TAL TECH

DOCTORAL THESIS

The Space-Cyber Nexus: Ensuring the Resilience, Security and Defence of Critical Infrastructure

Antonio Carlo

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY
TALLINN 2024

TALLINN UNIVERSITY OF TECHNOLOGY
DOCTORAL THESIS
32/2024

The Space-Cyber Nexus: Ensuring the Resilience, Security and Defence of Critical Infrastructure

ANTONIO CARLO

TAL TECH PRESS

TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies
Department of Software Science

The dissertation was accepted for the defence of the degree of Doctor of Philosophy (Applied Something) on 30 May 2024

Supervisor: Dr. Adrian Nicholas Venables,
Department of Software Science, School of Information Technologies,
Tallinn University of Technology
Tallinn, Estonia

Co-supervisor: Prof. Dr. Katrin Merike Nyman-Metcalf,
Department of Law, School of Business and Governance,
Tallinn University of Technology
Tallinn, Estonia

Opponents: Prof. Dr. Sergio Marchisio,
Università degli Studi di Roma "La Sapienza",
Rome, Italy

Prof. Dr. Alla Pozdnakova,
University of Oslo,
Oslo, Norway

Defence of the thesis: 20 June 2024, Tallinn

Declaration:
Hereby I declare that this doctoral thesis, my original investigation and achievement, submitted for the doctoral degree at Tallinn University of Technology, has not been submitted for any academic degree elsewhere.

Antonio Carlo _____
signature

ISSN 2585-6898 (publication)
ISBN 978-9916-80-160-4 (publication)
ISSN 2585-6901 (PDF)
ISBN 978-9916-80-161-1 (PDF)
DOI https://doi.org/10.23658/taltech.32/2024
Printed by Koopia Niini & Rauam

Carlo, A. (2024). *The Space-Cyber Nexus: Ensuring the Resilience, Security and Defence of Critical Infrastructure* [TalTech Press]. https://doi.org/10.23658/taltech.32/2024

TALLINNA TEHNIKAÜLIKOOL
DOKTORITÖÖ
32/2024

Kosmose ja kübervaldkonna vaheline seos: elutähtsa taristu vastupanuvõime, julgeoleku ja kaitse kindlustamine

ANTONIO CARLO

TAL TECH
KIRJASTUS

Contents

List of Publications

The present Ph.D. thesis is based on the following publications that are referred to in the text by Roman numbers.

I A. Carlo and P. Breda. Impact of Space Systems Capabilities and Their Role as Critical Infrastructure. *International Journal of Critical Infrastructure Protection*, 45(100680), 2024

II A. Carlo, N. P. Mantı, B. A. S. W. Am, F. Casamassima, N. Boschetti, P. Breda, and T. Rahloff. The Importance of Cybersecurity Frameworks to Regulate Emergent AI Technologies for Space Application. *Journal of Space Safety Engineering*, 10(4):474–482, 2023

III S. Bonnart, A. Capurso, A. Carlo, T. F. Dethlefsen, M. Kerolle, J. Lim, A. Pickard, A. Russo, and L. C. Zarkan. Cybersecurity Threats to Space: From Conception to the Aftermaths. In Space Law in a Networked World. *Brill | Nijhoff*, P.J. Blount, M. Hofmann (eds), 19(1):39–101, 2023

IV D. Jha, N. P. Mantı, A. Carlo, L. C. Zarkan, P. Breda, and A. Jha. Safeguarding the Final Frontier: Analyzing the Legal and Technical Challenges to Mega-Constellations. *Journal of Space Safety Engineering*, 9(4):636–643, 2022

V A. Salmeri and A. Carlo. Security-by-Design Approaches for Critical Infrastructure: Mapping the Landscape of Cyber and Space Law. *NATO Legal Gazette*, 42(1):97–113, 2021

VI A. Carlo. Cyber Threats to Space Communications: Space and Cyberspace Policies. *Studies in Space Policy*, A. Froehlich (eds), 33(1):55–66, 2021

Author's Contributions to the Publications

I The author of this thesis is the lead author of this article (first author and corresponding author), responsible for the majority of the article's content, including data collection, data analysis, manuscript writing, and coordination of the overall writing process.

II The author of this thesis is the lead author of this article (first author and corresponding author), responsible for the majority of the article's content, including data collection, data analysis, manuscript writing, and coordination of the overall writing process. The author was the primary contributor to the risk and vulnerabilities section, as well as the legal and policy aspects.

III The author of this thesis contributed to this book chapter, co-developing the study's theoretical framework, scenario design and case study. The author also co-wrote the manuscript and reviewed and assessed the final version. The author was the primary contributor to the section on boosting cyber resilience of space assets and was a co-contributor for the legal sections.

IV The author of this thesis contributed to this article, co-developing the study's theoretical framework, scenario design and case study. The author also co-wrote the manuscript and reviewed and assessed the final version. The author was the primary contributor to the section on the legal framework for cyber secure mega constellations.

V The author of this thesis is the lead author of this article (first author and corresponding author), responsible for the majority of the article's content, including data collection, data analysis, manuscript writing, and coordination of the overall writing process.

VI The author of this thesis is the sole author of this book chapter.

Abbreviations

AI	Artificial Intelligence
ACT	Allies Command Transformation
ASAT	Anti-satellite
ASI	Agenzia Spaziale Italiana
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CIA	Confidentiality, Integrity, and Availability
CISC	Center for Strategic and International Studies
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CSIRT	Computer Security Incident Response Team
EC	European Commission
EDTs	Emerging Disruptive Technologies
EO	Earth Observation
EPCIP	European Programme for Critical Infrastructure Protection
EPRS	European Parliamentary Research Service
ESA	European Space Agency
ESPI	European Space Policy Institute
EU	European Union
GDPR	General Data Protection Regulation
GEO	Geostationary Orbit
GLONASS	Globalnaya Navigatsionnaya Sputnikovaya Sistema
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
GSaaS	Ground Station as a Service
HQ	Headquarters
ICT	Information and Communication Technology
IHL	International Humanitarian Law
IRIS2	Infrastructure for Resilience, Interconnectivity and Security by Satellite
IT	Information Technology
LEO	Low Earth Orbit
LF	Low-frequency
MEO	Medium Earth Orbit
MFA	Multi-factor authentication
MoD	Ministry of Defence
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
OST	Outer Space Treaty
RQ	Research Question
SACT	Supreme Allied Commander Transformation
SGAC	Space Generation Advisory Council
SOC	Security Operational Centre
UN	United Nations

Terms

Confidentiality	"The property that information is not made available or disclosed to unauthorised individuals or entities" [104]
Critical Infrastructure	"An asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service" [58].
Cyber Security	"Cyber security is the IT security of all information technology systems which are and could be interconnected at data level in cyberspace" [13].
Information and communications technology	"Diverse set of technological tools and resources used to transmit, store, create, share or exchange information. These technological tools and resources include computers, the Internet (websites, blogs and emails), live broadcasting technologies (radio, television and webcasting), recorded broadcasting technologies (podcasting, audio and video players and storage devices) and telephony (fixed or mobile, satellite, visio/video-conferencing, etc.)" [138].
Information Security	"Ensures the confidentiality, availability and integrity of information. Information security involves the application and management of appropriate controls that involves consideration of a wide range of threats, with the aim of ensuring sustained business success and continuity, and minimizing consequences of information security incidents" [75].
Integrity	"The property that information (including data, such as cipher text) has not been altered or destroyed in an unauthorised manner" [104].
Jamming	"Deliberately radiating, reradiating, or reflecting electromagnetic energy to impair the use of electronic devices, equipment, or systems" [140].
Outer Space	"There is no clear physical line between airspace and outer space. Nevertheless, the area at 110 km above sea level is generally regarded as being part of outer space" [71].
Risk	"The likelihood of a vulnerability being successfully exploited by a threat, leading to a compromise of confidentiality, integrity and/or availability and damage being sustained" [104].

Space Infrastructure	"In addition to orbits and orbiting assets (e.g. satellites), space infrastructure also includes communication links and Earth-based components such as ground stations, launch pads, and launch vehicles" [117].
Spoofing	"Active attack that may be perpetrated by an internal or external attacker, in which an attacker masquerades as another one in order to gain an illegitimate advantage" [68].
Threat	"Any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service" [107].

1 Introduction

1.1 Problem Relevance and Core Challenges

Ever since the first artificial satellite was launched in 1957, the cyber and space domains have been closely interlinked [129, 149]. Today, operating in one domain is not possible without operating in the other. This has been recognised by a range of organisations including the North Atlantic Treaty Organization (NATO), which added cyberspace as a 'Domain of Operations' in 2016 [102], followed by space in 2019 [21, 103, 108]. This interconnection demonstrates that the space domain is an increasingly important sector for the management of critical infrastructures (CI) at the international level, with operators acting in multinational and transnational dimensions.

This means that many – if not all – CI depend on satellite systems. Telecommunications, air and sea transport, financial systems, homebanking, military communications and defence systems, scientific monitoring, and smart grids are all tied to space infrastructures. These consist of satellites, ground stations, and interconnections between them and other terrestrial systems [95, 117]. Questions about how space technology can secure the protection of CI are addressed at international, regional, and national levels. Public authorities can also use space technology to ensure the safety and security of their citizens [60]. Connecting capabilities in the space and cyber domains hence offers novel opportunities to enhance day-to-day activities, from safety and security to the speed of communication and data transfer.

However, this interconnection has also presented new challenges and vulnerabilities due to the increase of cyber-attacks [11, 45] that are aimed at 'disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure' [106]. As cyber capabilities can impact space assets either temporarily or permanently, both cyber and space domains are prone to disruption caused by large-scale incidents and natural disasters as well as other threats. The result is an even closer interconnection between the otherwise distinct areas of cyber and space infrastructures.

This interconnection has also led to an increasing interest in developing legal and political solutions to regulate and protect the two domains. This particularly applies to the telecommunications sector: an area of CI that society has become increasingly dependent on and that is characterised by an exponential increase in private actors. Yet this context is further complicated by the legal status of outer space as enshrined in Articles I and II of the 'Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies' known as 'Outer Space Treaty' or OST (1967) [71, 89, 96, 115, 132].

In addition, the fragmented nature of international law poses further legal challenges to the effective enforcement of existing national and international regulations in this space [96]. It is precisely the applicability of the international regulatory systems that are currently in force regarding space assets for CI that constitutes the starting point for regulatory action in this sphere of human activity. However, the lack of international cooperation complicates the development of further and more binding normative solutions for the international community. This is arguably why the four subsequent treaties on outer space (the 1968 Rescue Agreement [133], the 1972 Liability Convention [134], the 1976 Registration Convention [135], and the 1984 Moon Agreement [137]) did not inspire the same level of universal ratification as the OST [132].

Beyond the legal challenges of the space and cyber nexus, there are also a number of operational risks [24, 40, 49]. When space was first explored, some risks were minimised and pushed aside. Today, these must be reconsidered and given greater attention. Such

risks include for instance the security implications of increasingly interlinking telecommunication and location systems with other CI via satellite systems. In fact, security concerns should be considered throughout the life-cycle of satellite systems as these involves separate yet interlinked risks, from placing satellites into orbit to managing and terminating their activity.

1.2 Approach and Objective

The thesis aims to establish cyber and space as CI by exploring the various dynamics and elements involved in satellite cyber security, and the response of national and international institutions in reaction to the issues at hand.

It is not within the scope of this thesis to make a detailed assessment or list of all risks related to IT security and its linked assets or policies. Instead, the articles provide an analytical overview of the problem to better understand its implications and to offer material for discussion with the aim to encourage the development of solutions. As a result, this thesis focuses on the vulnerabilities and interconnections between different technologies that affect most areas of society, with a particular emphasis on their security implications. Due to the limited existing research on the space-cyber nexus, the thesis has been exploratory in its research design using a case-centred process-tracking approach for which different threats to satellite cyber security were considered as case studies in order to observe the results of current policies for the coordination of assets and policies at a regional and international level.

The first line of investigation consisted of a review of the current literature on this argument, which was useful for comprehending all of the nuances of the questions at hand. A range of publications (such as essays, articles, volumes, and conference papers) on outer space and cyberspace legislation were evaluated, with particular attention to the intersection between the two domains as well as any literature that addresses this interconnection. Through this, the author was able to identify a research gap on the connection and interplay between the domains. Although vast literature exists on outer space as well as on cyberspace, with quite a number of sources also discussing the two topics together, what is less covered is an analysis of how the areas interact or *should* interact with one another, especially with regards to their regulation. The author hence argues for the need to consider the space and cyber domains as CI that are naturally intertwined, rather than as two distinct areas of study with only few connection points.

A second line of investigation consisted of a review of national, regional and international legislation in both areas. Particular attention was paid to transnational solutions and to the provisions of international treaties applicable to the citizens of the countries that are party to them. A brief albeit exhaustive overview of the realities and dynamics of the security of space assets for CI showed that space assets play an important role in ensuring states' resilience by following legal standards based on the principle of security-by-design.

A third line of investigation focused on reviewing national, regional, and international policies on cyber and space. The review showed that although the two domains have been recognised as operational, their policies are still immature and under development. Hence, governance efforts in the space and cyber domains remain highly siloed, which has resulted in limited meaningful progress. The past four years have, however, shown at least some progression towards developing strategy documents that cover the improvement of cyber security in the space domain. Cyber and space policies also remain poorly integrated into the international arena despite their transnational characteristics. Yet, a detailed review of current documentation and activities confirmed that cooperation be-

tween nations and international bodies is essential for the recognition and development of the domains.

1.3 Research Questions

As Articles I, III, and VI (listed above) demonstrate, there is a lack of research that examines concrete instruments of cyber security, defence, and resilience in the space domain, and that evaluates and defines the criticality of cyber and space infrastructure. Articles II, IV, and V further address the lack of security awareness in the space domain which poses a risk to activities in space and linked infrastructure. In this context, the core research question to be answered is:

RQ: *How can space infrastructure and its activities be secured and defended from cyber incidents, and how can national and international institutions ensure the resilience of the cyber and space domain?*

To tackle this, the articles address the following sub-questions:

- **RQ.1:** What security arrangements have been adopted on this matter?
- **RQ.2:** What are the current (and future) prospects for the coordination of information security policies of satellite communication systems?
- **RQ.3:** What are the dynamics and elements involved in establishing the space-cyber security nexus as critical infrastructure?

Table 1 presents the aforementioned research and sub-research questions that are addressed accordingly in separate published articles:

Research Question	Publications
RQ	I, II, III, IV, V, VI
RQ.1	I, II, IV, V
RQ.2	I, III, IV, VI
RQ.3	I, III, V

Table 1: Publications and associated research questions

The thesis articles are interlinked in that they all respond to the core research question. Moreover, Table 1 shows which of the Articles address the additional sub-research questions. Along with the analysis, Articles II and III also provide a descriptive overview that forms the basis of the research presented in Article I. Article III describes the risks associated with ground, link, and space segments; while Articles V and VI outline the nature and key concepts of space law and policy.

2 Relevant Studies

During the research period of this thesis (2020-2023), the author conducted a thorough analysis of the current discourse on the past, present and future of the space and cyber domains. The range of consulted resources included Scopus and IEEE Xplore, as well as libraries, such as the United Nations Digital Library, national libraries, and the NATO HQ library. Overall, the author reviewed numerous articles, books, and committee agreements. The most relevant ones formed part of the author's publications and this thesis. All figures included in the text of this thesis were created by the author.

The following section provides an overview of the relevant information based on the reviewed literature and details how this thesis addresses the research questions identified in section 1.2.

2.1 Space and Cyberspace as Critical Infrastructures

In the 21st century, space and cyberspace have become vital to everyday life. Every second, millions of sensitive data sets travel via the Internet, enabling communication via satellite systems [10, 65, 74]. These can act both as agents (satellites that enable the Internet) and as objects (digital satellite management via intranet systems) [5]. They form part of the broader space infrastructure that also includes earth stations and their interconnections with other terrestrial systems [95]. CI such as telecommunications [3, 120, 153], air and sea transport [12, 69, 70, 81, 91, 92, 101, 119, 152], financial systems [2, 79, 145], online banking [4, 41, 43, 145], military communications and defence systems [15, 72, 100, 143, 144], scientific monitoring [150], and smart grids are thereby also linked to space infrastructure. As a result, virtually all CI depends on satellite systems [90] and space infrastructure.

The interruption or destruction of space infrastructure can significantly impact a country or a large geographic area. Such disruption could incur heavy costs to both economic and human resources. The uncertainty of whether and when operations can return to normal following an interruption underlines the criticality of these systems. Space and cyber are respective domains which are fundamental for CI to function and operate effectively. For these reasons, space infrastructure should be considered as CI [24, 90].

In general, interconnections between different CI systems developed at local, national, regional, or international levels can lead to cascading disruptions in associated systems. This phenomenon can increase the potential damage to CI systems. Such risk cascades do not only occur at systems' geographical vectors but also involve the geographically interdependent nature of the systems. This makes CI systems not only interdependent but also closely interlinked with cyberspace [66]. For instance, in the space domain, systems are fundamentally linked to CI assets such as telecommunication, remote sensing, and positioning technologies [52] – all of which are based on satellite systems.

Satellite systems consist of artificial satellites that orbit the Earth and transmit radio signals to land stations or mobile terminals. These signals can provide telephone, television, navigation, and Internet services. Their advantages include the ability to cover large and remote areas, flexibility and scalability, resistance to natural or human events that could damage terrestrial infrastructure, and ease of installation and maintenance. Yet, there are also a range of limitations to satellite systems: These involve their high cost, dependence on atmospheric conditions, latency (the delay between sending and receiving data), and their vulnerability to cyber or space attacks. Various research and innovation projects are underway to overcome these limitations and develop new generations of more economical, efficient, safe, and performant satellites. Some examples are low earth orbit (LEO) satellites, which reduce latency and power consumption; satellites in geosta-

tionary orbit (GEO), which increase signal capacity and stability; and medium earth orbit (MEO) satellites, which combine the advantages of the previous two types [1].

Satellites have become critical in guaranteeing Internet access, especially when providing access by other means is challenging. Using satellite systems for Internet access and overcoming the digital divide is a topic of interest for research and technological development. The digital divide refers to the inequality of opportunity between those who have access to digital technologies and those who are excluded or limited by them, whether for economic, geographical, social, or cultural reasons. Many areas of the world, mainly rural or isolated, are still to be adequately covered by terrestrial networks, such as optical fibre or mobile telephony. Yet, Internet access has become a fundamental resource for education, information, communication, work, and participation in public life. In this context, satellite systems can offer an effective and sustainable solution for ensuring a fast and reliable connection to all users, regardless of location.

Perhaps the most known example is the Starlink satellite-based Internet service. This innovative project aims to provide global high-speed, low-latency satellite Internet service. The project involves the launch of a constellation of thousands of small satellites in LEO that will link to each other via lasers. The Starlink service will reach remote and rural areas that lack terrestrial network infrastructure, thus offering a reliable and convenient connection around the globe. The project is currently under development (beta testing). Still, SpaceX has already launched over 1,700 satellites and begun offering a limited beta service in select areas of the United States, Canada, the United Kingdom, and other countries [147]. However, a precise date for the launch of the public service still needs to be determined, which will depend on several factors, including the availability of user terminals, regulatory authorisations, and network coverage [151]. In 2022, the company's owner, Elon Musk, offered Starlink services to Ukraine in the wake of Russian aggression [48].

Space technology also offers a range of applications beyond communication. One such example is the use of positioning-based services like food delivery or taxi services that rely on satellites for location data. Without positioning satellites, these services would not be possible over the internet [94]. Satellites are one of the main tools for remote sensing, as they can cover large areas of the Earth and transmit the collected data to ground receiving stations. Remote sensing is a technique that allows acquiring information about an object or surface without the need to come into physical contact with it. It can have various applications, including environmental monitoring, natural resource management, spatial planning, security and defence, meteorology, and climatology. Remote sensing is based on analysing the electromagnetic spectrum reflected or emitted by the observed object or surface. Depending on the wavelength used, remote sensing can be classified as optical, thermal, radar, or hyperspectral. Each type has advantages and disadvantages, depending on the atmospheric conditions, spatial and temporal resolution, sensitivity, and data complexity [78, 114, 146]. Using satellites as CI for positioning is an increasingly widespread and essential reality in the modern world as satellites allow for the precise location of people, vehicles, objects, and infrastructure globally, with applications in various sectors such as navigation, geolocation, security, agriculture, and the environment.

However, the use of satellites also carries challenges and risks – both technical and political. For example, satellites are vulnerable to interference, malfunctions, cyber and physical attacks, collisions with other space objects, and natural phenomena [90]. Inherent threats in space also include the risk of collisions between satellites and space debris, which could cause irreparable damage to vehicles in orbit and interfere with military or civilian operations that depend on them [100]. If the threat is of human origin, the harm

could be intentional, making the resilience of satellite systems crucial to ensure the security of any interconnected CI [123]. Furthermore, satellite systems are subject to international rules and standards, which can create conflicts or tensions between states that own or use them. For this reason, it is essential to ensure resilience, security, and cooperation when governing satellites to preserve their functions and prevent the exploitation of vulnerabilities [44, 62, 148].

Overall, space is a domain with both natural and artificial challenges and threats that can compromise the functionality and integrity of space systems [90]. The role of space as an instrument of protection is a highly topical and relevant issue, especially in a context of growing competition and conflict between leading world powers. Space systems can be used to protect national security and ensure the safety of society on the ground, as well as safeguard against potential threats and activities conducted in space. Space is a strategic resource for national and international security, as it allows essential functions such as observation, communication, navigation, and deterrence to be performed. However, space is also a vulnerable and congested environment, which requires responsible and cooperative management to avoid risks of collisions, interference, sabotage, or kinetic or non-kinetic attacks. Therefore, it is necessary to develop international space policies that can guarantee the protection of national and collective interests in space through strengthening surveillance and monitoring capabilities, ensuring compliance with international standards and the principles of applicable international law, fostering resilience and deterrence of space assets, and promoting dialogue and cooperation with other space actors [16]. To cope with these critical issues and support modern civilization, space systems must become more resilient, robust, and reliable.

2.2 Challenges of the Nexus

At the 15th European Space Conference, held in Brussels in January 2023, Josep Borrell, the High Representative of the European Union for Foreign Affairs and Security Policy, stated that "space has become a key strategic domain". Similar to the cyber domain, he notes that "[s]pace will become a kind of battlefield, a place where competition and confrontation will take place" [17]. The close interlinkage between the space and cyber domains brings various challenges [49]. These include risks associated with critical spatial infrastructures, which can cause different degrees of dependence, whether direct, indirect, secondary, or tertiary [66]. Such dependencies become increasingly difficult to describe, explain, and measure, especially when moving away from the initial infrastructure towards a 'system of systems' which links individual capabilities to offer broader functionality that is greater than the sum of its parts. Nonetheless, tracing such dependencies is not impossible. Various methods have been hypothesised for attempting to describe and analyse additional problems, many of which apply to critical spatial infrastructures. The increasing complexity of the relationships involved requires, however, further advances in the field of visualisation, as well as in modelling and simulation skills.

One of the most widespread methods to analyse such interdependencies requires a quantitative approach to examine the level of services provided by space systems or by a particular satellite system in proportion to the whole. This approach favours communication systems at the expense of other critical systems, such as meteorological satellites. Another methodology involves monitoring monetary fluxes between separate infrastructure systems, using economic exchange to measure relative importance and, thus, related criticality. The Australian government, for example, has used this method to describe the interconnections between CI, as in the case of agriculture, and the level of its dependence on other infrastructure systems [105].

This dependence on space systems is due to CI's interconnection and data exchange. Given the widespread use of space systems and their global reach, it is crucial to consider the implications of this dependence on resilience governance processes. This reasonably implies a collective approach to a collective problem: Risks, vulnerabilities, and threats must, therefore, be elaborated on and responded to collectively. Efforts at the national level are critical and likely form the backbone of the overall effort, as most of the resources and organisational capabilities are focused on the commitment to protect essential infrastructure geographically located within the nation. However, an over-reliance on individual efforts allows for security gaps to form, to which security professionals will inevitably be blind due to information asymmetries [90].

Cyber security is a vital branch to protect CI and interconnected systems and mitigate associated risks. It is the practice of protecting Information and Communication Technology (ICT), networks, and programmes from digital threats. While cyber security became a priority in government and private-sector space endeavours in the late 2000s, regulating space cyber security is now at the top of the agenda, as attacks have become more sophisticated within the past decade. For example, US Space Policy Directive-5 titled 'Cybersecurity Principles for Space Systems' [130] describes malicious cyber activities harmful to space operations as spoofing sensor data, corrupting sensor systems, jamming or sending unauthorised commands for guidance and control, or injecting malicious code and conducting denial-of-service attacks. All of the above are actions that cause regulatory challenges for law and policymakers in this discipline [23]. The consequences of cyberattacks targeting space systems and assets could include the loss of mission data, a decreased lifespan or capability of space systems or constellations, and the loss of positive control of space vehicles, potentially resulting in collisions that may impair systems or generate harmful orbital debris [31]. Therefore, it is essential to protect space systems from cyber incidents to prevent disruptions and ensure they can reliably and efficiently support the operations of national CI [16, 26].

The legal approach to cyberattacks needs to be more cohesive and set out to respond to the different ways such attacks are conducted. It also aims to address the underlying reasons, covering a broad spectrum of offensives, including attacks for criminal purposes or anarchist-insurrectional purposes to cyber warfare. The transnational nature of cyberattacks makes the strategies for identifying and countering them particularly complicated and calls for a wide range of solutions that can be adapted nationally and internationally. Most cyberattacks target sensitive computer systems as the perpetrator attempts to achieve a disruptive objective, whether they are individuals or, more commonly, groups of hackers. They are labelled as 'cyber criminals' by the victim states where the affected targets are located. During cyber warfare, members of the armed forces and sometimes civilians directly participate in hostilities under military command. While the primary motivation of cyber criminals is financial gain, their cybercrime activities can disrupt telecommunications networks and operations. On the other hand, State-sponsored cyber threat actors could have the intent and capability to conduct disruptive or destructive computer network attacks against telecommunications networks and infrastructure in connection with military operations [36].

While these actions fall under national legislation in times of peace and under International Humanitarian Law (IHL) during armed conflicts, the attackers themselves always fall under national laws. However, civilian hackers remain protected by IHL from being held directly accountable. Each incident, therefore, requires a case-by-case analysis. At the same time, a gap exists between the prosecution of common criminal acts and the indictment of institutions and states in general, based on their national or international

dimension. While national legal systems are attempting to adapt their legal instruments to these new forms of attack, it is challenging to find regulations and laws appropriate to space activities and attacks on space assets. International law is still based on preventive security and defence policies, leaving the intelligence services and military bodies to deal with cyberattacks. On the other hand, private individuals are forced to rely on external services and can only rely on national institutions after an attack has occurred.

Overall, cooperation at the international level has become fundamental to developing an appropriate risk assessment, legitimising a comprehensive approach to standards, ensuring commitment to sustainable practices that limit the creation of new space debris, and considering end-of-life disposal practices of satellite systems. However, this effort should not be left exclusively to nations with direct involvement in space activities (whether public or privately funded), although they undoubtedly hold a technological and financial advantage compared to other users. It is essential for all to recognise their universal dependence on satellite systems so that nations can collectively develop a policy framework that considers both benefits and challenges. Tackling the main obstacles to exercising global governance, such as sovereignty, accountability, stakeholder involvement, and jurisdiction, will avoid confusion and immobility in the future [8].

From a legal standpoint, as stated in the 1963 Space Declaration and reaffirmed in the 1967 Outer Space Treaty [132], outer space is a good for all of mankind; no country can appropriate it (in whole or in part) exclusively, and everyone should benefit from its use. Both the Moon Agreement [137], which relates to the activities of States on the Moon and other celestial bodies, and the Convention on the Law of the Sea [136], which discusses the notion of a 'common heritage of mankind' for the deep seabed, are also developing a broader principle that includes the establishment of a resource management system in common areas. However, this is an extensively interpreted solution that has yet to find international agreement, especially in relation to outer space. In fact, the Moon Agreement was signed by only a few states, none of which have significant space history, which puts this interpretation outside the realm of customary international law. As these are all principles of international law, it should be questioned to what extent these have been translated into national law since their creation.

In the absence of a body that has the power to adopt binding rules on outer space, the most widely used legal instruments at an international level remain voluntary agreements between countries [87]. Due to the lack of globally recognised international legislation, customary law plays a critical role as one of the sources of public international law. It operates based on countries following a particular custom which over time becomes "a general practice accepted as law" as per Article 38(1)(b) of the Statute of the International Court of Justice [73]. Examples of customary law often find their place in agreements, treaties, or conventions – so in written documents, often signed by many states. Another characteristic of customary law is evolution, so gradually including situations and factors that go beyond the limits of those described in specific treaties [20]. The existence of customary law does not diminish the importance of treaties, nor does it prevent the elaboration and introduction of specific international rules as the result of a consultation process.

Cyberspace law should follow a similar development and take shape through the combined provisions of agreements, treaties, conventions, and customary law. However, as cyberspace has involved private actors from the very beginning, such development has not taken place. Customary international law arises from the will of the states that take an active role in developing the rules and simultaneously agree to be bound by them. Yet, unlike outer space activities, activities conducted in cyberspace have never been new: Instead, they make use of new technologies while covering areas that are based on pre-

existing regulatory structures (e.g., the transmission of information, provision of services, and trade) [113]. It was only later that states realised that cyberspace was a powerful communication tool capable of modifying all information transmitted through it and that this meant preexisting rules had to be adapted, and new structures to more adequately regulate the use of cyberspace would need to be developed [80].

