defense (DoD) and the National Reconnaissance Office (NRO) play a considerably important role through the creation of entities like the Defense Innovation Unit (DIU) and the Space Development Agency (SDA). Civil-military integration with private actors is implemented cooperatively, through partnerships, with the idea of taking advantage

of companies' capacity for innovation. The approach is, overall, that of remaining a step behind, as "the government and defense sector appears content to be a fast follower" (Tai & Fukushima, 2024, p. 17).

China's own private environment appears in contrast to be characterized by a top-down model: two powerful State-controlled corporations, China Aerospace Science and Technology Corporation (CASC) and China Aerospace Science and Industry Corporation (CASIC), effectively control a vast amount of outer space-related activities when it comes to research and development (Tai & Fukushima, 2024). Most private capital movements are related to the Military-Civil Fusion (MCF), a national strategy that allows and encourages private actors to take advantage of State-owned resources and technology. In this sense, the most marked difference is that the Chinese NewSpace sector, still not as developed as the United States', functions within a framework that sees companies contributing to national objectives but with a greater portion of oversight and control on the part of the Chinese government (Tai & Fukushima, 2024). China also serves as both the host country and most developed partner of APSCO, which, as of 2025, counts eight full members and includes Bangladesh, Iran, Mongolia, Pakistan, Peru, Thailand and Turkey. In this context, with countries such as Bangladesh and Mongolia which struggle with local production of space objects, the role of private actors diverges substantially (Yan, 2020). Rather than pursuing innovation through profit-driven dynamics, companies (especially in least developed States) predominantly benefit from technology transfers from China and contribute to governmental initiatives mainly aimed at obtaining basic space access and capabilities.

While China and the United States are without doubt dominant actors, it would be a mistake not to consider other powers and their distinctive approaches: for example, another important point in the previously referenced ESPI report (2017) lies in analyzing the differences between the US and European private space ecosystems; the latter's disadvantage appears motivated by factors such as a smaller investment base, socio-cultural factors such as a reduced propensity to entrepreneurship and "delayed initiatives to foster entrepreneurship and/or leveraging a more prominent role of private actors" (p. 6). The last finding is that of increased fragmentation within the european market and an overall reduced demand: although the concept of few large industries owning most of a market

might cause concern for monopolistic behavior, at the same time those industries could possess enough capital for more significant investments. These issues notwithstanding, the European Union did, up to some degree, try to fill certain voids: one example is its acknowledgment that "a lot of innovation in the space field is driven by the private sector nowadays" (European Parliament, 2023, p. 8), and launch of initiatives like CASSINI, a program for investments aimed at supporting space start-ups and technologies with dual-use potential. Governments and organizations have, thus, overall reacted to this development through aiming to increase private sector growth and its integration within their policy agendas: going back to the United States, it can be noted that NASA, for example, established significant public–private partnerships during the 2010s decade, providing public funding and support for spaceflight capacities to companies like SpaceX and Boeing (Del Canto Viterale, 2023) or, even earlier, through its 2006 Commercial Orbital Transportation Services (COTS) programme, cooperating with and incentivizing private actors to produce vehicles that could be able to provide the ISS with transportation services (ESPI, 2017). Yet another case concerns how the Artemis Accords, as briefly referenced in Chapter 3, include within their framework the potential for utilizing space resources toward commercial purposes, a characteristic that aims to encourage and satisfy private actors and their expectations. These measures indicate how governments (or, more generally, public actors and frameworks) are trying to establish partnerships between heterogeneous actors to ensure success in common objectives: without input from industry, governmental actors would find it harder to keep up with technological advances.

At the same time, without oversight, companies risk misalignment with global public interests. For this and other reasons, governments may also need to regulate, up to an extent, private sector activities: its recent assessment, DIA (2022) has also taken into consideration commercial activities in outer space, noting also their role in producing a "growth of orbital objects" that will need to be managed through more precise monitoring to avoid collisions. Scholars like Cross and Pekkanen (2023) have also noted that, if not properly managed, private companies or individuals' tendency to prioritize their own objectives might seriously damage all areas of space cooperation.

The growing role of private entities in conflicts has been particularly evident in the context of the Russo-Ukrainian war. During the invasion of Ukraine, which began in 2022 and, as of 2025, is currently ongoing, government and military forces were effectively dependent on private satellite services for military uses that ranged from communication to intelligence and surveillance: since the initial phase of the war, SpaceX's Starlink constellation was used to guarantee continuous connection throughout Ukraine (OECD, 2022): the company sent thousands of Starlink user terminals funded by private donors and allied governments to Ukraine with the explicit aim to stop Russian efforts to block Ukrainian forces from internet access. Starlink proved to be remarkably effective and enabled Ukrainians to stay connected with the outside world and resist to Moscow's assaults on relevant infrastructure.

The Ukrainian war efforts on the part of the private sector were not limited to SpaceX and Starlink: small satellites operated by the U.S. firm HawkEye 360 and primarily used for commercial imaging, for example, helped detect Russian electronic warfare units through the geo-localization of GPS jamming signal (another example of dual-use technologies); private Earth-observation companies (Maxar, Planet, ICEYE) assisted by supplying high-resolution images that was not only helpful in revealing troop movements but also documented Russian war atrocities in real time; not only US-based actors played a role: for instance, Canada's MDA (a private company specialized in satellite systems and space operation) was instrumental in providing radar satellite images to Ukrainian forces, and the European Union helped the coordinated sharing of both commercial and classified imagery with military awareness purposes (OECD, 2022).

To a certain extent, large private entities have played a role that can be considered similar to those of spy agencies or defense contractors. The result, as the OECD (2022) observes, is that they have proven effective in wartime context by offering services that governments alone had issues supplying. This observation might also carry one potential downside: such a role was played while private entities maintained a considerable degree of relative independence and global agency. In the case of Ukraine and SpaceX, national forces became dependent on a system controlled by a private entity that was outside their control (and, to a certain extent, was not managed by governmental actors): a private agent could,

potentially, stop providing such services during emergency situations as a result of a cost-benefit analysis rather than because of national policy decisions on the part of elected representatives. Vulnerabilities may also not arise just because of active intents but due to a single private actor's dominance in a sector: if a system, service or technology with less to no competitors suddenly malfunctions, there might be problems or delays in replacing the functions it provides, as is expanded on in section 4. Some examples of low-probability, high-impact events pertaining to outer space security could thus be the unexpected dismissal of a crucial commercial service, like a satellite constellation software failure, or interruption of important private activities such as those undertaken by launch providers. The OECD (2022) report has also warned that private ownership of important, dependable space assets has the potential for unexpected consequences for national security and interests.

Taleb (2007) describes how contemporary complex systems are particularly subject to such unpredictable shocks due to "aggressive ignorance" of interdependency and the "misunderstanding of the causal chains between policy and actions" (2007): if current policy frameworks do not continuously keep accounting for private actors' growing role, the hypothetical events described would by exact definition count as "black swans", as they would also be underrepresented and underestimated. The lack of direct accountability for private firms in the context of international law means that an actor who is not even a party to relevant treaties could play a fundamental role in the start of a crisis, with all the dangers involved.

The outer space private market, in that regard, can certainly be defined as a complex system with three characteristics: an increasing number of privately owned space assets and objects; the ambiguities that derive from military and civilian dual-use; an absence of a universal and comprehensive regulatory system for commercial operations and behavior. In this sense, it can be argued that institutional "globalization", understood as the existence and solidification of shared standards that regulate economic competition and coexistence also among private actors, cannot as of now be fully applied to outer space activities.

However, it should be noted that although the phenomenon of private actors presents several challenges to space governance as it currently exists, it also offers

solutions. Townsend (2020), for example, argues in his book that commercialization could serve as a potential solution to his "orbital security dilemma", reassuring militarized space powers through private actors' very own functioning and structure: through shifting the provision of services like satellite communications shifts from national systems and classified frameworks to transparent platforms with market purposes, a State can manifest peaceful intents to other governmental actors and encourage the creation of a "positive sum" environment. Further proposals for cross-integration between the public and private sectors, as well as private actors' potential role in the future of space governance, will be discussed in Chapters 6 and 7.

4.4. Cyber-Warfare and Satellite Attacks

The growing reliance on space infrastructure for dual-use needs has potentially made satellites and their support systems primary targets for both cyber-warfare and physical attacks. NATO, for example, strongly depends on its own member states through their space assets to support operations of various nature: this means that a vulnerability in a single strategic satellite can cause consequences across multiple sectors and that an ASAT attack or, less directly, any operation able to disable satellite capabilities can impair decision-making, precision targeting, intelligence and even basic communication purposes (Unal, 2019).

The implication of current space systems being inextricably linked with digital ones is that their compromise is particularly disruptive in terms of military and strategic consequences. For example, the ViaSat incident, which constitutes the main case study for this section when it comes to cyber-attacks, appeared to demonstrate how informatic operations against satellites can be successfully integrated in military efforts, effectively putting together physical and digital warfare (ESPI, 2022).

While cyber-attacks represent a more sophisticated threat with potentially less margin for attribution, ASAT weapons, on the other hand, are both more identifiable, more direct and generally more physically destructive to space assets. The testing and potential use of these weapons, which destroy targets through impact, represents one of the most visible aspects of space militarization (Lauer, 2022; Secure World Foundation, 2024).

This section examines the dynamics of attacks targeting both satellites and their infrastructure, especially when considering the technical vectors and methods used in cyber-attacks, to historical cases related to the deployment of traditional anti-satellite (ASAT) weapons.

Cyber-attacks, which constitute the first topic of analysis, are characterized by three important aspects: their speed, their ability to cause damage often without preventive warnings and their difficulty in attribution, all aspects that complicate responses and increase miscalculation risks in a crisis (Unal, 2019); in essence, as the author also points out, if military planners are unable to rely on the integrity and

functionality of their satellites because of cyber-related threats, there is potential for increased confusion and reduced deterrence abilities.

They are also well distinct from, although sometimes complementary to, electromagnetic warfare, which aims to damage the hardware, rather than the software, of a satellite through attacks such as spoofing (attacking sensors or receivers) and jamming (which disturbs radio signals), causing considerable damage (IAI, 2023). The concept of "blended" attacks, which combines electronic jamming with cyber intrusions has widely been considered and implemented in military plans (Secure World Foundation, 2024)

All major spacefaring powers today either possess or are in the process of actively developing more advanced cyber-attack software and capabilities that could be used as offensive instruments toward other space systems. The United States, Russia, China and several other countries possess well-funded cyber programs and there is little doubt they will continue to invest resources aimed at expanding these capabilities for outer space use (Secure World Foundation, 2024): in fact, as the report points out, a former senior military official listed cyber-threats as the greatest danger when it comes to satellites, ranking them even above anti-satellite weapons.

Nations like Russia and China also appear to consider cyber-attacks against satellites as tools for asymmetric warfare, aimed at obstructing Western technological advantages in space: U.S. intelligence assessments have stated that these rivals are pursuing a full range of counter-space capabilities, focusing in particular on cyber and electronic attacks, which do not necessarily cause debris issue and have greater potential for plausible deniability, rather than traditional ASAT weapons (Secure World Foundation, 2024). Unlike ASATs, not every cyber-attack is strictly and outrightly destructive: one example, which comes from a leaked 2023 CIA document, is that of China supposedly building advanced tools capable of gaining control of enemy satellites (Secure World Foundation, 2024).

Russia, for its part, might have demonstrated a willingness to use cyber-attacks in warfare even before the Viasat incident, in which an attack from Russian hackers made thousands of KA-SAT terminals in Ukraine and across Europe ineffective (ESPI, 2022). In 1998, in what, if confirmed, would be one of the earliest

publicly known related attack, Russia allegedly took control of the German-U.S. ROSAT scientific satellite and, by aimed its solar panels incorrectly, permanently damaged the satellite's sensors (Secure World Foundation, 2024). NATO appears to take into serious consideration the potential for a satellite cyber-attack; there is little doubt that, if serious enough, a cyberattack could trigger Article 5's collective self-defense provision (Unal, 2019).

The cyberspace domain is also characterized by a lower threshold for access on the part of non-governmental actors such as organized groups of hackers and "hacktivists"; this is also due to increasingly lower costs for these operations. The Secure World Foundation (2024) provides several examples, such as the "Thrip" infiltration, in which the homonymous group of Chinese hackers managed to gain access to a communications company's systems with the goal of controlling its satellites, or the 14 hours shutdown of the network of Dozor-Teleport, a Russian satellite communications provider, caused by a cyber-attack for which both the Wagner group and a hacktivist collective have taken credit for. While non-state actors are not currently able to permanently disable satellites on their own due to lack of resources, these activities and reduced costs for operations appear to suggest a risk trend that appears worth considering. Cyber-attacks against satellite systems can occur through several vectors and usually require four elements: access to the system, the detection of a vulnerability, the execution of a malicious payload (malwares, for example, or an exploit script), and a command-and-control systems for the execution of the attack (Secure World Foundation, 2024).

Several types of satellite attacks are possible and listed, with relevant examples, in the SWF report (2024). Supply-chain attacks, in which a satellite is launched with already existing malware or using encryption which a rival State already knows how to break; ground segment intrusions, in which hackers access a satellite's centers of command and control; the most destructive type, which is also considered more difficult to enact, is an attack to the on-orbit systems of a launched satellite, of which if proven the previously mentioned ROSAT infiltration would be an example.

The 2022 KA-Sat attack, in particular, represented what the SFW report (2024) calls a "user segment, downlink" attack, in which the main target was "one

single consumer-oriented partition of the KA-SAT network, which is owned by the U.S. company Viasat" (ESPI, 2022, p. 5) and counted Ukrainian military and government agencies among those who utilized the service.

The attack was conducted and divided in two phases (ESPI, 2022): first, internet modems used by the Ukrainian government were targeted by a DoS attack (which, essentially, is a malicious effort to overload a system with internet traffic, thus making it non-accessible for users); once the modems were targeted, the attacker managed to gain access to a management segment of the SAT network and thus execute AcidRain, a malware which wiped the hardware of targeted modems and disconnected them from the network; access to the network was supposedly gained through "a misconfiguration of a Virtual Private Network (VPN) appliance" (p. 5), which is used to manage and secure a network's connections. Such an attack had enormous concrete repercussions: minutes after, approximately 30000 terminals in Ukraine and at least 5800 in other European countries were disabled; this included not only military terminals but also civil ones that supported wind farms (such as in Germany, where more than 5000 wind turbines lost remote monitoring), internet service providers and police communications in other European countries (Secure World Foundation, 2024).

The attack and its aftermath caused severe logistical issues, with Ukraine needing an immediate alternative for satellite communications, which was ultimately found in SpaceX's Starlink; Russia soon attempted to jam and cyber-attack the Starlink system as well. In May and June 2022, there were complaints on Russia's part about Starlink's role, and by November 2022 the pro-Russian hacker group "Killnet" claimed to have launched other cyberattacks of similar type against its infrastructure, though they were overall largely unsuccessful due to SpaceX's focus on cybersecurity (Secure World Foundation).

Because of their listed characteristics such as their unpredictability and speed, satellite cyber-attacks might be categorized as "black swans"; at the same time, given these repercussions on strictly unrelated objects, cyber-attacks tend to raise questions related to the application of sovereignty and national boundaries: France, for example, views even indirect and unintended consequences of a cyber-attack on its territory as a potential violation of its sovereignty; Germany, on the

other hand, has more restrictive requirements when it comes to defining similar operations as violations and, in the case of the KA-Sat attack, considered the damage indirect and temporary and, thus, not reaching the required “threshold” (ESPI, 2022).

The advent of cyber warfare in space also forces a reevaluation of how to respond to space incidents and find solutions for crises through pre-emptive measures: a proposal, for example, consists of cybersecurity certification for satellites, similar to vehicle-related ones, which might reassure customers and provide additional security, as established protocols are still somewhat lacking (ESPI, 2022). Another important development is the European Commission’s renewed interest in cybersecurity through innovative solutions: one example is that of its intention to “integrate the EU secure connectivity initiative into the EuroQCI initiative and develop Quantum Key Distribution (QKD)” (ESPI, 2022, p. 18), which is going to be analyzed more in depth in Chapter 5. Both NATO and the EU, through NATO’s strategic posture and the EU's 2023 Space Strategy for Security and Defence, aim to respond to developments through better coordination of their respective space assets (IAI, 2023).

Another remarkable initiative lies in “Space Cyber Wargames” between allied nations, with exercises that simulate attack scenarios on satellite systems in a controlled environment. Two examples are NATO’s Multi-Domain Space Deterrence Framework 2024 wargame in the Netherlands and the UK’s ‘Space Warrior’ series, which integrates space into traditional defence wargames to improve European states’ cooperation (ESPI, 2025).

Further shifts have been observed when analyzing space powers’ military doctrines and respective strategies, which focus specifically on two aspects: deterrence and damage reduction. In the case of cyber assets, deterrence by punishment (threatening retaliatory action) is generally considered more applicable than deterrence by denial (which aims to deter by making a possible enemy operation cost more than the potential benefits it could generate), although issues with attributability also create challenges the former (IAI, 2023). Given that completely preventing every single cyber-attack is unrealistic, militaries are investing in ways to minimize their catastrophic consequences: the focus is in

redundancy rather than absolute preventive measures for all satellites, which means ensuring that even if one space asset is compromised, sufficiently diversified others would be able to compensate (Unal, 2019),

If on one hand cyber-attacks represent silent threats, on the other the development and testing of ASATs directly show a nation's ability to hold rival outer space assets at risk and, at the same time, prepare military forces for the potential extension of a conflict into space (Lauer, 2022). Currently, four nations have already successfully enacted destructive ASAT tests: the United States, Russia, the People's Republic of China and India, with motivations and reasons that encompass aspects from the projection of resourcefulness or national status to outright military deterrence.

Both the United States and Russia (and, before, the Soviet Union) have a long history of ASAT research which dates to the Cold War era; The Soviet Union pioneered the world's first operational ASAT system, the Istrebitel Sputnikov (IS), which was tested several times from 1968 to 1982 and created significant debris; on the other hand, the most well-known early destructive test on the part of the United States occurred in 1985, when an F-15 fighter jet launched an ASM-135 missile that successfully destroyed the Solwind P78-1 satellite and created 285 pieces of orbital debris in the process (Secure World Foundation, 2024). More recently, after a long period characterized by “voluntary moratoria”, ASAT testing started reoccurring (Lauer, 2022); in that sense, China's 2007 ASAT test is widely considered to be a turning point for space security. Using an SC-19 ballistic missile, China destroyed its Fengyun-1C weather satellite at 865 km altitude, an event that was a source of international shock (Hammack, 2021).

The test, although being a technical success, managed to create the largest and most persistent debris field in history, with over 3500 fragments representing an increase in danger to all space assets. The test was seen as both a strategic response to the space dominance of the United States and China’s will to show itself as a space power, which, especially in the United States, "hardened the attitudes of those in national security policy-making circles arguing for 'space control' programs" (Hitchens, 2010, p. 15).

In 2008, a year later, the U.S. conducted Operation Burnt Frost, using a ship-launched SM-3 missile defense interceptor to destroy a malfunctioning satellite, USA-193. Although this operation was initially justified as a risk containing measure due to the satellite's technical issues, the operation was most likely conducted as an ASAT capability demonstration, especially given the timeframe of events (Lauer, 2022).

In recent years, ASAT-test conducting nations have further increased in number: in 2019, India conducted "Mission Shakti," its first successful test. An interceptor missile, a derivative of its Prithvi Defence Vehicle (PDV) MK-II, was launched from the Abdul Kalam Island launch complex and destroyed India's Microsat-R satellite at approximately 300 km altitude (Secure World Foundation, 2024). Indian officials justified the test as a deterrence act which was pursued in order to safeguard its space assets and responding to regional developments and challenges, especially concerning China (Lauer, 2022). To minimize international criticism India further argued that, given the comparatively low altitude, the resulting debris would de-orbit within weeks or months.

Lastly, after decades of abstaining from destructive tests, in 2021 Russia destroyed the inactive Soviet-era satellite Cosmos 1408, an operation which produced 1800 pieces of debris in a consistently used orbital area, having the effect of endangering ISS crew, which was forced to take shelter, and receiving international condemnation (Lauer, 2022; Secure World Foundation, 2024).

As anticipated earlier in this chapter, there is no binding international treaty prohibiting ASAT development and testing, which, given the dangers and consequences associated with ASATs tests, appears to be a considerable reason for concern (Lauer, 2022). In the absence of a formal treaty, a norm against destructive ASAT testing is beginning to emerge through non-binding commitments. In April 2022, the United States was the first to declare a self-imposed moratorium on such tests, with 37 other countries having joined as of 2024 (Secure World Foundation, 2024). Encouragingly (at least when considering the issue of orbital debris), aside from sporadic and demonstrative tests, major spacefaring powers like the United States appear to increasingly put primary focus on developing non-kinetic satellite attack technology (Lauer, 2022).

5. NEW TECHNOLOGIES: LIMITS AND OPPORTUNITIES

5.1. Overview

The analysis presented in the previous chapters has established that the international frameworks governing outer space, while historically significant, are being challenged by emerging problems. Chapter 3 has tried to examine the most relevant institutional actors and legal instruments, from the United Nations and subsequent treaties that were conceived during the Cold War to structures such as the ESA and the ISS. A central conclusion was that in many cases the structure of these mechanisms has not optimally adapted to several contemporary developments, which might lead to institutional impasses in the context of particularly challenging and unexpected crises.

In that context, Chapter 4 has aimed to examine the direct implications of these governance deficits for crisis management, particularly when it comes to "black swan" events. It identified the unchecked militarization of space, the rising role of private firms in security matters and the identification of several real-world crisis scenarios that might reveal weaknesses in both reactive and pre-emptive measures from institutional actors; if existing frameworks struggle to manage foreseeable accidents (such as the Iridium-Cosmos collision), their ability to address a true "black swan" event might arguably need to be even further reinforced.

This chapter aims to describe current relevant technologies and to analyze their role in addressing such crises, in order to evaluate both which benefits might be drawn from their use and their potential for new risks or vulnerabilities, which might create unforeseen problems with regard to their governance.

To structure this assessment, the chapter examines three specific technologies: Artificial Intelligence (AI), blockchain and quantum cryptography. Rather than providing a deep technical analysis of these technologies, the Chapter will mostly focus on their application in the political and security domains.

Section 5.2 will examine the opportunities AI presents for improving space security awareness through the automated analysis of sensor data and for enabling autonomous collision avoidance, a developing tool that is already being employed by large satellite constellations; another element resides in AI's potential for machine learning algorithms to detect anomalous satellite behavior. At the same time, the section will address the significant governance deficits AI creates, such as legal liability for the actions of autonomous systems under existing framework and the challenges that come with "black box" algorithms.

Following this, Section 5.3 will assess blockchain technology's potential to serve as a decentralized infrastructure which is able to create a single, verifiable and unalterable "source of truth" that does not require a central authority. The application of blockchain to guarantee reliability when it comes to supply chain for space hardware, minimizing the presence of counterfeit or compromised components, will also be explored. The analysis will then turn to the substantial limitations facing this technology, such as issues in the achievement of international consensus to first adopt a single protocol and technical issues related to information delays and storage capabilities.

Finally, Section 5.4 will evaluate quantum cryptography. This technology will be presented as a long-term, and potentially definitive, response to the threat of cyber-attacks on space assets. The principles of Quantum Key Distribution (QKD) will be discussed as a means of establishing provably secure communication channels which could protect military and civilian satellite functions and their ability to distribute sensible data. This potential, however, needs to be weighed against the technology's current early-phase stage, high cost and the considerable physical and technical obstacles to both its deployment in space and its ability to rapidly transfer a vast amount of data.

It is also worth noting, in the context of this general overview, that the application of each technology described within this Chapter must take into account the fact that certain types of black swan events pose an important threat to their functionality. For instance, a solar flare or coronal mass ejection (CME) can severely disrupt or damage satellite electronics, onboard sensors, and more generally its communication systems (Cliver et al., 2022). Given that artificial

intelligence, blockchain, and quantum cryptography systems heavily depend on uninterrupted access to electronic infrastructure, such an event could result in considerable damage, if not overtly catastrophic. AI systems used for detecting anomalies or avoiding collisions autonomously depend on a continuous flow of real-time telemetry and sensor data; hardware failure caused by radiation would critically disrupt the flow of data and greatly impair decision-making capabilities. At the same time, the distributed architecture of blockchains can only function if the participating nodes are operational and in sync. This whole premise can be challenged if computational units in space or even on the ground are turned off simultaneously. Quantum cryptographic networks may also be particularly more susceptible to the effects of the environment. Fundamentally, all these technologies might provide transformative resilience during crises, although any strategic deployment plans, especially in the context of preventing “black swan” events, must both consider operational resilience to space weather phenomena and the perspective of hostile actors physically disrupting the infrastructure needed for these technologies to effectively function.

Overall, this chapter aims to assess each technology not only for its potential to improve the management of existing risks, but also for the inherent danger of introducing new vulnerabilities through their own use. If implemented without a complete understanding of their potential failures and limitations, the tools described might arguably represent catalysts for "black swan" events which could be more impactful than the ones emerging technologies aim to prevent. The analysis will therefore focus on both aspects, with the intention to link the technical characteristics of AI, blockchain, and quantum cryptography to the theoretical framework of high-impact, low-probability events.

This more analytic chapter aims to prepare the reader for Chapter 6’s proposals in terms of the adoption of potential solutions to improve current institutional frameworks’ ability to respond, prevent and manage crises and “black swan” events when it comes to the utility which might be derived from the correct and rapid implementation of contemporary technologies.

5.2. Artificial Intelligence

This section aims to examine the role of artificial intelligence (AI) when it comes to the detection and response to black swan events in outer space, as well as the geopolitical and governance implications of its increasing application in the context of outer space. The analysis will be focused on the sociopolitical rather than technical dimension of AI application. As Wendt (2023) observes in examining a broad range of contemporary security threats, society often appears unprepared for new scenarios, a weakness that might prove particularly dangerous in the context of "black swan" events' occurrence. AI might prove particularly useful in forecasting and providing solutions to unexpected space incidents and improve the hindsight detection of underestimated crises, with several strategic and dual-use ramifications of AI, encompassing civil and military use, in space, while considering the existing potential for misuse.

Another point of interest is represented by the challenges current international frameworks face regarding the implementation AI-enabled space technologies (with a particular interest for crisis management) and the current influence of non-national actors on AI's development in outer space scenarios. For example, recent regulative measures such as the European Union's AI Act (2024), which aims to categorize AI systems by their risk potential and take measures accordingly, appear to lack specificity in dealing with their use in the context of outer space.

One of AI's most promising contributions to outer space governance is related to Space Situational Awareness (SSA), which can be described as the ability of a system to understand and react to the external environment of outer space, being instrumental to the functioning of early warning systems for anomalies or potential threats which might emerge. Black swan events in space (e.g., mass-scale collisions or debris-related accidents, systemic software failures) might be predicted more efficiently through data analysis. As Peng and Bai (2019) note, AI and Machine Learning (ML) techniques have to potential to increase accuracy of satellite orbit predictions and ensure greater precision in collision avoidance, even learning from historical orbital data to correct errors in trajectory models. In their study, a Support Vector Machine algorithm was trained on publicly available orbit

data to predict trajectory errors; the results showed significant improvements in accuracy; in this sense, more precise conjunction forecasts might be realized through the application of ML, lowering the probability of crashes and thus the accumulation of debris in satellite-populated orbits.

Traditional satellite operations have long depended on analysts when it comes to looking for signs of malfunctions, which is both time-expensive and prone to human mistakes. AI systems can instead continuously analyze datasets to look for signs of trouble which humans could miss. This has already started being applied by governmental actors: for instance, the U.S. Space Force has moved toward the integration of artificial intelligence into satellite monitoring through its Unified Data Library (UDL), which collects data from Space Domain Awareness (SDA) sensors to enable their analysis in real time (USSF, 2025). The UDL allows AI systems to continuously obtain and interpret data in order to detect potential issues and recommend strategies to minimize their impact. Another relevant effort is the identification of "standardized benchmark to evaluate the performance of Large Language Models in the context of space operations and other AI systems specifically for space operations" (p. 6) by the end of the last quarter of 2025, through which the Space Force aims to evaluate large language models in order to determine which ones are more adequate to sustain the unique challenges of outer space.

This approach represents a shift toward the adoption of both reactive and precautional measures, minimizing time between detection and response and using AI tools to predict potential challenges; with respect to the latter, one example showed in the report is how machine learning models can be instrumental in the detection of early indicators of satellite malfunction (e.g., irregular thermal signatures, power fluctuations or signal delays) and thus improving their maintenance and adaptability in context where rapid situational awareness is of fundamental importance. The German Space Operations Center analyzes how AI models can also learn from existing data in order to make efficient maneuver decisions in an orbit increasingly crowded with satellites and space assets; Ravi et al. (2023) propose a shift in responsibility from human satellite operators to AI systems for decision-making pertaining to collisions, with a focus on high-risk events. Their research uses 200 conjunction data messages (which are messages

satellites send to earth whenever an object that is near to it is detected) with high probability of collision retrieved from ESA datasets, with the aim of training machine learning models capable of decision-making which equates or exceeds operator-level quality. The models referenced by Ravi et al. (2023) target ambiguous events in which probability of collision ranges between 1E-5 (0.01%) and 1E-4 (0.01%). Although these numbers appear small, anything in the realm of 1E-4 is generally considered critically high due to both the number of objects in outer space and the potentially extreme severity of a collision's consequences. These are precisely the types of potentially "black swan" like scenarios in which predictive uncertainty is highest, with potential for underestimation.

AI-driven autonomous collision avoidance is already being implemented, for example, by SpaceX's Starlink communication satellites, which enjoy a degree of autonomous avoidance capabilities through the employment of onboard AI without having to receive ground input. According to a recent NASA–SpaceX joint spaceflight safety agreement (Nonreimbursable Space Act Agreement, 2021), Starlink satellites will maneuver as needed to avoid NASA assets to avoid uncoordinated responses. In six months, during the 2023-2024 period, the Starlink constellation appeared to perform approximately 50.000 maneuvers related to collision avoidance, also through its AI-based autonomous systems. Through automation in maneuvering, AI systems can minimize the probability of a chain reaction of crashes (often described as a Kessler Syndrome, a scenario which was briefly referenced in chapter 3).

AI can also arguably prove useful when it comes to non-strictly physical risks like satellite software anomalies and cyber-attacks, already referenced in the previous chapter of this dissertation. Modern satellites and ground stations face increasingly sophisticated cyber threats; as stated in section 4.4, loss of control or satellite blackout might constitute, if on a large enough scale, a black swan event. Space systems generate a considerable amount of data which could contain early signs of both software failures and unwarranted intrusions. AI algorithms, especially in the context of anomaly detection through the employment of machine learning approaches, are particularly efficient in data-scraping to look for causes of concern and report anomalies in real time. At the same time, some issues might stem from certain cybersecurity vulnerabilities that appear to be inherent to AI

systems. As Raska and Davis (2024) explain, AI algorithms are used to “process multiple data streams that provide situational awareness and intelligence of the operational environment” (p. 2), rendering said systems susceptible, for example, to data poisoning, which occurs when an AI model learns ineffective or dangerous behavior through defective training data, both due to errors or intentional manipulation on the part of a malicious actor. A concrete example might consist of a "data poisoning" attack that is designed to make the AI system systematically misinterpret reality during a military crisis; this risk might be complemented by a context of strategic overreliance, where human oversight is substituted by autonomous systems that are judged to be infallible, thus amplifying a crisis through the malfunction of the very technology that was designed to prevent it.

As previously noted, Lauer (2022), among others, analyzes how space is becoming “militarized” through both the testing ASAT weapons and the creation of harmful software and non-kinetic weapons. In this context, AI could accelerate the process through automating the search for vulnerabilities and executing less predictable attacks at scale. In order to understand AI’s implication in outer space operations, it is important to consider its limits and dangers, especially when it comes to its potential to exacerbate or allow for new crises to emerge. AI technologies, as of today, face difficulties in being integrated into existing frameworks: as Graham et al (2024) observe, the foundational treaties (the OST being one example) were established in an era dominated by human decision-making, one example being how Article VI of the OST (1967), which holds states internationally responsible for all national space activities but does not take into consideration AI liability issues.

In his book, Pagallo (2024) also observes how international law frameworks, which were almost entirely developed before the widespread use of AI, are inadequately equipped to manage the incremental autonomy of AI systems; it is observed how these systems lack, for example, the ability to clearly assign liability in the context of these systems’ autonomous operations and decisions, which is an issue that encompasses, but is not exclusive to, outer space as well. According to Graham et al. (2024) as well, this regulatory gap could become increasingly critical as AI systems are provided with a greater share of autonomy in decision-making. This ambiguity concerning liability for damages (concrete and

related example might take into account crashes or collisions caused by automated orbital maneuvers) remains unresolved in the context of our current frameworks.

The issues that emerge from automating AI decision-making are further complicated, as Graham et al (2024) argue, by unpredictability: even when AI algorithms are given well-defined parameters, their outputs can be difficult to foresee, especially in unaccounted situations where very little data is available. This phenomenon is well represented by neural networks being often described as "black box systems", due to how difficult it is to interpret their internal processes (Pagallo, 2024). One crisis example might be an autonomous maneuver that causes a collision due to an unprecedented glitch or an intentionally deceptive signal, with damage to either objects, the environment or individuals. This unpredictability, grouped with issues in attribution of responsibility, complicates risk management and provides several challenges when it comes to the viability of entirely autonomous systems.

AI may also constitute a terrain for several political challenges in the management of "black swan" events, as observed in a recent document (2025) submitted to the UN "Open-ended working group on the prevention of an arms race in outer space in all its aspects" on PAROS by the Centre for International Governance Innovation (CIGI). The first element of concern is related to how these systems' ability to "increase the speed, complexity and unpredictability of operations" (p. 2), rendering their decision-making procedures potentially able to effectively outpace negotiation processes and increase the risk of political escalation: a practical example might be an instance in which satellites or missile defense systems that are AI-operated and possess a certain degree of autonomy act on the basis of a false flag too rapidly to be managed by human oversight. The document also takes into consideration the dual-use nature of AI systems and its effect on reciprocal trust between international actors: AI "erodes traditional distinctions between military and civilian, offensive and defensive" (p. 3) in outer space, which might result in diplomatic complications and the implementation of precautional measures, leading to "security dilemma"-related scenarios. Another observation is related to how AI tools and the degree of success in their development on the part of different countries, creating a situation of inequality in which "only some actors possess the technical capabilities to monitor or respond to fast-evolving threats" (p. 3). A gap in AI abilities has two important implications:

firstly, that of incentivizing aggressive competition for the development of outer space capabilities through AI-related technologies, which might by itself become a cause of instability when it comes to the diplomatic relations of two space-faring actors; secondly, that of an actor miscalculating an adversary's ability in the case of undisclosed scientific breakthroughs on the part of the latter. Both scenarios might increase the probability of a large-scale crisis. It can overall be observed, with more depth being provided in chapter 6 when it comes to potential solutions, that AI innovation appears to challenge normative outer space frameworks; consequently, institutional actors must adapt to be able to incorporate AI appropriately.

When it comes to UN COPUOS, such challenges mostly consist of speed and transparency issues. COPUOS is consensus-based and intrinsically designed for human diplomacy and slow decision-making. A "black swan" event which is mainly caused by some form of AI escalation (e.g., two autonomous satellites misinterpreting their respective actions as hostile) would happen very rapidly, with the potential of making the complex and slow negotiation processes of COPUOS effectively irrelevant. It should also be noted how the "black box" nature of neural networks appears, as of today, to be incompatible with the UN's core principles of transparency and verification: the notion of COPUOS aiming to govern an actor whose decision-making process it cannot fully explain or comprehend might create a governance and normative vacuum and constitute a weakness in the context of a crisis.

The European Space Agency, on the other hand, might show particularly marked weaknesses when it comes to the liability gap which are created by AI use. As established, ESA missions are complex collaborations that benefit from contributions from member states. If a shared AI system which was developed by a contractor in one member state and then employed by another causes, for example, a collision accident, under current rules it would be hard to determine responsibility; such ambiguity could, during a related and large scale event, potentially weaken European cooperation precisely when there is a need for a unified and cooperative response.

Some of the issues which might be raised when it comes to autonomous AI systems being incorporated within the ISS framework might be political and come from control, especially in the case of proprietary algorithms: deploying a system which does not display a fully transparent decision-making process could, for partners involved, represent an obstacle to national sovereignty in the context of complex missions. For instance, an autonomous system for energy and resource management might, for instance during a solar storm, decide for optimization purposes to deprioritize a non-essential system in one partner's area to preserve a more important one in another one's. For the affected partner, this could potentially be interpreted as a partisan decision made by an algorithm which was developed by an international competitor. Such an interpretation might, as a consequence, severely weaken the founding principle of jurisdictional boundaries established in the IGA (1998), as well as the idea that resource allocation between partners would need human negotiation as a prerequisite. Such a scenario risks creating new crises that the current governance framework appears to be unprepared (and not built) to manage.

5.3. Blockchain Technology

This section aims to explore the structure and uses of blockchain technology, which employs a decentralized approach to recording data; while briefly referencing terrestrial applications for contextual awareness, particular attention will be paid to its main characteristics (immutability, distributed consensus and smart contract automation) and their relevance in outer space activities and its potential as a tool for effectively managing crises and "black swan" events in the outer space domain through the improvement of data integrity and cybersecurity along with space actors' decision-making capabilities.

Abdi et al (2020) provide a thorough description of how blockchain technology works: in essence, a blockchain can be described as an immutable distributed registry composed of blocks of transactions, which are cryptographically and sequentially linked and shared across a peer-to-peer network. A fundamental aspect of this technology is the absence of a controlling authority: network participants need to agree upon valid transactions and information; once consensus is reached, it cannot be altered without leaving observable traces. In short, blockchain can thus be described as a "a decentralized distributed and tamper-proof ledger that is shared among every P2P network participant" (p. 2). Many modern blockchains also support smart contracts, which consist of self-executing code that automatically enforces agreements when certain previously agreed upon criteria are met, such as specific emergency requirements. These characteristics make blockchain stand out from centralized databases traditionally used and constitute the basis for its applications when managing "black swans" and related risks in the context of outer space.

Although originally developed to support the cryptocurrency Bitcoin, blockchain technology is currently applied within a broad range of sectors (finance and healthcare being two prominent examples) due to its ability to provide secure and transparent data sharing among multiple parties without the need for multiple intermediaries (Abdi et al, 2020). Furthermore, specialists appear to suggest that blockchain-based solutions could significantly improve supply chain management and security in the space sector: a study by the Center for Space Policy and Strategy of the Aerospace Corporation (2020) pointed out how the Department of Defense

seeks to use blockchain technology for risk management and recommends its adoption to mitigate space systems' vulnerabilities when it comes to sabotage and tampering concerns.