Space law was born out of necessity, as the first satellite launch required a new regulatory framework to be developed. Over time, this legal regime has remained generic, but it can be adapted to accommodate specific concrete activities as they arise. No definition of what constitutes appropriation or the permitted use of space resources currently exists. As long as the use of outer space is mainly scientific and – above all – limited, the lack of that distinction will not be of impact. However, the exponential growth of private actors and states in space [116] underlines the need to define the lawful use of space resources to prevent the possibility of extensive use becoming exclusive and resulting in appropriation [97]. The recent adoption of specific national legislation on space resources has led to the distinction between use and appropriation on a global level. Examples are e.g. the U.S. Commercial Space Launch Competitiveness Act [141] and the adopted Luxembourg law on the exploration and use of space resources (Loi sur l´exploration et l´utilisation des ressources de l´espace) [86].

Space law is a legal framework that often deals with actors operating without a pre-existing legal framework. During the Cold War, the main actors involved in the use of outer space were the United States and the Soviet Union, who engaged in strategic conflict with the aim of dominating the world chessboard or, at least, countering the dominance of the other. Despite the polarisation, a range of collaborative exchanges took place on space affairs between the two superpowers. The fundamentally scientific nature of the activities, even if aimed at their subsequent use in the military, led to these superpowers collaborating in this domain [96].

The utilisation of space resources for military purposes has historically been subject to secrecy and political power. Nevertheless, this led to the creation of a basic legal framework. In the present era, with the growing number of private entities involved in space activities, there is a significantly higher demand for legal certainty to encourage investment and development. The hybrid use of satellite systems creates challenges in the development of standards for space [61] due to the differing nature of civil and military activities. These require different baselines to ensure their operations. This is especially true in the absence of technical standards pertaining to space systems' cyber security. This issue raises the question of which criteria should guide the regulatory process. For this, various factors must be considered, involving both state and non-state actors operating in space. Some possible criteria for developing spatial standards are listed below:

- Respect for international law, particularly the principles and treaties related to outer space, which recognise space as the common heritage of mankind and prohibit its militarisation and appropriation by individual states or entities. For example, the OST established that space is free for the exploration and use of all states and cannot be the subject of national sovereignty or territorial claims [132];

- Promotion of cooperation and transparency in exploiting the resources and opportunities offered by space to prevent harmful conflicts and competition to the security and sustainability of space itself. For example, the 2008 EU proposal for an international 'Code of Conduct for Space Activities' [55] suggested several voluntary measures for improving safety, liability, and accident prevention in space, such as the sharing of information on satellite movements and the notification of orbital manoeuvres;

- Safeguarding the space environment through preventing and reducing space debris, limiting harmful emissions, protecting biodiversity and space ecosystems, and compliance with ethical and scientific standards in space research and exploration [117]. For example, the 2010 UN Guidelines on Orbital Debris Mitigation Measures [139] recommend several actions for reducing the risk of collisions in space, such as controlling the operational lifespan of satellites and withdrawing them from orbit to end the mission;

- Protection of the rights and interests of citizens and communities that benefit from the services and applications provided by satellite systems, guaranteeing fair and non-discriminatory accessibility, quality, reliability, security, privacy, and protection of personal data. For example, the EU's 2016 General Data Protection Regulation (GDPR) [56] established a series of principles and obligations for the processing of personal data collected by satellite systems, such as informed consent of data subjects, data minimisation, cyber security, and the right to be forgotten.

2.3 Opportunities of the Nexus

Although there are only a few space systems which are continuously threatened by various critical issues, both artificial and natural, they have gained increasing importance for the economic, social, and political activities in advanced and developing societies. A 'system of systems' is a complex set of technological and social constructions with interdependent components that generate complex outputs. For instance, should services that are indispensable for life in a developed society be disrupted, this could jeopardise the continuity of the processes involved in the operation of the entire system. The dependence between society and space systems is a direct consequence of the variety of relevant services that are provided based on the capabilities of satellite technology. Some important examples include planet observation data and instant communications. However, satellite systems also offer the possibility of deploying other services in space, with varying degrees of criticality, and supporting different phases of the system's operation. A space service may be a good that becomes the object of direct consumption by an end user, or it may offer an intermediate value that contributes to generating the final result [9].

In addition, the digital management of the ground station of a satellite system can be outsourced through Ground Station as a Service (GSaaS) in the cloud, where tech giants such as Amazon, Microsoft, and Tencent play the main role. GSaaS responds to the demand for big data and emphasises the additional services offered to users, allowing them to use the integrated data generated by satellites [93]. Today, nearly 1,200 satellites operate in space on behalf of 60 states or commercial consortia, and their services are used by users around the world. The use of cyberspace is even more extensive, with over 3 billion users and an estimated exponential growth [98]. This has resulted in the development of an ever-closer interconnection between two otherwise distinct domains: outer space and cyberspace. Due to the critical nature of systems within the domains, especially in relation to CI, the growing interconnection between space and cyber has also triggered a growing interest in establishing political solutions and laws that regulate and protect these areas. The communication sector alone is in continuous expansion due to its democratisation and digitalisation, which has led to an exponential increase in the number of private operators.

The last 30 years have seen enormous advances in satellite technology: from GPS to smartphones, from web to home banking. All of this has profoundly changed our way of conceiving space and the possibilities it offers for supporting technological develop-

ments, both from a practical and economic point of view. The ubiquitous nature of space has transformed the domain into an extension of national and international public discourse [9]. However, this has also made outer space more congested, and dominated by competition and contestation. Space also has a range of applications in the military field, in which satellite systems guarantee the tracking of, for example, operational forces in the field, their command and control, and the guiding of drones, among other tasks [111]. Through communications networks in space, military air force and navy can also count on automated aerial retasking and flight capabilities in all weather conditions. To ensure space-cyber capabilities, it is crucial that private and public actors have the freedom to access the domain, the freedom to use it as needed, and the freedom to act within the domain. This includes the overall capability to invest in innovation for defence purposes (Figure 1).

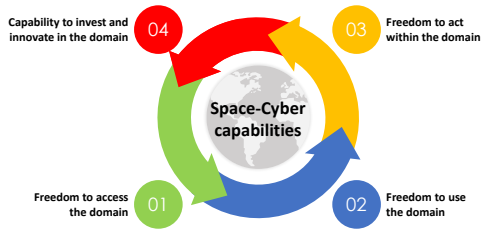


Figure 1: Space-Cyber capabilities.

In today's world, at least 70 nations make use of outer space using their own resources to pursue their national interests bypassing the US-Russian bipolarity that used to dominate the stratosphere [112]. Indeed, it has become crucial for states to have a presence in space not only to project military and political power but also to ensure a good quality of life for one's society, which increasingly depends on the development of national satellite telecommunications and infrastructure. It is hence important to closely monitor both civil and military activities on the ground, and to consider both public and private interests. While these activities have enabled considerable developments in outer space, they have also made it an area increasingly dominated by economic interests [64].

It is no coincidence that the number of space start-ups is growing around the world. Between 2014 and 2020, 295 investment operations were conducted with a value of €1,249 million in the EU alone. 57 of these took place in 2020 with a total value of €502 million, according to a report by ESPI [51]. This is today's reality where the development of advanced satellite technologies will enable data management at lower costs. This also creates opportunities for real colonisation, as shown by Amazon's Kuiper System and Space X's Starlink. Together, they plan to send 15,000 satellites into orbit to diffuse satellite Internet services [14, 121, 125]. These primary satellite activities involve a turnover of USD 340 billion per year. This does not even account for the secondary uses of satellite systems, including positioning, telecommunications, and monitoring infrastructures [126], [109]. Through these, delivery companies can save time by using GPS, which has revolutionised services including national and international trade, mobile technology, and transport [111].

It is crucial to update and secure space systems to ensure their resilience. Many governments, companies, and institutions have established ad hoc Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) coordi-

nated by Security Operations Centers (SOCs) to proactively address potential cyber incidents. However, in the event that these entities are unable to prevent an attack, there are various approaches to reconstructing the infrastructure. Organisations that have been attacked must not only address the damage caused by the attack itself but also its repercussions, such as the loss of trust and reputation. A more resilient system should be developed concurrently by public-private partnerships (PPPs), technical experts, and legal professionals. Strong national and international cooperation could lead to the sharing of best practices and unique know-how to prevent, strengthen, and reconstruct a system after a cyber incident. This sharing of information is the first step towards establishing "cyber diplomacy" – a strong tool to ensure good resilience and cyber capabilities.

2.4 Security and Defence

The increasing reliance on space systems places them in a vital position in the field of CI, despite operating in the most hostile environment known to humanity, which limits them technically and economically. The risks associated with the commissioning of these systems include particularly critical threats, such as the risk of collisions with space debris or the extent of the energies unleashed by space meteorological phenomena, which greatly lengthen the list of possible threats to space and ground-based systems [66]. All services offered by space systems rely on a limited and delicate set of resources. According to the database on space from the Union of Concerned Scientists, millions of consumers and billions of beneficiaries of space capabilities depend on just over 1,300 space systems, which must cope with very different situations dependent on the type and country of origin [131].

It is precisely this concentration of service capabilities that leads to unique opportunities for spatial economic development in the future. However, these capabilities also result in higher risks of dangerous interruptions, which can occur randomly or intentionally, such as in the case of cyber threats. Furthermore, all technologies related to satellites and other space assets must be regularly remotely updated from Earth. Although protected, these connections can still be attacked and hacked, allowing hackers to access all of the systems linked to the 'target' satellite [8]. So, to operate effectively, infrastructure systems heavily rely on space systems for intelligence gathering, command, coordination, and control capabilities. This is particularly important during emergency and crisis situations where space, cyber, security, and defence aspects overlap (Figure 2), underlining why space systems should be considered as meeting the operational requirements of CI. Although this dependence transcends national borders, the resources themselves are still considered under the jurisdiction of the countries of origin, where their movement and location exclude any territorial jurisdiction. This considerably increases the difficulty of implementing protective activities that are much more complex than those usually applied to ground infrastructure [90].

As a result, satellite infrastructures in space can be vulnerable to kinetic and non-kinetic capabilities created to harm or destroy them. The development of weapons that can disrupt the pre-established balance threatens space security [34]. These weapons are referred to as anti-satellite (ASAT) weapons [15, 40, 90] as they are designed to target satellites. Kinetic weapons rely on a projectile or other methods that can cause physical damage to the target. Satellites are particularly vulnerable to these attacks due to their restricted manoeuvrability and predictable orbits [110]. Non-kinetic attacks do not cause physical damage to the satellite but instead interfere with its sensors or software. Space infrastructure may be targeted by jamming (communications disruption), spoofing (data manipulation), and offensive hacks on communications networks, while actions could be directed at control systems or mission packages, as well as at ground infrastructure such

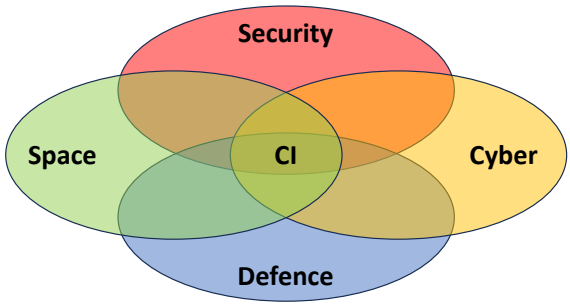


Figure 2: Interconnection between the space, cyber, security, and defence domains and CI.

as satellite control centres. Motivation for such attacks includes state offensives, military actions, organised criminals seeking large financial returns, terrorist groups seeking to advance their cause, or individuals or groups of hackers seeking personal visibility [118].

In addition, the space domain is changing from a selective environment managed by wealthy states and the academic world with adequate resources to one dominated by market forces. Today's technologies bring space capabilities within the reach of nations, international organisations, companies, and individuals. In fact, assets that until a few years ago were owned only by government agencies are now in the public domain and available for purchase on the market [84]. To tackle the security implications, ESA launched a project in 2019 called 'Funding and Support of Space-based Services for Cyber Security' aimed at companies developing innovative products and services in the field of ICT. This project looks at satellite-based initiatives that could mitigate cyber security risks and increase the resilience of existing services, infrastructure, and operations. The project also considers products that could improve the end-to-end cyber security of space applications. Key project areas are transportation (sea, land and air, including autonomous vehicles), energy, utilities, CI, finance, and public safety [46].

Most systems linked to CI are not initially designed for resilience. This design gap is where the concept of 'security by design' finds its raison d'être. This is also an area in which new European regulatory systems such as the GDPR [56] and the EU Cybersecurity Act [57] can make a difference by enforcing new norms and requirements. Technology manufacturers can also implement GPS-spoofing protections, such as GPS firewalls, to limit damage and filter malicious signals. Moreover, manufacturers can improve the security of public Global Navigation Satellite Systems (GNSS) to increase their independence. For example, the European Galileo system [50] was developed as an alternative to the American GPS technology and the Russian Globalnaya Navigatsionnaya Sputnikovaya Sistema (GLONASS) [9]. To further tackle the security and resilience of CI systems, it is also vital to establish standards and best practices. For instance, South Korea is currently developing an alternative system that uses e-Loran technology for satellite positioning systems using radio navigation technologies. This is an evolution of the old radio terrestrial navigation system that uses low-frequency (LF) radio waves and the time interval between signals received from three or more stations to determine a ship's or aircraft's position [99].

Some progress has also been made in building the legislative and institutional framework to protect and develop space CI. For example, the UN Committee on Peaceful Uses of

Outer Space has conducted various research studies and regularly publishes policy recommendations tackling threats, opportunities, and the implementation of new standards for achieving economic and security synergies. Furthermore, the EU's European Programme for Critical Infrastructure Protection (EPCIP) [47] identified space as one of the 11 CI in Directive 114/2008, underlining the need to improve its protection. Space was also mentioned in EU documents on cyberattack preparedness (COM(2009)149 [53]), with space and cyber infrastructure being intimately linked to each other. In addition, the development and security of space were highlighted in COM(2011)152 [54] titled 'Towards a European Union space strategy for the benefit of its citizens' and COM(2011)808 on the 'Horizon 2020 Framework Programme for Research and Innovation' [128].

A second approach to ensuring resilience lies in technological development: Quantum communications could change cryptography and data transmission security, as researchers at the Shanghai University of Science and Technology have demonstrated. In 2017, they sent quantum particles 1,200 kilometres from the Mozi satellite [127] launched almost a year earlier to distant ground stations. Their findings indicate that satellite transmission using quantum cryptography shows great promise: Even though the ratio of photons sent and received (one pair in 1 million) was still very low for application in the near future, the experiment nevertheless validated the principle for a (currently) non-hackable quantum communication protocol [83]. A simpler and immediately usable solution is multi-factor authentication (MFA). This can form part of a wider effort to secure employee password systems used to access relevant systems. A platform such as Keeper's Zero-Knowledge can provide IT administrators with complete visibility into employee password practices, allowing them to monitor their use and enforce security policies throughout an organisation [6].

Overall, the field of CI protection aims to follow a system approach that recognises the critical nature of infrastructures and their extensive interdependencies. Yet, challenges and risks are not easily predictable and not always preventable. Their impact cannot be entirely contained as disruptions tend to spread throughout the system of systems, triggering cascading failures that affect the supply of critical goods and services. This constitutes a key challenge not only for national governments but also for regional organisations, including the EU and NATO. In this framework, space systems have traditionally been considered less critical compared to other systems, such as energy, food, water, and health, which are constantly under threat. However, due to the critical interlinkages summarised above, the importance of space systems to CI and their links to command-and-control capabilities, information gathering, and emergency response should not be overlooked. The principles of CI protection should hence also be applied to critical space infrastructure to identify threats, mitigate vulnerabilities, and minimise disruptions [66]. Still, policymakers need to consider the differences between ground and space systems in this process: A one-size-fits-all approach would underestimate the inherent risks resulting from the strong interconnection between the two systems. Instead, space systems should be integrated into pre-existing security and risk prevention frameworks that follow a security-by-design approach and involve coordinated collective action at the international level.

3 Research Design

3.1 Strategy and Methods

This section outlines the research strategies and methods used to study the interrelations between outer space and emerging cyber technologies based on an analysis of relevant policies and legal considerations. Table 2 provides an overview of each article's research strategies, data collection methods, and corresponding research questions.

Article	Research Strategy	Data Collection Methods	Research Questions
I	Case study	Document Analysis Interviews Secondary data analysis Literature review	What are technical and legal mitigations to prevent a global or partial disruption of space critical infrastructure?
II	Case study	Document Analysis Interviews Literature review	What are the challenges and opportunities posed by the adoption of AI-based solutions to cybersecurity? What are the challenges to achieving cyber defence objectives in both civil and military operations?
III	Action-oriented research	Document Analysis Interviews Secondary Data Analysis Literature review	What are hostile cyber operations and how do they affect space systems?
IV	Case study	Document Analysis Survey Secondary Data Analysis Literature review	What are the legal and technical challenges to ensuring the cybersecurity of mega-constellations? How can amendments in policy and advancements in technology minimise risks?
V	Case study	Document Analysis Interviews Secondary Data Analysis Literature review	How can security-by-design approaches be applied to secure space critical infrastructure? How can national and international institutions mitigate cyber threats in space?
VI	Case study	Document Analysis Interviews Secondary Data Analysis Literature review	How do cyber risks impact space communication? What are the legal and policy challenges to space communication?

Table 2: Overview of methodological approaches used in each publication.

The subsequent paragraphs provide additional details on how these methods were applied across the different publications. To arrive at the research question, current literature on the connection between the space and cyber domains was reviewed. The aim was to examine any established interlinkages and recommendations put forward. This involved evaluating a range of publications, including essays, articles, volumes, and conference papers on outer space and cyberspace legislation. A critical literature review was conducted to gather insights from academic literature and new relevant publications as the field progresses. Further reviewed sources included policy papers from national and international institutions on cyber and space challenges. The literature review process revealed a significant increase in literature related to outer space and cyberspace over the past four years, with many sources noting their interconnection. However, it revealed a lack of literature that evaluates the depth, extent, and impact of this interlinkage and its regulation. This was followed by an analysis of national and international legislation across both domains. Particular attention was paid to transnational recommendations and solutions, and the provisions of international treaties applicable to the countries that are party to them.

Most of the data was collected through desk research (literature review, document analysis, secondary data analysis), as well as through surveys (Articles I and IV), and semi-structured interviews (Articles I, II, III, V, VI) [67]. The interviews were conducted with high-ranking policy officers from various private and public organisations (including international consulting firms, NATO, institutions of the European Union, the European Space Agency, national security authorities and Ministries of Defence). Each interview lasted approximately 45 minutes. These interviews were conducted on the basis of anonymity due to the scope and confidentiality of the information. The desk research for Articles I, III, IV, V, and VI also involved an in-depth evaluation of the realities and dynamics of the security of space assets for CI. This process focused on the resilience capacity of space infrastructure as well as the principle of security-by-design.

Most of the publications draw on case studies as the core research strategy (Articles I, II, IV, V, VI). This allowed for in-depth and focused investigations. Article I is an exploratory case study on the interconnection of space systems to CI. The article provides an overview of the legal and policy aspects of using satellite capabilities in CI to better understand their implications and to encourage the development of recommendations. Moreover, it underlines the importance of recognising space systems as CI.

Article II covers ongoing efforts to create frameworks and regulate interdependent uses of combined technologies such as AI and cyber security to counter emerging threats. The article aims to analyse the different tools that can be utilised to combat these threats, such as cyber ranges, digital twins, and taxonomy creation. The publication particularly elaborates on cyber security risk and vulnerability taxonomy to enable the future application of AI in the space security field. It also assesses to what extent a simulation of network digital twins can protect networks against persistent cyber-attacks in space, targeting users and ground segments. The article also highlights the associated risks and how emerging technologies, particularly AI-based EDTs, can be leveraged to mitigate these risks. Lastly, the paper also examines the impact of cyber attacks on Earth Observation (EO) operations and their resulting business impact (reputational, environmental, and social).

Article III is based on action-oriented research completed in collaboration with the Cyber and Space Working Group of the Space Generation Advisory Council (SGAC), a non-governmental organisation and professional network based in Vienna that 'aims to bring the views of students and young space professionals to the United Nations to advise the

United Nations on space matters' [124]. The chapter aims to provide an overview of hostile cyber operations and their effects on space activities. The article points to the political ambiguity of how the legal regime is applied and highlights the challenges of international law. Challenges and vulnerabilities are assessed by discussing existing security arrangements for different threats.

Article IV is a case study that explores the legal and technical challenges of ensuring the cyber security of mega-constellations. It focuses on policy amendments and technological advancements aimed at minimising risks. The research for the publication involved surveying governmental and non-governmental stakeholders.

Article V is part of the 42nd edition of the NATO Legal Gazette published by the Legal Office of the HQ Supreme Allied Commander Transformation (SACT). The Issue covers the legal aspects of space as NATO's most recent operational domain. The publication also addresses legal issues of space operations, including both military and "dual use" activities, and evaluates and analyses the interrelations between outer space and emerging cyber technologies.

Lastly, Article VI is a chapter from the book 'Outer Space and Cyber Space' published by the European Space Policy Institute. The case study focuses on cyber threats to space communication taking into consideration both military and civil operations. The publication also addresses the lack of shared definitions at the national and international levels.

Publications I, II, IV, V, and VI all present single case studies, while Article III is based on action-oriented research. As part of the research for this thesis, the author also had the opportunity to work with governmental and non-governmental stakeholders on three projects in the research field. Therefore, in addition to case studies, publications I, V, and VI also employ action research strategies [85] based on the author's involvement in the international security and defence environment. More specifically, an action research cycle was adopted that follows the Plan, Act, Observe and Reflect process to establish a baseline and evaluate the research results. This cycle was crucial for understanding the necessary path forward, particularly in a collaborative environment in which the Articles were created.

The publications combine approaches from political science, law, and information communication technology and examine the interdisciplinary character of themes within the cyber and outer space domains. Each article focuses on a specific issue and, in combination with the other articles, provides a better overview of the research topic aimed at ensuring the resilience of CI.

3.2 Limitations

This section outlines the limitations of the topic and this thesis. Although the identified clusters made it possible to investigate space and cyber security in its primary forms, the author's research process was limited by the following points:

- Firstly, the lack of international regulation of space activities has led to an increase in private satellite systems and the number of actors in space, from national security institutions and international organisations to academics and jurists. This has also resulted in biased information characterised by private or national interests, making the research process more intricate and complex;

- Secondly, due to the classified and sensitive nature of both the space and cyber domains, it remains difficult to gather open-source information, particularly on vulnerabilities that could threaten an actor's national security and/or economic interests;

- Thirdly, the space-cyber nexus continues to lack overall vision and remains poorly integrated into international regulatory frameworks. In fact, only a few sources, including those interviewed by the author, discuss the nexus in the current context due to the novelty of the topic, with some expressing a lack of understanding of the issue within the field of study;

- Fourthly, due to the minimal regulation of the space and cyber domains, technology has developed faster than its respective policy and legal dimensions. This discrepancy complicates policy discussions in the field, particularly on future actions and recommendations.

There are also various issues that do not lie within the scope of this thesis and were, hence, not discussed in detail. Nevertheless, their importance should not be disregarded in the wider context:

- The thesis does not delve into the utilisation of space and lunar resources as it is a vast topic that falls outside the scope of this thesis. However, the author acknowledges the importance of this subject and has explored the new legal, policy, and technical developments made by the private and public sectors. The author elaborated on these developments in an article for the NATO Legal Gazette [39];

- Over the past decade, climate change has become an increasingly important topic in legal and policy circles and has resulted in a shifted focus within the security and space domains. Although the author acknowledges the significant impact that climate change has on international security aspects and has addressed some of these in conferences [25, 42] and publications [30], this thesis does not specifically tackle this issue;

- The space and cyber sectors are vital to national security and defence, providing essential services and applications for monitoring, communication, and the management of operations. However, these domains are also vulnerable to threats, hence, much of the information in this sector is classified and accessible only to authorised individuals. The thesis answers the research questions determined in Chapter 1.3 based on mostly open-source information as of 2023. As more information becomes publicly available in the coming years, researchers will be able to draw more wide-ranging conclusions regarding the intricate relationship between space and cyber domains.

4 Evaluation

The evaluation of a research project mainly depends on how useful it is in adding to the understanding of a particular problem, event or phenomenon. This is done by filling a gap in the existing literature. The following section explains how the core research question (**RQ**) and the following sub-questions (**RQ.1-RQ.3**) were addressed in the research project's Articles. It also highlights how the project fills gaps in knowledge on the topic of CI management and protection.

The interconnected Articles aim to answer the core research question and its sub-questions. Although each Article responds to an independent issue, they should be viewed as different chapters of a single cohesive research project. The Articles build upon each other to answer the core research question taking into account current events and developments in the space and cyber domain. The thesis highlights the complex relationship between multiple fields, including transnational, international and national security and defence issues. It also discusses the various uses and possibilities of management and control of CI, including civil, military, technological, and legal aspects. The thesis argues that an overall vision can only be achieved by evaluating existing interconnections and proposing concrete solutions through actionable steps.

Overall, the six studies evaluate the strong link between satellite systems and critical ground infrastructure. This connection allows for a more comprehensive approach to the main issues surrounding their management and jurisdiction. The thesis covers the identification of the actors involved, their national and international recognition, and their authority to act on critical issues and risks in cyberspace and outer space. By employing different methods across the Articles, the author aims to provide a comprehensive view of the space-cyber nexus. These research methods allowed the author to develop the topic while conducting the research and redirecting more emphasis to the challenges at hand.

This study also emphasises the critical role of partnerships with the private sector and academia. Transparent communication can nurture positive public opinion and help steer regulatory discussions. Disclosing more information to the public could also help counter disinformation. However, partnerships of this nature come with inherent security risks and increased visibility, which often contradict the norms and practices of service providers. Therefore, the thesis warns that too much transparency risks revealing vulnerabilities to potential adversaries and that finding the right balance between transparency and security is key to ensuring a resilient space-cyber nexus.

4.1 Core Research Question

RQ: *How can space infrastructure and its activities be secured and defended from cyber incidents, and how can national and international institutions ensure the resilience of the cyber and space domain?*

Current Knowledge Gaps

The research on this topic is strongly fragmented, focusing only on specific aspects of satellite infrastructures or systems. The lack of information and interconnection does not allow for a general overview of the space-cyber nexus and its opportunities and challenges. Moreover, the lack of international protocols means that private actors are often responsible for managing the security of space infrastructures. What is missing is an overall vision and detailed proposals on how to harmonise the different views and challenges on the issue.

Results and Associated Publications

Article I describes outer space as a complex and strategic sector that involves various interests and actors and has a legal framework that is not well-defined or updated. The Article examines the legal and political aspects of using satellite capabilities in CI to understand the consequences and facilitate the development of recommendations. The Article addresses the potential impact of a cyber event on space assets and interconnected national and international CI. This Article summarises the main points of the conception of space systems as CI, which therefore requires inclusion in relevant protection frameworks and paradigms: Building resilient protection policies is key to recognising space systems as CI.

Article II, an analysis of cyber security risks and vulnerabilities, was conducted to facilitate future artificial intelligence use in space security. The paper also examines how a network of digital twins can effectively defend against constant cyber attacks in space, which target users and ground segments. To address these issues, the Article defines cyber security risks and vulnerabilities in space and evaluates the potential of simulating a network digital twin to prevent and counter cyber attacks on space and ground segments. To achieve this, the paper focuses on the case study of Earth observation (EO) operations, which are particularly sensitive to the reputational, environmental, and social impacts of malicious cyber activity.

Article III addresses hostile cyber operations, reconstructing their nature and characteristics to understand how they can influence space systems. It is vital to characterise space cyber threats to design and create protective measures to boost the cyber resilience of space assets. To achieve this, the paper reconstructs possible incident responses, analysing the ICT governance frameworks and strategies, technical strategies, and applying and enforcing the applicable laws given the related minimum requirements for risk mitigations (the Notion of Prudent and Reasonable Actor) as insurance aspects. The article analyses the relationship between the cyber legal framework and outer space with an in-depth analysis of the legal and political responses in state-to-state cyber relations.

Article IV addresses the legal and technical challenges to ensure the cyber security of mega-constellations and possible solutions and assets to minimise risks by applying specific policies and techniques permitted (or required by) technological progress. Mega-constellations are a relatively new phenomenon in the space industry, involving thousands of small satellites in low Earth orbit that provide global communications services. Small satellites typically have a small mass and use commercial off-the-shelf (COTS) components for their electronics and structure. For instance, Estonia's EST CUBE was the first of its kind to attempt the use of an electric solar wind sail (E-sail) and had a mass of 1kg. These mega-constellations present challenges for cyber security, as they can be vulnerable to various types of cyber attacks, such as jamming, spoofing, hacking, or cyber sabotage. These attacks can have serious consequences not only for the services provided by mega-constellations but also for the security of space and the sustainability of the orbital environment. For this reason, it is essential to adopt adequate cyber security measures for mega-constellations, including both technical and regulatory aspects. The Article hence analyses the concept of cyber security for mega-constellations, examining the main risks and possible solutions, both at the individual satellite and network level, to propose some policy recommendations to promote greater cooperation and coordination between space actors involved in mega-constellations.

Article V maps the landscape of cyber and space law, particularly concerning their nexus: The Article examines and discusses the legal and political implications of the rela-

tionship between outer space and new information technologies. It analyses how these two domains are increasingly interdependent and what challenges and opportunities exist for international security and cooperation. The paper specifically addresses how national and international institutions can mitigate cyber threats in space, focusing particularly on the possibilities offered by applying security-by-design approaches to protect critical space infrastructure. It also explores the potential role of multilateral organisations, such as NATO, to promote a responsible, equitable and strategic approach to managing these domains in compliance with the principles of international law and the United Nations Charter.