In the specific context of managing "black swan-like" crises, blockchain's defining characteristics of being unalterable without actors' consent and shared could make it useful as a single source of reliable data for multiple space actors (such as governments, international organizations or private companies) involved, which might prove considerably useful during an ongoing crisis: data recorded on a blockchain is immediately replicated throughout all network nodes, which ensures that everyone has real-time access to the same verified information.

One concrete application which is relevant to this dissertation can be found when it comes to situational awareness and traffic management in outer space, which requires multiple organizations to observe outer space assets to prevent collisions or otherwise undesirable behavior. Researchers have proposed blockchain-based frameworks to automate certain aspects of traffic management in outer space: for instance, the BESTA (Blockchain Enabled Space Traffic Awareness) concept uses blockchain technology to continuously compare observed satellite behavior to agreed norms and record relevant discrepancies, such as an anomalous deviation on the part of a satellite (Reed et al, 2020). In essence, blockchain provides a decentralized accountability mechanism for space operations which can significantly improve international responses to emergencies or irresponsible behavior in outer space and serves as a tool to aid decision-making.

Another aspect to consider pertains to improving data integrity and cybersecurity in space systems: as previous sections and chapters have widely explored, a successful informatic attack against either an in-orbit satellite or a ground station could either considerably worsen a crisis or constitute by itself a "black swan" event. A NASA-funded paper (De La Beaujardiere et al, 2018) explored how blockchain technology could reduce risk through decentralizing validation for commands and data and introducing multi-step verification mechanisms to improve safety and control in satellite constellations; this ensures, for example, that a dysfunctional command on the part of one ground station would not be followed unless the other authorized participants agree. One experiment in

the study concerned the use of smart contracts to handle cases in which there is "contention over which satellite should respond", in which "the blockchain handles the logic autonomously and sends the command to the nearest satellite" (p. 8).

Blockchain technology may also help when it comes to pre-emptive measures, one area being the reduction of vulnerability in outer space hardware supply chains, which involve a broad network of suppliers and manufacturers. Bikos & Kumar (2022) point out how, as the length of missions in outer space generally decreased, satellite system manufacturing shifted toward mass production and lower cost, prompting manufacturers to look for off-the-shelf components and generating several challenges related to quality control, with potential for increased risks, both physical and cybernetic. A single low-quality component could effectively constitute either a major problem during critical missions or, more generally, an important risk factor for the system involved. The authors call for increased application of blockchain and distributed ledger technology (DLT), which could be instrumental in preventing and detecting vulnerabilities through the verification in real time of a component's origin and the automation of alerts for items that do not respect relevant standards. There can also be an *ex-post* pre-emptive utility: if a satellite's component is reported to malfunction after it has been launched, blockchain technology can be used to trace the component back to the supplier, look for similar components sold by the same supplier in the context of other operations and notify actors involved (Bikos & Kumar, 2022). Authors note how blockchain technology's inherent transparency may extend to "Detection and isolation of cyber threats, accurate management of inventory levels, timely correspondence to product recalls, malfunction detection of parts and components" (p. 4).

Other notable applications of this technology include the "tokenization" of space assets, which could be represented as such for monitoring and control purposes. For example, a smart contract might be set up to automatically execute avoidance maneuvers in the case a collision risk between two tokenized satellites is detected on the ledger; at the same time, a smart contract can more generally instantly either enact predefined emergency protocols procedures or report to human operators. Similarly, blockchain-based insurance contracts aimed at managing space risks can prove useful in the context of crises, one notable case

being Etherisk's creation of a "DLT-based reassurance protocol to establish novel decentralized insurance services and products" (Bikos & Kumar, 2022, p. 1): in the context of these protocols, if satellite failure or damage occurs and is verified through blockchain consensus, previously agreed upon payouts could be automatically sent to the insured parties through the adoption of a smart contract. Automating risk transfer and operating on the basis of transparent rules that are pre-emptively agreed upon can both be instrumental to effective recovery in the aftermath of disasters and might support the financial side of black swan event management through the reduction of uncertainty and improved speed in crisis recovery.

Institutional developments related to blockchain and DLT application within ESA's Space 4.0 framework, which envisions increased automation and decentralization with the perspective of a space ecosystem that tries to put together technological innovation and sustainability through comprehensive regulatory measures. Bikos and Kumar (2022) note that the framework supports blockchain technology for "robust payments, supplier contracts, procurement, and full automation" (p. 4). NASA's Glenn Research Center, apart from previously mentioned experiments, also sponsored research into a "Resilient Networking and Computing Paradigm" using blockchain for deep space probes through a $300.000 grant, with the long-term goal to "achieve scalable decentralized cognitive networks in deep space" (Center for Space Policy and Strategy of the Aerospace Corporation, 2020, p. 10). Blockchain application is thus being considered to ensure that autonomous space assets are able to control and verify each other's actions through secure sharing of relevant data even in cases in which it is difficult or impossible to establish continuous and reliable contact with Earth: in the context, for example, of a Mars mission, which implies considerable communication delays, these assets could if necessary use a local blockchain network to coordinate a response and carry it out instantly. Such autonomy could be extremely instrumental in managing emergencies in deep space, with assets having no immediate reach to human judgement. Private actors have also started to shown interest to blockchain technology and its applications: the start-up SpaceChain, for example, has launched blockchain nodes on satellites and even on the International Space Station to experiment with cryptocurrency transactions in orbit and thus testing blockchain

technology in the context of space environments (Center for Space Policy and Strategy of the Aerospace Corporation, 2020).

Bikos and Kumar (2022) also note how, although carrying great potential, the use of blockchain technology in outer space remains largely in an embryonal phase, with most applications still being only conceptual and several challenges ahead, such as storage capabilities, the applicability of consensus protocols to outer space networks and the potential for transmission delays and limited visible time between satellite to “disrupt the whole ledger procedure” (p. 5).

Looking forward, the authors argue that DLT has the potential to be particularly significant for pre-emptive security and backward tracing, thus allowing to improve risk management when it comes to oversight of suppliers. With new standards for the blockchain-based control of supply chains being put in place such as those envisioned in ESA’s Space 4.0 framework, these technologies might also be employed for automated procurement, regulatory compliance and certification of parts (Bikos & Kumar, 2022).

Nevertheless, blockchain masks critical vulnerabilities that could trigger a black swan event, particularly when state-level actors are involved. The first one might be the misunderstanding of its security and validation model, with a distributed network that approves transactions, and is related to what is commonly called a "51% attack": this type of attack occurs when an entity or group takes control of more than 50% of the network's computational power. This majority control grants the attacker the power to prevent new, legitimate transactions from being confirmed or otherwise "manipulate and modify the information on the blockchain" (Aponte-Novoa et al., 2021, p. 2), effectively compromising it. While this scenario is currently prohibitively expensive for large networks, a state actor with sufficient resources could theoretically execute such an attack to temporarily disrupt specific, mission-critical blockchain systems; in a particularly vulnerable timeframe, this might constitute unrepairable operational damage to a mission in outer space; depending on the mission’s importance, in the context of overreliance on blockchain technology, the damages and overall impact caused might effectively qualify such a crisis to be regarded as a “black swan”. At the same time, the automation features of smart contracts might by themselves create new risks:

undetected bugs, which could be exploited by adversaries to establish control of the network, are difficult to reverse due to the blockchain's immutability and might require considerable resources to be fixed. The ability of smart contracts to directly execute an action may weaken current frameworks for democratic control and liability, amplifying the damage caused by what could otherwise be small “software bugs”. In that sense, it can also be argued that there are governance issues that need to be addressed: a blockchain for international use of outer space would ideally require both wide approval and shared security standards so that all actors involved are able to rely on such a system, sharing oversight to prevent these types of scenarios.

The main obstacle and potential issues which might arise from implementing blockchain technology in the UN COPUOS framework are related to national sovereignty. The UN framework is built, both when it comes to outer space governance and in general, on providing a forum for discussion between States that are ultimately sovereign. This might create risks for diplomatic crisis when the immutable record on the blockchain is politically contested by a powerful member state. The conflict between data on a blockchain and a sovereign state's political and diplomatic posture could, potentially, paralyze COPUOS’s current structure. Wholly similar issues would arise in the context of a dispute between ISS partners, which would take place in a consensus-based model as well.

When it comes to ESA, on the other hand, one issue that might come to mind is related to smart contracts’ automated nature and subsequent rigidity: politically negotiated frameworks like the "geographical return" principle, which benefit from and need a degree of flexibility to manage contributions and put different member states prerogatives together, would be weakened by the structure itself of a smart contract, which would potentially comply to outdated agreements during a "black swan" crisis, thus giving less room for diplomatic intervention.

5.4. Quantum Cryptography

The following section, which represents this Chapter's last one, has been written to provide, without technical pretenses, a basic description of quantum cryptography and related technology, especially in the context of its applications, and to explore its implications within the contexts of black swan events and crisis management.

Cryptography has traditionally been an important tool for international security and crisis response through its ability to ensure that sensitive communications remain confidential, especially in crisis scenarios, with encrypted messaging guarantees that only those who are intended to receive specific orders or data are able to read them, while digital signatures and secure hashes confirm the message origin and prevent a third-party from "eavesdropping".

Quantum cryptography aims to secure and encrypt communication channels by taking advantage of quantum mechanics principles (primarily quantum entanglement and quantum superposition) rather than mathematical and computational algorithms traditionally employed in the context of classical cryptography. As Carrasco-Casado et al (2016) state, given quantum cryptography's reliance on the laws of quantum physics, such technology could provide an encryption method that, hypothetically, promises unconditional security "even against a quantum computer attack" (p. 1). Such development could happen through Quantum Key Distribution (QKD), which is considered one of the most advanced branches of quantum information technology.

QKD aims to resolve the challenge of distributing cryptographic "keys" (which are used to encrypt and decrypt data) without the necessity for complex computational functions. Instead, QKD uses principles of quantum mechanics to ensure that any interception attempt can be detected. As previously referenced, this type of encryption might be secure even against the hypothetical scenario of a quantum computing attack, which might on the other hand compromise classical encryption methods.

Two main protocols embody the principles of QKD, as detailed by Carrasco-Casado et al. (2016): the BB84 and B92 protocols. The BB84 protocol

uses a measure defined as “Quantum Bit Error Rate (QBER)”, which enables users to analyze the statistical anomalies caused by interception attempts to determine whether a third actor has tried to intrude communication channels; especially when it comes to dealing with large-scale crises that require classified information to be securely shared, QKD might constitute a considerably important strategic asset for governmental and military actors.

Furthermore, Carrasco-Casado et al. (2016) specifically focus on the relevance of free-space QKD as an alternative to fiber-optic QKD, the main difference being the ability of the former to be “easily transported to different locations if required, as opposed to optical-fiber links, which are usually underground and cannot be easily operated” (p. 2), though observing that “In a realistic scenario, QKD will be implemented in metropolitan networks with a combination of optical-fiber and free-space links” (p. 6), due to the benefits derived from both, respectively, the guiding properties of the former and the flexibility advantages of the latter. Nonetheless, the ability of free-space quantum communication systems to be deployed or relocated as necessary might arguably be instrumental to react to crisis scenarios and unexpected “black swan” events, such as an unexpected, large-scale military conflict that requires a government to keep sensitive information, such as satellite data, as secure as possible. For example, if QKD were used between a military satellite and its ground station, an enemy would find it essentially impossible to operate undetected. Quantum keys could also be employed for the communication between different national space assets, enabling operations without fear of external interference. QKD might also be used to establish encrypted inter-satellite networks, securing them from large-scale cyber-attacks.

Real-world applications of QKD technology for communication and security purposes have already been considered by institutional actors, with concrete implementation efforts in the outer space sector: one example is the China-operated “Micius” satellite, which has been launched in 2016 and successfully enabled intercontinental QKD between China and Austria; the two countries established a secure key exchange over 7,600 km, using the satellite as a trusted relay to hold a 75-minute video conference which was effectively secured through quantum keys (Liao, 2018).

Although impressive, upon further scrutiny the technical implementations of the Micius launch did not prove flawless: as Miller (2025) observes, the decoy-state BB84 protocol used aboard Micius, although theoretically safe, possessed some implementation flaws that appeared to fail at ensuring absolute security for communication channels in creating side-channel vulnerabilities. More specifically, that tiny timing differences among the eight lasers that were on board would have allowed a hostile actor to distinguish signal pulses from decoy pulses in almost every case, which would have nullified “unconditional” secrecy in communication.

In security terms, this observation does not mean that QKD is a failed technology, but rather that its implementation in space, if not foolproof and thoroughly examined, may provide governmental actors with a false sense of security and excessive reliance, potentially leading to data exposure in the context of an emergency; at the same time, the physics of communication channels imposes other limitations, with even new techniques such as “two-field quantum key distribution”, which allowed for quantum keys to travel across more than 600 kilometers of optical fiber, delivered only about one encrypted bit per second, which is not sufficient, for example, in delivering the volume of sensor data that is expected in modern emergency response networks (Zhou et al, 2024). It is important to know, in that sense, that defensive tools that are considered impenetrable (and potentially overestimated from certain angles) can produce strategic complacency and be exploited by malicious actors in crises due to unforeseen factors. Overall, the implications of these findings give an important perspective on how technological overconfidence, by itself, might set the stage for the occurrence of a "black swan" event by creating information asymmetries. A state actor might integrate QKD operating under the assumption of unconditionally secure communication (possibly making it a "single point of failure"). If a hostile government or actor discovers an implementation-specific vulnerability, it would in that context obtain a decisive intelligence advantage: a government, for instance, that believes that its communications are secure might reveal strategic intentions or sensible data that could be exploited. In this context, the black swan event is not the intelligence breach itself but the sudden, catastrophic collapse of strategic stability that results from the exploitation of that breach, especially if the specific

vulnerability is not promptly discovered. Such an event would be characterized by its extreme impact (a rapid change in the balance of power because of information asymmetry), its improbability (given quantum cryptography's perception of inviolability), and predictability in hindsight (hardware flaws generally constituting a cause of risk). This example demonstrates how the greatest threat in the implementation of quantum technology resides in practical engineering flaws rather than the theoretical structure behind it, which may on the other hand amplify a false perception of security.

Arguably, security and logistical issues aside, the demonstration of data transmission through satellites in outer space that allow for video conferences is by itself a major step when it comes to real-world implementation; the experiment, overall, showed the feasibility of quantum technology, suggesting the future perspective for an eventual global network of space assets that are secured through quantum technology. Following China's lead, other nations and agencies are investing in quantum communications for space. The European Union, for instance, appears to be planning toward the construction of a EuroQCI satellite network for quantum encryption, aiming to invest resources toward the future commercialization of quantum technologies (Kaltenbaek et al, 2021). The authors also strongly argue toward the establishment, on the part of institutions, of a complete framework for the implementation of quantum technologies in space, which include technical benchmarks as well as structures and methods for effective certification that ensures testing against side-channel leaks such as those encountered in the context of the Micius systems; in order to successfully implement these technologies and define precise requirements that also take into account an "operational system with mission-critical uses [...] an interdisciplinary approach is required between quantum physicists, cryptography/security experts, and engineers" (Kaltenbaek et al, 2021, p. 3).

Overall, quantum cryptography and QKD technologies offer a meaningful advancement in securing communication channels, especially in high-risk scenarios which also include the involvement of space assets. Although its theoretical advantages are significant, there are still important limitations that are both operational and technical, with transmission rates and physical constraints that still limit fully integrating QKD into strategies related to risk and crisis management.

Security concerns also need to be highlighted, especially when considering a hypothetical scenario in which quantum cryptography is predominantly or exclusively used by state actors to transmit sensitive information: in order to avoid crises and “black swan” scenarios which might stem from information asymmetry, as well as fully account for the security concerns that might accompany engineering flaws in the technical and physical implementation of QKD, the potential for overreliance on quantum cryptography must be taken in consideration, along with appropriate standard-setting for relevant hardware.

The main problem of implementing QKD in institutional frameworks for outer space governance mainly comes, when analyzing both UN COPUOS and the European Space Agency, from budgetary constraints, although from different perspectives. When examining COPUOS, the main concern is political, as implementation of quantum technologies risks strengthening an already existing international divide, especially in secure communications: this derives from quantum technology’s high costs and complexity, potentially prohibitive for several national actors which already face challenges in increasing their budget for ordinary outer space activities and development. For the ESA, the challenge is more directly one of allocating budgetary resources, as devoting a portion of expenses to the development of quantum capabilities would strain the agency's already limited budget.

In the context of the ISS, a problematic aspect of introducing quantum cryptography would be that of weakening mutual trust among partners and operational transparency: this might constitute a serious threat, especially given the recent strains aboard the Station which were discussed in previous Chapters, for an institution which strongly depends on it for carrying out operations and experiments. If one partner, such as NASA, decided to establish a communication channel that others, like Roscosmos, could not independently verify, this could be perceived not simply as a technological security upgrade but as a sign of mistrust.

6. PROPOSED IMPROVEMENTS TO COOPERATION FRAMEWORKS

6.1. Enhancement of Crisis Response: Lessons from Global Health and Financial Crises

This section aims to describe how highly impactful events can disrupt entire institutional systems by revealing general weaknesses traced to the indicators previously referenced in Chapter 3: respectively, Preparedness (which this dissertation divides into the existence and efficiency of clear emergency protocols and what portion of agency budgets is devoted to monitoring and prevention of crises), Agility (divided in reaction speed and institutional centralization), Recovery (measured through crisis recovery speed and the ability to enact post-crisis improvement) and Normative Resiliency (which analyzes whether a framework is binding, whether it includes dispute settlement mechanisms and if its core principles still hold).

In order to understand the management of high-risk events in the context of outer space, lessons will be drawn from other systemic crises which have had considerable impact in the 21st century (namely the 2008 financial crisis and, more recently, the COVID-19 pandemic), with a focus on their causes, consequences and institutional actors' flaws in the context of preventive and reactive measures. Such an analysis might prove useful in applying useful information to a context, that of outer space governance, in which unforeseen crises could have a catastrophic impact on multiple sectors and would not simply be constrained, as seen before, to the space domain. Similarly, the two crises which have been taken into consideration share multi-factorial causes as well as severe consequences in multiple domains. These "lessons" can serve as an introductory step in discussing (as will be done in sections 2, 3 and 4 of this chapter) further implementation proposals the for discussed frameworks related to the other topics at hand, such as when it comes to integrating private actors or new technologies more effectively and to effectively modify protocols, treaties and soft law mechanisms.

The 2008 global financial crisis, which will be the first event analyzed in this section, was caused by a combination of global economic conditions, risky lending practices and structural weaknesses in the financial system. During the years that preceded the crisis, low interest rates and large capital inflows from surplus countries created a financial environment which encouraged increased borrowing and investment in the housing sector (Obstfeld & Rogoff, 2009). As a consequence, mortgage lending expanded rapidly in the United States, increasingly targeting what are defined "subprime borrowers" (borrowers with low credit scores which would not be eligible for loans under stricter conditions) with mortgages under very favorable conditions. This expansion was driven largely by easier credit supply rather than an effective improvement in borrowers' financial conditions and, thus, improved ability to repay the loan. At the same time, financial institutions increasingly bundled mortgages into complex securities that were sold globally; overly optimistic credit ratings on these securities and weak regulatory oversight had the effect of reducing incentives for careful lending and increasing financial risk (Brunnermeier, 2009). When house prices began to fall in the United States, defaults rose sharply, reducing the value of mortgage-backed securities and effectively causing what can be defined as a "run" on short-term funding markets. The sudden absence of liquid investments had a multi-sector impact and effectively made a localized crisis into an event with systemic consequences for the global market, often symbolically identified with the collapse of Lehman Brothers, one of the most important banks at the time.