Finally, Article VI highlights the lack of clear definitions and agreements on key terms and concepts that hinder cooperation and increase the risk of conflict. It explores the connection between cyberspace and critical satellite systems, evaluating how cyber risks impact space communication and offering a detailed picture of the legal and political challenges for current and future space communication. A crucial aspect to examine is the evolving relationship between cyber and outer space elements, both within and beyond their scope. This understanding will be key to understanding how these elements influence each other and how to ensure their resilience in the long term.

4.2 Research Question 1

RQ.1: *What security arrangements have been adopted on this matter?*

Current Knowledge Gaps

The research and analysis on potential and currently available solutions is fragmented. No concrete tools have been identified to secure the defence and resilience of cyberspace, outer space, and the nexus between them. A literature review of the current situation shows a lack of distinctive and coordinated vision between the different actors involved in protecting cyberspace and outer space. To counter emerging threats and ensure secure interactions, concrete defence tools based on a common strategy and strengthened cooperation between national and international actors must be developed. Currently, available solutions are analysed in a fragmented and non-integrated manner without considering the interdependencies and synergies between the two domains. This results in the ineffectiveness of measures that can be adopted, and a vulnerability of CI.

Results and Associated Publications

In the context of this study, security arrangements refer to the role of security, defence, and resilience in securing satellite systems against risks and threats.

Particularly Articles II and III apply the case study of satellite operations to extract the business implications of malicious cyber incidents, whether reputational, environmental, or social. The Articles demonstrate the crucial role that space systems play in the functioning and development of human societies despite their vulnerabilities to various natural and artificial risks. Space systems provide a range of essential services that rely on the technological expertise of satellites, such as Earth observation (EO), monitoring planetary phenomena, and real-time telecommunications. However, space services are not limited to those that directly reach end-users; they also include those that facilitate or enhance other activities in space, with different levels of criticality during different phases of the systems' life cycle. Hence, a spatial service can be a final product consumed by an end-user, as well as an intermediate product that contributes to the creation and adds to the value of the final product.

The study also highlights the use of cloud-based GsaaS for the digital management of

a satellite system's ground station. Companies like Amazon, Microsoft, and Tencent are currently the market leaders in providing Big Data solutions. These companies not only meet the demand for Big Data but also offer additional services to users, allowing them to make the most of the integrated data produced by satellites. This has transformed the nature of satellite systems, creating a truly interconnected CI for society. Lastly, to ensure safety, responsibility, and respect for human rights, Articles II and III propose the establishment of a regulatory framework that would integrate ethical and technical principles for the development and use of EDTs in space.

4.3 Research Question 2

RQ.2: *What are the current (and future) prospects for the coordination of information security policies of satellite communication systems?*

Current Knowledge Gaps
It is crucial to have a clear vision that goes beyond simply encouraging collaboration from all parties involved. At present, there is a lack of comprehensive evaluation of the different tools available, their range, and the potential for standardisation within a wider framework that can tackle the deficiency of an exact legislative and regulatory system that is universally accepted by both the private and public sectors. Additionally, a coordinated approach is needed which focuses on the policies and instruments at the nexus between the space and cyber domains. This current gap hinders the analysis of cooperative solutions at all levels, whether national, international, or transnational.

Results and Associated Publications
Article III presents the results of action-oriented research. This project was carried out in partnership with the Cyber and Space Working Group of the Space Generation Advisory Council (SGAC). The research project sought to analyse the impact of hostile cyber operations on space activities, from their inception to their consequences. The Article also assesses the current and future possibilities of coordinating information security policies of satellite communication systems. It highlights that protecting a satellite system from cyber threats is a complex task that requires a joint effort from all stakeholders, whether from the public or private sector, and involves addressing both technical and legal aspects. Thus, as the threats continue to evolve, keeping the system secure has become increasingly challenging. This Article is closely connected to Articles IV and V, as it makes use of their policy and legal findings to provide a comprehensive understanding of the nexus.

Article IV is an exploratory investigation into the legal and technical issues surrounding the cyber security protection of satellite mega-constellations and the policy changes and technological improvements that can mitigate these threats. To be able to recommend valid and concrete dynamics and assets, the study included extensive consultation between governmental and non-governmental actors. The Article argues that it is essential to establish consistent and comprehensive criteria to ensure the security and reliability of space systems, especially in the face of low-level threats. The ITU recommendations must be scrupulously respected by national authorities, especially as poor regulation can result in some private entities avoiding the process and generating dangers in orbit. The Article concludes that it is thus necessary to identify and follow the good practices of national structures or bodies, develop a guideline for future missions, and define a legal framework for space activities involving mega-constellations.

Article V explores the legal and political implications of the intersection between outer space and EDTs, paying particular attention to space operations involving military and civil

activities. It particularly focuses on analysing the challenges and opportunities that space offers to NATO and its Allies. The challenges posed by space and cyber activities are complex and, as such, require an adequate regulatory framework at both the national and international levels. This should take into account EDTs and the need for greater collaboration between global actors. A possible opening in this sense was offered by the United Kingdom's proposal to the UN on responsible behaviour in space, which stimulated a debate on promoting more responsible and sustainable management. However, international cooperation depends on the willingness to share the benefits of space. It can be undermined by the entry of numerous private actors into the space domain, generating competition and the potential for conflict. Although experts and analysts have highlighted the interconnection between space and cyber, there is still no clear and coherent definition of national policies and guidelines. Therefore, establishing a close relationship between outer space, cyber policies, and diplomacy is an indispensable tool to strengthen their strategic role in the future.

Finally, Article VI explores the challenges and opportunities that emerge from the interaction between the cyber and space domains from a political perspective. It analyses the main actors, norms and strategies that regulate this multidimensional field and discusses the implications for security, cooperation, and competitiveness at a global level. At present, there are several national and international regulatory frameworks governing the outer space and cyberspace domains. Yet, these are often insufficient or inadequate in light of emerging challenges. Moreover, there is no comprehensive vision for the coordination of policies and resources between the two sectors. This is a problem as activities in outer space and cyberspace are not only interconnected but also interdependent. For example, satellites are essential for communications, navigation, Earth observation and defence, but they are also vulnerable to cyber attacks and space interference. Likewise, cyberspace is a dimension that allows for information exchange, innovation, and cooperation, but also enables conflict, espionage, and sabotage. Therefore, it is critical for states and supranational institutions to work together and commit to preserving the peaceful character of these areas by implementing effective and mutually agreed-upon international regulations. Following this approach is vital to ensure the security and sustainability of space and cyber activities.

4.4 Research Question 3

RQ.3: *What are the dynamics and elements involved in establishing the space-cyber security nexus as critical infrastructure?*

Current Knowledge Gaps

At present, no discussion on establishing the space-cyber security nexus as CI can be found in the scientific literature. Although there is some discussion on the connection between the two domains (cyberspace and outer space) and between satellite systems and CI, the literature review process found a lack of in-depth reflection on the possibility of considering satellite systems as CI with the consequent protection and management specifications.

Results and Associated Publications

Article I argues that the space and cyber domains play a critical role in CI and are naturally intertwined and, hence, should be considered as such, rather than as two distinct areas of study with only a few connection points. This view is supported by a detailed scenario which considers the impact of a global satellite disruption event on terrestrial CI. Today, human life is marked by internet and satellite communications through e.g. geographical

positioning functionality. Every moment, masses of often sensitive data travel through the internet or intranet, enabling the development of communications through satellite systems, both as agents (satellite internet) and as objects (digital satellite management via intranet systems). This means that a significant number of CIs rely heavily on satellite systems for their proper functioning. Many critical systems such as telecommunications, air transport, sea transport, financial systems, home banking, military communications, defence systems, scientific monitoring, and smart grids rely on space-based infrastructures such as satellites and ground stations. As these space systems provide critical services for daily life, their disruption and destruction can result in high costs for a nation's economy and society. Therefore, building resilient protection policies is key to recognising space systems as CI. The European Programme for Critical Infrastructure Protection (EPCIP) is one of the first programmes that identified space-based systems as CI, alongside other infrastructures and services such as food security and water supply.

Article I is closely linked to Article II in that it emphasises the significance of space sustainability and refers to key studies such as the US commitment to refrain from conducting direct-ascent ASAT missile testing. Article II addresses ongoing efforts to create structures and regulate the interdependent uses of combined technologies such as AI and cyber security to counter emerging threats. The challenges and opportunities derived from adopting AI-based solutions aimed at achieving cyber security and cyber defence objectives in civil and military operations necessitate rethinking frameworks and ethical considerations. Current space and cyber security policies are inadequate to handle the challenges posed by the integration of space, cyberspace, and emerging technologies. This is particularly relevant for using emerging technologies in space activities and managing CI in complex environments.

5 Impact and Future Work

5.1 Impact

After more than half a century of space activities, ongoing scientific and technological progress, and increased international cooperation, Space 4.0 is entering this field, leaving its hallmark on what appears to be a new era of space activities. The space community is rapidly changing, and the world faces a growing need for dedicated space applications. Over the past decades, industries and governments have progressively relied on space data-centric systems, which has resulted in cyber threats to the space and cyber nexus.

The connection between security in cyberspace and outer space has hence become a topic of growing interest and relevance to the international community [7, 142]. Cyberspace is a crucial dimension for the command and control of space systems but also presents a potential source of threats and vulnerabilities. [16] The close interdependence between the sectors exposes satellite systems to a range of cyber threats, including hacking, sabotage, and cyber espionage. The space sector heavily relies on these complex satellite systems for data and information and the operation of CI, including communication, transportation, energy, and defence networks. Satellite systems are vulnerable to both physical and cyber threats, which can jeopardise the systems' functionality and integrity. Threats can range from interference, jamming, and spoofing to cyber-attacks, collisions with space debris, as well as anti-satellite and directed energy weapons. As satellites are used for various strategic purposes, including communication, navigation, observation, intelligence, and defence, such attacks can severely impact national and international security [26].

Therefore, it is vital to establish an integrated and multidisciplinary vision for security in outer and cyberspace and to develop effective measures to ensure the resilience of the space domain. Such a framework should pay particular attention to the challenges and opportunities that emerge from the interdependence between the domains' nexus. With this in mind, this thesis establishes an overview of space and cyber infrastructure as CI and presents initial guidelines for policymakers worldwide to consider the safety and resilience of space infrastructure in light of the growing number of cyber incidents. This thesis also aims to guide policymakers in securing satellite systems, such as the new European Union's IRIS2 Satellite Constellation, which seeks to provide improved communication capabilities and strategic autonomy to government users through a multi-orbital constellation of EU communication satellites.

Outer space is a strategic domain for human activities and an environment vulnerable to cyber-attacks. Likewise, cyberspace is a fundamental resource for development, innovation, confrontation, and conflict between space actors. The study's Articles I, III, IV, V provide an overview of the implications of a closely linked space and cyber nexus, analysing the challenges and opportunities that arise for international security and stability. These threats have severe consequences for the space sector and society in general, as the data and services provided by satellites are essential for many economic, social, and environmental activities. More specifically, satellite systems and cyberspace are linked by interdependence, complementarity, and mutual vulnerability. This highlights the need to define norms and principles for responsible behaviour in space and cyberspace, including promoting cooperation and dialogue between state and non-state actors and developing technologies and capabilities to protect and ensure the resilience of space systems.

The thesis also examines the need for universal cyber-resilience standards and strategies in a global context. Such strategies should address the prevention, detection, and response to and recovery from cyber incidents that can damage satellite systems. This also

requires collaboration between space operators, government agencies, the private sector, and the academic community to share information, best practices, and resources. Furthermore, the Articles I, II, III, VI underline the importance of developing standards and regulations that ensure the security of satellite systems from cyber threats, both domestically and internationally. This also implies greater awareness and training of end users, who must follow security recommendations and adopt responsible behaviours. Moreover, the author's research notes the need to invest in the research and development of innovative technologies that can strengthen the protection of satellite systems from cyber-attacks, such as quantum cryptography, artificial intelligence, and machine learning. These technologies can help predict, identify, and counter cyber threats effectively and efficiently.

The Articles I, III, V also identify potential measures to prevent and manage crises at the core of the space-cyber nexus, including developing a voluntary code of conduct to ensure the security, safety and sustainability of space activities, and adopting trust and transparency measures. Preventive diplomacy initiatives involve establishing consultation and dialogue mechanisms that seek to resolve potential disputes and reduce tensions and misunderstandings. Such initiatives should be reinforced by harmonising technical standards and legal norms across organisations to protect space and information systems in the long term. Finally, the thesis highlights the need to address the challenges and opportunities linked to the space-cyber nexus by adopting a holistic and cooperative approach involving all stakeholders.

5.2 Implications for Future Work

Innovation is the cornerstone of information security, particularly in space and cyberspace. In a constantly evolving landscape, keeping pace with the latest knowledge and activities is imperative to maintaining confidentiality, integrity, and availability (CIA). Each year, the challenges related to this CIA triad develop and evolve, making innovation not only necessary, but essential. To tackle these, it is crucial to bring together all stakeholders, including institutions, businesses, the scientific community, and civil society, in an integrated and collaborative approach. This will enable society to address the challenges and seize the opportunities of the space-cyber nexus.

For instance, space agencies and institutions responsible for cyber security should promote information sharing and best practices to prevent and counter cyberspace threats collaboratively. As the 2019 French Space Defence Strategy states, "France cannot act alone in [the space] domain, especially if there is a general deterioration of the situation. The aim is therefore to contribute to the consolidation of an allied military space community" [63]. This underlines why intergovernmental collaboration and a common vision of the strategic challenges of space for civil, military, and commercial solutions are essential. Cooperation between actors in the space and cyber domains should be incentivised to develop innovative and resilient solutions that ensure the sustainability of space operations and the protection of sensitive data. International organisations such as the UN, EU, and NATO, as well as individual nations can considerably impact how the space-cyber nexus will be governed in the future. Collaboration and information sharing will be essential; yet, due to the criticality of the data, start-ups and small private actors may 'race' to research and develop space and cyber technologies. This may cause greater polarisation among nations and international private companies, possibly leading to a few actors holding a monopoly on space capabilities.

It is challenging to predict the emergence of technological innovation in the long term, how technologies will be integrated into existing systems, and to what extent they will

be able to deal with threats. However, society will certainly become more dependent on EDTs, particularly in areas that are already heavily integrated, such as protecting and managing CI [38]. Raising awareness and encouraging a broad debate that considers all aspects and actors involved is necessary to ensure the business continuity and resilience of CI. Therefore, the scientific community should continue to conduct research that enables comprehensive and thorough reflections on these matters.

To ensure the defence and security of the space-cyber nexus, it is essential to enhance and coordinate research and innovation efforts. Moreover, it is crucial to identify and address any shortcomings and support the advancement of new defence and security capabilities in the space domain. Actors must share assessments of risks and threats, as well as maintain a common understanding of operations across the domains.

This thesis aims to help policymakers, national and international stakeholders, as well as private companies understand the importance of space, cyber and their interlinkage. In the current period of research and innovation, supranational organisations are formulating new comprehensive legal systems. For instance, the EU aims to unify the fragmented and diverse space regime with a new European space law [59]. In today's rapidly evolving world, these domains play a vital role in the control and dissemination of information. Some nations have increased investments towards national security and regulations to protect national interests. For example, in 2012, Italy introduced the 'Golden Power', which identified explicit domains for regulation and protection by the Italian Government with the power to impose specific conditions. However, this regulation is applicable only on a national level. Instead, governments should focus their national security on all strategic elements, from bilateral and multilateral agreements to the risks associated with the sharing of national know-how and technologies. Therefore, in a globalised world that looks to the stars, national interest and security begin well beyond the borders of a country, often right at the doorstep of a competitor.

6 Conclusions

Although space and cyberspace remain two distinct domains, their close interconnection and interdependence are now being recognised. Operations in outer space enable a variety of operations in cyberspace, just like cyberspace allows for control segments of systems to be operated in outer space. Ongoing discussions outside of formal multilateral channels are providing ideas and best practices for implementing new policies in both areas. However, the most pressing challenge remains the ever-changing landscape driven by new compliance rules, new software, new hardware, and the emergence of cloud technology. Every year, actors in the space domain face new cyber security challenges, requiring new global standards to be developed and shared for broader acceptance. Yet, applying a security-by-design approach to systems should merely be a starting point. Global and national actors must also aim to be at the forefront of technology to develop and maintain a comprehensive security landscape supported by policies that address the challenges inherent to the space and cyber nexus.

In the cyber domain, global communications now transcend territorial boundaries, creating a new realm of human activity and undermining the viability and legitimacy of geographic boundary law enforcement. Over the past years, actors in the cyber domain have developed shared guidelines and best practices, such as Computer Emergency Response Teams and Security Operational Centres, that could be the starting point for cyber capabilities in space. Yet, in the space sector, the law struggles to keep up with the technological and economic developments that see an increasing number of actors in outer space. This has resulted in new challenges for tackling security and defence in space. Particularly the security of satellite systems involves various vulnerabilities, such as systems' physical security, data and communications security, as well as their wider cyber security. However, international legal regulation on satellite system security develops only slowly due to various obstacles. Especially the privatisation of space activities requires greater legal certainty: As of now, there is no international legal framework that covers the security of space or provides a common definition of what 'safe space' constitutes.

Most importantly, new technologies and services, including self-driving vehicles, autonomous weapons, but also air transport, are becoming increasingly interconnected with the space and cyber nexus. This strong linkage raises questions on the consequences of one or both domains becoming the target of a malicious attack. Such an incident could cause a global economic meltdown as well as loss of life. Even if backup systems could help recover lost data or bridge unavailable systems, this process could take months or even years. In the meantime, cities and countries would grind to a halt, waiting for systems to become operational again. It is this vulnerability that makes society and economic markets so dependent on the space-cyber nexus. Given the complexity of the issues involved and the global impact of potential attacks, states and the wider international community must collaborate. Both private and public actors should work towards developing common policies and involve civil society where appropriate.

As the interconnections between the two domains continue to develop, our global society, policies, and laws struggle to keep pace. The more dependent we become on the space and cyber nexus, the more vulnerable we are when technology fails us. Yet, despite these vulnerabilities and their potential impact, this thesis argues that the opportunities that come with interlinking space and cyber capabilities offer considerable growth for our security, resilience, and defence and may ultimately outweigh any resulting vulnerabilities.

Thus, this thesis serves as a starting point for future research on the interconnection between space and CI. The existing literature presents a clear need to identify an overall

vision for CI management and protection, and to tackle the challenges at the nexus between space and cyber. The six presented articles address different challenges, ranging from critical space infrastructure to the role of space capabilities and the legal aspects of space as an operational domain. Together, they provide an overview of the challenges and opportunities that lie at the heart of the space-cyber nexus. The thesis aims to address the identified gap by suggesting a comprehensive approach that includes international standards, preventive diplomacy, and the harmonisation of rules. Such an approach will ensure the security and sustainability of space activities and information systems and present a first step towards better regulation of the field. Yet, this holistic approach can only be achieved if stakeholders cooperate to examine existing interdependencies and propose concrete actions.

List of Figures

List of Tables

References

[1] T. Ahmmed, A. Alidadi, Z. Zhang, A. U. Chaudhry, and H. Yanikomeroglu. The Digital Divide in Canada and the Role of LEO Satellites in Bridging the Gap. *IEEE Communications Magazine*, 60(6):24–30, 2022.

[2] A. J. Akande, E. Foo, Z. Hou, and Q. Li. Cybersecurity for Satellite Smart Critical Infrastructure. *Emerging Smart Technologies for Critical Infrastructure*, 44, 2023.

[3] C. Alcaraz and S. Zeadally. Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, 8:53–66, 2015.

[4] X. Aradhna, S. Kumar, and A. K. Shukla. Role of Multimedia Innovative Technology in Green Banking. *Contemporary Studies of Risks in Emerging Technology*, pages 275–297, 2023.

[5] ASI. Galileo: Il Nuovo Programma Europeo di Navigazione. *Il Sole 24*, 2008.

[6] K. A. Bamberfer, R. Canetti, S. Goldwasser, R. Wexler, and E. J. Zimmerman. Verification Dilemmas in Law and the Promise of Zero-Knowledge Proofs. *Berkeley Technology Law Journal*, 37(1):1–67, 2016.

[7] A. Barrinha. Strategic narratives and the multilateral governance of cyberspace: The cases of European Union, Russia, and India. *Contemporary Security Policy*, 2023.

[8] U. Betza. Cybersecurity of NATO's Space-based Strategic Assets. *Chatham House*, 2019.

[9] G. F. Bignami and A. Sommariva. *L'economia dello spazio: Le sfide per l 'Europa*. Irruzioni, 2017.

[10] M. A. Bille, K. Westburg, P. Kolodziejski, and M. Lutz. Guardian Scout: Military Space from the Pad Up. In AIAA, editor, *American Institute of Aeronautics and Astronautics*, 2023.

[11] K. A. Bingen, K. Johnson, and M. Young. Space Threat Assessment 2023. *Center for Strategic and International Studies*, 2023.

[12] A. Blokus-Roszkowska, S. Guze, K. Kołowrocki, and J. Soszyńska-Budny. Port Critical Infrastructure Network. *Journal of Polish Safety and Reliability Association*, 7(2):15–28, 2016.

[13] BMI. Cyber Security Strategy for Germany 2021. *Federal Ministry of the Interior, Building and Community*, 2021.

[14] E. Board. Satellite Internet: Amazon goes ahead with Kuiper. *Libero*, 2021.

[15] A. Bongers and J. L. Torres. Star Wars: Anti-Satellite Weapons and Orbital Debris. *Defence and Peace Economics*, 2023.

[16] S. Bonnart, A. Capurso, A. Carlo, T. F. Dethlefsen, M. Kerolle, J. Lim, A. Pickard, A. Russo, and L. C. Zarkan. Cybersecurity Threats to Space: From Conception to the Aftermaths. In Space Law in a Networked World. *Brill | Nijhoff*, P.J. Blount, M. Hofmann (eds), 19(1):39–101, 2023.

[17] J. Borrell. European Space Conference: Opening speech by High Representative/Vice-President Josep Borrell. In E. E. A. Service, editor, *15th European Space Conference*, 2023.

[18] P. Breda, A. Adbin, R. Markova, D. Jha, A. Carlo, and N. P. Mantı. Cyber Vulnerabilities and Risks of AI Technologies in Space Applications. In IAC, editor, *International Astronautical Congress*, volume D5,4,1,x70380, 2022.

[19] P. Breda, A. Adbin, R. Markova, D. Jha, A. Carlo, and N. P. Mantı. An extended review on cyber vulnerabilities of AI technologies in space applications: Technological challenges and international governance of AI. *Journal of Space Safety Engineering*, 10(4):447–458, 2023.

[20] I. Brownlie. *Public International Law*. Oxford University Press, 2003.

[21] K. Brunner. Space and Security: NATO's Role. *NATO Parlamentary Assembly*, 2021.

[22] A. Carlo. Artificial Intelligence in the Defence Sector. In J. Mazal, A. Fagiolini, P. Vasik, and M. Turi, editors, *Modelling and Simulation for Autonomous Systems*, volume 12619, 2021.

[23] A. Carlo. Cyber Threats to Space Communications: Space and Cyberspace Policies. *Studies in Space Policy*, A. Froehlich (eds), 33(1):55–66, 2021.

[24] A. Carlo. Opportunities and Challenges in the Cyber-Space Nexus. *Istituto per gli Studi di Politica Internazionale*, 2023.

[25] A. Carlo and N. Boschetti. Modelling the Impact of Space Situational Awareness Disruption on the European and Arctic Security Landscape. In J. Mazal, A. Fagiolini, P. Vašík, A. Bruzzone, S. Pickl, V. Neumann, P. Stodola, and S. L. Storto, editors, *Modelling and Simulation for Autonomous Systems*, volume 13866, 2023.

[26] A. Carlo and P. Breda. Impact of Space Systems Capabilities and Their Role as Critical Infrastructure. *International Journal of Critical Infrastructure Protection*, 45(100680), 2024.

[27] A. Carlo and F. Casamassima. Securing Outer Space through Cyber: Risks and Countermeasures. In IAC, editor, *International Astronautical Congress*, volume D5,4,3,x64939, 2021.

[28] A. Carlo and F. Casamassima. Space Industry: Applications and Implications of Digital Transformation. In IAC, editor, *International Astronautical Congress*, volume D5,2,9,x65506, 2021.

[29] A. Carlo and F. Casamassima. Going Digital, Staying Secure: Cyber ERM Activities in a Post-Pandemic Setup. In IAC, editor, *International Astronautical Congress*, volume D6,4,9,x70417, 2022.

[30] A. Carlo, F. Casamassima, G. Costella, and A. Salmeri. Going Green, Staying Strong: An Operational Roadmap for "NATO Climate" Legal and Policy Tools. *NATO Legal Gazette*, 43(1):47–58, 2022.

[31] A. Carlo and N. Giannakou. Active Debris Removal: The Legal Challenges and the Way Forward. In AIDAA, editor, *XXV International Congress of Aeronautics and Astronautics*, 2021.

[32] A. Carlo, L. Lacroix, and L. Zarkan. The Challenge of Protecting Space-based Assets against Cyber Threats. In IAC, editor, *International Astronautical Congress*, volume E9,2.D5.4,11, 2020.

[33] A. Carlo, N. P. Mantı, B. A. S. W. Am, F. Casamassima, N. Boschetti, P. Breda, and T. Rahloff. The Importance of Cybersecurity Frameworks to Regulate Emergent AI Technologies for Space Application. *Journal of Space Safety Engineering*, 10(4):474–482, 2023.

[34] A. Carlo, N. P. Mantı, P. Breda, M. R. de Beaumont, and D. Jha. Towards a Resilient Cyber Architecture for Space Infrastructures: Mitigating the New Attack Vectors. In IAC, editor, *International Astronautical Congress*, volume D5,4,5,x78079, 2023.

[35] A. Carlo, N. P. Mantıa, B. Aswam, F. Casamassima, N. Boschetti, P. Breda, and T. Rahloff. Understanding Space Vulnerabilities: Developing Technical and Legal Frameworks for AI and Cybersecurity in the Spatial Field. In IAC, editor, *International Astronautical Congress*, volume D5,4,7,x704606, 2022.

[36] A. Carlo and N. Perucica. Artificial Intelligence: Walking the Line between Military Deterrence and Interstate Cooperation. In USSTRATCOM, editor, *6th Annual U.S. Strategic Command Academic Alliance Conference and Workshop*, 2021.

[37] A. Carlo and G. Petrovici. Legal Challenges of Space 4.0: The framework conditions of legal certainty among States, International Organisations and Private Actors in the changing landscape of space activities. In IAC, editor, *International Astronautical Congress*, volume E7,1,8,x46219, 2018.

[38] A. Carlo and L. Roux. Emerging Technologies and Space. In J. Mazal, A. Fagiolini, P. Vasik, M. Turi, A. Bruzzone, S. Pickl, V. Neumann, and P. Stodola, editors, *Modelling and Simulation for Autonomous Systems*, volume 13207, 2022.

[39] A. Carlo and A. Salmeri. Legal Solutions for the Peaceful, Sustainable and Strategic Utilization of Lunar Resources. *NATO Legal Gazette*, 42(1):165–177, 2021.

[40] A. Carlo and N. Veazoglou. ASAT Weapons: Enhancing NATO's Operational Capabilities in the Emerging Space Dependent Era. In J. Mazal, A. Fagiolini, and P. Vasik, editors, *Modelling and Simulation for Autonomous Systems*, volume 11995, 2020.

[41] L. Caviglione and F. Davoli. Satellite Communications and Peer-to-Peer Networking: Architectural Hazards and Interoperability Issues. In *10th Ka and Broadband Communications*, 2004.

[42] L. Cesari, A. Carlo, T. Dethlefsen, N. Manti, D. Stefoudi, and L. Roux. Space as NATO's Operational Domain:The Case of the Cyber Threats against GNSS. In IAC, editor, *International Astronautical Congress*, volume E9,2,7,x66298, 2021.

[43] J. Chavan. Internet banking-benefits and challenges in an emerging economy. *International Journal of Research in Business Managemen*, 1(1):19–26, 2013.

[44] K. Y. Chen, C. A. C. Heckel-Jones, N. G. Maupin, S. M. Rubin, J. M. Bogdanor, Z. Guo, and Y. Y. Haimes. Risk analysis of GPS-dependent critical infrastructure system of systems. *IEEE*, pages 316–321, 2014.

[45] CSIS. Significant Cyber Incidents. *Center for Strategic and International Studies*, 2023.

[46] L. Duquerroy. Cyber Security and Space Based Services. *European Space Agency*, 2019.

[47] EC. Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection. *Official Journal of the European Union*, COM(2006) 786, 2006.

[48] Economist. How Elon Musk's satellites have saved Ukraine and changed warfare. *The Economist*, 2023.

[49] EDA. Enhancing EU Military Capabilities Beyond 2040: Main Findings from the 2023 Long-Term Assessment of the Capability Development Plan. *European Defence Agency*, 2023.

[50] EPRS. Galileo Satellite Navigation System: Space applications on earth. *European Parliamentary Research Service*, 2019.

[51] ESPI. ESPI Report 78 - Space Venture Europe 2020. Enterpreneurship and Invest-ment in the European Space Sector. *European Space Policy Institute*, 2020.

[52] ESPI. Europe, Space and Defence from "Space for Defence" to "Defence of Space". *European Space Policy Institute*, 2020.

[53] EU. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Critical Information Infrastructure Protection - Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. *Officail Journal of the European Union*, 149, 2009.

[54] EU. COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COM-MITTEE OF THE REGIONS - Towards a Space Strategy for the European Union that Benefits its Citizens. *Officail Journal of the European Union*, 152, 2011.

[55] EU. International Code of Conduct for Outer Space Activities. *European External Action Service*, 2014.

[56] EU. Regulation on the protection of natural persons with regard to the process-ing of personal data and on the free movement of such data, and repealing Direc-tive 95/46/EC (Data Protection Directive). *Official Journal of the European Union*, L 119(1), 2016.