The recovery process followed by institutions after the 2008 global financial crisis can overall show how heterogeneous actors can cooperate when confronted with large scale challenges. In the weeks following the collapse of Lehman Brothers, central banks around the world intervened in a coordinated fashion and cut interest rates in order to stabilize markets, and G20 nations issued a joint declaration, a rare occurrence, in which they committed to collectively take measures and enact reforms (G20, 2008). In the analysis of Brende (2020), CEO of the World Economic Forum, the most important lesson of 2008 was that global coordination appeared from each party's distinct self-interest, that is to say, from every major economy recognizing that such actions would constitute its own national priority. In an interdependent system, an economic crisis of those

proportions threatened all and brought even rival powers to establish cooperative measures to contain it. Which brings out similar themes when considering the outer space domain, which is similarly interconnected, with assets and debris that move in orbits which are not as clear-cut as national boundaries are: debris resulting from massive collisions, for instance, might damage space assets belonging to any actor. Thus, when relevant actors consider a "black swan" event in outer space might represent a trans-boundary threat (as G20 governments understood the consequences of their respective economies being interlinked), motivation to undertake coordinated action increases. Financial authorities after 2008 also created institutional mechanisms to manage future crises which might, when appropriate, be taken as examples in the context of outer space governance for relevant improvements in discussed indicators: new bodies like the Financial Stability Board (FSB) were established with the aim of monitoring systemic risks and issuing early warnings, and central banks developed emergency instruments to provide liquidity. One example when it comes to translating these ideas to space would be an International Space Crisis Committee operating through the involvement, for example, of the United Nations framework or the G20, which would convene immediately after a major space incident and include representatives of governments, space agencies such as NASA and Roscosmos, regional actors like ESA and relevant private operators (such as SpaceX). In that sense, each improvement resulting from such a body would affect all institutions and frameworks involved; its functions could include sharing data, coordinate emergency responses (like debris removal efforts or frequency reallocation if communications satellites are lost) and agree on unified messaging and public communications in the context of a crisis. In this sense, this would serve as a “stability board” for outer space whenever a potentially disruptive threat would emerge and improve the preparedness indicator by both establishing specific crisis protocols and obtaining an independent budget for maintaining and carrying out its activities. Just as the FSB monitors banks once considered “too big to fail”, an analog in space could routinely analyze critical space assets (e.g., navigation or weather satellite constellations) and facilitate support in the case of unforeseen failure. The creation of such a committee would address, for instance, the consensus-building weaknesses of UN COPUOS. The ISCC would not replace COPUOS's function in the long-term development of norms, but would instead play

the role of an operational arm of sorts which is designed for rapid response. Its utility would thus come from pre-delegated authority granted through and within the UN framework, through legal instruments which would define clear prerequisites for its activation. This mechanism directly bypasses the "very low" Agility of COPUOS and effectively increases "reaction speed" and "institutional centralization" indicators. For the European Space Agency, whose exclusively peaceful mandate was identified in the previous chapters as a relevant weakness in the context of managing security-related events, the ISCC would provide a framework through which ESA could contribute with its considerable technical expertise without the need for violating its founding convention. Finally, for the ISS, the ISCC could serve as an impartial and third-party forum for reference which could serve as a tool for de-escalation processes and technical-operational mediation; this would, most importantly, strengthen the "dispute settlement mechanisms" micro-indicator by providing further avenues to discuss pending issues.

This body would serve multiple purposes; for instance, if GPS network operations were incapacitated by a solar storm, it could be instrumental to facilitate an international plan which might activate backup services from other systems and ensure continuity for these services. Another relevant practice is stress-testing and scenario planning. After the events of 2008, banks started to routinely go through regular stress tests that were aimed at evaluating their resilience to extreme market shocks, and regulators use the results to mandate corrective measures. The space community could adopt a similar approach by simulating crisis scenarios to test current frameworks, a topic which might also take into consideration the indicators discussed to significantly implement stress tests with clear parameters in mind; these operations would also ensure greater prediction of crisis recovery time and help in anticipating improvements, potentially helping to improve the Recovery indicator.

Risk and crisis management in outer space might also benefit from analyzing the global response to the international health crisis which was represented by the COVID-19 pandemic, which has shown the importance of rapid and transparent sharing of data as well as flexibility in coordinating multiple governmental actors through the World Health Organization’s leadership. Under

the World Health Organization's International Health Regulations (2005), the 196 member-states are under the obligation of monitoring public health threats and report events which may constitute a cause for international concern: in practice, however, early pandemic responses were limited by transparency issues and delays in reporting; in other words, global frameworks ought to include mechanisms that are able to ensure that information is shared quickly and that countries honor their obligations, especially in the context of a crisis. Recognizing these shortcomings, WHO member states are now amending the IHR to incorporate COVID-19 lessons which include both faster reporting timelines and stronger verification of governmental reports, with the most recent ones having reached international consensus on June 1st, 2024; work is also being done on drafting a new international pandemic agreements, though some experts argue it appears to be lacking in several respects such as ensuring compliance through enforcement mechanisms and ensuring accountability (Lazarus, 2023). These events appear to demonstrate just how important clear communication channels and enforceable commitments are: as Lazarus (2023) also notes, treaties without compliance and accountability provisions are often unable to reach proposed objectives. Applying this to space, one proposal is to establish emergency communication protocols which resemble the IHR's focal points in the context of the previously discussed Space Crisis Committee. For instance, each spacefaring nation could designate a focal point that would be responsible for giving advice on threats which contain potential for escalation (e.g., malfunctioning space objects or otherwise debris-generating events) in order to better coordinate response actions. Just as the IHR created National Focal Points for disease outbreaks, a network of Space Crisis Focal Points could make for easier, faster and more transparent real-time communication between different actors during a crisis. Lamm et al. (2022) point out how rapid precautionary maneuvers (e.g. moving satellites based on credible warnings) and prompt notifications to mitigate harm, and how waiting for perfect information might lead to hesitant responses which might arrive too late; improving rapidity in data sharing, in this sense, might lead to more reactive implementation. Another lesson from global health are the benefits derived from the presence of pre-established contingency plans and practiced coordination: prior to COVID-19, the WHO and national governments had conducted pandemic simulations and, to a degree, developed plans for a response, yet many of those plans were shown to be

insufficient for a pandemic on that scale: this element reinforces the already-stated need for stress-testing preparedness through crisis procedures. Some examples might include simulating orbital collisions scenarios and practical reaction procedures (e.g., sharing tracking data, activating backup satellites, issuing public warnings and so forth), thus identifying points of failure and improving both efficiency and trust on the part of relevant actors. In the medical sector, Lamm et al. (2022) also advocate specific crisis leadership training and even psychological preparedness for taking action under a context of extreme stress. This aspect can be transposed to the outer space domain: space agencies and operators might also adjust chains of command to designate and train operators who can be "empowered immediately at times of crisis to carry out necessary tasks" (p. 2), in our case to make rapid decisions about emergency procedures such as collision avoidance, investigating sudden and disruptive anomalies or even handling communication to the public.

It can be noted how this approach might be implemented at the institutional level, although it would need to be handled carefully to respect State sovereignty and ensure national governments are in the conditions to comply: the WHO's Director-General is under the authority to declare a Public Health Emergency of International Concern (PHEIC), which initiates and speeds up an information sharing process (IHR, 2005). A comparable mechanism in space could be empowering the head of an international body (realistically either the UN Secretary-General or the UNOOSA Director) to declare a "Space Emergency" when criteria are met (e.g., a collision affecting multiple countries' assets), which would bring all actors to implement agreed emergency procedures and provide a context in which an International Space Crisis Committee would be empowered to act. Finally, and especially in the context of previously agreed upon plans, flexibility and adaptability are of fundamental importance, as plans will often prove incomplete or at least need to be adapted through context-specific information. During COVID-19, for example, guidelines evolved rapidly as new knowledge on the virus was discovered and implemented, allowing political and technical decision-makers to work on specific policies in real-time. Governance frameworks for outer space should, arguably, share such feature: for example, satellite operators might initially follow predetermined rules and procedures for collision avoidance, but a process to

quickly revise the protocol if ineffective, possibly rooting such changes in experts' technical feedback, could be beneficial in managing the issue at hand. Institutions' Agility, as described in Chapter 3, might be improved through centralizing and improving the speed of decision-making authorities. As observed in previous chapters, consensus-based bodies are usually slow, and international space governance is currently driven by those same mechanisms, the main example, the main example being the UN COPUOS. During a fast-moving emergency, waiting for full international consensus could prove to be unsustainable. Therefore, part of improving crisis response might be pre-delegating some powers to a smaller team or an individual to take initial action in a pre-determined situation, while consultations with a wider group take place at the same time; other than improving Agility, this would also be beneficial when it comes to the establishment of emergency procedures which might be more binding and, thus, improve normative resiliency to a degree.

Effective crisis response also benefits transparent and honest communication, as seen in the context of the pandemic; it is important in the outer space context as well, especially when an event displays its potential for panic and misinformation. Lamm et al. (2022) reference the principle to communicate clearly, rather than through approximate guessing, which could arguably prove useful in maintaining unity among heterogeneous actors. This means that if an organization does not yet know all the facts (for example, the cause of an anomaly), it should still share with related operators what is known and acknowledge what is uncertain, rather than remain silent. A predetermined communication protocol could also improve Preparedness through ensuring that any nation or company detecting a major orbital incident proceeds to inform a central entity, which in turn distributes verified information globally, mirroring in a way WHO's role when it comes to outbreak updates: the emphasis, as Lamm et al. (2022) argue, is on a single trusted channel to relay data and information, as fragmented messaging from different authorities might cause both confusion, redundancy and reduced efficiency. In the context of a Space Crisis Committee, this might translate to the establishment of an official international bulletin for emergencies.

However, the implementation of a Space Crisis Committee at the international level might face several political obstacles, mainly due to great power

competition and state tendency to preserve national sovereignty. Persuading, for example, the United States, China and Russia to agree to a "Space Emergency" declaration would need, as a prerequisite, what would constitute substantial change in approach, as these nations would likely perceive such a mechanism as potentially able to weaken their sovereign right to design a response to threats on their own accord. Mutual suspicion that shared instruments might be used to constrain legitimate military or commercial space activities under pretense of crisis management. Another issue may lie in funding such a committee: major financial contributors might attempt to obtain a greater share of influence, potentially compromising the committee's neutrality. Therefore, just as in Brende's (2020) analysis of the 2008 crisis, spacefaring actors might arguably only overcome these issues once they perceive the potential for a potential "black swan" event so severe that the logic of mutual self-preservation would be temporarily forced to override the impulses of zero-sum competition, if not outrightly in its wake or aftermath.

6.2. Integration Between Public and Private Sector

This section aims to analyze how improved public-private coordination could contribute to improving discussed resilience indicators through the integration of private actors into crisis planning, information-sharing and decision-making mechanisms, especially in the context of "black swan" events. Section 4.3 has already detailed how "New Space" actors are now acquiring an increasing amount of influence when it comes to shaping outer space activities and the consistent and considerable growth of the private outer space sector (Del Canto Viterale, 2023). However, current international frameworks largely remain state-centric, with all subsequent challenges: if, on one hand, the private sector's innovation and resources have accelerated progress in space technology and services, on the other hand international frameworks that do not fully take these actors into consideration might risk being limited when it comes to their ability to manage crises, or even failing to anticipate specific crisis contexts which might be generated by miscalculation on the part of these actors, a topic which has broadly been referenced to in chapter 4 when it comes to specific real-case scenarios (such as the Ka-Sat cyber-satellite attack) and their strategic implications. With an effective lack of pre-established emergency protocols at the international level, especially ones that include private operators, and few real-time international crisis management mechanisms to manage private involvement and coordinate a response, an unforeseen crisis (which might also be initiated by the failure of a private system itself, such as the autonomous collision-avoidance software scenario referenced in section 3.5) currently supersedes the current boundaries of outer space governance frameworks, which were written in an era when only nations had the resources to produce and launch satellites. As was also noted by Wesel and Lambach (2021), the voluntary nature of many guidelines contributed to a situation in which, while some companies adhere to best practices, others may not, which potentially creates regulatory weaknesses.

In the context of the establishment of an International Space Crisis Committee, ensuring that large companies are to some degree included alongside state actors are involved would mean that those who own or control the infrastructure needed to manage a threat are directly involved in coordinating the

response. This cooperation would be particularly important when it comes to improving the resilience of both the European Space Agency and the International Space Station. For the Agency, whose main weaknesses include its limited budget and considerable restrictions on military actions, partnerships with private companies would be a considerable added benefit, as said private actors would provide it with resources and agility to provide backup services during a crisis, improving "resource allocation" and thus Preparedness. For the International Space Station, which now relies on commercial providers for critical transport, further integration with the private sector would be instrumental in reinforcing private-public joint emergency protocols in a context increasingly characterized by commercial dependence. This involvement might happen through either the most influential private actors being directly represented or the establishment of an advisory council within the committee.

On a more general note, private actors' assistance might include rapidly sharing data on the incident, raise private capital and resources for emergency measures and using company channels to contribute to unified public communications: private companies often possess a vast amount of important real-time data which might complement those already used by national governments and public agencies, for example by involving these actors in the previously discussed procedure of communicating potential causes for concern to specific focal points. It can also be said that in cases such as a cyber-attack or the systemic failure of a strategic server on the network of a private company, the latter's operators would be the first to detect any anomalous process. A mandatory and immediate reporting protocol would allow the committee to both assess the potential and scope of consequences and issue warnings in less time, which might also turn a potential "black swan" event into a manageable crisis and improve Agility through increasing "reaction speed", by ensuring faster responses through more efficient real-time data-sharing. It might also be argued that involving the private sector in crisis management would directly improve Preparedness by establishing clear and more complete crisis protocols (and even an independent capacity, or increased budget, for the execution of emergency procedures); the latter, in particular, would be instrumental in avoiding accidents like the 2009 Iridium-Cosmos collision by providing a pre-emptively clearer picture of the outer space environment.

Both when it comes to crisis and risk management and as a general approach, outer space governance framework might benefit from more structural inclusion of private sector perspectives in international forums, which could allow them to more efficiently provide political actors with advice at the international level (e.g., reviewing the practicality and analyzing the application of a debris removal measure). As Townsend (2020) noted and as reported in Chapter 4, private companies possess a very different structure than that of governments and space agencies, and their profit-seeking nature, which is not necessarily aligned with the interests of a single government or national power, might create interdependence that stabilizes relations, thus reducing what the author characterizes as the orbital security dilemma: this aspect is important to mention, given its implicated potential for reinforcing preparedness. Given how predictable and safe orbital environment is a prerequisite for long-term profitability (which is of interest to a company), governments might be more incentivized to cooperate diplomatically to devote more resources toward prevention protocols and crisis management strategies if these see the involvement, to a degree, by a mutually trusted actor. Both "KPI recovery speed" and "post-crisis improvement ability" would be improved as well by guaranteeing opportunities to private actors: after a crisis, companies have an immediate financial incentive to both assist in reconstruction and invest to innovate through interventions which might complement those of public institutions and speed up a system's effective recovery. Commercial interests (needless to say, if properly regulated) may even have a positive impact on Normative Resiliency through their potential for self-enforcement: if a company violates best practices and safety norms, it might lose customers in the public sector. Additionally, national laws can obligate private outer space actors to create their own emergency response plans for their assets (e.g., an emergency plan for losing control of an orbital asset that is tailored for its specific characteristics), requiring them, just like aviation regulators regulate airlines, to conduct regular risk assessments and provide subsequent reports. This approach also reinforces Normative Resiliency of governance by ensuring that some rules are binding on relevant actors.

It must also be considered that, to ensure effective involvement and private actors' cooperation, states might benefit from strengthening their national regulatory frameworks. This involves enacting comprehensive space legislation

that mandates companies and their private space assets to comply with certain legal obligations in cases of extreme emergencies, with appropriate compensation or "good faith" liability exceptions potentially taking place to balance costs and benefits. This ensures that private actors cannot opt out of crisis measures and also addresses the scenario discussed in Chapter 4, which imagined a context in which a private actor might be able to withdraw a fundamental service during an emergency; at the same time, oversight on the formation of monopolies in which a single company might be the only one to provide a country with a specific service or function might be needed for both the political concerns listed above and in section 4.3, as well as for avoiding the establishment of "single points of failure" in which specific errors on the part of said company compromises an entire service or operation, potentially causing a "black swan" event by themselves. International regulations are also necessary because their absence might undermine the "Preparedness" and "Normative Resilience" indicators through both lack of transparency by private actors, where a company's reluctance to fully share proprietary data leads to incomplete Crisis Protocols and thus increase vulnerabilities, and a "race to the bottom" which sees outer space companies invest in countries with minimal restrictions to reduce operational costs, potentially at the cost of safety and adherence to shared protocols, which would, in the case of a crisis caused by a private actor, erode the strength of dispute settlement mechanisms.

6.3. Adaptation of Treaties, Protocols and Soft-Law Mechanisms

This section will focus on improving outer space treaties and protocols (either binding or not) as evaluated under the macro and micro-indicators previously established and discussed. The core legal instruments discussed thus far, which range from the 1967 Outer Space Treaty (OST) to later soft-law initiatives like the Artemis Accords and technical guidelines, established fundamental norms and were instrumental in conducting peaceful space activities, but were not designed with contemporary "black swan" scenarios in mind: scenarios such as the diversification of actors and technological change have allowed for the emergence of new threats and effectively exposed considerable gaps in current frameworks. In order to improve the resilience of space governance frameworks, relevant proposals would be expected to improve performance in macro-level indicators and establish specific procedures like emergency protocols or verification processes.

The first focus of analysis consists of the founding treaties of space governance (the Outer Space Treaty, Rescue Agreement, Liability Convention, Registration Convention and, lastly, the Moon Agreement). As stated in previous chapters, while these principles have proven themselves to be remarkably successful in establishing core values when it comes to outer space governance, it is also true that they have been drafted during the 1960s and 70s, under assumptions that no longer hold and with no specific provisions envisioning contemporary threats. One fundamental issue, for instance, lies in the lack of enforcement and compliance mechanisms, with The OST (1967) and subsequent UN treaties effectively unable to enact concrete responses in the case a state violates them. Compliance thus far appears to have depended on mutual interest and normative pressure: as long as no one effectively had a strong motive to violate the contents of the treaties, the system held. It has already been observed how such "good-will based" systems might show their weaknesses in real-world developments: Chapter 3 has described how, after Russia's invasion of Ukraine in 2022, frameworks have weakened, with ESA interrupting missions with Russia and, at the same time, Russia threatening to quit the ISS. If, for instance, a spacefaring power made the decision to take advantage of a particular crisis scenario to either place weapons of

mass destruction in space or unilaterally appropriate resources, the treaties themselves do not offer instruments to enforce their established principles. As Lazarus (2023) observes, treaties that are not able to include compliance and accountability provisions reveal themselves unable to enforce their content and achieve their proposed aims, which is an important reason why the "Normative Resiliency" macro-indicator includes a binary micro-indicator which checks whether a policy framework is binding or not; it can be argued, in that sense, for adaptations that introduce clearer obligations and be enriched, as stated in Chapter 3, by crisis-specific protocols. Additionally, the proliferation of soft law instruments in recent years, while positive in flexibility, has introduced fragmentation and inconsistency. The 21 LTS Guidelines adopted by COPUOS in 2019, for instance, although holding up well as a set of best practices, are non-binding and implementation is voluntary. As Wesel & Lambach (2021) argued, the voluntary nature of debris mitigation measures led to divergent national standards that are not uniformly followed.

Given previously discussed shortcomings, proposals can be categorized along three lines: upgrading treaties or creating new binding agreements; the development of crisis-specific protocols or operational arrangements that are able to provide treaties with emergency instruments and additional procedures; strengthening and harmonizing soft law mechanisms to ensure their ability to complement, rather than cause divisions, in the governance system, potentially serving as a middle-step towards binding rules for the future.

One of the most direct ways to reinforce space governance is to negotiate new treaty provisions targeting the known gaps and allowing margin of improvement when it comes to the "endurance of core principles" micro-indicator. One example of this would be revisiting the PAROS concept in a form that could take into account new military developments such as tests and uses of ASAT weapons. Such an aspect would reinforce emerging tendencies, such as the self-imposed moratoriums such as the one put in force on the part of the United States (Lauer, 2022). Drafting a binding multilateral treaty or protocol could be narrowly focused (e.g., prohibiting the testing or use of any weapon that intentionally destroys or disables a space object in a manner that might create enduring debris), potentially improving its chances of acceptance as it addresses a specific danger

without considering the topic of militarization at large. Another area for treaty development could consist in either drafting a treaty that assigns clear liability or cost responsibility for excessive debris creation or strengthening the existing Liability Convention (1972). To improve this framework's resiliency, one idea could be to update it to a no-fault liability regime for orbital collisions, in a similar way to how the Liability Convention already attributes absolute liability for surface damage. If every collision in orbit carried automatic liability for the owner of the debris-generating object, this might constitute an incentive toward better debris mitigation and more careful operations. At the same time, it can be argued that a binding commitment on the part of spacefaring powers toward assisting each other in removing harmful debris might encourage cooperative responses to crisis scenarios. This might provide some context as to how section 6.2's ISCC proposal would concretely operationalize. In essence, an improvement might be constituted by a law which explicitly enables and gives a framework for joint crisis response. The Rescue Agreement (1968) provides a precedent: it obliges assistance to astronauts in distress. One can imagine that, through a similar process, a treaty can be drafted which binds states to notify others of high-risk, emergency situations and to subsequently provide assistance of some sorts (e.g., allowing other actors to access satellite control if such control is needed to prevent a crash). Another important aspect when it comes to the Convention (1972) concerns updating it to better understand and face contemporary liability issues: a central weakness in the current liability regime is that it was written in an entirely state-governed era of outer space operations which also strictly relied on human decision-making. One improvement proposal would be to supplement such convention by adding a protocol that explicitly tries to clarify liability issues by incorporating private actors and autonomous systems into the normative framework of the foundational outer space governance treaties, thus at least addressing Pagallo (2024) and other scholars' observations by recognizing the existence of technological developments. By providing a better framework for defining fault and liability in these contexts, it would constitute an improvement to the "dispute settlement mechanisms" micro-indicator, especially for collaborative frameworks like the ESA and ISS, which have increasingly relied on the aforementioned technologies and actors, and would remove legal ambiguities which could obstruct coordinated responses.

In addition to more comprehensive treaty changes, emergencies might benefit from more specific protocols because they may be agreed upon faster and can thus be operationalized within a shorter time framework. Specifically, countries might set up an "International Space Crisis Protocol" (ISCP), possibly as a resolution from the UN General Assembly or as an addition to existing treaties. This would require nations to promptly report any serious incidents that could endanger space activities worldwide. For instance, if a country's satellite loses power and starts falling apart, creating debris, that country would need to notify an international contact right away instead of trying to hide it. The protocol would identify a central authority, such as the UNOOSA emergency hotline or the previously proposed ISCC, to collect and share these reports. It would also outline how to consult and provide help; any country spotting a potential threat (like predicting a collision or noticing an issue with another nation's satellite) should inform the affected state and the international community. This builds on Article IX of the Outer Space Treaty, taking it further by enforcing compliance and ensuring a clear process; in this context, the ISCP could also formalize the discussed idea of National Space Crisis Focal Points. Another key aspect is having pre-negotiated rules of engagement for crisis situations (e.g., how to respond if a satellite seems to be under a cyber-attack, as discussed in Chapter 4 regarding how responsibility might be assigned if a private satellite gets hijacked). A protocol could detail the steps to take, with affected parties able to communicate through secure channels, thus being able to minimize retaliatory pre-emptive responses. Additionally, if a space object is in danger of uncontrolled re-entry, the protocol would establish how to notify, track, and make decisions about possible interceptions or evacuations on the ground; as a consequence of planning out and agreeing on strategies for different space crisis scenarios ahead of time, Preparedness might overall be increased by strengthening the "crisis protocols" micro-indicator. At the same time, the ISCP could improve both "reaction speed" and "institutional centralization" by, respectively, creating a legal obligation to report a potential crisis event (e.g., in the case of loss of signal from a satellite or detection of a cyber-attack) to a central body within a short timeframe, thus formalizing and accelerating the initial steps of a crisis response, and by delegating a limited degree of a pre-defined authority to a smaller, empowered body which is

able to declare an emergency, an act which would delegate it with the ability of enforcing actions without requiring a full consensus vote.

When it comes to optimizing the efficiency of soft-law instruments such as guidelines, principles or otherwise informal agreements, which might reduce current risks while future binding agreements are negotiated, one key aspect could be represented by harmonizing standards in a way that ensures a consistent frame of reference for all major actors. This could involve consolidating various guidelines into a single instrument that is endorsed by the UN and updated regularly, possibly reinforced by a periodic review mechanism where, every few years, states report on how they have implemented the guidelines and share lessons learned. Such transparency might encourage compliance as well as allowing governmental actors to identify which guidelines are not being followed and might necessitate more binding instruments such as treaties. As for when it comes to the Artemis framework, diplomatic efforts should aim to bridge normative differences. For instance, the concept of preserving historic sites on the Moon (part of the Artemis Accords) could be brought to COPUOS to seek broader approval without being embedded in the broader context of the Accords, which several spacefaring actors view with suspicion (de Zwart, 2021). A similar framework could lead to at least general assembly resolutions that clarify what constitutes as acceptable behavior before a consistent legal regime is established in many other sectors, such as future scenarios for resource mining and appropriation. The main objective would be to avoid the creation of context with two competing sets of rules; if soft law initiatives can be universalized or, when not possible, at least be made mutually intelligible, such an approach might improve crisis management and response for all actors involved, improving reaction speed and thus Agility: in the context of a global space crisis (a fitting example would be a solar flare, which would hinder various satellites no matter their respective ownership), response would be greatly impaired if actors cannot work together because of either mistrust or adopting much different normative instruments; shared understanding of normative tools, possibly coupled with joint exercises aimed at simulating crises in order to understand whether such understanding effectively functions, would arguably be beneficial for all parties involved. In that sense, a further suggestion could be represented by creating an expert-driven document that interprets how existing law applies to the

management of crises in outer space, including proposing rules of engagement and behavior while also not being a treaty or even a formal law instrument: such document's structure could resemble, by all intents and purposes, that of the Tallin Manual for Cyber Warfare (Schmitt, 2013). Such an instrument would be instrumental to guaranteeing an authoritative interpretation of how existing laws apply to new crisis scenarios, possibly allowing norms and procedures to adapt much faster than the treaty amendment process. This directly improves the framework's ability to learn and formalize improvements, which is encompassed by the "post-crisis improvement ability" micro-indicator, under Recovery.

Further improvements might come from complementing soft law by tying it to reputational incentives by means of scoreboard systems: international recognition can be given on the part of the UNOOSA to countries and companies with excellent safety records, creating positive peer pressure. Soft law instruments and guidelines might also play a role in anticipating the two trends, which are discussed at length in this and previous chapter, of private actors and new technologies by discussing and approving resolutions on the matter through COPUOS and other widely recognized international bodies.

It can be summed up that, when it comes to resilience indicators, upgrading treaties and protocols would dramatically improve current frameworks by several means. They would, for instance, provide them with more specialized protocols, binding dispute resolution and enforcement mechanisms, all of which are currently lacking and constitute well-established weaknesses.

6.4. Implementation of New Technologies

Chapter 5 discussed the potential benefits and risks for outer space activities of several contemporary technologies (namely artificial intelligence, blockchain technology and quantum cryptography). This section focuses on how said technologies can be implemented when it comes to improving indicators for institutional resilience and better management of black swan events; in order to do so, the focus will be that of aligning them with the previously mentioned Preparedness, Agility, Recovery and Normative Resilience macro-indicators and all micro-indicators connected.

Artificial Intelligence, which is the first focus of analysis, has been shown in Chapter 5 to be particularly helpful when it comes to improving space situational awareness. By integrating AI/ML algorithms into monitoring systems and crisis management protocols, as the US Space Force is doing with its UDL (USSF, 2025), frameworks for outer space governance might directly improve their preparedness; early warnings become more reliable and could reduce false alarms and derived spending. Other than the US Space Force, organizations such as the European Space Agency and the IIS, which to a degree might find use in monitoring outer space traffic, might integrate AI into their systems and procedures to provide all actors with better information. Such an effort might directly improve "crisis protocols" and provide benefits to "resource allocation" by ensuring greater efficiency when it comes to budgetary costs. At the same time, AI might improve "reaction speed" by automating maneuvers that would otherwise need human decision-makers; it might also be considered how, in a broader crisis, AI-driven simulations and decision-support tools might be considerably useful for testing relevant measures and preparing human operators: AI could, in this sense, be used to run hypothetical crisis scenarios, thus identifying systemic weaknesses in coordination and communication, which would allow involved frameworks to adapt and improve their Agility before being confronted by actual crises. In terms of Recovery and Post-Crisis Improvement, AI provides valuable tools as well. Immediately after a disruptive event, AI might help assist in both assessing damage and analyze data for relevant adjustments, improving both micro-indicators. If an unexpected crisis happens to disable space assets, AI diagnostic systems could quickly determine

which ones are functional by analyzing relevant information and then prioritize the redistribution of tasks between surviving satellites, helping to determine how to distribute resources optimally among them in order to keep up the most important services. This kind of adaptive reconfiguration accelerates the "recovery speed" indicator; moreover, AI implementation can be used to enhance "post-crisis improvement ability" by learning from data related to previous experiences, as each space crisis provides abundant information that AI can analyze to plan future, more effective interventions. AI algorithms might, after a crisis, be employed to find patterns that humans might miss and thus new warning signs. Normative Resiliency could be increased through responsible use of AI, which would require establishing norms and boundaries related to human control, which go beyond the liability issues already discussed, although in different respects, both in Chapter 5 and section 3 of this Chapter. This might be realized by restricting the use of fully autonomous weapons systems in space, which would strengthen "endurance of core principles" by ensuring that technology cannot bypass human judgment in critical moments. Furthermore, frameworks could effectively use AI while also promoting technical transparency measures. For instance, autonomous satellites might be programmed to communicate intended actions through a shared protocol before they are able to execute those same actions, which would make their behavior both predictable and verifiable. This function might also be instrumental to provide clear data during a incident or crisis, which would make it easier to determine responsibility and thus help with dispute settlements (regardless of the previously discussed liability debate).

Blockchain technology, on the other hand, is particularly useful when it comes to creating reliable, real-time information channels and automating crisis protocols, which makes the technology particularly suited for improving Preparedness and Agility indicators. Preparedness is enhanced by blockchain's inherent transparency as well as its ability to serve as a "single source of truth" that provides credible information for diversified actors. Such a feature might improve the "crisis protocols" micro-indicator by providing a common operational framework, which might constitute something of vital importance during a large-scale crisis. The "resource allocation" micro-indicator might also be improved, as blockchain smart contracts might be used to help framework assign resources

automatically and more efficiently, with less margin for human error. Smart contracts' automation potential might also be employed to improve the "reaction speed" micro-indicator by making agreed crisis protocols automated procedures. One example might be constituted by maneuvers for collision avoidance: with a blockchain-based approach, a smart contract could hold a pre-negotiated rule (perhaps based on physical, concrete data such as satellite mass, remaining fuel, mission priority) and, as soon as the blockchain receives a particular signal, the smart contract automatically decides which satellite should move, subsequently sending the command. Such a concept has been proposed in the form of BESTA (Reed et al, 2021), which has been discussed in Chapter 5. It can also be argued that blockchain technology's characteristics might be used to improve both the Recovery and Normative Resilience macro-indicators by virtue of its tamper-proof history of transactions and operations stored in a ledger: this ensures that a source of data that is immutable and thus able to be reviewed in order to analyze flaws and upgrade relevant protocols after a disruptive event (thus improving "post-crisis recovery ability"; at the same time, every possible deviation on the part of an actor from pre-determined and immutable rules and protocols is rendered more visible, potentially improving "enforceability" and providing increased context for resolving disputes.

Quantum cryptography, particularly Quantum Key Distribution (QKD), might potentially improve all indicators of an institutional framework's resilience by strengthening the security of communication infrastructures. In terms of Preparedness, it can be argued that international space crisis plans effectively rely on the ability to send both warnings and instructions in a way that is both fast and secure. As mentioned previously, QKD can guarantee that the keys used to encrypt messages are known only to the legitimate parties, providing encryption even under the hypothetical scenario of an hostile actor possessing unlimited computing power. This communications security is a form of preparedness: implementing QKD as part of a standard protocol (for example, an emergency network where all key actors switch to quantum-encrypted channels during a space emergency) might ensure safe communications and thus improve an outer space governance framework's "crisis protocols" micro-indicator by improving their protocols' quality. Agility in crisis response is also enhanced by quantum cryptography, mainly by preserving

the rapid flow and integrity of communications in a particularly demanding crisis context. In a scenario where one country's satellites are malfunctioning because of a malicious cyber-attack, if a country or organization validly fears that related communications are compromised, they might resort to secondary, slower methods, losing much needed time. QKD ensures that even during active cyber warfare, there is a segment of communication that remains secure and reliable. This allows leaders and operators to make rapid decisions with confidence, thus improving the "reaction speed" micro-indicator. Additionally, quantum keys can be shared among multiple parties to create coalition networks quickly. If a sudden multi-actor response group forms (for example to manage a detected collision risk, potential large-scale threat depending on the objects colliding), they could use pre-positioned quantum key satellites to establish secure links between all major participants within hours, something that conventionally would require exchanging encryption keys through slower diplomatic means. All these improvements mean that an institution armed with quantum cryptography can react to surprises more swiftly and effectively, without having to consider fragility when it comes to communication channels: quantum-secure communication directly supports this also by ensuring that crisis talks or data exchanges cannot be intercepted or falsified. When analyzing potential for improving the Recovery macro-indicator, it should be considered that quantum cryptography might contribute by enabling recovering actors to coordinate operations while being reasonably shielded from hostile interference. After a disruptive event in space, secure communication is a fundamental aspect. as false reports or leaked information can constitute an obstacle towards recovery. Quantum-encrypted channels eliminate that vulnerability: recovery teams can share damage assessments, command sequences, and recovery schedules over QKD-secured links knowing they are authentic and confidential. This assurance can thus improve the "recovery speed" micro-indicator by reducing the need for fact-checking information. It also means recovery decisions (which often contain sensitive data and information) remain directed strictly to intended actors. Quantum cryptography being implemented across institutional frameworks for outer space governance might also strengthen Normative Resilience when considering the diplomatic dimension of international cooperation: two clear example are the "enforceability" and "dispute settlement mechanisms" micro-indicators, which arguably benefit when related emergency negotiations remain

private, reducing the risk that public leaks will force governmental actors into rigid postures. If offensive cyber capabilities become ineffective against quantum-secured systems, states may also be less inclined to develop or deploy them: in a long term perspective, adoption of quantum cryptography within an institutional framework could thus improve the “endurance of core principles” micro-indicator through ensuring peaceful use of space (at least when it comes to the encryption domain), as such principle effectively relies on states being able to cooperate without fear of or manipulation. Overall, integrating quantum cryptography into outer space governance frameworks would be instrumental for improving virtually all key macro-indicators.

7. THE FUTURE OF SPACE GOVERNANCE

The following Chapter attempts to provide a more discursive examination of future perspectives for space governance. While the preceding contents of this dissertation have diagnosed current weaknesses attempting to suggest specific solutions for arising issues, this chapter acknowledges how the current trajectory which has been observed could ramify in the future; the continuous emergence of new outer space powers, the diversification of interests and engagements in this domain and the over space as a competitive domain versus a global commons approach all suggest how future governance challenges, especially when it comes to crisis management, might be shaped. This chapter, therefore, might be useful to contextualize this dissertation's discussion within a broader context.

7.1. The Rise of New Space Powers

During the Cold War era, outer space was largely within the United States and the Soviet Union's domain, as their rivalry constituted the core of the early race for outer space. In the 21st century, the bipolar paradigm of the Cold War left room for an increasingly multipolar structure, in which many nations started to cultivate spacefaring ambitions by developing their own autonomous capabilities. This rise of new governmental actors, alongside already recognized leaders, is rooted in the consideration that these capabilities currently constitute an important segment of projecting national power: advances in, and possession of, space-related assets and services have become a status symbol in international affairs, despite the high costs and technical challenges which are related to their implementation and maintenance.