[57] EU. REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). *Officail Journal of the European Union*, EU 881, 2019.

[58] EU. DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUN-CIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC). *Officail Journal of the European Union*, 333/164, 2022.

[59] EU. Safe, secure and sustainable space activities - EU Space Law. *European Commission*, 7052281, 2023.

[60] Eurisy. Space 4 Critical Infrastructure – Public Administration. *Eurisy*, 2022.

[61] G. Falco, W. Henry, M. Aliberti, B. Bailey, M. Bailly, S. Bonnart, N. Boschetti, M. Bottarelli, A. Byerly, J. Brule, A. Carlo, G. D. Rossi, G. Epiphaniou, M. Fetrow, D. Floreani, N. G. Gordon, D. Greaves, B. Jackson, G. Jones, R. Keen, S. Larson, D. Logsdon, T. Maillart, K. Pasay, N. P. Mantii, C. Maple, D. Marsili, E. M. Miller, J. Sigholm, J. Slay, C. Smethurst, J. D. Trujillo, N. Tsamis, A. Viswanathan, C. White, E. Wong, M. Young, and M. Wallen. An International Technical Standard for Commercial Space System Cybersecurity - A Call to Action. In ASCEND, editor, *Methods and Considerations for Cyber Protection of Space Assets*, 2022.

[62] R. Filjar, M. C. Damas, and T. B. Iliev. Resilient satellite navigation empowers modern science, economy, and society. *Materials Science and Engineering*, 2021.

[63] F. M. for the Armed Forces. Space Defence Strategy. *Journal officiel du Grand-Duché de Luxembourg*, 2019.

[64] A. Froelich. *Post 2030 -Agenda and the Role of Space. The UN 2030 Goals*. Springer, 2018.

[65] N. B. Garg, A. Garg, M. Bansal, R. Popli, R. Kumar, and D. Singh. Role of Satellite Communication in the Current Era. In Springer, editor, *Computer Aided Constellation Management and Communication Satellites*, volume 987, 2023.

[66] A. Georgescu, A. V. Gheorghe, M. Piso, and P. F. Katina. *Critical Space Infrastructures: Risk, Resilience and Complexity*. Springer, 2019.

[67] C. Glesne. *Becoming Qualitative Researchers*. Longman, 1999.

[68] J. Granjal, E. Monteiro, and J. S. Silva. Security in the integration of low-power Wireless Sensor Networks with the Internet: A survey. *Ad Hoc Networks*, 24, 2015.

[69] C. Große. Airports as Critical Infrastructure: The Role of the Transportation-by-Air System for Regional Development and Crisis Management. In IEEE, editor, *Institute of Electrical and Electronics Engineers*, 2019.

[70] R. Hedel, G. Boustras, I. Gkotsis, I. Vasiliadou, and P. Rathke. Assessment of the European Programme for Critical Infrastructure Protection in the surface transport sector. *International Journal of Critical Infrastructures*, 14(4):311–335, 2018.

[71] S. Hobe, B. Schmidt-Tedd, and K. Schrogl. *Cologne Commentary on Space Law: Volume 1 - Outer Space Treaty*. Carl Heymanns Verlag, 2009.

[72] O. Hoernig and D. Sood. Military Applications of Commercial Communications Satellites. In IEEE, editor, *Military Communications Conference Proceedings*, 1999.

[73] ICJ. Statute of the International Court of Justice. *International Court of Justice*, 1945.

[74] R. T. Ioannides, T. Pany, and G. Gibbons. Known Vulnerabilities of Global Navigation Satellite Systems, Status, and Potential Mitigation Techniques. In IEEE, editor, *Institute of Electrical and Electronics Engineers*, volume 104, 2016.

[75] ISO. Information technology — Security techniques — Information security management systems — Overview and vocabulary. *International Organization for Standardization and International Electrotechnical Commission*, ISO/IEC 27000, 2018.

[76] D. Jha, P. Breda, A. Carlo, L. Zarkan, D. Stefoudi, and N. P. Mantı. Safeguarding the Final Frontier: Analyzing the Legal and Technical Challenges to Mega-Constellations, Managing Risk in Space. In IAASS, editor, *International Association for the Advance-ment of Space Safety Conference Managing Risk in Space*, 2021.

[77] D. Jha, N. P. Mantı, A. Carlo, L. C. Zarkan, P. Breda, and A. Jha. Safeguarding the Final Frontier: Analyzing the Legal and Technical Challenges to Mega-Constellations. *Journal of Space Safety Engineering*, 9(4):636–643, 2022.

[78] D. Jiang and K. Wang. The Role of Satellite-Based Remote Sensing in Improving Simulated Streamflow: A Review. *Water*, 11(8), 2018.

[79] H. E. Kierolff. Satellite Power System (SPS) Financial/Management Scenarios. *U.S. Department of Energy*, 1978.

[80] K. Kittichaisaree. *Public International Law on Cyberspace*. Springer, 2017.

[81] L. S. Lawal and C. R. Chatwin. Enhancing public safety and security of critical national infrastructure utilizing the Nigerian satellite augmentation system (NSAS). In O. S. of Nigeria, editor, *Nigerian Society of Engineer Annual Conference*, 2015.

[82] M. Lecas, A. Carlo, J. Mendoza, N. Moraitis, G. Leterre, B. G. Gonzalez, T. Owen, D. Raghu, G. Rotola, A. Salmieri, and M. Das. This Is Our Space: Contributions from the Young Generations for Sustainable Space Activities. In IAC, editor, *International Astronautical Congress*, volume E3,4,10,x68775, 2022.

[83] J. Liu, G. Zhao, J. Wu, W. Jia, and Y. Zhang. Unified Management Platform of Quantum and Classical Keys in Power Communication System. *Springer, Cham*, 905:695–705, 2019.

[84] D. Livingstone and P. Lewis. Space, the Final Frontier for Cybersecurity? *Chatham House*, 2016.

[85] H. Lune and B. L. Berg. *Qualitative Research Methods for the Social Sciences*. Pearson, 2017.

[86] Luxembourg. Loi sur l´exploration et l´utilisation des ressources de l´espac. *Journal officiel du Grand-Duché de Luxembourg*, A674(7093), 2017.

[87] F. Lyall and P. B. Larsen. Space Law. A Treatise. *Routledge*, 2009.

[88] N. P. Mantı, A. Carlo, R. Markova, D. Jha, P. Breda, A. Abdin, and N. Boschetti. AI Sys-tems to Ensure Cyber Security in Space. In IAC, editor, *International Astronautical Congress*, volume D5,4,2,x70423, 2022.

[89] S. Marchisio. *Lezioni di diritto aerospaziale*. D'Anselmi Editore, 2000.

[90] S. Marchisio and U. Montuoro. *Lo spazio cyber e cosmico: Risorse dual use per il sistema Italia in Europa*. Giappichelli, 2019.

[91] S. Marullo, J. Pitarch, M. Bellacicco, A. G. Sarra, D. Meloni, F. Monteleone, D. Sferlazzo, V. Artale, and R. Santoleri. Air–Sea Interaction in the Central Mediterranean Sea: Assessment of Reanalysis and Satellite Observations. *Remote Sensing*, 13(11), 2021.

[92] A. Mawuli and C. D. Livingstone. Maritime cybersecurity threats: Gaps and directions for future research. *Ocean and Coastal Management*, 236, 2023.

[93] E. Mayerick, A. Pickard, T. Rahloff, S. Bonnart, A. Carlo, and K. Thangavelm. Ground Station as a Service: A Space Cybersecurity Analysis. In IAC, editor, *International Astronautical Congress*, volume D5,4,5,x66555, 2021.

[94] M. Mejía-Kaiser. Space Law and Unauthorised Cyber Activities. *NATO Cooperative Cyber Defense Centre of Excellence*, 2013.

[95] A. Meloni and L. Atzori. The role of Satellite Communications in the Smart Grid, in IEEE Wireless Communications. *IEEE Wireless Communications*, 2(2):50–56, 2017.

[96] K. N. Metcalf. *Activities in Space - Appropriation or Use?* Iustus Förlag, 1999.

[97] K. N. Metcalf. A legal view on outer space and cyberspace. *NATO Cooperative Cyber Defence Centre of Excellence*, 2018.

[98] P. Meyer. Outer Space and Cyberspace. A tale of Two Security Realms. *International Cyber Norms: Legal, Policy and Industries perspectives*, 2016.

[99] P. Moreira. Nautel Lands Large Korean Contract. *Entrevestor*, 2018.

[100] R. A. Morgan. Military Use of Commercial Communication Satellites: A New Look at the Outer Space Treaty and Peaceful Purposes. *Journal of Air Law and Commerce*, 60(1):237–326, 1994.

[101] M. Mukherjee, K. Abhinay, M. Rahman, S. Yangdhen, S. Sen, B. R. Adhikari, R. Nianthi, S. Sachdev, and R. Shaw. Extent and evaluation of critical infrastructure, the status of resilience and its future dimensions in South Asia. *Progress in Disaster Science*, 17, 2023.

[102] NATO. Warsaw Summit Communiqué. *NATO Press Release*, 2016.

[103] NATO. London Declaration. *NATO Press Release*, 2019.

[104] NATO. Security within the North Atlantic Treaty Organization (NATO). *North Atlantic Council*, C-M(2002)49-REV1, 2022.

[105] N. Nguyen. *Infrastructure and Australia's food industry: Preliminary economic assessment*. Australian Bureau of Agricultural and Resource Economics and Sciences, 2013.

[106] NIST. Guide for Conducting Risk Assessments: Information Security. *National Institute of Standards and Technology*, Special Publication(800-30), 2012.

[107] NIST. Security and Privacy Controls for Information Systems and Organizations. *National Institute of Standards and Technology*, Special Publication(800-53), 2012.

[108] K. Nyman-Metcalf, H. Mölder, A. Kasper, and A. Carlo. *Survey on "Space as NATO's fifth military environment international law and dual-use space systems in this context"*. Ministry of Foreign Affairs, 2022.

[109] S. Pace, G. Frost, I. Lachow, F. D. Fossum, D. K. Wassem, and M. Pinto. Positioning System: Assessing National Policies. *RAND*, 1995.

[110] S. Panato. Air and Space Power in NATO-Future Vector Part II. *Joint Air Power Competence Centre*, 2014.

[111] A. M. Petruzzelli and U. Panniello. *Space economy. Storia e prospettive di business*. Angeli, 2020.

[112] S. D. Pippo. Space Technology and the Implementation of the 2030 Agenda. *UN Chronicle*, 2018.

[113] P. P. Polanski. *Customary Law of the Internet. In search for a Supranational Cyberspace Law*. T. M. C., 2007.

[114] A. B. Pour, Y. Park, T. S. Park, J. K. Hong, M. Hashim, J. Woo, and I. Ayoobi. Regional geology mapping using satellite-based remote sensing approach in Northern Victoria Land. *Polar Science*, 16(6), 2018.

[115] A. Pozdnakova. Oceans as Spaceports: State Jurisdiction and Responsibility for Space Launch Projects at Sea. *Journal of International Maritime Law*, 26, 2020.

[116] A. Pozdnakova. Pollution of the Marine Environment by Spaceflights. *Cambridge University Press*, 2022.

[117] A. Pozdnakova. Space Infrastructure for a Sustainable Arctic: Opportunities and Challenges of Spaceport Development in the High North. *The Arctic Institute - Center for Circumpolar Security Studies*, 2022.

[118] R. P. Rajagopalan. Electronic and Cyber Warfare in Outer Space. *United Nations Institute for Disarmament Research*, 3, 2019.

[119] F. Reuschling, N. Carstengerdes, T. H. Stelkens-Kobsch, K. Burke, T. Oudin, M. Schaper, F. Apolinário, I. Praça, and L. Perlepes. Toolkit to Enhance Cyber-physical Security of Critical Infrastructures in Air Transport. *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: Securing Critical Infrastructures in Air Transport, Water, Gas, Healthcare, Finance and Industry*, pages 254–287, 2021.

[120] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly. Identifying, understanding, and analyzing critical infrastructure interdependencies. In IEEE, editor, *Institute of Electrical and Electronics Engineers*, volume 21, 2001.

[121] V. Robecco. Space warfare Musk-Bezos. “Unnecessary satellites Amazon". *Newspaper*, 2021.

[122] A. Salmeri and A. Carlo. Security-by-Design Approaches for Critical Infrastructure: Mapping the Landscape of Cyber and Space Law. *NATO Legal Gazette*, 42(1):97–113, 2021.

[123] K. Schrogl. *Handbook of Space Security: Policies, Applications and Programs*. Springer, 2020.

[124] SGAC. Startegic Plan for 2022. *Space Generation Advisory Council*, 2022.

[125] R. Sharp. Jeff Bezos and Elon Musk reignite space feud: World’s richest men spar over their satellite internet projects with the SpaceX founder blasting Amazon for ’hamstringing’ Starlink. *Daily Mail*, 2021.

[126] SIA-Bryce. State of the Satellite Industry report 2017. *Satellite Industry Association*, 2017.

[127] J. Song. Micius Heralds an Era of Quantum Communications. *Bulletin of the Chinese Academy of Sciences*, 30(3):151–154, 2016.

[128] U. Tatar, A. V. Gheorghe, O. F. Keskin, and J. Muylaert. Space Infrastructures: From Risk to Resilience Governance. *IOS Press*, 57, 2020.

[129] F. Tronchetti. *Fundamentals of Space Law and Policy*. Springer, 2013.

[130] D. J. Trump. Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems. *White House*, 85(176), 2020.

[131] UCS. UCS Satellite Database. *Union of Concerned Scientists*, 2023.

[132] UN. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies. *General Assembly*, RES 2222(XXI):13–15, 1967.

[133] UN. Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space. *General Assembly*, RES 2345(XXII):5–7, 1968.

[134] UN. Convention on International Liability for Damage Caused by Space Objects. *General Assembly*, RES 2777(XXVI):25–28, 1972.

[135] UN. Convention on Registration of Objects Launched into Outer Space. *General Assembly*, RES 3235(XXIX):16–18, 1976.

[136] UN. United Nations Convention on the Law of the Sea. *United Nations*, page 3–134, 1982.

[137] UN. Agreement Governing the Activities of States on the Moon and Other Celestial Bodies. *General Assembly*, RES 34(68):77–80, 1984.

[138] UN. Guide to Measuring Information and Communication Technologies (ICT) in Education. *United Nations*, 2009.

[139] UN. Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space. *United Nations Office for Outer Space Affairs*, 2010.

[140] US. Communications Techniques: Electronic Counter-Countermeasures. *United States Army*, FM 24-33, 1990.

[141] US. U.S. Commercial Space Launch Competitiveness Act. *U.S. Congress*, H.R. 2262(114-90), 2015.

[142] V. Varadharajan and N. Suri. Security challenges when space merges with cyberspace. *Space Policy*, 2023.

[143] A. Varshney, M. Neebha, V. Sharma, and A. D. Andrushia. Low-Cost L-Band to KuBand Frequency Reconfigurable BAR64-02V Controlled Antenna for Satellite, Military, and Radar Applications. *IETE Journal of Research*, 2023.

[144] V. W. Wall. Military Communication Satellites. *Satellite Systems Division*, 1968.

[145] J. Wang. From aperture satellite to "Internet finance": Institutionalization of ICTs in China's financial sector since 1991. *Telecommunications Policy*, 42(7), 2018.

[146] Z. Wang, L. Bai, G. Song, J. Zhang, J. Tao, M. D. Mulvenna, R. R. Bond, and L. Chen. An Oil Well Dataset Derived from Satellite-Based Remote Sensing. *Remote Sensing*, 13(6):23–46, 2021.

[147] M. C. Weinzierl, K. Lucas, and M. Sarang. SpaceX, Economies of Scale, and Revolution in Space Access. *Harvard Business School*, 2021.

[148] T. Westbrook. The Global Positioning System and Military Jamming: geographies of electronic warfare. *Journal of Strategic Security*, 12(2):1–16, 2019.

[149] D. Whalen. The Origins of Satellite Communications 1945-1965. In AIAA, editor, *41st Aerospace Sciences Meeting and Exhibit*, 2003.

[150] Y. Xiao, Q. Yuan, J. He, and L. Zhang. Remote sensing image super-resolution via cross-scale hierarchical transformer. *Geo-spatial Information Science*, 236, 2023.

[151] A. Yadav, M. Agarwal, S. Agarwal, and S. Verma. Internet From Space Anywhere and Anytime - Starlink. In *Advancement in Electronics and Communication Engineering*, 2022.

[152] Y. Yassien, M. Ezzeldin, M. Mohamed, and W. El-Dakhakhni. Air Transportation Infrastructure Robustness Assessment for Proactive Systemic Risk Management. *Journal of Management in Engineering*, 36(4), 2020.

[153] A. F. Zobaa and T. J. Bihl. Security Methods for Critical Infrastructure Communications. *Big Data Analytics in Future Power Systems*, pages 85–106, 2018.

Acknowledgements

The successful completion of this doctoral thesis would not have been possible without the support and feedback of numerous individuals. Academic research and writing rely heavily on ongoing support and collaboration with colleagues, mentors, and friends.

I would like to express my deepest gratitude to my supervisor, Prof. Dr. Katrin Nyman-Metcalf, for her guidance and mentorship throughout my PhD degree. Over the past four years, she always supported and believed in me. Without her unwavering support and encouragement, I would not be here today. I would also like to express my deep appreciation to my supervisor, Dr. Adrian Nicholas Venables, who guided me and whose valuable insights allowed me to complete this PhD.

I am also thankful to my co-authors with whom I shared a common objective and passion in the field of space and cyber security. My gratitude further extends to the Department of Software Science of the School of Information Technologies and the general TalTech staff for always being responsive and helpful when navigating administrative university matters.

Thanks also to my past and present colleagues at NATO and Eurofighter. You have always been supportive, and the many talks have been very helpful for discussing and gaining different views. I would further like to acknowledge the people I met on this journey through the countless professional conferences, workshops, projects, and summer schools I attended throughout Europe over the past years.

Most of all, I would like to thank my family for supporting me throughout this journey. My parents have always been present passing on the love to learn more. I further want to thank Kim for her time, patience, and support throughout the entire PhD journey.

Abstract
The Space-Cyber Nexus: Ensuring the Resilience, Security and Defence of Critical Infrastructure

Ever since the first artificial satellite was launched in 1957, the cyber and space domains have been closely interlinked. Operating in one requires operating in the other. This interdependence has been acknowledged by international organisations like NATO, which declared cyberspace and outer space as operational domains in 2016 and 2019, respectively. Space is a crucial sector for managing critical infrastructure (CI) globally, with actors operating in multinational and transnational fields. As a result, most CI depends on satellite systems. The use of satellite capabilities to protect CI and the linked legal and political implications are the focus of this thesis. Taking into account recent events and advances in space and computing, the thesis aims to address how space infrastructure and its activities can be secured and defended from cyber incidents, and how national and international institutions can ensure the resilience of the cyber and space domains.

This is a complex topic due to the field's transnational implications and its continuous technological development which requires a comprehensive understanding of all related aspects. This thesis aims to provide an overview of the overall picture and offers a starting point for reflections on the importance of the space-cyber nexus. The literature review involves central documents on security and defence aspects issued by national and international bodies as well as legal and scientific researchers. The research findings are then evaluated primarily based on their significance and contribution to understanding a specific problem, event, or phenomenon in the field. The objective here is to fill a gap in the existing literature on the topic of CI management and protection. The field particularly lacks an overall vision, which is an essential tool to identify solutions to the challenges posed by the interconnection between outer space and cyberspace.

To address this, the author uses qualitative and quantitative methods as well as tailored interviews to analyse the risks and vulnerabilities of space infrastructures and their interconnections with other CIs, including telecommunications, energy, and security. Following an analysis of existing regulatory and policy frameworks, the author then proposes recommendations to improve the resilience and governance of space infrastructure.

The thesis presents six authored articles published in scientific journals or books. The articles tackle different challenges, such as the definition of critical space infrastructure, cyber threats to space communications, the role of space capabilities in defence and security, and the legal aspects of space as an operational domain for NATO. While each article addresses a specific aspect of the space-cyber nexus, together, they provide an overview of the two domains' challenges and opportunities. In light of cyber and physical threats that can compromise the functionality and reliability of CI, the thesis highlights the need to establish rules and principles for the responsible use of space and cyberspace. Encouraging cooperation and dialogue between all actors involved and strengthening the protection of space systems is critical to ensuring the resilience, security, and defence of CI.

The author proposes measures to address crises in space and cyberspace, including international standards, preventive diplomacy, and harmonisation of rules to ensure the security and sustainability of space activities and information systems. The thesis also takes into account the challenges and opportunities of EDTs in the space-cyber nexus such as encryption quantum technology, artificial intelligence, and machine learning to improve the security of satellite systems. Overall, the author argues that a holistic and cooperative approach between stakeholders is needed and can only be achieved by examining existing

interdependencies and proposing practical solutions through concrete actions.

The strong connection between satellite systems and terrestrial CI is crucial to their protection and functioning. However, the more dependent society becomes on the space and cyber nexus, the more vulnerable it is to technology failing. Despite these vulnerabilities and their potential impact, the author concludes that the opportunities that come with interlinking space and cyber capabilities offer considerable growth for global security, resilience, and defence and may ultimately outweigh any resulting vulnerabilities.

Kokkuvõte

Kosmose ja kübervaldkonna vaheline seos: elutähtsa taristu vastupanuvõime, julgeoleku ja kaitse kindlustamine

Alates esimese kunstliku satelliidi orbiidile saatmisest 1957. aastal on küber- ja kosmosevaldkonnad olnud omavahel tihedalt seotud. Ühes valdkonnas tegutsemine eeldab ka teises tegutsemist. Seda vastastikust sõltuvust on tunnistanud rahvusvahelised organisatsioonid nagu näiteks NATO, kes nimetas küberruumi ning avakosmose tegevusvaldkondadeks vastavalt 2016. ja 2019. aastal. Kosmos on globaalselt ülioluline sektor elutähtsa taristu haldamiseks ja sektoris osalejad tegutsevad rahvusvaheliselt ning riikidevaheliselt. Sellest tulenevalt sõltub enamik elutähtsast taristust satelliitsüsteemidest. Käesoleva doktoritöö fookus on satelliitside suutlikus kaitsta elutähtsat taristud ning sellega seotud õiguslikud ja poliitilised küsimused. Võttes arvesse hiljutisi sündmusi ja edusamme kosmoses ja andmetöötluses, on doktoritöö eesmärk käsitleda kuidas kosmosetaristu ja selle tegevust saab kaitsta küberintsidentide eest ning kuidas riiklikud ja rahvusvahelised institutsioonid saavad tagada küber- ja kosmosevaldkonna vastupidavusvõime.

Vaadates küsimuste riikidevahelisust ja pidevat tehnoloogilist arengut, on teema keeruline ning nõuab sügavat arusaamist kõikidest seonduvatest aspektidest. Doktoritöö eesmärk on anda ülevaade ja pakkuda alust kosmose ja kübervaldkonna vahelise seose tähtsuse arusaamiseks. Kirjanduse ülevaade hõlmab olulisi riiklike ja rahvusvahelisi julgeoleku- ja kaitseaspekte käsitlevaid dokumente lisaks teadustekstidele. Uurimistulemusi vaadatakse peamiselt vaatevinklist, mis on nende olulisus ja panus konkreetsete probleemide lahendamisel või eri sündmuse ja nähtuse mõistmisel. Eesmärk on täita lünk olemasolevas kirjanduses elutähtsa taristu haldamise ja kaitse teemal. Eriti puudub valdkonda üldine visioon, mis aga on oluline nende probleemidele lahenduste leidmiseks, mis tulenevad avakosmose ja küberruumi vastastikusest seotusest.

Teema käsitlemiseks kasutab autor kvalitatiivseid ja kvantitatiivseid meetodeid ning kohandatud intervjuusid, et analüüsida kosmosetaristute riske ja haavatust ja selle seost muu taristuga, sealhulgas telekommunikatsioon, energeetika ja julgeolek. Olemasoleva õigus- ja poliitikaraamistiku analüüsile tuginedes teeb autor seejärel ettepanekuid kosmosetaristu vastupanuvõime ja juhtimise parandamiseks.

Doktoritöö koosneb kuuest teadusajakirjades või -raamatutes avaldatud artiklist. Artiklites käsitletakse erinevaid väljakutseid, näiteks kriitilise tähtsusega kosmosetaristu määramine, küberohud kosmosesidele, kosmose roll kaitses ja julgeolekus ning kosmose kui NATO operatiivvaldkonna õiguslikud aspektid. Kuigi igas artiklis käsitletakse kosmose ja kübervaldkonna vahelise seose eri konkreetseid aspekte, koos vaadates annavad artiklid ülevaate kahe valdkonna väljakutsetest ja võimalustest. Pidades silmas küber- ja füüsilised ohud, mis võivad kahjustada elutähtsa taristu funktsionaalsust ja usaldusväärsust, rõhutatakse vajadust kehtestada reeglid ja põhimõtted vastutustundlikuks kasutamiseks. Sektori kõikide osalejate vahelise koostöö ja dialoogi julgustamine ning kosmosesüsteemide kaitse tugevdamine on ülioluline, et kindlustada elutähtsa taristu vastupidavusvõime, julgeolek ja kaitse.

Autor pakub välja meetmed kosmose- ja küberruumi kriiside lahendamiseks, sealhulgas rahvusvahelised standardid, ennetav diplomaatia ning reeglite ühtlustamine, et tagada kosmosetegevuse ja infosüsteemide turvalisus ja jätkusuutlikkus. Doktoritöö võtab ka arvesse kujunemisjärgus tehnoloogiatega seotud probleeme ja võimalusi kosmose ja kübervaldkonna vahelises seoses, näiteks krüpteerimise kvanttehnoloogia, tehisintellekt ja masinõpe satelliitsüsteemide turvalisuse täiustamiseks. Üldiselt väidab autor, et on vaja terviklikku ja koostöövalmis lähenemisviisi ja seda on võimalik saavutada ainult olemas-

oleva vastastikuse sõltuvuse uurimise kaudu, mille alusel saab pakkuda praktilisi lahendusi konkreetsete meetmete kaudu.

Satelliitsüsteemide ja maapealsete elutähtsa taristu vaheline tugev seos on otsustava tähtsusega nende kaitseks ja toimimiseks. Seda rohkem ühiskond sõltub kosmosest ja küberruumist ja nendevahelisest seosest, seda haavatavam on ühiskond näiteks tehnoloogia ebaõnnestumise juhul. Vaatamata haavatavustele ja selle võimalikule mõjule järeldab autor, et kosmose- ja küberruumi omavaheline seos suurendab märkimisväärselt ülemaailmset julgeolekut, vastupanuvõimet ja kaitset, mis lõppkokkuvõttes võib kaaluda üles samast seosest tulenevad nõrgad kohad.

Appendix 1

I

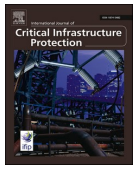
A. Carlo and P. Breda. Impact of Space Systems Capabilities and Their Role as Critical Infrastructure. *International Journal of Critical Infrastructure Protection*, 45(100680), 2024

international journal of critical infrastructure protection 45 (2024) 100680

Contents lists available at ScienceDirect

International Journal of Critical Infrastructure Protection

journal homepage: www.elsevier.com/locate/ijcip



Impact of space systems capabilities and their role as critical infrastructure

Mr. Antonio Carlo [a,*], Dr. Paola Breda [b]

[a] Tallinn University of Technology Estonia
[b] International Space University Italy

ARTICLE INFO

Keywords:
Outer space
Cyberspace
Critical infrastructure
Space systems
Cybersecurity
Responsive space

ABSTRACT

The cyber domain has led to growth in current satellite capabilities, which have become essential due to the increased use of both civil and military critical infrastructure (CI) management systems. In recent decades, outer space has proven to be an increasingly critical sector for the international management of commercial CI, with private operators acting on both multi- and transnational levels. However, the space domain is characterised by not only opportunities but also risks and threats. As the security implications of space were not sufficiently considered at the beginning of the space era, some of the predominant risks currently extend into the commercial sphere. These risks must be considered to ensure the resilience of connected CIs in outer space. Security is a vital issue in the cyber and space domains and should be considered in every phase of a space system's life cycle, from the development and manufacturing of space assets to their deployment and end of life. This involves CI in several sectors, each of which exhibits different but interrelated risks. For example, telecommunications and location systems increasingly require the use of CI, which creates a fragile interdependence that is extremely vulnerable to threats. This paper underlines the importance of recognising space systems as CI and emphasises the need for a better integration of these assets in a system-of-systems analysis. The consequences of global satellite disruption on terrestrial CI are used to support this view. In such a disruptive scenario, mitigation measures based on in-orbit servicing or responsive space capabilities, for example, would allow CI to be restored to first ensure national security followed by commercial activities. Moreover, this paper provides an overview of the legal and policy aspects of using space systems' capabilities in CI to better understand their implications and encourage the development of recommendations.

1. Introduction

Today, outer space is congested and dominated by competition and contestation. In the past 30 years, miniaturisation, connectivity, and sensor performance advancements have enabled a wide range of space capabilities, including positioning, navigation, and timing (PNT), telecommunications, Earth observation (EO), and remote sensing. These capabilities have resulted in widely used and affordable services with a space component, such as international logistics, personal finance, precision agriculture, weather services, and emergency management. Even the globally connected web is partly made possible through space services that ensure database synchronisation and communication.

All of this has profoundly changed the ways in which space, the possibilities it offers for supporting technological developments, and its potential for operational use are perceived. Outer space has thus become increasingly significant for society and an extension of the national and international 'agora' [1,2].