China, whose exponential progress in outer space (among other sectors) has fundamentally altered the balance of power in orbit, stands out as the most rapidly advancing actor. As analyzed in the context of a report from DIA (2022), Chinese capabilities saw astounding progress, going from the first mission crewed by China's astronauts in 2003 to assembling its own modular space station by 2022, achieving the first landing on the Moon's far side and also successfully completing a Mars rover mission. Contextually, it is important to remind how within the previous decade China and Russia have intensified their cooperation and established several common positions on issues and policies related to outer space governance, often in opposition to Western preferences (Liu, 2024). Alongside Russia, China views dominance in the space domain as essential to national security and power projection. Beijing and Moscow have now considerably expanded their space-based assets and "are now seeking ways to expand their own capabilities and deny the U.S. a space-enabled advantage" (DIA, 2022, p. IV). As discussed in Chapter 4, both countries established specialized military space units in 2015, with Russia reconstructing its previously existing Space Forces and China creating the People's Liberation Army Strategic Support Force to incorporate space and cyber-warfare into its existent military doctrine, substantially increasing budgetary investments towards that sector. Other than China, India represents the second major emerging actor in the outer space sector. Although for a long period of time

India's space program essentially focused on civilian and developmental objectives, essentially respecting the core principle of peaceful uses of outer space, this posture has recently changed as a reaction of other powers increasing their military space capacities, with the previously discussed "Mission Shakti" being the first evident signal of a change of approach when it comes to developing ASAT capabilities (Lauer, 2022). The central point of this observation would be that of trying to observe a broader pattern, which is not only limited to military aspects, of emerging powers acting to ensure both their security and their autonomy: multiple countries are now developing satellites, launchers and other assets, which show how the distribution of power in outer space appears to follow a multilateral trend. In fact, several other countries beyond those already mentioned, ranging across different regions, are following that same trend. In the Middle East, for example, governments that historically were not leading space players have been working on costly and ambitious initiatives within the course of the past two decades, as Paikowsky (2024) analyzes. The most active among these are the United Arab Emirates (UAE) and Saudi Arabia, which have begun to invest in space initiatives as part of their respective national strategies, with varying motivations. One of these is their perception of space technology and capabilities as important for economic modernization and diversification, with the perspective of reducing their reliance on oil export (especially in the context of a "post-oil" economy) by stimulating the high-tech sector and increasing their development of human capital (Paikowsky, 2024). On the other hand, as previous chapters consistently state, space assets are also valued for national security and communication purposes, all of which influence a country's strategic stability, which is particularly prized in a regional context as volatile and fragile as the Middle East currently is. The UAE, for instance, has distinguished itself by established its national space agency in 2014, as well as, in 2020, sending the Hope probe to Mars, which made the UAE the first Arab nation to reach its surface (Paikowsky, 2024). In 2019, it has also sent its astronauts on a space mission aboard the International Space Station in 2019, which constituted an important symbolic milestone. Saudi Arabia, for its part, created the Saudi Space Commission in 2018, investing in its own space capabilities and following suit, with Saudi astronauts flying to the ISS in 2023. It is also important to consider, however, that West Asian states are still lacking when it comes to certain advanced capabilities; for example, Israel remains the only national actor in

the region that can independently place satellites into orbit (Paikowsky, 2024). Generally, emerging space powers often depend on collaborating with more established actors for launches and similar important activities. Similar patterns are visible in other regions, from Turkey investing in the autonomous development of its satellites to the emergence of regional blocs in Africa and Latin America. An important development is represented by the establishment of new cooperative bodies, for instance the African Space Agency, which was created by the African Union in 2022, and the Latin American and Caribbean Space Agency, formed in 2021, both of which follow the trend described within this section.

Another notable example of a cooperative framework, which was briefly mentioned in Chapter 3, is APSCO, whose membership as of 2025 includes China alongside Bangladesh, Pakistan, Iran, Turkey and other national actors; China effectively serves as the group's leader, providing the lion's share of technical expertise, training programs and relevant endeavors which aim to help less-developed member states to develop their own outer space capabilities (Yan, 2020). APSCO essentially shows how emerging (yet resourceful) spacefaring powers like China can further grow their role and influence through soft power and regional influence: analysts like Yan (2020) have pointed out that APSCO's organizational structure is deeply hierarchical in nature. Such developments might provide a reflection on how multilateral cooperation in outer space might continue to serve the strategic interests of a limited group of countries in spite of more widely distributed autonomous capabilities. Just as the United States has built coalitions and partnerships (for instance through the Artemis program), China might be in the process building its own group of aligned states through mechanisms such as APSCO.

The rise of new space powers is important in the context of this dissertation for its institutional implications. As for other domains, a multipolar outer space environment is inherently more complex (and, arguably, less stable) than a bipolar one. With more actors which can act autonomously in space, the risk for confrontations and hostility might increase sensibly. We have already seen warnings signs of this emerging instability when, in Chapter 4, India's ASAT test in 2019 has been referenced, which saw international concerns and condemnation.

It should also be noted how obtaining a consensus on new binding norms and general principles might constitute a harder task when dozens of actors press for the consideration of their respective national interests. If, on one hand, growing membership in related international forums such as UN COPUOS and diverging points of view on issues, as well as the inclusion of new voices from what is generally defined as the "global south" constitute a signal of a more representative international discussion, it could also give way to slower decision-making. For instance, debates over principles such as "space as a global commons" or the freedom to exploit space resources have been growing consistently (this will be discussed later in section 3): this implies how existing core treaties like the OST (1967), drafted in a context in which only few governments could be defined as spacefaring powers, are being tested by outer space multilateralism. Thus, questions arise about how to enforce norms, especially given how in outer space governance such enforcement is only backed by voluntary norms and great-power leadership, the latter of which appears to be relatively weakening.

In conclusion, if not properly managed, multipolarity in the governance of Outer Space might increase the potential for large scale crises by increasing instability and rendering long-standing norms outdated or otherwise insufficient. To avoid such a scenario, supranational governance frameworks might need to carefully balance widely distributed national interests with international cooperation across all its aspects and dimensions, as will be explored within the next section.

7.2. National Interests, Supranational Institutions and International Cooperation

Although its structure has considerably changed, ever since the Cold War the governance of outer space has been defined by the tension among how different strategic interests cause rivalry even as technical and scientific progress would, to a degree, encourage cooperative endeavors. The difficult balance of such a "push-pull" dynamic, as defined by Theresa Hitchens (2010), between competition and shared benefits on the other, now appears to undertake a major stress-test as spacefaring powers are using their related budget for national military space commands, anti-satellite weaponry and exclusive partnerships, reflecting a more competitive approach. At the same time, as it has already been widely established across this dissertation, the management of crises in outer space (especially when considering events classifiable as "black swans") necessitates a reinforcement of international cooperation across all of its dimensions, with mechanisms and institutions which can serve as coordinators and thus mediate between sovereign interests, rather than purely being directed by their respective national ambitions.

If a realist international relations perspective is to be taken as an approach, it can be argued that outer space simply serves as an extension of international competition. States seek security and prestige in orbit, which might lead to rivalries among superpowers and a "zero sum" approach (one example being how the United States and China are developing parallel lunar programs). Cross and Pekkanen (2023) suggest that great power competition might be resurging in space, with an adversarial approach overcoming more traditional routes and channels for diplomacy; they also note that, if diplomatic mechanisms reveal themselves unable to withstand such change, outer space could become the main arena of 21st century superpower competition. The "Astropolitik" approach adopted by several realist theorists also appears to suggest a growing view of outer space as an arena for struggle and competition (Cross & Pekkanen, 2023). Concrete policies which seem to suggest such a trend, such as the establishment of various national "space forces" and the increasing production of military and duel-use equipment in outer space, have been widely mentioned across previous chapters, the main argument being

that their consequences (like orbital debris or heightened mistrust) might generate disruptive crises which no single national power may be able to resolve by itself.

International institutions have attempted to balance national self-interests and promote the establishment of technical standards, shared forums for effective dialogue and negotiation (such as UN COPUOS) and the drafting of relevant norms: as of today, their effectiveness decreases as they appear to be under a stalemate, with important norms remaining unaddressed due to powerful national powers having the ability to veto or invalidate norms which are perceived as contrary to respective interests and increasing distrusts among rival actors. One example was the effective failure of the Moon Agreement (1979): its implication that lunar mining benefits should be shared was rejected because of major powers refusing to deprive themselves of future benefits derived from lunar resources' exploitation, and to this day the Agreement enjoys no effective impact in outer space governance, having been ratified by very few national governments (de Zwart, 2021). Given how proposed normative instruments risk collapsing when threatening a State's potential derived benefits, it might be reasonable to suggest that universal frameworks only work when they are able to account for sovereign interests (or, in other words, whenever powerful actors find it more beneficial to enforce norms rather than the opposite). Such an example was represented for several decades by the ISS framework, which was carefully structured to respect each side's interests through the establishment of an intergovernmental governance structure, avoiding supranational regulation and allowing national jurisdiction across different segments of the Station; functional cooperation between Russia and the United States, as noted by Farsaris (2021) and in Chapter 3, withstood several crises, although barely overcoming that of the Russo-Ukrainian 2022 war. It must also be repeated that the ISS is also not a global framework, with rival states, most notably China, setting up their own independent projects. The European Space Agency's geographical return principle (which has been analyzed in detail in Chapter 3) is another example of effectively reconciling national interests with cooperative needs: governments can internally justify participation to the Agency as funds invested turn into jobs and contracts and, at the same time, the Agency itself is able to set long-term agendas (Beaumier et al, 2024). With the diversification of space actors, both governmental and commercial, outer space governance and diplomacy

is becoming more complex, with traditional instruments such as the UN being currently unable to encompass and supervise the entire process. Cross and Pekkanen (2023) point out how space diplomacy now includes several mechanisms that range from formal negotiation channels to informal inter-agency information exchange, including even technical collaborations with and between private companies. The authors identify three key diplomatic mechanisms which can lead to improve cooperative endeavors in outer space governance: communication, persuasion and bargaining, which take particular directions and shapes when applied in this specific context. Communication might, for example, be represented by transparency measures such as data sharing to prevent collisions; persuasion could be the effective promotion of responsible behavior through bilateral agreements or joint statements; bargaining often takes the shape of partnership deals between diverse actors. The effectiveness of these mechanisms in outer space, Cross and Pekkanen (2023) argue, will determine both the specific areas and the depth of international collaboration in space, determining whether spacefaring actors will go back toward militarized competition.

One of the most central points of such a reflection, which was also touched on in section 6.1, is that of mutual dependence on space systems for various purposes. In fact, interdependence may encourage cooperative endeavors from a place of self-interest: certain collective goods, like maintaining an environment which is sustainable in outer space, might be preserved because the benefits which national actors derive from it is greater than those which come from any other arrangement. It can be argued that it was this very notion which led the U.S. and Russia to continue to operate the ISS even when under very strained relations. In a similar way, the United States and China have engaged in intermittent diplomatic discussions, as both worry about the consequences of accidents or cases of miscommunication. Importantly, diplomacy in outer space is now no longer a process which is exclusively managed by governments. In that sense, as Del Canto Viterale (2024) argues, we might face a period of transition in which a more complex, multi-level system is beginning to emerge. In this new context, power is distributed among many more states and non-state actors, with diversified issues in which security, commercial uses of space and technical-scientific operations are strictly interrelated; as a consequence, effectively managing the “global space

system" will require diverse actors, which may range from national governments and intergovernmental institutions to private sector and scientific networks (Del Canto Viterale, 2024). Such a development would show that, rather than through the dominance of a single supranational entity, governance of outer space would be handled by the interaction of separate and diverse actors, frameworks and institutions: in a context characterized by this feature, diplomacy in outer space would, essentially, operate to ensuring that such a system's layers are able to work together and avoid conflict. Outer space diplomacy would, essentially, follow a direction in which governance does not simply reside within a single institution but, rather, work through several coordinated mechanisms.

The interaction between sovereign interests and collective governance does not limit itself to outer space activities; rather, it is a very broad and characteristic feature of international cooperation. In that sense, space governance might benefit from observing similar themes occur in separate areas such as climate change, global health and ensuring non-proliferation of nuclear weapons. In the climate regime, there is a tension between reducing the drastic consequences of global warming and single States' reluctance to sacrifice their own economic growth in the short and medium terms. National actors only agreed to organized institutional cooperation when the Paris Agreement (2016), a flexible framework which effectively allowed them to set their own goals and commitments, was adopted. This development might arguably be described as similar to an issue widely described in previous chapters when describing outer space governance, which sees binding treaties failing to gain traction but, on the other hand, guidelines and soft law instruments be more easily implemented. When it comes to global health, WHO provides guidelines and encourages data sharing, but it cannot, by itself, force sovereign states to be transparent or to coordinate if they choose not to do so. This has parallels as for how, despite having reached a consensus on principles of notification and consultation in the Outer Space Treaty, states have nonetheless chosen not to abide by those same principles when conducting military testing; those precedents show that international cooperation mechanisms, at their core, depend on political will to follow them, something that might be weakened by reciprocal mistrust among governmental actors. The Nuclear Non-Proliferation Treaty (1968) is another example of a legal framework which relies on constant

negotiation and the role of institutions like the IAEA, which inspects and verifies compliance with the treaty's objectives. When it comes to outer space governance, there is no verification mechanism enforced to inspect for military space activities which may be in violation of previous agreements or norms; this is largely because there was no political will on the part of leading spacefaring powers to create any entity with the objective of monitoring their space activities in that way.

Supranational mechanisms can, overall, serve as mediators only up to the extent that states allow them to. International relations theory appears to suggest that as long as the international system is anarchic (no world government), states will only empower institutions when it's in their interest to do so. In space governance, there are signs that the interests of states may gradually align when it comes to certain threats (like orbital debris, planetary defense against asteroids, or harmful interference) for which it is recognized that coordinated action may become the rational choice. At the same time, the emergence of new and variegated actors thus far described makes unilateral dominance increasingly less plausible; furthermore, the interconnectedness and interdependence of space assets could create a context in which hostile actions are considered mutually detrimental, encouraging a pluralistic idea of security. Such a scenario would, at the same time, improve crisis response to an external threat by ensuring greater coordination and reduce the potential for an internally generated "black swan" event (for instance, due to a conflict caused by diplomatic tensions).

It can overall be stated that supranational mechanisms have an important but somewhat constrained role in outer space governance. The most successful examples of cooperation in space show that institutions work best as mediators rather than as if they themselves were sovereign authorities. If able to understand their role and maintain that delicate balance, supranational institutions may leave room for governments being able, when necessary, to cooperatively manage black swan events or unforeseen challenges and operate toward achieving collective goals in space even under the constraints represented by a competitive context.

7.3. The Debate on Space as a Global Commons

This section aims to focus on the question of whether outer space should be treated as a global commons, which represents a fundamental and contentious issue in space governance. In principle, "global commons" refers to a domain beyond national jurisdiction that all states may use but none can appropriate, and which should be used for the benefit of all humanity. International documents have referenced this same concept: for example, the Brundtland Commission in the 1980s considered outer space, alongside both Antarctica and the oceans, as a global commons, and the OECD has defined global commons as "natural assets outside national jurisdiction", explicitly citing outer space as an example (Pic, Evoy, & Morin, 2023). At the same time, however, this is not how outer space jurisdiction is predominantly defined in the context of legal documents and frameworks. For instance, although the OST (1967) defined the exploration and use of outer space "the province of all mankind", it did not make use of the term "global commons." In fact, there is no global consensus on this particular definition: on the contrary, the United States government has been especially clear in rejecting it, with a 2020 Executive Order stating that it does not consider space as a global commons. Other major spacefaring powers have similarly tried to avoid that definition when drafting or producing official treaties and policies. This specific ambivalence reflects a deeper debate about the implications of the commons concept when it comes to outer space activities (Secure World Foundation, 2022; Pic et al., 2023).

Proponents of the global commons framing argue that it carries important normative weight. Describing outer space as a global commons is seen as a symbol of collective responsibility aimed at protecting the space environments for the common good of all nations. The main point brought forward by proponents is that formally recognizing space as a global commons could constitute an incentive toward a framework that is more able to prohibit harmful activities and, aligning with the core principles of the OST (1967), ensure equal access and benefit to all countries, including emerging actors (Pic et al., 2023). On the other hand, critics fear that labeling outer space as a global commons might risk introducing new constraints which could disincentivize innovation and investments: more commercial perspectives argue that labeling space a commons could lead to

redistributive international measures such as the requirement to share profits from space mining or restrictions on commercial uses, potentially providing international bodies with the power to interfere with national or private space endeavors (Goehring, 2021). Examining the legal foundations, Gohering (2021) also analyzes how the term "global commons" effectively lacks a clear normative definition, which may lead to different interpretations and expectations: one interpretation is that of being free to use and access without exclusion, while according to another it is a matter of a shared heritage which would require collective oversight and an equitable distribution of resources. States have tried to interpret such a concept according to their own prerogatives: for instance, the United States and several like-minded national actors have proceeded to establish frameworks which aim, in particular, to reject explicitly the notion of the "common heritage", which is judged as stricter. This is further shown by the structure and contents of the Artemis Accords (2020) with regard to resource extraction, which is in line with the United States' general approach and has been discussed in previous chapters. This aspect is also shared by the national programs and partnerships of Russia and China, which adhere to the no-appropriation principle found in the OST (1967) while stopping short of establishing any new multilateral "commons" regime. Essentially, formal establishment of such a regime appears to be viewed with distrust by major actors seeking to avoid governance arrangements that might in the future limit their operating freedom and economic profits (Goehring, 2021; Pic et al., 2023).

It should be noted how the language of "commons" is effectively rare when examining concrete operational agreements, especially among leading powers. A recent comprehensive study which comprised 1042 space-related arrangements found that concepts related to the global commons are virtually absent in these contexts (Pic et al., 2023). Even references to outer space as the "common heritage of humankind" or the "common interest of all" appear infrequently and have been mostly confined to high-level declarations or within the declaratory means of international forums. In particular, there is no mention of this notion when analyzing bilateral agreements between spacefaring powers (Pic et al., 2023). Another instance of this tendency is found in China's International Lunar Research Station initiatives; in fact, just as that of the Artemis Accords, these initiatives never explicitly invoke a "global commons" framing. Furthermore, Pic et al. (2023) also

observe that even when commons-related principles are mentioned, they do not necessarily mean that different operational rules are being applied. Agreements that contain wording such as the "benefit of all humanity" or similar notions still rely on similar mechanisms and obligations as those that do not, indicating that the label has so far been largely abstract in nature. Their findings lead to the conclusion that a clearly defined, as well as operationalized, global commons perspective for space "has yet to be articulated and institutionalized" (Pic et al., 2023). In other words, this notion has not matured into a concrete governance model and remains somewhat disconnected from the management of day-to-day activities in outer space.

As earlier chapters have described, the international framework of outer space governance was met with increasing difficulty to approve, in the context of international forums such as UN COPUOS, proposals related to new norms, especially when binding (Martinez, 2021). A commons-based approach would inherently need considerable transparency and an high level of reciprocal trust among actors engaging in negotiations, which constitutes a difficult and perhaps unrealistic goal to reach when it comes to current developments. Toyoma (2021) makes an insightful point arguing that, although international cooperation (which he analyzes mainly under the lens of its technical dimension, related to how joint development of related technology would ease single States' respective financial burdens) is in fact essential for countering emerging outer space threats, diplomatic tensions complicate the overall picture, making actors resist frameworks that demand shared responsibilities.

The main reason for discussing the commons debate in the context of crisis management is that it can be argued for its relevance to existing practical challenges. One of those is represented by the extensively discussed issues related to space debris-related crises. Given the problem of increasing debris (especially in LEO), it should be noted how no single actor "owns" orbital regions under the current framework, and thus all share concerns related to keeping such regions as secure and usable as possible. This situation, as approached by Wang (2013), might constitute an example of a potential "tragedy of the commons", which consists of short-term benefits which derive from users exploiting a resource (e.g., launching satellites, testing ASAT weapons, etc.) but paying a potentially greater collective

cost under a long-term perspective (increased risks for collisions and major loss of capabilities). As Wang (2013) also notes, outer space currently constitutes a typical commons simply because of every state having the right to use it without some power being able to formally exclude others: it follows that, without restraint, such resource faces the risk of being polluted. The debris problem is then discussed under the lens of basic property rights and issues related to externalities. Without clear ownership or accountability measures for orbital, the author warns that no actor would be provided with sufficient incentives to autonomously invest in structurally preventive measures. Wang (2013) also provocatively suggests that, to escape this trap, one solution might be that of introducing some form of property rights or other similar mechanisms that to some degree are similar to a process of privatization, which would as a consequence internalize the externalities of debris creation (Wang, 2013). This perspective implies that, on one hand, understanding and treating orbits purely as "global commons" could have unfortunate effects which would be undesirable for the totality of actors involved, also reflecting on how pragmatic governance might address the issue by assigning responsibilities or usage caps, which would have the effect of environments such as LEO being managed as a shared but regulated resource.

This perspective does not constitute the only one in the field, with others, such as Wesel and Lambach (2021), focusing on simply working on such issues by strengthening cooperative regimes rather than through privatization. In this context, space debris is predominantly approached as a global commons problem which requires innovative collective approaches and solutions. The authors take previously existing principles related to the management of "common-pool" resources to argue how an inclusive system of governance would be more effective than "top-down" treaties among governments. In their proposal, several actors (which include state actors as well as private ones and international organizations) would coordinate to prevent debris accumulation (Wesel & Lambach, 2021). This approach is also presented as more pragmatic and politically feasible in the current era in comparison to pressures for new comprehensive and binding space treaties that face the risk of being obstructed by major powers. Voluntary guidelines, shared operational standards which include transparency measures and data-sharing initiatives could become international norms. Some follow-ups might be

represented by current real-world developments such as IADC mitigation guidelines being now followed by many space agencies and the previously discussed U.S. unilateral moratoria on ASAT tests (Lauer, 2022). Although national actors avoid using "global commons" terminology, these measures could be seen as small, incremental steps toward the idea of outer space being a common heritage to be protected through a "distribution of power" approach which is inclusive toward minor actors and improves reciprocal transparency and trust among powers. It would also be useful to analyze which recently created international frameworks are consistent with some of the ideas of preserving outer space as a "global commons". Martinez (2021), for instance, sees the adoption of the Long-Term Sustainability (LTS) Guidelines by COPUOS as consistent with the idea of preserving outer space as a global resource. Although the word "commons" does not appear in the guidelines, the idea of ensuring that the use of outer space remains possible for all through shared responsibilities aimed at ensuring collectively beneficial outcomes appears in line with the "global commons" understanding and spirit. Successful implementation of these guidelines, as Martinez (2021) emphasizes, would need the cooperation, involvement and compliance not only of governments but also by private sector and civil society.

L. Martinez (2021) observes how, at their core, states' motivations to either cooperate or compete in space are heavily influenced by the overall configuration of power and interests on Earth, providing an analytical framework to understand these motivations: arguably, if leading states perceive that their security or economic advantages are best preserved through unilateral freedom of action, then they could be expected to resist commons-oriented governance; on the opposite side, if the risks and costs of an unregulated domain are perceived as being too high, cooperative constraints could be implemented without as much resistance: with satellite numbers increasing along with related collision risks, as well as commercial space actors rising in recent years (potentially making previous frameworks obsolete), governments appear forced to acknowledge a new degree of interdependence.

A report from the Secure World Foundation titled "is space a global commons?" (2022) insightfully notes how outer space is far from being a single structure, consisting instead of several different sub-domains such as low earth orbit

(LEO), geostationary orbit (GEO), the Moon, as well as other celestial bodies each with very different characteristics and pressures. The report argues how some technical aspects related to these sub-domains (e.g., the radio-frequency spectrum and orbital slots in GEO) already possess management mechanisms that strongly resemble a "global commons" management approach. Others, like questions related to the extraction and management of space resources (especially in deep space), still constitute a legal gray area: the main argument is that parts of outer space could be treated as commons through collective international agreement even if they are not inherently commons by nature (Secure World Foundation, 2022). Other insights include the exploration of creative solutions which would include recognizing certain environmental features of space themselves as having legal personhood or establishing new kinds of property rights that are intrinsically structured to incentivize preservation. Such exploratory ideas, although needing practicality in application, support the concept that in order to improve institutional resilience of space governance frameworks relevant actors might benefit from a mixture of traditional cooperation based on treaties and innovative tools which might be more tailored to the contemporary system's current developments (Secure World Foundation, 2022).

It can be concluded that, although the global commons framework is still broadly a focus of debate, it is increasingly central to how we think about the future of space governance as well as connected to the themes explored in previous chapters of this dissertation, as institutional resilience (especially in the context of crises, even more so when characterized as "black swans") is strongly shaped by how effective international cooperation can be within a domain which displays the intrinsic potential of producing externalities and threats that are beyond single actors' control. Collective action might prove itself to be necessary to prevent irreversible harm caused by heterogeneous factors which range from debris to particularly disruptive military conflicts in which outer space assets play a critical role. Whether the notion of space as a global commons will become more formally relevant or not would depend, as Hitchens (2010) outlined in discussing space multilateralism, on whether mistrust and competitive instincts "pull" states away from ceding any authority or "push" towards acceptance of the limits that a true global commons regime would necessarily require (Hitchens, 2010).

8. CONCLUSIONS

The previous chapters have tried to show and describe how contemporary developments in outer space activities outpaced the evolution of international regulatory frameworks as well as how the current scenario might risk to increase the probability of disruptive crises in this domain. This thesis aims to give an overview as to whether and how current cooperation frameworks for the governance of outer space can be improved to manage crises, particularly under the hypothetical scenario of unpredictable "black swan" events (Taleb, 2007); another important aspect of the implied research question pertains to the role emerging technologies such as AI, blockchain and quantum cryptography might play in addressing crises and improving said frameworks. Through seven chapters of analysis, the research examined both the strengths and weaknesses of existing space governance arrangements, investigated historical and hypothetical crisis scenarios and explored technological innovations with the objective of identifying specific governance gaps and attempting to propose appropriate solutions; overall, this dissertation emphasizes the importance of establishing pre-emptive measures and ensuring proactive adaptation in space governance. One of the main dangers analyzed within the entirety of this body of work relates to how, without updates to our cooperative frameworks, the increasingly accelerated pace of change in outer space could further complicate the reactions of institutions which may be unprepared for large-scale, unforeseen events.

A central finding is that today's international frameworks, while historically important for the establishment and continuation of peaceful outer space activity, contain significant weaknesses when confronted with emerging threats and extreme crisis scenarios. Chapter 3 takes into consideration several ones, analyzing how many different governance structures were forged decades ago under considerable different assumptions from those emerging from contemporary developments. Treaties like the OST (1967) established broad principles (e.g. the non-appropriation of space, use of space for the benefit of all and the prohibition of weapons of mass destruction in orbit), which has been recognized as having been instrumental to prevent conflict in space for over half a century. Intergovernmental projects the International Space Station (ISS) further proved that rival nations can

jointly achieve and maintain shared initiatives in space through carefully balanced agreements, especially when it comes to sharing operational standards and cooperating on technical feats, even under periods of strong political tensions like the 2014 Crimea crisis (Farsaris, 2021). Regional institutions like the European Space Agency (ESA) have shown the importance of incentives when used to align national interests with collective goals, with one important example being its "geographical return" principle, which ensures member states benefit directly from funds invested (Beaumier, Couette, & Morin, 2024). The latter examples show that meaningful collaboration on outer space initiatives is achievable when institutional frameworks can put together sovereignty concerns and the pursuit of shared objectives.

Despite these strengths, the current regime shows clear weaknesses when it comes to their respective abilities to manage crises: for instance, many existing agreements lack binding enforcement or rapid response mechanisms, making effective crisis coordination rely on national governments' political will, which in turn depends on their respective national strategic objectives. These weaknesses have been measured through the lens of four main macro-indicators (Preparedness, Agility, Recovery, Normative Resiliency) which try to describe and broadly encompass the elements taken in consideration by existing crisis management literature as well as several related micro-indicators. Throughout the dissertation, the concept of "institutional resilience", which refers to the capacity of governance frameworks to absorb shocks and adapt to unforeseen events, has essentially constituted its central topic. By applying this concept to space institutions, this thesis attempts to bring together multidisciplinary insights from international law, astropolitics and crisis management theory to evaluate whether current frameworks are sufficiently prepared.

As observed in Chapter 4's case studies, international responses to outer space emergencies have often been insufficient in real world scenarios, as proven by events like the 2009 Iridium–Cosmos satellite collision or several anti-satellite (ASAT) weapon tests in the 21st century, to which the global community largely reacted through formal expressions of concern or the drafting of non-binding guidelines, without establishing protocols that are effectively enforceable. COPUOS, which constitutes the main multilateral forum at the international level,

appears to suffer from the same limitations of the larger UN framework in that it can debate norms and issue recommendations, but it does not possess the power to enforce compliance or to coordinate real-time crisis responses. This means that in a sudden orbital disaster or hostile act in space, it cannot provide or enforce an authoritative international emergency plan which is ready to deploy. Some of the main weaknesses in governance appear to be related to decision-making, issues concerning legal liability and authority (especially when it comes to the emerging issues of autonomous systems and private actors) and reliance on bilateral arrangements instead of reaching decisions through multilateral discussions. Historically, outer space constitutes no exception, substantial legal or policy changes tend to happen during the aftermath of an impactful crisis rather than before, within the optic of introducing preventive measures. This reactive tendency is especially dangerous in the context of "black swan" events: chain-reaction collisions between satellites or a large-scale cyber-attack on satellite networks could cause enormous disruptions before relevant actors and framework are able to put together a comprehensive response, with the additional result of exposing our systems' current dependence on space assets. The absence of pre-agreed crisis protocols or enforcement tools in current frameworks represents thus a very relevant vulnerability.

Chapters 4 has shown how various threats, ranging from militarization to commercial space actors and cyber threats, could further introduce increasing strain on governance structures as they struggle to adapt. Outer space is increasingly seen as a strategic domain by major powers, which have reacted by adjusting their own willingness toward more militarized approaches, signaling how norms against the weaponization of space are now undergoing a process of erosion (Defence Intelligence Agency, 2022; Lauer, 2022). Such competitive approach might constitute a culprit for hostility and crises, as accidents in orbit could touch national security interests and escalate conflict, even if just through miscommunication (Cross & Pekkanen, 2023; Hammack, 2021). At the same time, the rise of private space actors appears to create new complications (as well as opportunities) for crisis management. Commercial satellite operators now provide fundamental services while not being formal parties to treaties and often remaining outside traditional chains of command, which remain largely government centric. For instance, the

Ka-Sat attack has shown how, without specific international law that addresses such scenarios, governments face the struggle of coordinating with corporate entities without a general frame of reference. These developments have shown that space governance must now take into consideration a complex, multi-level and polycentric system of actors and interests (Del Canto Viterale, 2024). Chapter 7 previously discussed how the growing ambitions of emerging actors mean that any effective framework must be more inclusive and adaptive than those of the past: if not properly managed, a multipolar environment could mean increased instability and the potential for large-scale crises because of current norms failing to adapt and thus being rendered obsolete; a context which left room for unrestrained competition, for instance, could negatively affect both the risk for a truly devastating black swan event in orbit and frameworks' coordination in responding to it.

This dissertation attempts to contribute by offering several proposals to strengthen international frameworks and improve resilience. In order to propose comparable methods for space governance, Chapter 6 used experiences from other international fields that have faced transnational crises, particularly public health and finance (Lamm et al., 2022). One suggestion is to set up quick coordination procedures for space crises, similar to pandemic alarm systems or disaster response protocols, so that countries and pertinent organizations are prepared to respond cooperatively in the event that satellites malfunction or are attacked. In order to facilitate quick information exchange and group decision-making in the critical hours after an incident, this could entail specific communication channels connecting space agencies, military space commands, and significant private operators. The chapter also highlights the importance of including the private sector into cooperative structures, arguing that formal public-private collaborations for space crisis management should be established, as institutional actors would benefit from the assets and capabilities that firms possess.

Another major area of improvement lies in updating and expanding the legal regime to address pressing gaps; one of these consists in the lack of any treaty provision that prohibits or regulates ASAT tests and space weaponization, which constitutes a dangerous omission given both the debris and mistrust generated by these tests (Lauer, 2022). The drafting of a targeted agreement which would ban the

most harmful ASAT activities or, at least, establish liability and notification requirements for testing that create orbital debris, could serve as a first step toward a more comprehensive regulation of the issue. It is also important to consider how nations are starting to plan towards activities such as lunar mining, which imply a need to revisit the "collective heritage" principle of the Moon Agreement (1979) and reconcile it with national interests to prevent the absence of a legal framework which can be adopted and respected by major powers (de Zwart, 2021; Mavroeidi, 2019). The research suggests that adaptive diplomacy, possibly starting with soft law frameworks which would eventually be able to evolve into binding norms, will be required, given how universalist frameworks have been largely unadopted when perceived as contrary to the strategic interests of national powers, as it has been evidenced by the failure on the part of the Moon Agreement to gain broad support. On a positive note, arrangements like the Artemis Accords (2020) show that parties are willing to endorse updated principles related to exploration and resource use, although, as of today, these accords remain non-binding and non-universal (de Zwart, 2021).

Chapter 5 aimed to analyze the role of emerging technologies by evaluated tools like artificial intelligence (AI), blockchain, and quantum communications, all of which appear to give several opportunities to improve space operations and governance, ranging from space situational awareness improvements through AI to the ability of blockchain technology to create unalterable records which would increase transparency and trust among actors, as well as improve supply chains, up to QKD's promise of theoretically unbreakable encryption for satellite links (Carrasco-Casado et al., 2016). These technologies, if incorporated responsibly, could potentially strengthen the overall resiliency of space systems and institutional frameworks by a substantial level, as well as improving both monitoring and enforcement. On the other hand, without proper regulation and oversight, these technical tools could themselves introduce further risks and strategic instability, especially if pre-existing regulatory issues (such as that of liability for autonomous systems) are not solved. In that sense, this dissertation serves as an attempt to put together technological implementation and institutional policymaking, arguing for greater communication between these two domains. These findings suggest that, although remaining important, the current outer space governance framework needs

to be updated to sufficiently face modern challenges. This thesis aims to contribute to the current literature by systematically identifying specific, measurable weaknesses (legal ambiguities, lack of enforcement, slow consensus procedures, exclusion of relevant actors, etc.) and by providing analogies to other global governance regimes from which solutions can be incorporated. It also integrates emerging technology not just as an external factor to be regulated, but as a potential instrument for regulators themselves. In doing so, the attempt is to approach the subject from different perspectives rather than by focusing narrowly on a single treaty or issue.

It is also important to acknowledge some of the limitations of this thesis. The first one lies in the inherently unpredictable nature of "black swan" events, which means that any proposals can only reduce, rather than eliminate, the element of surprise in space crises. The issues and themes discussed within the dissertation encompass a broad and diversified range of topics; as such, the recommendations are conceptual frameworks that would require further refinement and examination, both juridical and technical, before being implemented. For example, detailed technical reporting assessing the feasibility of proposed technological implementation of quantum cryptography, blockchain technology or autonomous systems were beyond the scope of this study. The rapid evolution of space activities also implies that some findings could need to be expanded once new actors, technologies, or conflicts that were not fully anticipated in the research may arise. Despite these limitations, the approach of this dissertation is that of identifying the systemic nature of the problem, thus aiming to connect different sectors and perspectives to ensure that recommendations are not compartmentalized or isolated.

In conclusion, it can be said that current cooperation frameworks can be improved by making them more agile, inclusive, and able to withstand crises, with emerging technologies being able play an important role in this transformation if properly regulated; in fact, international frameworks for outer space governance need dedicated crisis management protocols and institutions that are able to respond rapidly to emergencies, much like health governance has plans for pandemics (Lamm et al., 2022). Such frameworks should preferably work toward pre-emptive coordination rather than *ex post* reaction. Improvement also means updating normative instruments in order to reduce weaknesses, which requires inclusive

negotiation across an increasingly diverse range of spacefaring actors: states will need to cooperate not only with each other but also with private companies and various emerging entities, integrating these players into institutional networks and decision-making processes for crises. Technological innovations, implemented within such an inclusive cooperative framework, may act as multipliers for governance and risk management by increasing the speed and effectiveness of collective responses. Thus, the establishment of more resilient institutional frameworks, especially in the context of managing black swan events, would greatly benefit from the interaction of the technological, normative and political domains. Such interaction would enable actors to move beyond reactive approaches and, instead, establishing the foundation for an outer space governance system which could prove more capable of anticipating crises, coordinating responses and preserving stability in orbit even under disruptive conditions.

BIBLIOGRAPHY

Articles

1. Abdi, A. I., Eassa, F. E., Jambi, K., Almarhabi, K., & AL-Ghamdi, A. S. (2020). Blockchain platforms and access control classification for IoT systems. In *Symmetry*, 12(10), 1663. https://doi.org/10.3390/sym12101663
2. Aoki, S. (2024). Outer Space Treaty and Fundamental Principles. In *International Space Law in the New Space Era: Principles and Challenges* (pp. 66–85). Oxford University Press. https://doi.org/10.1093/9780198909415.003.0004
3. Aoki, S. (2024). Legal frameworks for space security. In *The Oxford Handbook of Space Security* (pp. 38–58). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780197582671.013.3
4. Aponte-Novoa, F. A., Orozco, A. L. S., Villanueva-Polanco, R., & Wightman, P. (2021). The 51% attack on Blockchains: A Mining Behavior study. In *IEEE Access*, *9*, 140549–140564. https://doi.org/10.1109/access.2021.3119291
5. Beaumier, G., Couette, C., & Morin, J. F. (2024). Hybrid organisations and governance systems: the case of the European Space Agency. In *Journal of European Public Policy*, 1–31. https://doi.org/10.1080/13501763.2024.2325647
6. Bikos, A. N., & Kumar, S. A. P. (2022). Enhancing space security utilizing the blockchain: Current status and future directions. In *2022 IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE)* (pp. 77–82). IEEE.
7. Brandenburg, M., & Lieberman, S. (2022). Critical Spaces: European and U.S. Institutions for Outer Space. In *Astropolitics*, *20*(1), 93–111. https://doi.org/10.1080/14777622.2022.2098014
8. Brende, B. (2020). Global cooperation is more vital than ever. This is why. *World Economic Forum*. https://www.weforum.org/stories/2020/07/global-cooperation-is-more-vital-than-ever-this-is-why/
9. Carrasco-Casado, A., Fernández, V., & Denisenko, N. (2016). Free-space quantum key distribution. In H. Henniger & O. Bouchet (Eds.), *Optical*

Wireless Communications (pp. 589–607). Springer. https://doi.org/10.1007/978-3-319-30201-0_27

10. Cliver, E. W., Schrijver, C. J., Shibata, K., & Usoskin, I. G. (2022). Extreme solar events. *Living Reviews in Solar Physics*, *19*(1). https://doi.org/10.1007/s41116-022-00033-8
11. Cross, M. K. D., & Pekkanen, S. M. (2023). Introduction. Space Diplomacy: The Final Frontier of Theory and Practice. *The Hague Journal of Diplomacy, 18*(2-3), 193-217. https://doi.org/10.1163/1871191x-bja10152
12. Del Canto Viterale, F. (2024). Global Governance of the Space System: A Multilevel Governance Analysis. *Systems*, *12*(9), 318. https://doi.org/10.3390/systems12090318
13. De La Beaujardiere, J., Mital, R., & Mital, R. (2019). Blockchain application within a Multi-Sensor satellite architecture. *IGARSS 2022 - 2022 IEEE International Geoscience and Remote Sensing Symposium*, 5293–5296. https://doi.org/10.1109/igarss.2019.8898117
14. De Zwart, M. (2021). To the Moon and Beyond: The Artemis Accords and the Evolution of Space Law. In *Issues in Space* (pp. 65–80). https://doi.org/10.1007/978-981-15-8924-9_6
15. Dixon, C. K. (2016). The U.S. response to NEOS: Avoiding a black swan event. *Naval Postgraduate School (U.S.)*. https://www.hsdl.org/?abstract&did=796638
16. Farsaris, A. E. (2021). The International Space Station (ISS) intergovernmental agreement as a precedent for regulating the first human settlements on Mars. In *Studies in space policy* (pp. 63–74). https://doi.org/10.1007/978-3-030-65013-1_6
17. Fleck, A. (2022). The U.S. and China Lead the Space Race 2.0. In *Statista*. https://www.statista.com/chart/28667/countries-are-leading-the-space-race-20
18. Goehring, J. S. (2021). Why Isn't Outer Space a Global Commons? In *Journal of National Security Law & Policy, 11*(4), 573–590. https://ssrn.com/abstract=3867606
19. Graham, T., Thangavel, K., & Martin, A. (2024). Navigating AI-lien Terrain: Legal liability for artificial intelligence in outer space. In *Acta*