Currently, more than 70 countries use their own space resources to pursue their public or private interests, thereby bypassing the US–USSR bipolarity that dominated the race to outer space until the end of the Cold War. Because the Earth's atmosphere does not stop abruptly, the definition of a physical boundary to identify space activities has never been unique. The Kármán line, located at an altitude of 100 km, is recognised by the international community, including the Fédération Aéronautique Internationale (FAI), as the boundary between Earth's atmosphere and outer space. However, the US military and the National Environmental Satellite Data and Information Service (NESDIS) identify space to begin at an altitude of approximately 80 km. In addition, each national space regulator can potentially define the altitude at which licensing for space activities starts. Aside from the minimum altitude used to define space activities, presence in space has become fundamental – not only as a matter of national security but also for upholding the status quo and people's quality of life. Said quality has become proportional to the degree of development of a nation's satellite

* Corresponding author.
E-mail address: ancarl@taltech.ee (Mr.A. Carlo).

https://doi.org/10.1016/j.ijcip.2024.100680
Received 26 March 2023; Received in revised form 12 April 2024; Accepted 19 April 2024
Available online 26 April 2024

capabilities.

Thus, it is no coincidence that space startups are on the rise on the global stage. According to the Start-up Space report by Bryce Aerospace, between 2012 and 2022, 1796 investment operations were conducted. In the last two years alone, the investments amounted to US$60 billion, 422 of which were in 2022, totalling US$8 billion [3,4]. These investments have enabled the development of increasingly complex satellite technologies, allowing huge amounts of data to be managed at gradually lower costs. Such developments have paved the way for the democratisation of outer space [5].

Yet, the increasing use of space by commercial, private, and governmental actors does not appear to be accompanied by mature international and national legislation or policy frameworks for regulating space activities, which should start with the acknowledgement of space as critical infrastructure (CI). For example, services provided by the entire satellite business are often taken for granted by common users, which means that the implications of a (partial) disruption of satellite capabilities in the short and long term are not well understood.

1.1. Problem statement and approach

The purpose of this paper is to find support for the statement that space systems should be recognised as CI by governments, international and national organisations, and authorities. It serves as an explanatory case study for presenting the interconnection of space systems to CI as well as for underlining their role as the backbone of the entire infrastructure.

Moreover, this paper delves into the tight connection between cyber and space domains, both of which have been identified as the backbone of conventional CI. In previous research, the present author demonstrated that the space and cyber domains are mainly dealt with as two distinct areas of study with only a few connection points, as opposed to being unified under the same policy framework. This work further elaborates on this topic [6].

As cyber capabilities can impact space assets temporarily as well as permanently, both the cyber and space domains are prone to disruption caused by large-scale incidents and natural disasters. As such, an example of an implication of a disruption of service on a global scale is used to understand this interconnection using qualitative data. Mitigations and preventive measures against such a scenario are explained accordingly. The discussion of risks and mitigations is extended to include both civil and military domains to underline the global impact of space systems.

Moreover, an overview of existing governance is provided for an enhanced understanding of the implications of the use of space systems as CI and to encourage the development of recommendations. Existing policies that consider the resilience and protection of space infrastructure attempt to address the question of how space technology can secure the protection of CI. However, the policy frameworks appear to be too premature to be translated into technical specifications and operations when applied to space systems.

The data collection methods employed to support these problem statements were an analysis of documents and a review of the available literature. Lastly, the limitations of the approach as well as suggestions for the next steps are discussed.

1.2. Terminology

Table 1. Key Terminology and Concepts in This Paper

Table 1
defines the important terminology and concepts discussed in the paper:.

Critical infrastructure (CI)	An asset, facility, equipment, network, or system, or a part of an asset, facility, equipment, network, or system, that is necessary for the provision of an essential service [7].
Cyberspace	A virtual dimension in which information is transmitted, processed, and stored through digital communication networks.
Defence and security systems	A set of technologies, strategies, rules, and organisations intended to protect people, infrastructure, information, and national interests from internal and external threats. This work covers both the cyber and space domains. From a strategic-military point of view, outer space is a fundamental sector for defence and security. Its importance is becoming increasingly evident as it becomes an integral and irreplaceable part of military planning and crisis response.
Information and communications technology (ICT)	A term that encompasses all technologies that relate to integrated telecommunications systems, computers, audio–video technologies, and related software that allow users to create, store, and exchange information.
Outer space	The region that lies outside of the Earth's atmosphere and other celestial bodies.
Space systems	Airborne, ground, and in-space systems that support space operations and business. Note that satellite systems are a subcategory of space systems.
Risk	The likelihood of a vulnerability being successfully exploited by a threat, leading to compromised confidentiality, integrity, and/or availability, and also damage being sustained [8].
Threat	Any circumstance or event with the potential to adversely impact organisational operations and assets, individuals, other organisations, or the nation through an information system via unauthorised access, destruction, disclosure, or modification of information, and/or denial of service [9].

1.3. Overview of the paper

The paper is structured as follows. Section 2 describes the importance of space systems as critical infrastructure and their role as a backbone for conventional critical infrastructure, together with cyberspace. Recent policies aimed at recognizing space as critical infrastructure are presented, as well as the share market of the space business, and the definition of integrated systems. Section 3 presents a qualitative assessment of a scenario involving satellite service disruption to underline the impact of the space infrastructure on the civil and military domain, as well as mitigations to such an event. Dependencies within the space infrastructure are presented in Section 4. Section 5 shows how cyberspace governance can serve as a reference to develop governance and policy frameworks for space. Limitations to the approach and future work are underlined in Section 6. Conclusions are drawn in Section 7.

2. Space systems as critical infrastructure

CI comprises complex networks and systems, such as industries, institutions, and distribution structures, which operate synergistically to produce a continuous flow of the goods and services that are essential for the organisation, functionality, and economic stability of industrialised countries [10].

Today, most CI is highly computerised and uses digital tools for control, management, and operation. CI is key to numerous sectors, including banking and finance, telecommunications, energy and utilities, transport and distribution, industry, public administration, information services, healthcare and social welfare systems, food and water supply, postal services, education and research, emergency services, and security and defence [11]. While the growth of satellite systems has enabled CI to be more interconnected, it has also resulted in CI systems becoming more interdependent. Since satellites play a critical role in the monitoring of CI to ensure its security and resilience, the rapid development of satellite capabilities has validated the need for investment in

their construction and placement in orbit.

Thus, societies have become increasingly dependent on the functioning of space systems that today support their nations' economies, governance processes, and cultures [12]. Space systems have also become the backbone for even pre-existing CI and are essential in crisis and emergency management. For example, the European Copernicus Programme's Emergency Management Service uses satellite remote sensing and in situ / open data sources to provide crucial geospatial data for assisting the management of natural disasters, human-made emergencies, and humanitarian crises [13]. Fig. 1 illustrates how conventional CI depends on space and cyberspace:

Regarding the interdependencies amongst CIs, one of the objectives of cyberspace is to enable the safety and cybersecurity of space systems, which in turn serve the entire conventional CI [14]. While cyberspace has already been recognised as CI, space systems are still not universally recognised as such. Building resilient protection policies is therefore key to recognising space systems as CI. Actual policies rated to national space infrastructure in Western countries are discussed as examples following paragraphs. The following discussion focuses on the European Union since the presence of national laws of the member states increases the complexity of the local implementation of a resilient space infrastructure.

The European Programme for Critical Infrastructure Protection (EPCIP) was one of the first programmes to identify space-based systems as CI [12]. Space was mentioned as one of the 11 CIs in Directive 114/2008 on the identification of European CIs, in the assessment of the need to improve their protection, and in EU documents on cyberattack preparedness (COM-2009–149 and COM-2011–163), as space and cyber infrastructures are intimately linked. In addition, the development and security of space received special attention in COM-2011–152, titled 'Towards a European Union space strategy for the benefit of its citizens', and COM-2011–808, titled 'Horizon 2020: The Framework Programme for Research and Innovation' [15]. The EPCIP was developed to identify and defend European CI by applying a series of common minimum standards to protect the national CI of member states [16].

It is worth to mention that the Critical Entities Resilience Directive (2557/2022) will supplant Directive 114/2008 [17]. The Directive includes a taxonomy of critical infrastructures shared with the cyber-focused NIS 2 Directive [18], identifying already the nexus between space and cyber. Both directives were approved in the same time frame, including lessons learned from European interdependencies understood during the pandemic and the war in Ukraine. While the Annex of the Directive identifies space as one of 11 domains for European Critical Entities, the Directive makes it mandatory for all EU states without space in the national system to introduce it in their national law by 17 October 2024. This Directive demonstrates the effort of the EU in coordinating the definition of protection measures for space infrastructures that shall be implemented on the national level rather than defining their operations. Nonetheless, it shall be reminded that the most important European space systems are those owned by the EU (e.g. Galileo, Copernicus, the future IRIS2) rather than by the single member states.

In the United Kingdom, a policy paper on National Space Strategy from February 2022 [19] recognises space as vital to the nation's security and resilience. The paper defines it as part of the UK's critical national infrastructure (CNI).

Australia also recognised the engagement of CI stakeholders to support space technologies. In 2018, the Security of Critical Infrastructure Act 2018 (SOCI) was published, which covers legislation, regulation, and compliance for space technologies. However, no CI assets are currently defined in the SOCI Act for the space technology sector.

Furthermore, in the United States, space is not yet identified as CI; however, most of the space systems in orbit meet the definition of CI defined in Presidential Policy Directive 21 (PPD-21) and are covered under existing infrastructures, such as communication or ICT. However, the importance of officially recognising space as the 17th US CI sector has been pushed forward, such as by Auburn University's McCrary Institute [20].

In January 2023, the European Union (EU) and the North Atlantic Treaty Organization (NATO) announced the formation of the Task Force on the Resilience of Critical Infrastructure [21,22], which aims to cover four sectors – namely energy, digital infrastructure, transport, and space. The urgency of such resilience has certainly been underlined by recent events related to the weaponisation of energy and acts of sabotage against the Nord Stream gas pipelines, which occurred on 26th September 2022 [23].

Lastly, the United Nations (UN) Committee on the Peaceful Uses of Outer Space has conducted various research projects and regularly publishes policy recommendations to UN Member States on threats and opportunities as well as the implementation of new standards for achieving economic and security synergies [24].

2.1. Space business beyond critical infrastructures

To understand the drive for growth in the use of – and the consequent dependence on – space systems in the absence of complete, reliable, and verifiable data regarding the number of users and beneficiaries as well as the intensity of use, one can observe the development of associated industries.

According to the annual State of the Satellite Industry Report, the global space economy exhibited growth of +12% during 2016–2021 (US $344.5 billion in 2021), with the satellite industry itself growing by +7% (US$260.5 billion in 2021) [25]. This dynamic has surpassed that of general global growth, giving shape to a growth trend that has remained constant regardless of the broad and generalised economic consequences of the 2008 global financial crisis and the COVID-19

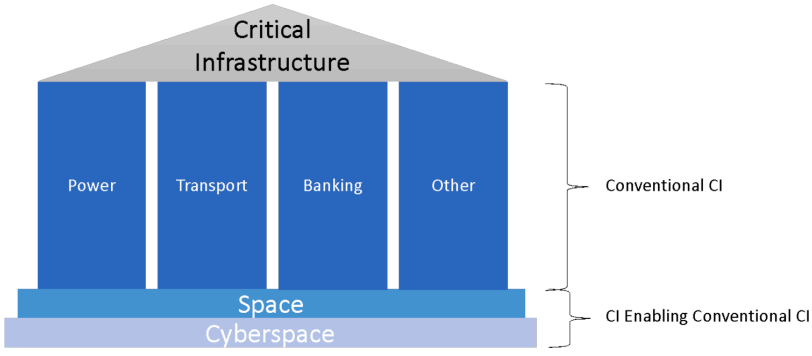


Fig. 1. Interdependency amongst critical infrastructures.

pandemic of 2020–2021. While the branches of satellite manufacturing and launch services exhibited rather steady revenues between 2016 and 2021 (−1.5% and +3%, respectively). Moreover, revenues associated with the ground segment increased by +25% in the same period, mainly due to the increasing demand on connectivity, broadband, and satellite radio installations. By contrast, satellite services (telecommunications and remote sensing) registered a reduced revenue of −8% [26]. Most launch contracts are currently dominated by payloads in the small satellites class (hereinafter 'smallsats' – below 600 kg), with a share of 95% of the total number of spacecrafts launched in 2022 (+1% compared with 2021) [27]. This is mainly due to the large number of low Earth orbit (LEO) broadband telecommunications smallsats launched in the past two years (e.g., Starlink and OneWeb).

Based on the increasing growth of the space business, agreeing on and adopting policies and governance on a global level to regulate space assets as CI appear to be crucial. Most importantly, this is because space assets are usually integrated into a system of systems, which is discussed in the next subsection.

2.2. Integrated systems in the space domain

A 'system of systems' refers to a complex set of technological and social constructs that generate interdependent complex outputs. It is a collection of resources and capabilities that creates a new and more complex system [28]. In line with Aristotle's 'the whole is greater than the sum of its parts', this system of systems offers more functionality and performance than simply the sum of each system. This principle also applies to CI and its services, as the interruption or compromise of a single element can jeopardise the continuity of the wider operational processes of the entire system. Hence, as the number of space systems is limited, the continuous threat posed by various critical issues (including artificial and environmental threats) poses a risk not only to the space ecosystem but also to all connected CIs.

Furthermore, the importance of space systems in economic, social, and political activities has grown significantly. For example, satellites provide various services such as EO data and instant communications, leading to an increased interdependence between society and space systems. Moreover, satellite systems offer the possibility of deploying other services in space, supporting different phases of the system's operation with varying degrees of criticality. While some of these space services may become commodities to be directly consumed by end-users, others may act as intermediate goods that bring added value to a different end-user service. [1]

The geographically interdependent nature of space systems and their lack of segregation pose cyber and physical risks to the system's security [11,29]. To address such critical risks, space systems' hardware and software must become independent of one another, and more resources must be invested into making these systems more resilient, reliant, and robust.

The services offered by space systems are provided by a rather limited set of fragile resources. According to the Union of Concerned Scientists' collaborative database on space, millions of consumers and billions of beneficiaries of space capabilities depend on 7561 satellites [30]. Although these systems differ vastly in their technical development based on their country of origin, they can nevertheless be interlinked and synced [31].

Consequently, space systems should be defined as CI since the disruption or destruction of their services would have a considerable impact on an entire geographical region. As the services offered by space systems are critical to the daily lives of a nation's citizens, such disruption or destruction could impose heavy costs on the nation's economy and society (see Section 3 for a qualitative scenario). Uncertainty exists not only in the length of the disruption itself but also in relation to the time required for CI to fully restore functionality – should this even be possible – following an incident [12]. Several possibilities to restore a CI from a satellite service disruption are also discussed in Section 3.

2.3. Space systems for defence

Since space systems have both civil and military applications, summarising the impact of such systems on defence and security is worthwhile. Space communications have significantly improved military strategy by providing air and naval forces with automated aerial retasking and flight capabilities, regardless of weather conditions [32]. Satellites also play a crucial role in the battlefield by enabling the tracking of operational forces, command and control, and the use of drones. All of these benefits are made possible by the use of outer space.

In general, in the military, the space domain is recognised as an increasingly crucial sector for the management of CIs at the international level, as demonstrated by NATO, which added cyberspace as a 'Domain of Operations' in 2016 [33], followed by space in 2019 [12,34].

The dependency of infrastructure systems on space systems' command, coordination, and control, as well as intelligence-gathering capabilities (especially in emergency and crisis management), clearly indicates that space systems meet the requirements for being deemed critical. Although this dependency transcends national borders, the resources themselves are still considered to be under the jurisdiction of their country of origin (launching state). According to Article VII of the Outer Space Treaty [35], their movement and location lie outside of any territorial jurisdiction. This has made the implementation of protective activities much more difficult and complex than those usually used in localised terrestrial infrastructures [12].

Space might also host numerous weapons systems. Depending on the final target, these weapons can intercept assents in space and/or on Earth. In the 1950s, the USSR and the United States developed weapons systems to target competitors' assets from space. As a result, actors with satellite technology also developed strategies for preventing their adversaries from using these services by disabling their space platforms. This led to the creation of anti-satellite weapons (ASAT), which function by denying, disrupting, disabling, destroying, or deceiving their targets (known as the '5Ds'). The kinetic destruction of satellites has permanent and irreversible effects. In addition to targeting space-based assets, the ground facilities that support them can also be attacked. ASAT weapon systems can be classified into two categories, namely hard-kill and soft-kill weapons [36].

Hard-kill ASAT weapons are based on the use of a projectile or other methods for achieving the kinetic destruction of the target. Due to the predictability of satellite orbits and their restricted manoeuvrability, satellites are particularly susceptible to such attacks. The most common hard-kill ASATs are ballistic missiles and other satellites used as kamikaze satellites. Kinetic physical attacks can cause permanent damage to the targeted systems and display a significant amount of force that is easily traceable and observable. In such an attack, orbital debris could be produced, which could harm other satellites positioned in similar orbits, leading to the Kessler effect. To date, no country has launched a kinetic attack against another country's satellite; however, the United States, Russia, China, and India have successfully tested direct-ascent ASAT weapons against their own satellites.

By contrast, soft-kill ASAT attacks interfere with the satellite's sensors (through jamming, spoofing, or blinding through powerful lasers) or its software (through cyberattacks). For example, on 24th February 2022, a cyberattack disrupted broadband satellite internet access [37]. The attack disabled modems that communicate with Viasat Inc.'s KA-SAT satellite network, which provides internet access to tens of thousands of people in Ukraine and across Europe [38]. Such attacks can render a satellite inoperable without destroying it, which poses a potential threat to other space assets and could disrupt telecommunications systems. The impact is not limited to government or military objects but also affects the civilian population.

3. Disruption of satellite services

To support the claim that space systems should be considered CI, this section considers the worst-case scenario of a simultaneous failure of satellite constellations without pre-warning. Although the probability of a simultaneous failure of all satellites in Earth orbit is highly improbable, this scenario will assist in understanding the interconnection between conventionally accepted CI and space systems. The logic behind this chain is as follows:

- CI provides the global population with services;
- Space systems monitor CI to prevent service disruption using space applications (Global Navigation Satellite System [GNSS], EO, and communications) and/or actively interact with CI to enable these services;
- Space systems become CI.

The research [39] has summarised the short- and long-term consequences of global satellite disruption. The literature has identified two possible causes for such an event, although both are highly unlikely: a solar storm with a magnitude comparable to the one experienced during the Carrington event of 1859, also known as a mega solar storm, and the Kessler effect, which is caused by a space debris chain reaction. However, a survey of private and public space actors [39] demonstrated that cyberattacks are feared as a more likely cause for such a service disruption compared with the previous two. Fig. 2 summarises the timeline of events from time zero ($T + 0$) to one week after a satellite service disruption:

Note that this list of effects is not exhaustive, and the economic consequences are not quantified in this paper. Rather, the focus is on understanding the global consequences of a failure of space infrastructure.

Moreover, this section describes the worst-case scenario, a global service disruption, to help the reader understand the impact of space infrastructure on daily business. The effects of a partial or minor service disruption would be milder.

3.1. Impact on the civil domain

Independently of the cause of global service disruption, at $T + 0$, immediate consequences would derive from the loss of GNSS signal, especially on transportation infrastructure. Traffic on the road without navigational aid would become congested; maritime traffic would suffer from a lack of navigational aid in open waters and at ports; and airborne flights would lack guidance from the Air Traffic Management network, GNSS, and Satellite-Based Augmentation System (SBAS) systems, while the remaining fleet would be immediately grounded. Furthermore, search and rescue services would be impacted and wouls struggle to respond to emergencies. This scenario is exacerbated by the increasing use of automated transportation systems and collision-avoidance systems that depend on GNSS.

A collateral effect of the loss of GNSS is the unavailability of timestamps, which are the core of technologies used for timestamping financial transactions and managing power grids. The scenario summarised in [39] reveals that the financial system would be affected within a few hours by a global service disruption ($T + 2$ h), directly followed by power blackouts due to uncontrolled overload, and then the unavailability of broadcasting and telecommunication services that rely on time synchronisation and syntonisation (within $T + 8$ h). The effects of an unsynchronised power grid caused by the loss of timestamps would manifest from $T + 1$d. The electronic infrastructure (e.g., cash dispensers and digital services) would also be affected.

The loss of space assets for EO would have significant effects on subsequent days of the global service disruption. The user segment would be unable to receive warnings about adverse weather conditions, hurricanes, and natural disasters, while the food supply chain would start to break down from a combination of missing EO and GNSS services, such as in precision agriculture and commercial fishing. At $T + 1$ w from service disruption, the world economy would collapse and face bankruptcy and unemployment, followed by turmoil.

3.2. Additional impacts on the military domain

While the consequences discussed in Section 3.1 would apply independently to civil and military applications, additional implications must be considered for the military domain which is also highly dependent on civil infrastructures. To minimise the consequences of the disruption of CI caused by the disruption of the space systems infrastructure, governments would highly likely prioritise the recovery of military and strategic infrastructure for matters of national security. Commercial satellites for weather predictions, disaster management, and aerial and sea surveillance for civilian applications would likely be restored second.

In fact, military assets and national security would be equally

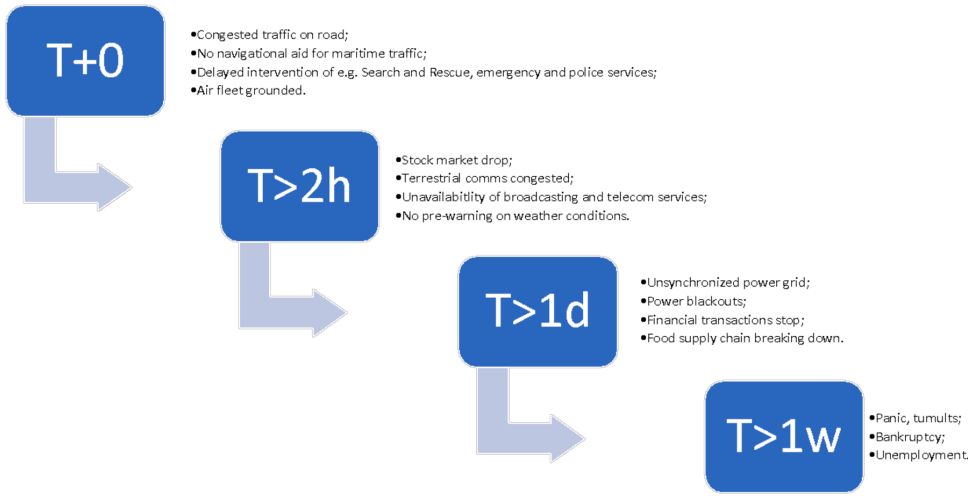


Fig. 2. Worst case scenario for a global satellite service disruption: Consequences after 2 h, 1 day, and 1 week.

affected by a global service disruption, mainly for the following reasons: (a) modern weapons systems rely on accurate navigation systems for high precision-strike capabilities (GNSS/SBAS); and (b) autonomous systems like drones and unmanned aerial vehicles (UAVs) require a significant bandwidth capacity. To understand how the use of bandwidth has increased in only 10 years to support military operations, a U. S. Department of defense (DoD) report states that 542,000 coalition forces participated in Operation Desert Storm in 1991 and relied on 99 Mbps of bandwidth, while in Operation Iraqi Freedom (2003) and Operation Enduring Freedom (2001), 350,000 coalition forces relied on 3200 Mbps of bandwidth from the space system infrastructure [40]. All military assets depend on high-bandwidth communications and their contractors, not only in the United States.

An interesting mitigation for this scenario that would serve to restore military capabilities is the concept of responsive space, which is presented in the following subsection.

3.3. Responsive space

In recent years, the concept of responsive space systems has been adopted to mitigate, amongst others, a scenario that includes a disruption of satellite services. Responsive space is an important concept for counteracting the loss of space systems as CI in the short term. Because it was initially used by the military, an overview is first provided in this sense.

While the term 'responsive space' is not yet used by NATO, it is an element that ensures persistent space support [41]. Some of NATO Member States, however, already intend for its definition to be a combination of resilience methods and alternative solutions that ensure persistent support to strategic operations [42]. Thus, responsive space is an evolving discipline of military space support. Most ongoing research and development proceeds are restricted information within a state, and therefore, only a few examples are public [41]. In 2005, the U.S. DoD introduced a new business model named Operational Responsive Space (ORP), which underlines the importance of having responsive launch capabilities for launchers as well as satellite solutions for complementing larger space programmes [40]. In September 2020, Germany inaugurated the Responsive Space Cluster Competence Centre (RSC3) of the German Aerospace Centre (Deutsches Zentrum für Luft- und Raumfahrt [DLR]) [41]to explore the technological basis for a national responsive space capability and demonstrate key technologies in space [43]. France and the UK have not directly stated the term responsive space in their national policies [42]. The Responsive Space Capabilities Memorandum of Understanding between the Departments and Ministries of Defence of Australia, Canada, Germany, Italy, the Netherlands, New Zealand, Norway, the UK, and the USA remains to be addressed [41].

The EU also supports commercial projects for the research and development of products to ensure European defence capabilities. For example, the European Defence Fund (EDF) was allocated a budget close to €8 billion for 2021–2027, encouraging the participation of small and medium-sized enterprises in the bids [44]. One of their tender opportunities covers the topic of responsive space systems.

Based on the scenario presented in Section 3, to recover the strategic infrastructure in a timely manner, governments have two options: (1) providing on-orbit spares for Intelligence, Surveillance, and Reconnaissance (ISR) systems, or (2) launching new systems to replace disabled ones [45].

For the first option, the availability of orbital transfer vehicles (OTVs) on the market would be crucial. Recent research focused on the European market indicates that operators are rushing to get their respective OTVs into service [46]. Such vehicles can be developed for multiple functionalities, such as the last-mile delivery of payloads, hosted payloads, debris removal, and on-orbit servicing, to name just a few. The availability of on-orbit spares for ISR systems, however, would likely be negatively affected by the same events that damaged the remaining fleet in case of global disruption of satellite services. In addition, assuming that on-orbit spares were available and still functional, they might have become obsolete compared with those satellites to be replaced [45]. On-orbit servicing could be an alternative approach, which would first require a dedicated launch of, for example, an OTV that contains spare parts. Such a service is still not well established, mainly because it is associated with high risks due to complex rendezvous and docking manoeuvres.

As of today, the only successfully demonstrated technology is the Mission Extension Vehicle (MEV) of Northrop Grumman. The first docking to a client satellite in geostationary Earth orbit (GEO) was completed by MEV-1 in February 2020, followed by MEV-2 in April 2021 [47].

Instead, the European space industry is in the process of developing a technology demonstrator. In September 2022, Thales Alenia Space was chosen by the European Commission to lead the European Robotic Orbital Support Services In-Orbit Demonstrator (EROSS IOD), funded by the EU through the Horizon Europe programme [48]. The programme, which started in 2023, aims to demonstrate satellite rendezvous, capture, docking, refuelling, and payload exchange capabilities, with the final purpose of providing maintenance and upgrades on-orbit to extend a satellite mission.

Returning to the recovery strategies for CI after global satellite service disruption, launching new systems to replace the disabled ones seems to be the preferred option. For both military and commercial actors, the need for quick, responsive launches is universally acknowledged. While the military usually relies on small, solid-fuelled launch vehicles based on intercontinental ballistic missile (ICBM) technology [45], additional options include commercial mini launchers and air-launched solutions. The availability of orbital and suborbital launch sites worldwide as of 2023 [49] also indicates that extending the responsive space concept to include commercial launchers and launch sites across the globe would increase the availability of launch sites and orbit accessibility in case of a global service disruption [50]. A European Space Policy Institute (ESPI) report from 2018 [51] indicated that micro launchers can maximise the flexibility, schedule, and (partially) the availability of a launch through a dedicated allocation for smallsats. Nonetheless, commercial and military launch operators should be prepared to cope with shorter launch notifications, reduced assembly times, and storage challenges, leading to potentially less effective prices [51] if responsive space is to be the business case in focus.

In the context of a responsive space strategy at the national level, it appears crucial to enhance the development of policies and governance related to the replacement of CI in space.

4. Interdependencies within the space infrastructure

The close interconnection of individual systems in this system of systems makes it increasingly difficult for legislators and security experts to identify where one infrastructure ends and another begins. This is due to the fluidity and interconnectivity of modern infrastructure systems, which are neither static nor bound to one geographical location. Perhaps licensing authorities for space activities could support the process of drawing the boundaries around the space infrastructure and identifying the interface points to the conventionally accepted CI. For instance, if a space regulator requires the space manufacturer and/or operator to license its asset before being launched into space, the licensing process itself could provide an indicative boundary between space systems. Assuming that space asset A is licensed by authority X for a declared functionality or mission profile, space asset A can be part of an interconnected system and interface with space asset B during its life cycle. Asset B can be either a copy of asset A (e.g., for GNSS) or licensed by another authority Y for a different functionality or mission profile (e.g., refuelling orbital station). Authorities X and Y, as well as the asset manufacturers/operators for A and B, will have to interact to define the interfaces within the global space system C. While defining the boundaries of system C, a risk assessment should be provided to assess the

effects on conventional CI due to a global failure of C, or a local failure of A or B, as well as their mitigation actions.

Because of the development of new capabilities and degrees of efficiency, the transformation within the system of systems constitutes, from a safety perspective, a clear development towards greater dependence and, therefore, a decrease in security.

The interdependence of CI systems is what makes their interconnection simultaneously the origin and product of a system of systems. It is therefore logical that all CIs are characterised by a mix of risks that include those of critical spatial infrastructures, which are transmitted to the last outputs through the channels of interconnections, creating different degrees of dependence (e.g., direct, indirect, secondary, or tertiary) [11].

4.1. Direct dependency

This subsection supports the statement that the dependence of CIs on space systems is increasing for various heterogeneous and independent reasons [11].

First, economic conditions for access to space are evolving, reducing restrictions on access to the space industry (or at least making it less difficult). The reduction in costs is offset by the increase in the capacity and services offered (e.g., ridesharing for launches), while competition and technological innovation make it possible to envisage, in the short term, further developments capable of radically changing the space industry itself. The cost of necessary financing as well as insurance solutions is decreasing as a result of an enhanced understanding of risks, an improved hazard profile, and the gradual formation of a framework for business activity that addresses uncertainties (e.g., the responsibility of individual elements of space systems). For instance, market capacity and premiums have stabilised since 2020, with US$579 million in premium income being registered in 2022 against $294 million in insured losses [52]. The reduction in insurance for LEO assets, however, is also due to the fact that many operators in LEO are not insuring their launches or satellites (e.g., SpaceX) [53].

Second, new developing countries are increasingly skipping some infrastructure steps to adapt directly to their space substitutes, to reduce initial costs and develop more rapidly, beyond the economic advisability of such a leap or the foresight of such a choice in the face of the difficulties involved in managing security. Rapidly developing nations are giving up the installation of cable communications in favour of wireless communications, moving directly to payment systems and banking services that do not require the physical infrastructure, which is still present in developed nations, at least as 'buffer systems'. At the same time, already developed nations continue to use pre-existing infrastructure systems that are still economically usable or non-depreciable, transforming dependence on the full spectrum of space systems into a patchy scenario [54].

4.2. Indirect dependency

There is also a circumstantial criticality, where the eventualities and environmental factors determine whether the relationship between the space system and the single CI becomes even more important and potentially dangerous, where the interruption or destruction of space systems would cause more than significant discomfort. A good example is satellites used for communications. They can be replaced in everyday use by means of terrestrial application, but not if an extreme weather phenomenon makes them the only reliable means of command and coordination. Governmental agencies worldwide already recognise the impact that space weather activities might have on the space segment functionality; therefore, they support space weather prediction services as well as their interaction with international agencies. The monitoring of solar activity and cosmic ray intensity variation are provided, for example, by the European Space Agency's Space Weather Service Network [55] and the National Oceanic and Atmospheric Administration's Space Weather Prediction center [56]. The information freely available to the user segment allows the despatch of pre-warnings or alerts for potential service disruption or malfunction in the satellite fleet.

In addition, a further indirect criticality is generated by the chain of interconnections with other CIs. To understand how this can easily happen, imagine an agricultural system characterised by non-intensive and less productive farms where precision agricultural systems are not used and natural resources are administered with the support of information collected through satellites. In this case, the agricultural infrastructure should be almost immune to disruptions to the space infrastructure. Yet, this is not the case. When the time comes for the country's farmers to obtain loans, secure crops, or transport them to the market, especially the international market, they use CIs that depend on space systems, namely the financial infrastructure and that of international transport (this implies their indirect dependence). Their dependence, in this case, may be indirect, but it is still appreciable and measurable [54].

4.3. Traceability of dependencies

The increasing complexity of the relationships involved within CIs also requires further advances in the field of visualisation as well as in modelling and simulation skills. One of the most widespread methods requires a quantitative approach to the level of services that are provided by space systems or a particular satellite system and their proportion to the whole. However, this solution seems to favour communication systems rather than EO-critical systems such as meteorological satellites.

Another methodology involves monitoring monetary flows between separate infrastructure systems, using economic exchange as a means of measuring relative importance and thus related criticality. The Australian government, for example, has used this method to describe the interconnection between CI and the level of its dependence on other infrastructure systems, as is the case in the agriculture sector [57]. Efforts at the national level are certainly critical and are likely to form the backbone of the overall effort, as most of the resources and organisational capabilities are focused on the commitment to protecting CI geographically located at the national level. However, an over-reliance on individual efforts allows for the formation of security gaps to which security professionals will inevitably be blind as a result of information asymmetries [12].

Cooperation at the global level should not be delegated exclusively to nations that own assets in space (public or private) and/or can provide space access, although they undoubtedly hold a technological and financial advantage since they are not the only users. In fact, it is important for all countries that recognise their dependence on space systems to participate in the development of a policy framework that considers their demands and fears. Elements such as sovereignty, accountability, stakeholder involvement, and jurisdiction are the main obstacles to the exercise of global governance, but the alternative is now there for all to see, namely a confused congery of interests, aspirations, immobility, and prevarication [54].

4.4. Suggested approach for the protection of space critical infrastructures

The realisation of risks in CI is not easily predictable or preventable, and its effects cannot be entirely contained. All of this has, to date, been a daily challenge for governments at the national level, with increasing development in regional organisations such as the EU and NATO, but only for land infrastructure. In this framework, however, space systems have been relegated to a marginal position compared with more essential systems that continually face serious threats. The precepts of CI protection should be applied to critical space infrastructures, identifying threats, mitigating vulnerabilities, and minimising disruptions [11].

Nevertheless, policymakers and decision-makers should not

transpose the philosophy of protecting CI from terrestrial systems to space because this would underestimate the risks inherent in the strong interconnections between the two systems. Rather, space systems should be integrated into pre-existing security and risk-prevention frameworks as a consequence of full awareness of their importance to implement and evolve the protection of CI around the world.

For example, the SmartSat report on satellite cyber security [58] attempted to identify key elements from CI resilience that can be transferred to space infrastructure as part of a global strategy [59,60]. When comparing space systems against terrestrial digital infrastructure, it is evident that technology, ownership, and management are more complex in space. Major reasons are identified in the inaccessibility of the system and the difficulty of assessing the intent of a moving space object. The authors of the report encouraged readers to learn from the definition of resilience for cyber–physical systems in terrestrial CI and tailor it to space CI. Energy and power were identified as CI, which indicates the most understanding of resilience and the most similarities to space systems. [61] The regulation of power grids and energy CI, as well as their risk management and resilience, can be used by policymakers to draft protective measures for space CI [62].

5. Governance of cyberspace applied to space

Section 2 demonstrated that the inclusion of space as CI irremediably creates an interconnection with cyberspace. As such, a similar governance to cyberspace could also apply to space infrastructure. This section supports the basis for the fundamental aspects of cyberspace that require greater international cooperation and suggests improvements for its governance.

5.1. Enhancing international cooperation in cyberspace

Following the discussion in Section 2 where space and cyberspace CI were presented as the backbone of the conventionally accepted CI, the question of how to regulate those backbone infrastructures acquires full significance. Three fundamental aspects for the governance of all CI that need greater international cooperation are cybersecurity, Internet governance [63,64], and freedom of expression. Since space and cyberspace are enabling and supporting conventional CIs, the same governance aspects apply to them as shown in Fig. 3.

Including space systems in the definition of CIs requires an additional reasoning step regarding how such infrastructure should be regulated. Because the safety and security of space systems are primarily guaranteed through cyberspace, it is beneficial to start the assessment from the available legislations, policies, and frameworks valid for cyberspace.

Considering the three aforementioned fundamental aspects of cyberspace, nature itself requires a multilateral and cooperative approach between the actors in international relations [65]. Specifically:

- The realisation and maintenance of IT security require the realisation of a public–privat partnership at an international level, with different cooperative phases. Considering the ubiquity of cyberspace and the interdependence and interconnectedness of different CIs at the international level, all states should commit to combating threats that come from cyberspace and that produce real effects.
- Internet governance should be based solely on the multistakeholder model, starting with the awareness that companies or private entities cannot univocally control essential activities related to the network. The Internet Corporation for Assigned Names and Numbers (ICANN) should move onto the path of transparency, structuring, empowering, and becoming more inclusive, thus truly representing a multistakeholder framework, if it is to continue to act as a private regulator [33].
- Freedom of expression could be guaranteed by the high inclusive capacity of the UN, which – with the support of the scientific community – should spread a culture of awareness and empowerment amongst all Internet users [63]. The universal right to access the Internet should be guaranteed and, in turn, constitute a guarantee for freedom and the maintenance of cyberspace, understood as a global common.

States should not rely solely on public–private partnerships that enable a handful of people to scrutinise public and private portions of the IT infrastructure management systems, including satellites. Intelligence and specialised law enforcement agencies should become more evolved but must remain supervised and accountable to a democratic government to guarantee security and legitimacy [66]. States should thus strive for a strategy that guarantees a balance between these actors

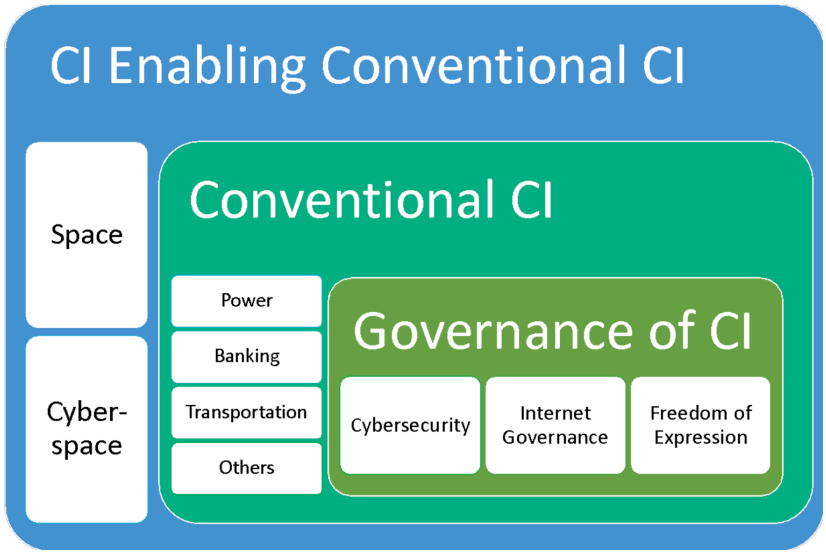


Fig. 3. Governance of critical infrastructure extended to space and cyberspace.

and ensures the greatest possible resilience in an area increasingly contested by emerging threats.

5.2. Governance of defence and security systems

If sponsored by a state, threats can also give rise to military escalations. To respond to threats from cyberattacks, states should set up alert structures capable of receiving notification from public and private entities to ensure the greater resilience of the entire Internet-based system. In this context, 'dialogue tables' open to the international community should be envisaged, which could identify, for example, confidence-building measures (CBMs) applicable to cyberspace, working to mitigate both the risk of military escalation and the risk of proliferation of cyber weapons. An initiative undertaken by the Organization for Security and Co-operation in Europe (OSCE) titled 'Confidence-building measures to enhance cybersecurity' is based on open dialogue between Member States and provides for the application of CBMs to cyberspace to prevent the aforementioned military escalations [67].

Section 2.3 introduced the concept of ASAT weapons for defence. In this sense, a global policy that bans the use of such weapons to increase the safety of space infrastructure is likely not applicable. However, a code of conduct can potentially be established by all nations that operate in space. For example, due to the critical nature of the orbits used by the US, Russia, China, and India to test their ASAT systems, the US committed 'not to conduct destructive, direct-ascent ASAT missile testing, and [stated] that the United States seeks to establish this as a new international norm for responsible behaviour in space' [68].

During the 77th session of the UN General Assembly's First Committee on Disarmament and International Security [69], the US proposed a resolution banning ASAT testing, adopted on 1st November 2022. Many nations were influenced to adopt a self-imposed moratorium due to the US's commitment to it. This was the first major international step towards governing defence and security in the space domain in the last decade.

6. Limitations and next steps

This paper suggests selecting the following as a starting point for the definition of policy and regulations of space as CI: governance for cyberspace, due to the interconnection of space and cyberspace as a backbone for terrestrial CIs; existing governance for terrestrial CI (e.g., energy and power), due to similar features shared with space systems CI; and defence agreements or codes of conduct to regulate military activities in outer space. However, the lack of an overall vision and the poor integration into interconnected international regulatory frameworks do not yet allow for a clear identification of the implementation phase on a global level.

In answering the questions about what security arrangements have been adopted to deal with space systems as CI, it was identified that international agreements on the security of space systems are proceeding slowly. This is because there are various obstacles to their development, including the different sensitivities of the states on the issue of the security of space systems, the difficulty of reaching a consensus on a common definition of 'safe space', and the lack of an international legal framework for the security of space.

These agreements should address several issues, including the definition of a legal framework for the security of space, the development of cooperation mechanisms between states to prevent and mitigate threats to the security of space systems, and the promotion of information sharing and cooperation between space system operators.

Based on the experiences recorded up to now, the authors suggest that resolutive potential would involve, for example, the intervention of regulatory action by international bodies such as the UN, multi-stakeholder consultation tables, and organisms that promote self-regulatory solutions.

7. Conclusions

This article has summarised the main points of the conception of space systems as CIs that require inclusion in appropriate protection frameworks and paradigms. Space systems can be described as 'critical' as they are important enablers of functional applications for properly functioning in a technologically developed and interconnected society.

Today, the world faces challenging security issues of both a natural and human-made nature, such as continuous environmental pressures that can cause spontaneous interruptions or terrorist acts precisely aimed at interrupting the operation of one or more CIs.

The disruption or destruction of space systems would cause significant damage to the critical terrestrial infrastructure, resulting in material and human losses, as well as a collapse in the confidence of investors and consumers worldwide. Restoring space capabilities after a service disruption would most likely be prioritised for defence and security assets, using concepts of operations based on, for example, responsive space and in-space servicing, depending on the severity of the damage.

The recent developments of the Russo-Ukrainian conflict have demonstrated the increasing role of the cyber domain, especially for communications and military assets. They have also brought issues such as logistics and the degree of resilience of computer and satellite systems to the forefront of public debate. Nonetheless, the conflict has also underlined the importance of including space systems as CI and defining the interlinkages within cyberspace. Space systems have their peculiarities in terms of risks, such as space weather and space debris, and they are also increasingly vulnerable to human disturbance efforts through the development and proliferation of anti-satellite weapons and technologies, as well as attacks and infiltrations in the connection and control of computer systems. The governance of space systems is still under development, although attempts are being made to identify critical links between terrestrial, space, and traditional CIs in international regulatory frameworks and policies. Being the backbone of conventional CI, regulation and governance of space systems should become a priority in the agenda of governments and policymakers. Negligence in doing so could result in heavy consequences on society and the global economy in the not-too-remote event of significant disruption of services associated with space systems.

CRediT authorship contribution statement

Mr. Antonio Carlo: Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Formal analysis, Conceptualization. **Dr. Paola Breda:** Writing – review & editing, Writing – original draft, Visualization, Investigation, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper

Data availability

No data was used for the research described in the article.

References

[1] G.F. Bignami, A. Sommariva, The economy of space. challenges for Europe, Rome, Lit (2017) 35.
[2] A. Froelich, Post 2030-Agenda and the Role of Space: The UN 2030 Goals and Their Further Evolution Beyond 2030 For Sustainable Development, Springer, Vienna, 2018, p. 66.
[3] Report, in: Report, 2018, Bryce Space and Technology, Washington, 2017.
[4] Bryce Tech, Start-up Space: Update on Investment in Commercial Space Ventures, 2024. Available at: https://brycetech.com/reports/report-documents/Bryce_Start_Up_Space_2023.pdf.

[5] Space Venture Europe 2020. Entrepreneurship and Investment in the European Space Sector, European Space Policy Institute, ESPI, Vienna, 2020, p. 14.
[6] A. Carlo, Outer Space and Cyber Space. Studies in Space Policy, in: A. Froehlich (Ed.), Cyber Threats to Space Communications: Space and Cyberspace Policies, Springer, Cham, 2021, p. 33.
[7] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC), Off. J. Eur. Union 333/164 (2022).
[8] North Atlantic Treaty Organization, Security Within the North Atlantic Treaty Organization (NATO), North Atlantic Council, C-M(2002)49-REV1, 2022.
[9] NIST, Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology, Special Publication, 2012, pp. 800–853.
[10] R.S. Radvanovsky, A. McDougall, Critical Infrastructure: Homeland Security and Emergency Preparedness, CRC Press, Boca Raton, 2018, https://doi.org/10.4324/9781315164687.
[11] A. Georgescu, A.V. Gheorghe, M.I. Piso, P.F. Katina, Critical Space Infrastructures: Risk, Resilience and Complexity, 8, Springer, New York, 2019, https://doi.org/10.1007/978-3-030-12604-9.
[12] S. Marchisio, U. Montuoro, Lo spazio cyber e cosmico: risorse dual use per il sistema Italia in Europa, Turin, Giappichelli (2019) 127.
[13] European Commission, Copernicus Programme. Available at: https://www.copernicus.eu/en/copernicus-services/emergency.
[14] E. Mayerick, A. Pickard, T. Rahloff, S. Bonnart, A. Carlo, K. Thangavel, Ground Station as a Service: A Space Cybersecurity Analysis, in 72nd International Astronautical Congress – Dubai, United Arab Emirates, 25-29 October 2021, IAC-21,D5,4,5,x66555.
[15] U. Tatar, A.V. Gheorghe, O.F. Keskin, J. Muylaert, Space Infrastructures. From Risk to Resilience Governance, IOS, Amsterdam, 2020, p. 305.
[16] A. Salmeri, A. Carlo;, Security-by-Design Approaches for Critical Infrastructure: mapping the Landscape of Cyber and Space Law, NATO Legal Gazette (2022) 42.
[17] Official Journal of the European Union, Directive (EU) 2022/2557 off the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557.
[18] Official Journal of the European Union, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, in: Amending Regulation (EU) No 910/2014 and Directive (EU), 1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), 2018. /Available at, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02022L2555-20221227&qid=1712664417933.
[19] National Space Strategy, UK Space Agency, 2022. Available at, https://www.gov.uk/government/publications/national-space-strategy/national-space-strategy#:~:text=From%20the%20first%20warning%20of,Critical%20National%20Infrastructure%20(%20CNI%20).
[20] F. Cilluffo, M. Montgomery, S. Cardash, K. Shields, Cyberspace Solarium Commission 2.0 (CSC) – Time to Designate Space Systems as Critical Infrastructure (2023).
[21] European Commission, Launch of the EU-NATO Task Force: strengthening our resilience and protection of critical infrastructure, Statement (2023). Available at, https://ec.europa.eu/commission/presscorner/detail/en/statement_23_1705.
[22] NATO, NATO and European Union launch task force on resilience of critical infrastructure, NATO Media (2023). Available at, https://www.nato.int/cps/en/natohq/news_212874.htm.
[23] European Commission, Critical Infrastructure: commission proposes a Blueprint to improve response to disruptive cross-border incident, Brussels (2023). Available at: https://ec.europa.eu/commission/presscorner/detail/e%20n/ip_23_4350.
[24] G. Falco, W. Henry, M. Aliberti, B. Bailey, M. Bailly, S. Bonnart, N. Boschetti, M. Bottarelli, A. Byerly, J. Brule, A. Carlo, G.D. Rossi, G. Epiphaniou, M. Fetrow, D. Floreani, N.G. Gordon, D. Greaves, B. Jackson, G. Jones, R. Keen, S. Larson, D. Logsdon, T. Maillart, K. Pasay, N.P. Mantii, C. Maple, D. Marsili, E.M. Miller, J. Sigholm, J. Slay, C. Smethurst, J.D. Trujillo, N. Tsamis, A. Viswanathan, C. White, E. Wong, M. Young, and M. Wallen. An international technical standard for commercial space system cybersecurity - a call to action. In ASCEND, editor, Methods and Considerations for Cyber Protection of Space Assets, 2022.
[25] Bryce Tech, State of the Satellite Industry Report 2022, 2023. Accessible at, https://brycetech.com/reports.
[26] Satellite Industry Association, State of the Satellite Industry Report 2015, Bryce Space and Technology, Washington, 2015. Available at, https://brycetech.com/reports/report-documents/SIA_SSIR_2015.pdf.
[27] Bryce Tech, Smallsats by the Numbers 2023 (2023). Accessible at: https://brycetech.com/reports.
[28] A. Carlo, L. Lacroix, L. Zarkan, The Challenge of Protecting Space-based Assets against Cyber Threats, in: 71st International Astronautical Congress, 2020, p. x59386. IAC-20,E9,2.D5.4,11.
[29] A. Carlo, Opportunities and Challenges in the Cyber-Space Nexus, ISPI (2023). Available at: https://www.ispionline.it/en/publication/opportunities-and-challenges-in-the-cyber-space-nexus-153013.
[30] Union of Concerned Scientists, UCS Satellite Database. Available at: https://www.ucsusa.org/nuclearweapons%20/space-weapons/satellite-database.html#.VmXWlnYrLIv.
[31] A. Messeni Petruzzelli, U. Panniello, Space Economy, Milan, Angeli (2020) 48.
[32] M. Castells, Comunicazione e Potere, Milan, Egea (2014) 175.
[33] U. Pagallo, Il diritto nell'eta` dell'informazione: il riposizionamento tecnologico degli ordinamenti giuridici tra complessita sociale. Lotta Per Il Potere e Tutela Dei Diritti, Giappichelli, Torino, 2014, p. 85.
[34] A.F. Uricchio, Nuove Piraterie e Ordinamenti Giuridici Interni e Comunitari, Cacucci, Bari, 2017, p. 329.
[35] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, entered into force Oct. 10, 1967, 18U.S.T. 2410, 610U.N.T.S. 205.
[36] A. Carlo, N. Veazoglou, ASAT Weapones: Enhancing NATO's Operational Capabilities in the Emerging Space Dependent Era, 19, MESAS, Palermo, Italy, 2019, https://doi.org/10.1007/978-3-030-43890-6_34. Available at.
[37] European Parliament, The role of cyber in the Russian war against Ukraine: its impact and the consequences for the future of armed conflict (2023). Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf.
[38] CyberPeace Institute, Case Study: Viasat, 2022. Available at, https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat.
[39] C. Van Camp, W. Peeters, A World without Satellite Data as a Result of a Global Cyber-Attack, Space Policy 59 (2022), https://doi.org/10.1016/j.spacepol.2021.101458.
[40] A.K. Cebrowski, J.W. Raymond, Operational Responsive Space: a New Defense Business Model, US Army War Coll. Q. 35 (2005).
[41] D. Zimber, T. Vasen, Responsive Space for NATO Operations - Part 2, Joint Air Power Competence Centre 32 (2021).
[42] W. Jung, T. Vasen, Responsive Space for NATO Operations, JAPCC, J. Ed. 31 (2021).
[43] ASD Eurospace, Information Note Amazon Kuiper - Eurospace TF New Flagship secure Connectivity (2020). Available at: https://eurospace.org/wp-content/uploads/2020/11/information-note-amazon-kuiper_18112020.pdf.
[44] European Defence Fund. Available at: https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf_en.
[45] T. Vasen, Responsive Launch of ISR Satellites: a Key Element of Space Resilience? Joint Air Power Competence Centre 27 (2018).
[46] A. Parsonson, Top European Launch Companies of 2022 - The European Spaceflight Power Ranking, European Spaceflight Ltd (2023). Available at, https://europeanspaceflight.com/top-european-launch-companies-of-2022-the-european-spaceflight-power-ranking/.
[47] J. Anderson, Mission Extension Vehicle (MEV): award-Winning Satellite-Life-Extension Servicing Vehicle, SpaceLogistics - a Northrop Grumman Company (2012). Available at: https://www.northropgrumman.com/wp-content/uploads/Mission-Extension-Vehicle-MEV-fact-sheet.pdf.
[48] Horizon Europe, European Commission. Accessible at: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en.
[49] Bryce Tech, Orbital and Suborbital Launch Sites of the World 2023 (2023). Available at: https://brycetech.com/reports.
[50] Bryce Tech, 2022 Orbital Launches Year in Review (2023). Available at: https://brycetech.com/reports.
[51] M. Tugnoli, M. Sarret, M. Aliberti, European Access to Space: Business and Policy Perspectives On Micro Launchers, European Space Policy Institute, Vienna, 2018.
[52] P.B. De Selding, Kratos: expect 13-15% annual growth in our space business; showcase ground contract with Intelsat (2023). Accessible at: https://www.spaceintelreport.com/kratos-expect-13-15-annual-growth-in-our-space-business-showcase-ground-contract-with-intelsat/.
[53] Federal Communications Commission, Order and Authorization and Order on Reconsideration - Request for Modification of the Authorization for the SpaceX NGSO Satellite System (2021). Available at: https://docs.fcc.gov/public/attachments/FCC-21-48A1.pdf.
[54] B. Biringer, E. Vugrin, D. Warren, Critical Infrastructure System Security and Resiliency, 77, CRC Press, Boca Raton, 2013, https://doi.org/10.1201/b14566.
[55] European Space Agency, Space Weather Service Network. Available at: https://swe.ssa.esa.int/current-space-weather.
[56] National Oceanic and Atmospheric Administration, Space Weather Prediction Center. Available at: https://www.swpc.noaa.gov/.
[57] N. Nguyen, L. Hogan, K. Lawson, P. Gooday, R. Green, K. Harris-Adams, T. Mallawaarachchi, Infrastructure and Australia's food industry: preliminary economic assessment, Australian Bureau of Agricultural and Resource Economics and Sciences, Canberra 13(2013). Available at: https://www.researchgate.net/publication/265966027_Infrastructure_and_Australia%27s_food_industry_Preliminary_economic_assessment.
[58] SmartSat, Satellite Cyber Resilience Whitepaper - Technical Report, 8, 2022. Available at, https://smartsatcrc.lbcdn.io/uploads/Satellite-Cyber-Resilience-Whitepaper-FINAL.pdf.
[59] R.K. Knake, Internet Governance in an Age of Cyber Insecurity, Council Foreign Relat. 56 (2010) 12.
[60] U. Gori, S. Lisi, Information warfare 2013. La protezione cibernetica delle infrastrutture nazionali, Milano, Angeli (2014) 31.
[61] P. Breda, A. Abdin, R. Markova, D. Jha, A. Carlo, N.Pelin Mantı, An extended review on cyber vulnerabilities of AI technologies in space applications: technological challenges and international governance of AI, J. Space Saf. Eng. (2023).
[62] G. Christou, Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy, Palgrave Macmillan, London, 2016, p. 81.
[63] E. Bertolini, V. Lubello, Internet: Regulation and Protection of Fundamental Rights, Aracne, Rome, 2013, p. 112.
[64] T. Detti, G. Lauricella, Le Origini di Internet, Milano, Mondadori Bruno (2013) 195.
[65] U. Gori, L.S. Germani, information warfare 2011. La sfida della Cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale, Milano, Angeli (2011) 48.

[66] C. Cencetti, Cybersecurity: Unione Europea e Italia. Prospettive a confronto, Quaderni IAI Pubblicazioni, 2014, p. 105. Available at, http://www.iai.it/sites/default/files/iaiq_12.pdf.
[67] G. Cassano, G. Scorza, G. Vaciago, Diritto dell'internet. Manuale opertivo. Casi, legislazione, giurisprudenza, Padova, Cedam (2012) 744.
[68] The White House, Vice President Harris Advances National Security Norms in Space: new U.S. Commitment on Destructive Direct-Ascent Anti-Satellite Missile Testing (2022). Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/18/fact-sheet-vice-president-harris-advances-national-security-norms-in-space/.
[69] United Nations, Destructive direct-ascent anti-satellite missile testing. General Assembly, 2022. Available at, https://documents-dds-ny.un.org/doc/UNDOC/LTD/N22/630/36/PDF/N2263036.pdf?OpenElement.

Appendix 2

II

A. Carlo, N. P. Mantı, B. A. S. W. Am, F. Casamassima, N. Boschetti, P. Breda, and T. Rahloff. The Importance of Cybersecurity Frameworks to Regulate Emergent AI Technologies for Space Application. *Journal of Space Safety Engineering*, 10(4):474–482, 2023

Journal of Space Safety Engineering 10 (2023) 474–482

Contents lists available at ScienceDirect

Journal of Space Safety Engineering

journal homepage: www.elsevier.com/locate/jsse

The importance of cybersecurity frameworks to regulate emergent AI technologies for space applications

Antonio Carlo[a,*], Nebile Pelin Mantı[b], Bintang Alam Semesta W.A.M[c], Francesca Casamassima[d], Nicolò Boschetti[e], Paola Breda[f], Tobias Rahloff[g]

[a] Tallinn University of Technology, Tallinn, Estonia
[b] PIL Department, Faculty of Law, Istanbul University, Istanbul, Türkiye
[c] Skolkovo Institute of Science and Technology, Skolkovo, Moscow Oblast, Russia Federation
[d] IT & Security Governance, Dedalo GRC Advisory, Rome, Italy
[e] Sibley School of Mechanical and Aerospace Engineering, Cornell University, Ithaca, New York, United States
[f] International Space University, Illkirch-Graffenstaden, France
[g] Duale Hochschule Baden-Württemberg (DHBW) Mannheim, Mannheim, Germany

ARTICLE INFO

Article history:
Received 5 May 2023
Received in revised form 30 July 2023
Accepted 7 August 2023
Available online 26 August 2023

Keywords:
Cybersecurity
Artificial intelligence
Earth observation
Cyber risk
Emerging disruptive technologies

ABSTRACT

Over the past decades, industries and governments have progressively been relying upon space data-centric and data-dependant systems. This led to the emergence of malicious activities, also known as cyber-threats, targeting such systems. To counter these threats, new technologies such as Artificial Intelligence (AI) have been implemented and deployed. Today, AI is highly capable of delivering fast, precise, and reliable command-and-control decision-making, as well as providing reliable vulnerability analysis using well-proven cutting-edge techniques, at least when applied to terrestrial applications. In fact, this might not yet be the case when used for space applications. AI can also play a transformative and important role in the future of space cybersecurity, and it poses questions on what to expect in the near-term future.