Astronautica, 217, 197–207. https://doi.org/10.1016/j.actaastro.2024.01.039

20. Hammack, K. (2021). International relations in Space: The role of miscalculation, militarization, and weaponization. In *Astropolitics*, *19*(3), 230–236. https://doi.org/10.1080/14777622.2021.1982538
21. Hitchens, T. (2010). Multilateralism in Space: Opportunities and Challenges for achieving space security. In *Space and Defense*, *4*(2). https://doi.org/10.32873/uno.dc.sd.04.02.1160
22. Hodgkins, K., & Routh, A. (2021). "Chapter 3 Emergence of and perspectives for a new paradigm in space diplomacy". In *A Research Agenda for Space Policy.* https://doi.org/10.4337/9781800374744.00011
23. Kipping, D. (2021). Black swans in astronomical data. In *Monthly Notices of the Royal Astronomical Society*, *504*(3), 4054–4061. https://doi.org/10.1093/mnras/stab1129
24. Klein, J. J., & Boensch, N. J. (2024). NewSpace and new risks in space security. In *The Oxford Handbook of Space Security* (pp. 761–782). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780197582671.013.42
25. Kaltenbaek, R., Acin, A., Bacsardi, L., Bianco, P., Bouyer, P., Diamanti, E., Marquardt, C., Omar, Y., Pruneri, V., Rasel, E., Sang, B., Seidel, S., Ulbricht, H., Ursin, R., Villoresi, P., Van Den Bossche, M., Von Klitzing, W., Zbinden, H., Paternostro, M., & Bassi, A. (2021). Quantum technologies in space. In *Experimental Astronomy*, *51*(3), 1677–1694. https://doi.org/10.1007/s10686-021-09731-x
26. Kofler, R., Drolshagen, G., Drube, L., Haddaji, A., Johnson, L., Koschny, D., & Landis, R. (2018). International coordination on planetary defence: The work of IAWN and the SMPAG. In *Acta Astronautica*, *156*, 409–415. https://doi.org/10.1016/j.actaastro.2018.07.023
27. Lamm, R., Rahman, U., & Chojnacki, K. (2022). Crisis management checklist: lessons learned from the SARS-CoV-2 pandemic. In *Global Surgery Education, 1(1)*, 31. https://doi.org/10.1007/s44186-022-00033-0
28. Lauer, R. S. (2022). When states test their Anti-Satellite weapons. In *Astropolitics*, *20*(1), 1–26. https://doi.org/10.1080/14777622.2022.2078194

29. Lazarus, J. V., Pujol-Martinez, C., Kopka, C. J., Batista, C., El-Sadr, W. M., Saenz, R., & El-Mohandes, A. (2023). Implications from COVID-19 for future pandemic global health governance. In *Clinical Microbiology and Infection*, *30*(5), 576–581. https://doi.org/10.1016/j.cmi.2023.03.027
30. Liao, S.-K., Cai, W.-Q., Handsteiner, J., Liu, B., Yin, J., Zhang, L., Rauch, D., Fink, M., Ren, J.-G., Liu, W.-Y., Li, Y., Shen, Q., Cao, Y., Li, F.-Z., Wang, J.-F., Huang, Y.-M., Deng, L., Xi, T., Ma, L., ... Pan, J.-W. (2018). Satellite-relayed intercontinental quantum network. In *Physical Review Letters, 120*(3), 030501. https://doi.org/10.1103/PhysRevLett.120.030501
31. Liu, Y. (2024). A research on China–Russia arms control cooperation in outer space: achievement, challenge, and prospect. In *China International Strategy Review*. https://doi.org/10.1007/s42533-024-00166-5
32. Martinez, L. (2021). "Chapter 2 International cooperation and competition in outer space". In *A Research Agenda for Space Policy*. https://doi.org/10.4337/9781800374744.00010
33. Martinez, P. (2021). The UN COPUOS Guidelines for the Long-term Sustainability of Outer Space Activities. In *Journal of Space Safety Engineering, 8*(1), 98–107. https://doi.org/10.1016/j.jsse.2021.02.003
34. Mavroeidi, E. (2019d). The Effectiveness and Applicability of the Moon Agreement in the Twenty-First Century: Will there be a future? In *The Space Treaties at Crossroads: Considerations de Lege Ferenda* (pp. 35–48). https://doi.org/10.1007/978-3-030-01479-7_33
35. Meyer, P. (2016). Dark forces awaken: the prospects for cooperative space security. In *The Nonproliferation Review, 23*, 495 - 503. https://doi.org/10.1080/10736700.2016.1268750
36. Migaud, M. R., Greer, R. A., & Bullock, J. B. (2020). Developing an adaptive space governance framework. In *Space Policy, 55*, 101400. https://doi.org/10.1016/j.spacepol.2020.101400
37. Miller, A. (2025). Micius, the world's first quantum communication satellite, was hackable. 411-415. *2025 International Conference on Quantum Communications, Networking, and Computing (QCNC)*. https://doi.org/10.1109/QCNC64685.2025.00070

38. Obstfeld, M., & Rogoff, K. (2009). Global imbalances and the financial crisis: products of common causes. CEPR Press, Paris & London. https://cepr.org/publications/dp7606
39. Paikowsky, D. (2024). Perspectives on membership in the Space Club in West Asia. In *The Oxford Handbook of Space Security* (pp. 435–454). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780197582671.013.24
40. Peng, H., & Bai, X. (2019). Machine learning approach to improve satellite orbit prediction accuracy using publicly available data. *The Journal of the Astronautical Sciences*, *67*(2), 762–793. https://doi.org/10.1007/s40295-019-00158-3
41. Pekkanen, S. M. (2024). Japan's grand strategy in outer space. In In *The Oxford Handbook of Space Security* (pp. 334–362). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780197582671.013.19
42. Pic, P., Evoy, P., & Morin, J. (2023). Outer Space as a Global Commons: An Empirical Study of Space Arrangements. *International Journal of the Commons*, *17*(1), 288–301. https://doi.org/10.5334/ijc.1271
43. Rahi, K. (2019). Indicators to assess organizational resilience – a review of empirical literature. *International Journal of Disaster Resilience in the Built Environment*, *10*(2/3), 85–98. https://doi.org/10.1108/ijdrbe-11-2018-0046
44. Raska, M., & Davis, M. (2024). The "AI wave" in space operations. In *The Oxford Handbook of Space Security* (pp. 596–613). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780197582671.013.50
45. Ravi, P., Zollo, A., & Fiedler, H. (2023). AI for satellite collision avoidance – Go/No go decision-making. German Space Operations Center (GSOC). https://www.hou.usra.edu/meetings/orbitaldebris2023/pdf/6043.pdf
46. Reed, H., Dailey, N. D., Carden, R., & Bryson, D. (2020). Blockchain Enabled Space Traffic Awareness (BESTA): discovery of anomalous behavior supporting automated space traffic management. ASCEND 2022. https://doi.org/10.2514/6.2020-4105

47. Schmitt, M. N. (2013). Tallinn Manual on the international law applicable to cyber warfare. In *Cambridge University Press eBooks*. https://doi.org/10.1017/cbo9781139169288
48. Tai, M. C., & Fukushima, Y. (2024). Techno-Security Space innovation. In *The Oxford Handbook of Space Security* (pp. 123–139). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780197582671.013.46
49. Toyoma, G. (2021). Countering threats in space through international cooperation. *Space Policy*, *55*, 101387. https://doi.org/10.1016/j.spacepol.2020.101387
50. Unal, B. (2019). Cybersecurity of NATO's space-based strategic assets. Chatham House. https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf
51. Wang, P. (2013). Tragedy of Commons in outer space - the case of space debris. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2260856
52. Wendt, J. A. (2023). Artificial intelligence, genome, cyberspace and space – contemporary threats to the security of the state and nations. *Revista Română De Geografie Politică*, *25*(2), 54–63. https://doi.org/10.30892/rrgp.252101-364
53. Wesel, L., & Lambach, D. (2021). Tackling the space debris Problem: A Global Commons perspective. *8th European Conference on Space Debris*. https://conference.sdo.esoc.esa.int/proceedings/sdc8/paper/230/SDC8-paper230.pdf
54. Yan, Y. (2020). Capacity building in regional space cooperation: Asia-pacific space cooperation organization. *Advances in Space Research*, *67*(1), 597–616. https://doi.org/10.1016/j.asr.2020.10.022
55. Yaniz, F. (2022). Outer Space's legal framework, challenges, and policies. In *Advanced sciences and technologies for security applications* (pp. 3–22). https://doi.org/10.1007/978-3-030-95939-5_1
56. Zhou, L., Lin, J., Ge, C., Fan, Y., Yuan, Z., Dong, H., Liu, Y., Ma, D., Chen, J., Jiang, C., Wang, X., You, L., Zhang, Q., & Pan, J. (2024). Independent-optical-frequency-comb-powered 546-km field test of twin-field quantum key distribution. *Physical Review Applied*, *22*(6). https://doi.org/10.1103/physrevapplied.22.064057

Books

1. Aliberti, M., Cappella, M., & Hrozensky, T. (2019). *Measuring space power*. Springer. https://doi.org/10.1007/978-3-030-15754-8
2. Friedl, M. (2023). *The COPUOS Briefing Book*. Secure World Foundation. https://cdn.prod.website-files.com/66dcc6872f6ed23bce1db235/68555ba6936c9b96e98f6e64_COPUOS%20Briefing%20Book_English_Web.pdf
3. Jakhu, R. S., & Pelton, J. N. (2017d). *Global Space Governance: an international study*. Springer. https://doi.org/10.1007/978-3-319-54364-2
4. Moltz, J. C. (2024). *Crowded orbits: Conflict and Cooperation in Space*. Columbia University Press. https://doi.org/10.7312/molt15912
5. Pagallo, U. (2024). *The new laws of outer space: Ethics, Legislation, and Governance in the Age of Artificial Intelligence*. Bloomsbury Publishing. https://doi.org/10.5040/9781509976218.0012
6. Pekkanen, S. M. (2024). *The Oxford Handbook of Space Security*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780197582671.001.0001
7. Taleb, N. N. (2007). *The Black Swan: The Impact of the Highly Improbable*. Penguin UK.
8. Townsend, B. (2020). *Security and stability in the new space age: The Orbital Security Dilemma*. Routledge. https://doi.org/10.4324/9781003001843

Reports

1. Aerospace Corporation. (2020). *Blockchain in the space sector* (Report No. OTR202000244). Center for Space Policy and Strategy. https://aerospace.org/sites/default/files/2020-03/Jones_Blockchain_03052020.pdf.
2. Defense Intelligence Agency. (2022). *Challenges to security in space: Space reliance in an era of competition and expansion* (DIA Publication No. DIA_E_00039_A). U.S. Department of Defense. https://www.dia.mil/Military-Power-Publications.
3. European Parliament. (2023). *EU Space Strategy for Security and Defence*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/754598/EPRS_BRI%282023%29754598_EN.pdf
4. European Space Agency (2019). *ESA spacecraft dodges large constellation*. https://www.esa.int/Space_Safety/ESA_spacecraft_dodges_large_constellation#:~:text=Collision%20avoidance%20manoeuvres%20take%20a,possible%20outcomes%20of%20different%20actions
5. European Space Policy Institute. (2017). *The Rise of Private Actors in the Space Sector*. https://www.espi.or.at/wp-content/uploads/2022/06/ESPI-report-The-rise-of-private-actors-Executive-Summary-1.pdf
6. European Space Policy Institute. (2022). *The War in Ukraine from a Space Cybersecurity Perspective: Lessons Learned from Viasat and Starlink Interventions*. https://www.espi.or.at/wp-content/uploads/2022/10/ESPI-Report-84.pdf
7. European Space Policy Institute (ESPI). (2025). *Simulating the future of European security: Wargaming for space operations*. https://www.espi.or.at/briefs/simulating-the-future-of-european-security-wargaming-for-space-operations/
8. Istituto Affari Internazionali. (2023). *Il dominio spaziale e la minaccia cyber*. https://www.iai.it/sites/default/files/iai2306.pdf
9. NASA Office of Inspector General. (2024). *NASA's Management of Risks to Sustaining International Space Station Operations through 2030*

(Report No. IG-24-020). https://oig.nasa.gov/wp-content/uploads/2024/09/ig-24-020.pdf

10. North Atlantic Treaty Organization. (2019). *NATO's overarching Space Policy*. https://www.nato.int/cps/en/natohq/official_tests_190862.htm
11. Organization for Economic Co-operation and Development. (2022). *A New Landscape for Space Applications – Illustration from Russia's War of Aggression against Ukraine*. https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/11/how-the-war-in-ukraine-is-affecting-space-activities_8fb979f7/ab27ba94-en.pdf
12. Secure World Foundation. (2010). *2009 Iridium-Cosmos Collision Fact Sheet*. https://swfound.org/media/6575/swf_iridium_cosmos_collision_fact_sheet_updated_2012.pdf
13. Secure World Foundation (2022). *Is space a global commons?* https://swfound.org/media/207517/swf_brief_is_space_a_global_commons_pp2301_final.pdf
14. Secure World Foundation. (2024). *Global Counter-Space Capabilities: An Open-Source Assessment.* https://swfound.org/media/207826/swf_global_counterspace_capabilities_2024.pdf
15. United Nations General Assembly. (2016). *Report of the Open-ended Intergovernmental Expert Working Group on Indicators and Terminology relating to Disaster Risk Reduction*. https://docs.un.org/en/A/71/644
16. United Nations Office for Outer Space Affairs. (2024). *UNOOSA Annual Report 2024*. https://www.unoosa.org/documents/pdf/annualreport/UNOOSA_Annual_Report_2024.pdf
17. United States Space Force. (2025). *2025 Data and AI Strategic Action Plan*. U.S. Department of Defense. https://www.spaceforce.mil/Portals/2/Documents/SAF_2025/USSF_Data_and_AI_FY2025_Strategic_Action_Plan.pdf

Legal and Governmental Frameworks

1. Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space (1968). United Nations Office for Outer Space Affairs. https://www.unoosa.org/pdf/gares/ARES_22_2345E.pdf
2. Artemis Accords: Principles for Cooperation in the Civil Exploration and Use of the Moon, Mars, Comets, and Asteroids for Peaceful Purposes (2020). NASA. https://www.nasa.gov/wp-content/uploads/2022/11/Artemis-Accords-signed-13Oct2020.pdf
3. Centre for International Governance Innovation (CIGI). (2025). From principles to practice: Addressing emerging technologies in space governance. Submission to the Open-ended Working Group on the Prevention of an Arms Race in Outer Space (OEWG on PAROS), Second Session, United Nations General Assembly, A/AC.297/2025/NGO/2. https://docs-library.unoda.org/Open-ended_Working_Group_on_Prevention_of_an_Arms_Race_in_Outer_Space_-_(2025)/A.AC_.297.2025.NGO_.2.pdf#:~:text=it%20more%20difficult%20to%20uphold,often%20occurring%20without%20attribution%20or
4. Convention on International Liability for Damage Caused by Space Objects (1972). United Nations Office for Outer Space Affairs. https://www.unoosa.org/pdf/gares/ARES_26_2777E.pdf
5. Convention on Registration of Objects Launched into Outer Space (1975). United Nations Office for Outer Space Affairs. https://www.unoosa.org/pdf/gares/ARES_29_3235E.pdf
6. European Parliament. (2024). *Own-initiative resolution on EU-Japan relations (P9_TA(2023)0463)*, Official Journal of the European Union C / 2024 / 4167. https://eur-lex.europa.eu/eli/C/2024/4167/oj/eng
7. European Space Agency (ESA) (1975). *Convention for the Establishment of a European Space Agency.* https://treaties.un.org/Pages/showDetails.aspx?objid=08000002800df46b
8. European Union. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 March 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*. Official Journal of the European Union, L

168/1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

9. Government of Japan, Ministry of Defense. (2022). *National Defense Strategy*. https://www.mod.go.jp/en/d_act/d_policy/national.html .
10. Group of Twenty (G20). (2008). *Declaration of the Summit on Financial Markets and the World Economy*. https://www.g20.utoronto.ca/2008/2008declaration1115.html
11. Guidelines for the Long-term Sustainability of Outer Space Activities (2019). United Nations Office for Outer Space Affairs. https://www.unoosa.org/documents/pdf/PromotingSpaceSustainability/Publication_Final_English_June2021.pdf
12. Inter-Agency Space Debris Coordination Committee (IADC). (1993). IADC Space Debris Mitigation Guidelines. https://www.iadc-home.org/documents_public/file_down/id/4114
13. International Space Station Agreements. (1998). Intergovernmental Agreement on Space Station Cooperation. NASA. https://www.state.gov/wp-content/uploads/2019/02/12927-Multilateral-Space-Space-Station-1.29.1998.pdf
14. Japan-U.S. Security Consultative Committee (SCC)**.** (2023). *Joint Statement of the Security Consultative Committee: Strengthening Alliance for a Free and Open Indo-Pacific*. Ministry of Foreign Affairs of Japan. https://www.mofa.go.jp/files/100704433.pdf
15. Moon Agreement. (1979). Agreement Governing the Activities of States on the Moon and Other Celestial Bodies. United Nations. https://www.unoosa.org/pdf/gares/ARES_34_68E.pdf
16. NASA & SpaceX Spaceflight Safety Agreement. (2021). *Nonreimbursable Space Act Agreement for flight safety coordination with NASA assets*. https://www.nasa.gov/wp-content/uploads/2015/01/nasa-spacex_starlink_agreement_final.pdf?emrc=4143e0
17. Outer Space Treaty. (1967). Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies. United Nations. https://www.unoosa.org/pdf/gares/ARES_21_2222E.pdf

18. Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space. (2007). United Nations Office for Outer Space Affairs. https://www.unoosa.org/pdf/publications/st_space_49E.pdf
19. Strategic Partnership Agreement between the European Union and Japan. (2019). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:4359401
20. The White House. (2022). *National Security Strategy*. https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf
21. Treaty of Mutual Cooperation and Security between the United States of America and Japan. (1960). U.S. Department of State. https://www.mofa.go.jp/region/n-america/us/q&a/ref/1.html
22. United Nations Committee on the Peaceful Uses of Outer Space (UN COPUOS). (1959). Peaceful Uses of Outer Space. United Nations Office for Outer Space Affairs. https://www.unoosa.org/pdf/gares/ARES_13_1348E.pdf
23. United States Mission to the United Nations & Permanent Mission of Japan. (2024, April 19). *Joint statement on behalf of the United States and Japan on the draft Security Council resolution on weapons of mass destruction in outer space*. U.S. Mission to the United Nations. https://usun.usmission.gov/joint-statement-on-behalf-of-the-united-states-and-japan-on-the-draft-security-council-resolution-on-weapons-of-mass-destruction-in-outer-space/
24. World Health Organization (WHO). (2005). International Health Regulations (2005), Third Edition. https://www.who.int/publications/i/item/9789241580496