Challenges and opportunities deriving from the adoption of AI-based solutions to achieve cybersecurity and later cyber defence objectives in both civil and military operations require rethinking of a new framework and new ethical requirements. In fact, most of these technologies are not designed to be used or to overcome challenges in space. Because of the highly contested and congested environment, as well as the highly interdisciplinary nature of threats to AI and Machine Learning (ML) technologies, including cybersecurity issues, a solid and open understanding of the technology itself is required, as well as an understanding of its multidimensional uses and approaches. This includes the definition of legal and technical frameworks, ethical dimensions and other concerns such as mission safety, national security, and technology development for future uses.

The continuous endeavours to create a framework and regulate interdependent uses of combined technologies such as AI and cybersecurity to counter "new" threats require the investigation and development of "living concepts" to determine in advance the vulnerabilities of networks and AI.

This paper defines a cybersecurity risk and vulnerability taxonomy to enable the future application of AI in the space security field. Moreover, it assesses to what extent a network digital twins' simulation can still protect networks against relentless cyber-attacks in space against users and ground segments. Both concepts are applied to the case study of Earth Observation (EO) operations, which allows for conclusions to be drawn based on the business impact (reputational, environmental, and social) of a cyber malicious activity. Since AI technologies are developing on a daily basis, a regulatory framework is proposed using ethical and technical approaches for this technology and its use in space.

Acronyms/Abbreviations: AI, Artificial Intelligence; DDoS, Denial-of-service attack; DL, Deep Learning; DT, Digital Twin; EO, Earth Observation; EDTs, Emerging Disruptive Technologies; EVT, Experientable Virtual Twin; GNN, Graph Neural Network; IP, Internet Protocol; ML, Machine Learning; MBSE, Model Based Systems Engineering; RF, Radio Frequency.

* Corresponding author.
E-mail addresses: ancarl@taltech.ee (A. Carlo), np_manti@yahoo.com (N.P. Mantı), BintangAlamSemesta.WisranAm@skoltech.ru (Bintang Alam Semesta W.A.M), fcasamassima8@gmail.com (F. Casamassima), nb624@cornell.edu (N. Boschetti), paola.breda@community.isunet.edu (P. Breda), contact@tobiasrahloff.com (T. Rahloff).

https://doi.org/10.1016/j.jsse.2023.08.002

1. Introduction

Over the last decade, the fourth industrial revolution, also known as Industry 4.0, has brought significant scientific and technological progress that has deeply affected spatial data-centric and data-dependant systems. Given the inherent criticality of the space sector, scientific and technological progress has also resulted in the emergence of new malicious capabilities targeting space systems. Amongst the countermeasures adopted to tackle malicious activities is the development and deployment of the so-called Emerging Disruptive Technologies (EDTs), such as Artificial Intelligence (AI), which are highly capable of delivering fast and reliable command-and-control decision-making actions, as well as providing reliable vulnerability analysis using well-proven cutting-edge techniques.

The significant advances made in the field of AI in the last decades has contributed to human progress in a wide range of scientific fields, such as robotics and machine learning. Moreover, it has substantially contributed to boosting current space efforts. AI is applied in many fields ranging from mission planning and designing, processing extensive amounts of data collected by satellites, assisting navigation systems as well as enhancing satellite imagery [1].

High-quality and precise satellite imagery is particularly important for Earth Observation (EO) and monitoring activities, defined as “the gathering of information about planet Earth’s physical, chemical, and biological systems via remote sensing technologies, usually involving satellites carrying imaging devices” [2]. Remote sensing provides unique capabilities and advantages such as observing wide areas, contributing to the increasingly accurate development of early warning or weather detection systems, allowing for the collection of data without jeopardising national sovereignty, rapid measuring of acquired images, and ensuring operational continuity of sensors for long-term data collection [3].

In recent years there has been an increasing use of Machine Learning (ML) and AI technologies for EO applications. In fact, the exponential growth of data collected by satellites, now in the order of several petabytes, requires the use of technologies for a quick and accurate analysis [4]. An example of this use is the PhiSat-1 (or Φ-Sat-1), the first European satellite to use AI to efficiently send EO data back to Earth. More specifically, the hyperspectral camera collects a significant number of images, some of which have poor quality due to external factors, such as cloud coverage. Φ-Sat-1’s artificial intelligence chip filters them to return only usable data, autonomously discarding those images that cannot be used [5].

The use of AI to support EO and monitoring activities has raised some challenges, more specifically deriving from the adoption of AI-based solutions to achieve cybersecurity and later cyber defence objectives in both civil and military operations. This includes the definition of legal and technical frameworks, ethical dimensions, and other concerns such as mission safety, national security, and technology development for future uses.

The objective of this paper is to propose a regulatory framework using ethical and technical approaches to regulate the use of AI in space, specifically applied to EO and system health monitoring. To achieve the objective, the paper develops a cybersecurity risk and vulnerability taxonomy for the future applications of AI in space. Network digital twins’ simulations are considered as mitigation example to protect networks against relentless cyber-attacks.

2. New technologies and their impact on cybersecurity

New technologies are a set of applications of scientific knowledge that offer a significant improvement over an established technology for a given process. The definition of “new” is in a continuous redefinition as technology changes over time in a cyclical way. These new technologies are a focal point for the development of our society and are discussed frequently for their potential use in both the civil and military domain. AI, as one of these innovations, accelerates technologic transformation and provides both opportunities and threats in the cyber realm.

AI, ML, Deep Learning (DL) and others are disruptive technologies that have been at the centre of attention for their potential use in conflict, deterrence, assurance, and competition. AI is often used as an umbrella term for a large variety of disciplines. Although its use is increasing in multiple domains, AI still does not have a universally accepted definition. The term Artificial Intelligence appeared for the first time in a workshop at Dartmouth University in 1956. John McCarthy, also known as the father of AI, defined AI as “the science and engineering of making intelligent machines” [6]. Referring to intelligent machines, computer scientist Elaine Rich regards AI as “the study of how to make computers do things at which, at the moment, people are better” [7].

Further differentiation should be made on the type of AI – weak, strong, and super [8], and on its uses - offensive or defensive. The distinction is provided by the range of functions and capabilities that each of the three type of AI supports. Nowadays, most progress has been made in weak, or narrow, AI. This is specialised on a very narrow range of functions, such as pre-programming assistance. Weak AI repeats similar codes that were predefined by their makers and classifies them accordingly. This kind of AI has entered the market and private homes. It is now widely used through smart devices such as smart-homes, phones, and cars. Strong AI instead aims to duplicate human intellectual abilities by copying them. While even more advanced, super AI seeks to outperform human intelligence with the increasing computational power that computers are able to elaborate [9].

The digitalisation of society presents new opportunities to improve data-driven multimedia services [10]. Data can take multiple forms, including text, audio, images, and videos. These data flow through different media such as the Internet of things, web sites, social networks, and have the possibility to be enhanced by AI, allowing for a transformation of the data making it dynamic. The dynamism of the data allows for the analysis of a large number of data by ML algorithms in a fast and reliable way. [11]

With regards to the development of AI technologies, after a period of so-called “AI winter” referring to a decline in interest and funding in AI technologies, an era of “AI spring” has entered. In fact, only this technology raised an estimated US$ 6.9 billion in the first quarter of 2020, although covering all industries and not only space [12].

It is also important to distinguish between artificial intelligence and automation. Whereas automation refers to a “broad category describing an entire class of technologies rather than just one” [13] including robotics, AI can be regarded as a type of automation that replaces “human labour in tasks both physical and cognitive” [13]. AI-driven security, like monitoring, threat hunting, incident response, and other time-intensive duties, can heighten exposure of the assets and vulnerability to cyber adversaries [14]. It becomes more important to understand risks and vulnerabilities of systems and integrated technologies.

3. Risk and vulnerabilities

One of the most important particularities of space data is its “instrumental” nature and the fact that the data received from satellites need to be converted into meaningful information. Therefore, specific AI methods to leverage advances in physical parameters extraction are needed and used. AI itself, on the other hand, can represent different uses, such as ML and DL methods, which are mainly used for image classification or object segmentation. The effective use of space data could require hybrid AI methods, encompassing mathematical models for the satellite orbit, the

physics of electromagnetic propagation and scattering, signal processing, machine learning, or knowledge representation [15].

3.1. Overview of cyber risks against AI space assets

It is not an easy or reliable matter to estimate the probability of a cyberattack. A cyber risk can be defined as the product of threats, vulnerabilities and impacts over the possible mitigations [16].

The use of AI bears some risks varying from lack of AI implementation traceability, data sourcing and privacy violations, as well as black box algorithms and lack of transparency, which require the adoption of a system-focused policy to track, assess, prioritise, and control cyber-AI risks. In addition, the use of AI can introduce program bias into decision making processes. As algorithms become considerably more complex, it is difficult to make a comprehensive overview of existing security vulnerabilities, as well as adopting cyber security measures to prevent any attack.

Other risks to AI are data sourcing and privacy violations since unfettered access to satellite data creates privacy-related legal and ethical problems. Either governmental and non-governmental entities as well as civilians, in the wrong hands, can become a source of national security threats, like revealing the position of secret military bases and global peacekeeping operations [17].

As well as black box algorithms, lack of transparency is one of the major concerns related to AI. AI-based decision-making tools can become target and be attacked by cyber means. Unintended consequences can be the obsolescence of existing controls, increased complexity in operations, and the possibility of cascading errors, which take place when only one part of the system fails, while the other parts compensate for the failed component [18]. This in turn overloads these nodes, causing them to fail as well, prompting additional nodes to fail one after another.

3.2. Overview of AI cyber vulnerabilities

AI, and in particular weak AI, is a cyber vulnerable technology. AI systems are not only embedded with traditional forms of cyber vulnerabilities, particularly the ones deploying machine learning, but are also depending on how AI works and learns. Existing attack surface composed of coding errors can be complemented by additional, and unpatchable errors, which can render the system using AI more open to attacks [19]. Attack codes to exploit vulnerabilities of AI systems have already proliferated in space by many States and agencies. On the one hand machine learning vulnerabilities further enable hackers to manipulate systems' integrity (causing them to make mistakes), confidentiality (causing them to leak information), and availability (causing them to cease functioning), while AI cyber defensive techniques are limited and hard to keep up with new means.

The uses of ML algorithms can help to identify and defend against computer-based vulnerabilities [20] and threats by automating the detection of an attack and its response. On the other hand, offensive AI algorithms can render cyberattacks increasingly difficult to block or defend against, by enabling rapid adaptation of malware to adjust to restrictions imposed by countermeasures and security controls [21].

In terms of AI cyber security, vulnerability refers to a weakness in hardware, software, or procedures. Risk on the other hand, refers to the potential for lost, damaged, or destroyed assets. Starting from the mission execution level to the data analysis, AI systems still have significant limitations and vulnerabilities, particularly regarding predictability, verifiability, and reliability. Both AI systems and AI-enabled systems deployed in different contexts in space can be attacked. AI attacks are enabled by inherent limitations in the underlying AI algorithms that currently cannot be fixed. Therefore, they are different from traditional cyberattacks that are caused by "bugs" or human mistakes in codes. An attack can target security in the training algorithm (e.g., adversarial machine learning), or vulnerabilities in the training process (e.g., data poisoning attacks). On the other hand, vulnerabilities in the platform on which the AI system runs can also have an impact on the classification results. An example is a concrete proof-of-concept attack to prove the feasibility and impact of platform attack, or a higher-level qualitative analysis to reason about the impact of large vulnerability classes on AI systems [22].

4. Cybersecurity risk and vulnerability taxonomy

AI technologies are one of the enabling and innovative technologies that can both reduce and augment cybersecurity risks and vulnerabilities. A cyber taxonomy would help to align cybersecurity definitions and terminologies to enable the categorisation of potential risk and vulnerabilities. Understanding technical aspects will help to shape legal and policy aspects.

Even if one might intuitively think that space assets can be challenging to attack, they are prone to multiple risks, even of a cyber nature. Satellites are the core of many industrial sectors such as telecommunications and, in the case of transportation, are the elements that, if disabled or destroyed, completely prevent operations. In addition, the importance of cyber risks for the space sector stems from the fact that there are no common standards and regulations in this field; that supply chains are particularly complex to manage; and that often these types of attacks deliver significant benefits to a relatively low price and visibility.

Cyber threats can affect all segments of a space operation, so both space, link, and ground segments need to be monitored and protected [23]. If kinetic threats aim to destroy or physically harm targets, and electronic threats aim to intercept or disable RF communications, cyber threats target data directly. The complexity of an attack is relatively low. Private hacker groups or individuals with low budgets can pose a threat. Space cyber threats can be analysed under two main categories, thus as technical cyber threats and as social engineering cyber threats. The former exploits the technical weaknesses of the various segments of space activities, while the latter exploits the deception or psychological manipulation of the victims in order to penetrate a system.

Technical cyber threats include a variety of attacks like signal hijacking, seizure of control, data corruption, data interception, Denial-of-service attack (DDoS) and Internet Protocol (IP) satellite attacks. Protection against signal hijacking is particularly important in telecommunications satellites. Using an antenna connected to a computer, the attacker can identify a free communication slot in a transponder and use the bandwidth capacity in excess. In this way, the attacked asset will be used to relay malevolent information, even if the actual risk consists of possible cross-talk interferences or denial of service. Another vulnerability is related to the Command and Control (C2) link which retrieves data from the subsystems. An intrusion into the C2 link of a satellite operator can make it possible for an attacker to seize control of the satellite. This could lead to an unintended change of orbit or a change of attitude to deteriorate optical instruments in an EO satellite. An intruder in the C2 link could also take control of the entire communication subsystem of the satellite leading to the interception of uplink data or the corruption of the downlink [24]. A DoS attack to the ground segment and the C2 link could block the control of the satellite's operations and the data collection. Hacker groups can also detect IP addresses from satellites providing internet connectivity and then initiate a TCP/IP connection from a stolen IP address [25].

Social engineering cyber threats include phishing, pretexting, baiting attacks, quid pro quo attacks, tailgating. Such attacks are not addressed to the technology directly, but to the human oper-

ators. These practices involve different ways of manipulating the victim's behaviour and psychology. As an example, if phishing exploits human naivety or distraction, a baiting attack exploits human curiosity. Quid pro quo and tailgating (or piggybacking) involve the deception of the victim and camouflage.

In addition to the two categories described above, another way of targeting space systems by means of cyber attacks is to disable or infiltrate the systems that monitor flight, position, and collision probability of space assets, in other words the Space Situational Awareness networks. These attacks have two main objectives: to prevent the observation of space traffic and promote traffic congestion; to hide the presence of spacecraft from the eyes of a competitor.

4.1. Overview of EO-assets security risks

With the rapid growth of internet services and dependence on the interconnected physical and digital technologies in the 21st century, cyber-physical security is persistently raised as one of the prevalent types of research in the modern digitalisation realm. Cyber-physical security addresses security concerns for physical systems used to maintain and implement cybersecurity solutions. At the same time the practical angle of AI is gradually emerging to contribute to the advancement of the automated and integrated cyber-physical systems using the ground-breaking AI techniques.

Recently, most space defence agencies customised the backbone of cyber-physical security by gradually augmenting the technical purpose of AI which consists of identifying, collecting, analysing, interpreting as well as neutralising and recovering from interference and intrusion, while constantly blocking doubtful actions on cyber-physical technologies including data communication protocol, data transmission bandwidth, and data management with secure protection [26].

The cyber-physical adversaries essentially can be expressed under two necessary intrusion parameters: cyber-threats and cyber-attacks. It is hard to devise AI-based automatic tools consisting of well-operated techniques of threats and attacks. Furthermore, the intrusion parameters also elaborate AI, ML, and DL for probing the intrinsic features representation from the existing cyber-physical security big data set. They have been deployed to various real cyber-physical security cases, for instance identifying, predicting, and scrutinising particular sets of threats and attacks which occurred in the field of EO [27]. However, the cyber-physical systems which are supported by AI enable the development of transformative approaches to ensure effectiveness and optimality in such a way that achieve the desired outcomes [28].

On the other hand, in the context of space-based EO-assets, the most urgent need is to progressively develop sustained and trustworthy data handling including other core-technical capabilities, such as data-fetching, data-recognition, data-streamwise, and data-delivery in the form of image and/or non-image types. It leads to implicitly unlocking the long-term intersection research activities between EO-assets and space-security. Thus, there is the need to set up and maintain reliable statistical information for detailed multi-temporal and multi-spatial data provision to uphold continuous surveillance and mapping transformations.

As an example, the development of high-fidelity decision support tools referred to as digital twins (DT), allows to counteract the advanced persistent malicious threats and lethal attacks during incessant reconnaissance missions. Other use cases of digital twins are vulnerability detection through visual adversarial analytics, advanced real-time intrusion monitoring, and resilience assessment on active cyber physical threat intelligence systems.

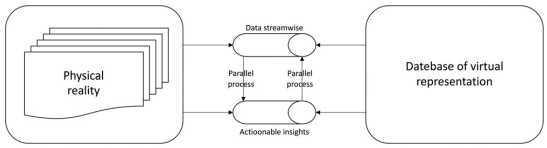


Fig. 1. Essential building blocks of Digital Twin.

5. Technical countermeasures

There are different ways to enhance AI countermeasure in the space domain including but not limited to Network Intrusion Detection System (IDS) and DT.

IDS has the capability to define a trend of the average network behaviour. The trend would be the baseline of the network activities which would allow to identity possible malicious events in the network. The enhance of IDS with AI would futter allow to have a quick and targeted response in the occurrence of an event [29].

Another possible countermeasure to optimise AI in space applications can be the application of DT in combination with AI. A DT is a high-fidelity digital model of a physical system or asset that can be used to optimise operations and predict faults of the physical system. For space applications, DT can be potentially used for cybersecurity incident predictions. The integration of digital twin technology and AI has significant effects in aeronautics such as for flight detection simulation, failure warning, aircraft assembly, and even unmanned flight. Therefore, the use of this technology for space is a good starting point to list technical benefits associated with cyber physical systems.

The notion of DT was firstly proposed by Michael Grieves and conceptualised as a subsidiary part of the strategic diagnostic and prognostic toolset in the context of product life-cycle management [30]. It is basically understood as the essential engineering advancement in the production and operation of technology, while it also offers digital representation of a real-world or physical object to the reformation of a virtual replica, including its process throughout its lifecycle and the required real-time and historical data [31]. The virtual replica can be used for further analysis which can deliver actionable insights in the form of the desired key-performance measurements. This allows to enhance both tangible and intangible products in terms of eight vital values: real-time remote monitoring-control; predictive maintenance-scheduling; scenario-risk assessment; synergy of abnormalities detection; informed decision support system; personalization of products and services; efficiency and safety; and documentation and communication [32]. Aside from these, the necessary key-terms from various thrived definitions of DT being constantly proposed and formally used can be simply characterised according to three elementary components: the physical reality, a virtual replica, and the bi-directional data flow. The latter occurs in the form of information exchange using cutting-edge cognitive systems [33] between the physical reality and the virtual replica, which comprises data streamwise and actionable insights (Fig. 1).

5.1. Architecture of a network digital EO twin

The cutting-edge network DT architecture proposed by one of the co-authors [34,35] is summarized in this paragraph. The DT architecture is compared with the technical white paper developed by a team of industrial practitioners from scalable Network Technologies enterprises [36]. The analysis includes the additional technical explanation on how to carry out the comprehensive idea

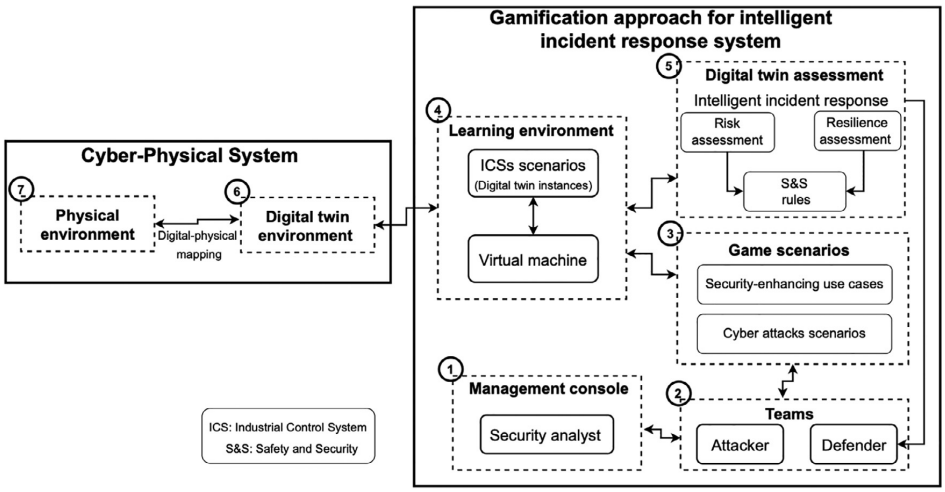


Fig. 2. Network Digital Twin in the context of Intelligent Incident Cyber-Physical Response System [34,p.7].

of network DT in modelling, simulating, monitoring, and assessing the existing EO-assets threats taxonomy.

By definition, network DT is the digital simulation-based model of the communication network integrated with its operating environment and the application of the traffic carried by it. To satisfy its intended goals, the network DT must have sufficient fidelity to accurately reflect and propagate the network dynamics due to the tangible interaction amongst the communication protocols, topology, traffic, and physical environment. A network DT can be further upgraded by incorporating cyber vulnerabilities and defences. The cyber-enhanced network DT can be used to verify and validate the cyber resilience of the simulated system in an adversarial environment, while analysing its behaviour and resilience under various collections of spiteful intrusion and interference scenarios [36]. The visualisation of network DT architecture developed by industrial practitioners and academic researchers is provided in Figs. 2-3.

5.2. Building blocks of a network digital-EO twin

A breakthrough approach in formalising the main building blocks of network digital-EO twin for handling the RF intrusion and interference is discussed hereby. The approach derives from existing technical suggestions for remote-sensing EO activities conducted by authorised space-based research and development institutions, space military and defence enterprises.

The main idea behind the development of network digital-EO twins is the collaboration between three essential pillars, which are Experientable Virtual Twin (EVT), reliable adversarial ML models, and advanced AI solver using Graph Neural Networks (GNN), as shown in Fig. 4. GNN is strongly chosen as a neural network solver for developing a highly resilient, secure, and lightweight architecture model of data-driven networks, including the capability of detecting particular anomalies. These pillars can be identified as the essential building blocks for EVT for AI space systems in order to align with the latest scientific research and breakthrough cybersecurity solutions.

EVT basically combines the underlying notion amongst MBSE (Model Based Systems Engineering), simulation-based technology, and DT itself. Besides, it is created to comply with high-fidelity simulation-based systems engineering processes for a variety of different applications, from the development of verification, training, optimization, testing, validation, up to the realisation of intelligent systems [37].

6. Legal and policy aspects of the proposed taxonomy

Not only satellites but also satellite data have to be a priority subject of international dialogues on cyberlaw and international security. AI development and use in the space sector bears a regulatory vacuum, except for some national provisions for technology. Cyber security and safety dimensions of AI have not been regulated at all.

The expanding variety of space stakeholders and those able to use emerging technologies effectively in their system designs will create unique challenges for each actor, system and uses, that may not be applicable in other areas. Therefore tailored regulations for cybersecurity and AI in space will be required in order to regulate both technology and the use of emerging technologies for cross-domain challenges, while watching implementation for compliance to the constituent values, to make the policy and law regulations germane to domain (space-cyber) and technology related cyber challenges [38].

6.1. Design of AI cyber policy for/in space

The use of AI technology in space without adequate verification and acceptance tests in the engineering phase could create a high level of risk. While imperatives for policymakers and legal designers are different, technical, policy and legal aspects of cyber resilience and cyber protection of space assets imply cooperation and open visions. Recognizing the problem, identifying vulnerable systems, and taking steps to mitigate risks before undesired consequences, for the present uses of emerging technologies, not excluding the possible and future uses for space activities, is a common focus for policymakers, engineers and legal professionals.

For space, cyber security policy 'defines and documents any organisations' statement of intent, principles and approaches to ensure effective management of cybersecurity risks in pursuit of its strategic objectives', it is proactive, not reactive, and has to answer to rapid technological changes and challenges. While law, on the other hand, has a more reactive approach and it clearly defines actions, regulates, and protects against violations of core values. In

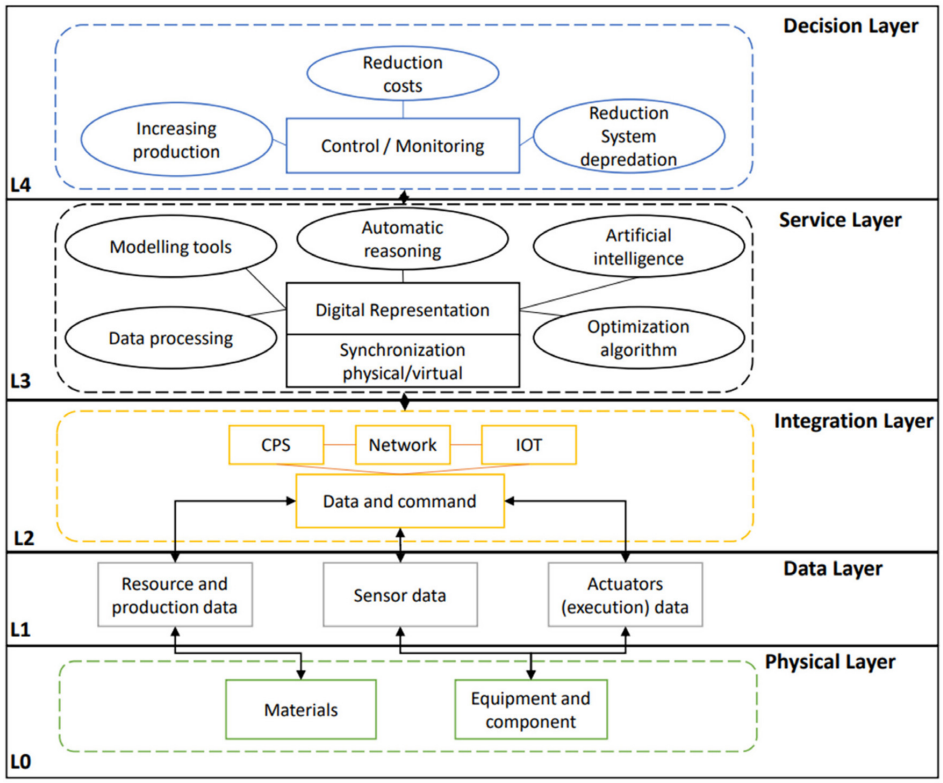


Fig. 3. Network Digital Twin in Hierarchical Layer-by-Layer mode from the bottom level L0 to the top level L4 [35, p.7].

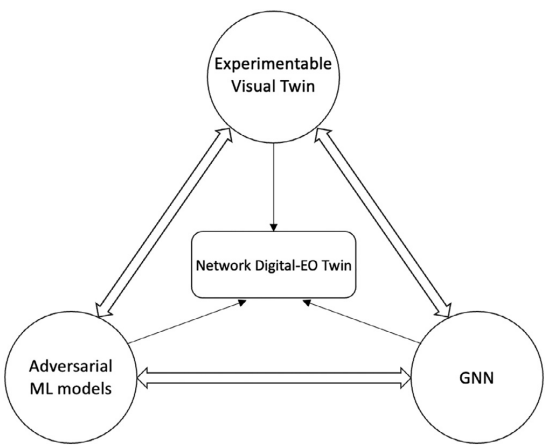


Fig. 4. The Primary Building Blocks of Network Digital-EO Twin.

terms of cybersecurity and AI, policymakers have to consider many parameters such as the security impacts of AI technology.

From the cybersecurity aspect, AI can have an impact on the national and international landscape in multiple forms, in physical and non-physical environments. It will increasingly be used as a tool to help carry out cyberattacks or to defend against cyberattacks by nations and private space actors for future missions. While generating new modes of informational warfare, its use will expand the threat landscape, and might contribute to the destabilisation and generation of new forms of weaponization for conventional and non-conventional actors. With the growth of AI, the intrusion caused by obtaining and retaining the data is not a fixed impact but will vary according to the quality of data and what the scope of cyber intrusion will be, as analytic processes change and develop, and the legal and policy frameworks will have to catch up with them [39].

Embedded artificial intelligence in space systems, services, processes, and decision-making, is shifting attention on how the data are and will be used by the software, particularly by complex, evolving algorithms, and the consequences of their uses. Security focused policies for AI underline the importance of transparency, testing, and accountability for algorithms and their development. However, operationalizing these policies in practice requires the establishment of legal responsibility for the occurrence of harmful consequences as a result of the use of artificial intelligence.

AI cyber security space policy, therefore, has to find a perfect balance between innovation and resiliency for all four segments (ground-link-user-space) [23], as well as space actors, including space vendors, contractors, and governments. Space cyber security is on the agenda of US and European actors [40] to set the framework for the urgency of having guidelines taking into consideration the particularities of space and technology challenges, and bring different actors together on a common set of principles.

In terms of policy and regulation, the main focus for agencies and governments will be to reduce the risk of attacks on AI systems, and to mitigate the impact of successful attacks. Therefore;

(a) The first consideration, before creating an AI cybersecurity policy and regulation, is the classification of AI systems on a risk basis and on the intended purposes, in line with existing product safety legislations.
(b) The classification of AI depends not only on the function performed, but also on the specific purpose and modalities for which that system is used. Agencies and actors, therefore, need to understand firstly the system particularities. While reinforcing specific controls depending on the nature of the risk in technical terms, in legal terms AI must be regulated by "sets of harmonised rules for the development and use" of AI systems.
(c) The third phase will be creating regulations, sanctioning also cyber attempts and their consequences.

The development of an effective space cybersecurity policy will require designing cyber resilient systems and therefore adopting cybersecurity as a priority (in line with existing technical standards and regulations), not as an afterthought. Therefore this implies: (a) defining security elements before defending ground-based systems, networks and space assets, and first minimising risks and vulnerabilities; (b) following the adoption of cybersecurity best practices for both technologies used and their components (e.g., Cognitive Computing, ML, DL, Neural Networks, Natural Language Processing). Bearing in mind the critics directed at Space Policy Directive-5 [41], setting security frameworks would require designing actual risk management frameworks, on the basis of collaboration between governments, private initiatives and operators. Designing security frameworks in official documents can only be effective with (a) standardisation, (b) modernisation, (c) transformational initiatives, and (d) verifications through experience and understanding which tools/designs/policies are effective and which are not. In these terms, exercises and game-playing like wargames and hack-a-sats can help to open and develop dialogues, to set common grounds and principles, and clearly see 'how to's' in order to build a living, adaptable, up-to-date, and reactive policy capable of resilience and rapid evolution against threats.

6.2. Liability in terms of AI cybersecurity for/in outer space

Cyber attacks and other new technologies such as AI or blockchain were unknown during the adoption of the Liability Convention [42] and how the Convention will be able to cope with new challenges posed by harmful 'activities/interferences' committed by using these new technologies were as well unknown during the era of its adoption.

The presence of cybersecurity vulnerabilities in new and emerging technologies poses great risks. While providing consistency and time advantage to assess data, AI bears varying risks, and one of the important ones is "Unclear Legal Responsibility" for many aspects originated from the technology. Firstly, the Tallinn Manual, in Rule.11. reasons that only cyber attacks of sufficient "severity," "invasiveness," and "military character" amount to uses of force [43]. In terms of the Liability Convention, the 'injurer' and 'target' are the space objects. The first consideration as to the applicability of the Liability Convention for the cases of cyberattacks against software or software-defined space assets is based on "whether the software is covered by the term 'space object", and the answer is positive [44].

Another reason for uncertainty is the difficulty to foresee the final results of the implementation of AI and lack of precedents as to problems that will arise from the use of AI, and cases that are specific to incidents involving AI cyber security [17]. As to the liability under international space law, the use of AI and rise of cyber security and safety issues are significant concerns and challenges regarding the interpretation of Art. III of the Liability Convention, for the determination of 'fault' and the establishment of causal link between the fault and the damage.

In terms of cyber-attacks, compared to other types of interference targeting space assets, low-intensity cyber-attacks are mainly physically non-destructive, with latent intervention, and have a low threshold to access [45]. However, both Art.30 of the Tallinn Manual [46] and Art.1 of the Liability Convention [47] require 'damage' to 'life, health, and property', and neither of these documents foresee mechanisms to impose liability for low-intensity cyber attacks, which can be considered as a legal vacuum for ongoing low-intensity cyber threats against space objects including software.

In terms of liability, a famous Roman law maxim, "sic utere tuo ut alienum non laedas", which states that "each must use his property in a way that does not cause injury to another's", can be a hint to understand and discuss possibilities for the realm in outer space and cyber security of space technologies. In order to strengthen international peace and security in space, within an unstable cyber environment, and minimise threats, application of cyber due diligence can be considered as one of the options.

A state is responsible for failing to take action, either generally or with respect to the conduct of individuals, according to due diligence care as the particular obligation requires [48]. States are obliged under international law to exercise due diligence in preventing their territories from being used to perpetrate harmful conducts that will interfere with the rights of other states. The principle of due diligence would require states to set standards and norms to govern and protect their cyber infrastructure, cyber activity, and people engaged in cyber activities. However due to the lack of established international law on AI, space and cyber, as well as the different features between cybersecurity and space security, and the uses of technology, victims are left to navigating unknowns, since the wrongdoer is often unknown, the types of wrongful acts are intentional human/State actions, the damage is to personal data theft and systems, and attribution coms with the difficulty of identifying those responsible.

As underlined in many occasions, the UN Group of Governmental Experts (GGE) indicated the importance of procedural obligations to prevent harm and encourages states to cooperate "to mitigate malicious ICT activity emanating from their territory" [49]. Uses of emerging technologies like AI require attention.

In conclusion, the future regulation of liability generated by cyber attacks/interferences against space technologies has to find and design a balance. Whether through national or international norms, addressing the attribution-response gap will be difficult. Therefore, in order to regulate the legal regime as to the use and the consequences of these uses for EDTs, States and industries have to understand and redefine the following:

(a) "'Harm' considering the technology used and the environment in which the technology is used;
(b) The likelihood and the degree of the technology used that contributed to the harm;
(c) The risk/ known vulnerabilities within the technology and environment the technology used;
(d) The Informational asymmetry, the degree of ex-post traceability and intelligibility of processes within the technology that may have contributed to the cause;
(e) The degree of ex-post accessibility and comprehensibility of data collected and generated by the technology;
(f) The kind and degree of harm potentially and actually caused [50].

Even if the harm is caused/originated by a cyber-attack, the liability is conditional upon the intent of the perpetrator or negligence of the operator. In order to counter general expectations of reasonable care and regard for harms to sovereignty between

States, due diligence can serve in the absence of a legal regime. However, the legal vacuum for non-state actors, commericial space activities, as well as low-intensity cyber interference, remains.

A state can be liable for an act of transboundary harm, even if the activities giving rise to the harm were not themselves breaches of international law. The Liability Convention rather envisages the damages caused by impact, than damage inflicted through activity. Malicious transboundary cyber conduct committed by non-state actors can exceed the conduct committed by states. Since the international legal regime is based upon the sovereignty equality of its member states, international law demands the existence of effective international legal rules that provide states with protection from non-state actors that commit malicious cyber conduct from the territory of other states.

7. Conclusions

The world is transitioning into a new era. The importance of space as a military and strategic domain as well as an economic domain requires policy making and legal regulation of responsibilities for governments and growing private space actors, as well as outsider adversaries using emerging technologies in space and against space assets.

AI technologies are expected to be used more extensively in future space missions, and augmented use of these new technologies and cybersecurity concerns as to the latter, brings more topics to discuss to the security of future space missions and to the applicability of existing norms for new technology driven challenges. However, cyber-attacks on space assets are different from the cyber-attacks targeting other kinds of critical infrastructure. This is because numerous States and now private actors are engaged in space activities, and considering the augmentation of services provided from space, the regulation of the new relationships requires new discussions, beyond existing frameworks provided by international space law.

AI is enabling progress and innovation in the space sector and helps to provide robust solutions to the most relevant problems. Therefore, creating processes and frameworks to use AI technologies requires taking into consideration particularities of the technology, in the first place, in order to ensure clarity in normative and policy grounds, and to respond to cyber security requirements timely. Neither existing space policy nor cybersecurity policy is prepared for the challenges created by the meshing of space, cyberspace and emerging technologies, especially designed for space assets and use of emerging technologies in space activities. In order to ensure adaptable/compatible use of emerging technologies with other technologies in complex environments, the adoption of responsive universal principles and regulatory frameworks becomes an important agenda for authorities, governments and industry. In the absence of dialogue and formal policy and regulations, it will become difficult to use emerging technologies, minimise and mitigate risks, develop and use technologies for future missions within a security framework and to build robust defences against emerging technological threats.

Therefore, it is essential to note that there are important, technological challenges such as the use of AI-enabled DT technologies with full performance. These challenges might depend on the scale and integration complexity of the applications, besides the uses for space missions. The main challenges to consider are issues related to data, including trust, privacy, cybersecurity, convergence and governance, acquisition and large-scale analysis. While DT promises many advantages, this technology is under development and far from maturity in the near future. The existing limitations for more mature and complex implementations of DTs across all domains, including both space and cyber, will also require overcoming communication network related obstacles on the technical aspect, which also creates another difficulty for the widespread adoption of this technology and makes accessibility difficult. Trust in technology is another challenge, since the information flowing from various levels of indicator systems presents a challenge for developing common policies and standards. Therefore, lack of standards, frameworks and regulations for DT implementations is one of the main challenges and has many aspects to consider. For complex implementations of this technology in specific environments, regulations will become more difficult in the future, considering the access related problems to sensitive data by private and military actors, and the adoption of uniform methodologies for data security and authenticity.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Antonio Carlo: Supervision, Project administration, Conceptualization, Writing – original draft, Writing – review & editing. **Nebile Pelin Mantı:** Writing – original draft, Conceptualization. **Bintang Alam Semesta W.A.M:** Writing – original draft. **Francesca Casamassima:** Writing – original draft. **Nicolò Boschetti:** Writing – original draft. **Paola Breda:** Writing – original draft, Writing – review & editing. **Tobias Rahloff:** Writing – original draft.

References

[1] SERRANO, I., How artificial intelligence is advancing space efforts, 10 August 2021. Available at: https://www.geospatialworld.net/blogs/how-artificial-intelligence-is-advancing-space-efforts/#:~:text=Scientists%20use%20AI%20to%20control,communication%20between%20Earth%20and%20space, (*Accessed on 06.07.22*).

[2] Group on Earth Observation, What is earth observation?. Available at: https://www.earthobservations.org/g_faq.html, (*Accessed on 06.07.22*).

[3] European Space Agency, Role of EO in understanding climate change. Available at: https://climate.esa.int/en/evidence/role-eo-understanding-climate-change/, (*Accessed on 05.07.22*).

[4] C.M. GEVAERT, Explainable AI for earth observation: a review including societal and regulatory perspectives, Int. J. Appl. Earth Obs. Geoinf. 112 (2022) 1–11.

[5] EO Portal, PhiSat-1, https://directory.eoportal.org/web/eoportal/satellite-missions/p/phisat-1, (*Accessed on 04.07.22*).

[6] John McCarthy, father of AI, intelligent systems, IEEE Xplore 17 (5) (2002) 84–85.

[7] L.I.A.O. Matthew, in: Ethics of Artificial Intelligence, Oxford University Press, Oxford, 2020, p. 3.

[8] Artificial intelligencePlato Stanford Encyclopedia of Philosophy, 2018 July 12Available at https://plato.stanford.edu/entries/artificial-intelligence/ .

[9] CARLO, Antonio, Artificial intelligence in the defence sector, MESAS20, Prague, Czech Republic, 2021, pp. 269–278. doi:10.1007/978-3-030-70740-8_17.

[10] RADANLIEV Petar, DE ROURE David, "New and emerging forms of data and technologies: literature and bibliometric review". Available at: https://link.springer.com/article/10.1007/s11042-022-13451-5#Abs1.

[11] P. RADANLIEV, D. DE ROURE, C. MAPLE, O. SANTOS, Forecasts on future evolution of artificial intelligence and intelligent systems, IEEE Access 10 (2022) 45280–45288 https://ieeexplore.ieee.org/document/9761872?source=authoralert.

[12] E.R.T.E.L. Wolfgang, in: Introduction to Artificial Intelligence, Springer, Cham, 2017, p. 2.

[13] GAYNOR Michael, *Automation and AI sound similar, but may have vastly different impacts on the future of work*, Washington: Brookings, 29 January 2020. (*Accessed on 04.07.22*). Available at: https://www.brookings.edu/blog/the-avenue/2020/01/29/automation-and-artificial-intelligence-sound-similar-but-may-have-vastly-different-impacts-on-the-future-of-work/.

[14] BOOZ, ALLEN, HAMILTON, "The role of artificial intelligence in cybersecurity". Available at: https://www.boozallen.com/s/insight/publicat,on/role-of-artificial-intelligence-in-cybersecurity.html.

[15] M.A.C. WILLIAMS, Carmen, Earth observation big data challenges: the AI change of paradigm, European AI Platform, EU AI Alliance, Futurium, European Commission, 2020 January 29. https://ec.europa.eu/futurium/en/european-ai-alliance/earth-observation-big-data-challenges-ai-change-paradigm.html.

[16] Gregory FALCO, Eric ROSSENBACH, Confronting cyber risk: an embedded endurance strategy for cybersecurity, OUP (2022) 5.
[17] Kate JONES, Marjorie BUCHSER, Jon WALLACE, Challenges of AI, Chatham House, 2022 March 22. https://www.chathamhouse.org/2022/03/challenges-ai.
[18] P. DU, X. BAI, K. TAN, et al., Advances of four machine learning methods for spatial data handling: a review, J. Geovis. Spat. Anal. 4 (2020) 13. Available at https://link.springer.com/article/10.1007/s41651-020-00048-5#citeas.
[19] Lorenzo PUPILLO, Stefano FANTIN, Afonso FERREIRA, Carolina POLITO, Artificial intelligence and cybersecurity: technology, governance and policy challenges, in: Report of a CEPS Task Force, 2021, p. 36. May 28.
[20] Roman YAMPOLSKIY, AI is the future of cybersecurity, for better and for worse, Harv. Bus. Rev. (2017) May 8. https://hbr.org/2017/05/ai-is-the-future-of-cybersecurity-for-better-and-for-worse.
[21] Matt SWAYNE, Researchers detail privacy-related legal, ethical challenges with satellite data, Pennsylvania State University, Phys.org. (2019) July 12Available at https://phys.org/news/2019-07-privacy-related-legal-ethical-satellite.html?deviceType=mobile .
[22] Ashley Hyowon Kim ASHLEY, The Impact of Platform Vulnerabilities in AI Systems, Massachusetts Institute of Technology, 2020 *Ph.D*. Dissertation. https://dspace.mit.edu/handle/1721.1/129159.
[23] A. CARLO, L. LACROIX, L. ZARKAN, The Challenge of protecting space-based assets against cyber threats, IAC-20,E9,2.D5.4,11,x59386, 71st International Astronautical Congress, 2020.
[24] M. MANULIS, C. BRIDGES, R. HARRISON, V. SEKAR, A. DAVIS, Cyber security in new space: analysis of threats, key enabling technologies and challenges, Int. J. Inf. Secur. 20 (2021).
[25] Gregory FALCO, Cybersecurity principles for space systems, J. Aerospace Inf. Syst. 16 (2) (2019) 61–70.
[26] TORRES Martínez, COMESAñA, J. IGLESIA, C. GARCIA-NIETO, P.J. Review: machine learning techniques applied to cybersecurity, Int. J. Mach. Learn. & Cyber 10 (2019) 2823–2836, doi:10.1007/s13042-018-00906-.
[27] A. SALIH, S.T. ZEEBAREE, S. AMEEN, A. ALKHYYAT, H.M. SHUKUR, A survey on the role of artificial intelligence, machine learning and deep learning for cybersecurity attack detection, in: 2021 7th International Engineering Conference "Research & Innovation amid Global Pandemic" (IEC), 2021, pp. 61–66.
[28] How AI can ensure better cyber security?, Innefu Labs. Available at: https://www.innefu.com/blog/how-ai-can-ensure-better-cyber-security (*Accessed on 10.07.22*).
[29] P. RADANLIEV, D. DE ROURE, C. MAPLE, et al., Super-forecasting the 'technological singularity' risks from artificial intelligence, Evolv. Syst. 13 (2022) 747–757, doi:10.1007/s12530-022-09431-7.
[30] Matt TREMBLAY, The digital twin: the benefits of taking an incremental journey, Marit. Execut. (2020) November 3Available at https://www.maritime-executive.com/editorials/the-digital-twin-the-benefits-of-taking-an-incremental-journey . (*Accessed on 27.07.22*).
[31] Confronting cyber risk: an embedded endurance strategy for cybersecurity (textbook).
[32] Digital twins for IoT applications: a comprehensive approach to implementing IoT digital twins, Sep 2019, Available at: http://www.oracle.com/us/solutions/internetofthings/digital-twins-for-iot-apps-wp-3491953.pdf.
[33] Scott APPLEGATE, A. Stavrou, Towards a cyber conflict taxonomy, International Conference on Cyber Conflict, 2013.
[34] SUHAIL, Sabah, ZEADALLY, Sherali, JURDAK, Raja, HUSSAIN, Rasheed, MATULEVIČIUS, Raimundas, SVETINOVIC, Davor, Security attacks and solutions for digital twins, 2022.
[35] R. da SILVA MENDONÇA, S. de OLIVEIRA LINS, I.V. de BESSA, F.A. de CARVALHO AYRES Jr., R.L.P. de MEDEIROS, V.F. de Lucena Jr., Digital twin applications: a survey of recent advances and challenge, Processes 10 (4) (2022) 744, doi:10.3390/pr10040744.
[36] Automated creation of network digital twins handbook, scalable network technologies, © 2021 SCALABLE network technologies, Inc. All Rights Reserved PN MRL141217 QualNet and EXata are registered trademarks of SCALABLE Network Technologies, Inc.
[37] M. SCHLUSE, M. PRIGGEMEYER, L. ATORF, J. ROSSMANN, Experimentable digital twins–streaming simulation-based systems engineering for Industry 4.0, IEEE Trans. Ind. Informat 14 (2018) 1722–1731 April.
[38] R. HARRISON, D. VERA, B. AHMAD, A connective framework to support the lifecycle of cyber–physical production systems, in: Proc. IEEE, 109, 2021, pp. 568–581.
[39] Paulius ČERKA, Jurgita GRIGIENĖ, Gintarė SIRBIKYTĖ, Liability for damages caused by artificial intelligence, Comput. Law Secur. Rev. 31 (3) (2015) (pp.376-389), pp.383-384.
[40] A. CARLO, Cyber threats to space communications: space and cyberspace policies, in: A. Froehlich (Ed.), Outer Space and Cyber Space. Studies in Space Policy, Springer, Cham, 2021 33.
[41] Executive office of the president "space policy directive-5: cybersecurity principles for space systems" (2020) 09 September. Available at https://www.federalregister.gov/documents/2020/09/10/2020-20150/cybersecurity-principles-for-space-systems.
[42] Convention on international liability for damage caused by space objects entered into force Oct. 9, 1973, 24U.S.T. 2389, 961U.N.T.S. 187.
[43] Rule 11, Tallinn Manual specifically notes that [a] cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.
[44] Anna HUROVA, Liability for a cyber attacks on a space objects, Czech Yearbook Int. Law XXI (2021) 57 pp.57-24.
[45] Tallinn manual 2.0 on the international law applicable to cyber operations, Michael N. Schmitt (Ed.), 2nd Ed. 2017. http://csef.ru/media/articles/3990/3990.pdf.
[46] Tallinn Manual 2.0, Art. 30. qualifies a cyber attack as cyber operation, 'whether offensive or defensive', If it is reasonably expected to cause 'injury or death to a person, damage or destruction to objects.
[47] Art.1 of the Liability Convention defines the term 'damage' as 'loss of life, personal injury or other impairment of health or loss of or damage to property' of States or persons, natural or juridical, or property of international intergovernmental organisations.
[48] Under the doctrine of state responsibility, states are responsible for "wrongful" acts that are attributable to the state and breaches of an international obligation. Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, Art. 2, Rep. of the Int'l Law Comm'n on the Work of Its Fifty-Third Session, U.N. Doc. A/56/io, at 68 (2001) [hereinafter Draft Articles on State Responsibility].
[49] UN, General Assembly, A/70/174, Developments in the field of information and telecommunications in the context of international security Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Section 17(e), https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf (*Accessed on August 20, 2022*).
[50] Bernhard A. KOCH, Liability for emerging digital technologies: an overview, J. Eur. Tort Law 11 (2) (2020) 115–136, doi:10.1515/jetl-2020-0137.

Appendix 3

III

S. Bonnart, A. Capurso, A. Carlo, T. F. Dethlefsen, M. Kerolle, J. Lim, A. Pickard, A. Russo, and L. C. Zarkan. Cybersecurity Threats to Space: From Conception to the Aftermaths. In Space Law in a Networked World. *Brill | Nijhoff*, P.J. Blount, M. Hofmann (eds), 19(1):39–101, 2023

CHAPTER 3

Cybersecurity Threats to Space: From Conception to the Aftermaths

Sébastien Bonnart, Andrea Capurso, Antonio Carlo, Thea Flem Dethlefsen, Mclee Kerolle, Jonathan Lim, Aaron Pickard, Antonia Russo, and Laetitia Cesari Zarkan

1 Introduction*

Invisible to the human eye, up beyond the atmosphere, a cloak made of satellites, signals, and data fluxes mantles our planet. It is intertwined with the surface of the Earth through antennas, receivers, and other ground segments that elaborate and distribute the services provided from outer space. Understanding how hostile cyber operations are put in place and what consequences they produce is a crucial need for all involved in space activities. In today's interconnected context, underestimating the risks that come from the cyber domain may expose space infrastructures and the services depending on them resulting in irreparable damages.

For this reason, this chapter aims to provide a general overview of hostile cyber operations and their effects on space activities, from the start to the aftermath. Section 2 addresses the attack surface for hostile operations through a survey of hardware, software, space and ground segments, and the radio frequency spectrum. It identifies where space assets are vulnerable and sets the ground for the second section, which outlines the different strategies for protecting those vulnerabilities. Section 3 starts with the IT governance strategies a company or organization can implement. Improving IT governance mechanisms concerning space-related technologies is vital to encourage positive cyber behaviors, improve top-level decision making, reduce the possibility and effect of catastrophic incidents, and enable better strategic planning vis-a-vis cybersecurity matters. Section 3.2 presents an overview of the technical strategies to be adopted in space systems to mitigate risks related to cyberattacks. Section 4 exemplifies the consequences of previous hostile cyber operations

* The opinions expressed are those of the author and do not reflect the official opinion of the European Commission.

 | DOI:10.1163/9789004527270_004

against space assets. It addresses the impact and effects of hostile cyber operations, including the long-term or short-term consequences of the different nature and purposes of the targeted system and the kind of attack perpetrated against the system/satellite. Consequences range from unauthorized access to classified information and the outage of critical infrastructure. Section 4.2 addresses the subsequent reconstructing and incident response at both an organizational and international level. Section 5 and 6 deal with the legal implications of hostile cyber operations. Section 5 addresses the challenges of applying public international law, as Section 5.1 examines the political ambiguity over how the existing legal regime is applied, Section 5.2 looks at the technical challenges of attribution, and finally Section 5.3 looks at the legal boundaries that exist for target precision for a hostile cyber operation when it comes to collateral victims. Section 6 examines the private international aspects of a hostile cyber operation, including incidents where the perpetrators and victims are non-state actors. Section 6.1, therefore, addresses the contractual provisions that may cover a cyber operation, Section 6.2 the private arbitration and Section 6.3 the courts that can settle possible disputes relating to a breach can be solved. Section 6.4 explores how private actors can protect themselves through insurance. Finally, Section 7 provides a conclusion.

2 Overview of Cyber Geography

The first section of this chapter presents the cyber-geography of space missions. Section 2.1 starts by defining the mission components and maps the attack surface,[1] from ground segment, space segment to the orbits. Section 2.2 outlines how these systems communicate through for example satellite telecommunication and the architecture of the networks that transmit data. The purpose of this section is to provide an overview of the structure of space systems and how the different segments are interconnected which will be used to understand the weaknesses of the systems that will be explored further in Section 3.

1 "Attack surface" is defined as "[t]he set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from." Ron Ross et al, *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, NIST Special Publication 800–160, v. 2 (2019) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf.

2.1 *Space Mission Anatomy*

2.1.1 Ground Segment

The ground segment is the part of a space system located on earth. It is usually the largest part of the system in terms of mass, volume, and power consumption. The main components of a traditional ground segment are the user segment, the ground station, spacecraft control and payload control.[2] The user interface or user segment can have multiple forms depending on the mission. It allows users to benefit from the space service directly through the spacecraft or through the payload control. This can, for instance, take the form of a GPS guidance system, a satellite phone, or TV antenna.

The ground station is the ground segment subsystem used to communicate with the spacecraft. It features an antenna, a transmitter, a receiver, amplifiers, and a steering mechanism, all coordinated by an antenna control system.

The spacecraft control subsystem, also referred to as the mission operations center, is interfaced with the space segment through ground stations, and maintains the spacecraft bus in operational conditions.[3] The spacecraft control subsystem monitors on the ground telemetry received from the sensors aboard the spacecraft. The spacecraft control subsystem also issues necessary commands such as collision avoidance maneuvers, sends configuration/software updates. and enables the payload aboard the space segment to operate.

The mission is accomplished by the space segment's payload, which is commanded from the ground by the payload control center. Similar to the spacecraft control subsystem, the payload control is connected with the spacecraft through antennas and controls the instruments in order to ensure completion of the mission and satisfaction of the users. The nature of the payload's operation depends on the mission.

A ground segment may be composed of more than one instance of each of these components,[4] either to provide redundancy or due to the mission's characteristics. For instance, an earth observation mission may have a spacecraft control center co-located with a payload control center, as well as multiple antennas to control the spacecraft and payload. Moreover, there can be a distinct set of antennas for direct payload data reception at the end user's

---

2 Consultative Committee for Space Data Systems, *Mission Planning and Scheduling*, Report CCSDS 529.0-G-1 (2018) https://public.ccsds.org/Pubs/529x0g1.pdf.

3 Gail A. Johnson-Roth, Geraldine A. Chaudhri, & William F. Tosney, *Ground Segment Systems Engineering Handbook*, Technical Operating Report TOR-2016–01797 (The Aerospace Corporation 2016) https://apps.dtic.mil/dtic/tr/fulltext/u2/1067478.pdf.

4 Consultative Committee for Space Data Systems, *Security Architecture for Space Data Systems*, *Recommended Practice* CCSDS 351.0-M-1 (2012) https://public.ccsds.org/Pubs/351x0m1.pdf.

facilities. A web interface may allow customers to order images via the payload control center through the Internet.

2.1.2 Space Segment

The space segment is composed of the spacecraft and its subsystems. The largest part of the space segment is the "bus." The bus includes the vehicle's structure, power generation, communications, attitude determination and control, avionics, and other mission-specific systems.[5] The payload is entirely mission dependent, providing the fulfillment of the mission's purpose using the resources provided by the bus. It is common to have a dedicated communication system as part of the payload. The space segment from a mission can range from being a single sub-system hosted by the International Space Station (ISS) to a large constellation of inter-connected satellites.

2.1.3 Orbits

The majority of space systems are orbiting the earth. The four main categories of orbits are: low earth orbit (LEO), medium earth orbit (MEO), geosynchronous equatorial orbit (GEO), and highly elliptical orbit. For the purpose of this chapter, this section will offer a brief overview on the commonly used orbits of low earth orbit and geosynchronous equatorial orbit. LEO characterizes spacecraft orbiting at altitudes between 100 km and 2000 km. These spacecrafts complete a full revolution in about 90 minutes. Key uses of LEO are new communications constellations, earth observation satellites with both scientific and military purposes, modern crewed spaceflight, as well as parking orbits used by spacecraft heading to more specialized orbits. Orbital parameters affect the visibility of the satellite from any particular point on Earth, and therefore the accessibility of ground users to the spacecraft. Not all spacecraft in LEO are visible from everywhere on Earth during an orbit. If the latitude of a point is extreme enough and the orbital inclination of an object is low enough, the object may never be visible from a particular point. As an example, a satellite in a circular orbit with an altitude of 820 km never offers visibility windows longer than 15.5 minutes at a time.[6] If visible, it will appear to move across the sky. A fixed omnidirectional antenna or a directional antenna with azimuth and elevation control may communicate with it.

---

5 NASA, *State-Of-The-Art Small Spacecraft Technology* (2020) https://www.nasa.gov/smallsat-institute/sst-soa-2020.

6 Shkelzen Cakaj et al., "Communications Durations with Low Orbiting Satellites," 4th IASTED International Conference on Antennas, Radar, and Wave Propagation (2007) https://publik.tuwien.ac.at/files/pub-et_12772.pdf.

GEO, also called geostationary orbit, describes the orbits of some spacecraft at an altitude of about 36000 km in a circular orbit over the Earth's equator. At this altitude, the revolution time for the satellite around the Earth is exactly the same as the one rotation of Earth. This orbit is heavily used by broadcast and telecommunication services. An object in GEO is either always visible or always invisible from any particular point on Earth. Satellites in GEO appear with a fixed position in the sky for an observer on Earth, and ground stations can use directional antennas that do not move to communicate with them.

Spacecraft may also orbit or land on other celestial bodies. Such operations, as well as any others where the vehicle is more than 2 million kilometers from Earth, are considered by the International Telecommunication Union to be in "deep space," as opposed to "near Earth space."[7] This has technical implications for the spacecraft's design, as well as how it transmits data back to Earth. An object in deep space's visibility from the Earth varies, based on what celestial body it is orbiting or landed on, and where that body is relative to the Earth – typically in the reference frame of the Sun. Now that the space mission components have been identified, this section continues by addressing the interconnections and attack surface they offer.

2.2 *Data, Links and Networks*

Having presented the main components of space missions, the next step is to demonstrate how they communicate together. Space missions use two main data fluxes. One is telemetry and control (TM/TC), which goes both ways between the satellite and the control center. The other is payload data that, depending on the mission, can be from space to ground (for instance, earth observation or navigation data), or both ways (such as telecommunications data).[8]

Telemetry contains the data allowing mission control to assess the health state of the spacecraft. After immediate analysis, data is archived in the mission control center for long term study of the satellite behavior. Telecommands are orders from the mission control center to the satellite.[9] These can be parameter

7 Marc Siebert et al., "Developing Future Deep-Space Telecommunication Architectures: A Historical Look at the Benefits of Analog Research on the Development of Solar System Internetworking for Future Human Spaceflight," *Astrobiology,* 19, no. 3 (6 Mar 2019): 462–477, https://www.liebertpub.com/doi/10.1089/ast.2018.1915 and ITU, *Handbook on Space Research Communication* (2014) https://www.itu.int/dms_pub/itu-r/opb/hdb/R-HDB-43-2013-OAS-PDF-E.pdf.

8 Consultative Committee for Space Data Systems, *Mission Planning and Scheduling*.

9 P. Soerensen et al., "The Flight Operations Segment," *ESA Bulletin*, n. 106 (2001) 88–95, http://www.esa.int/esapub/bulletin/bulletin106/bul106_7.pdf.

adjustments for subsystems from the bus, collision avoidance maneuvers, and switching to redundant subsystems. Some telecommands have immediate effect, while others can be triggered at a specific time or by an event. For instance, some critical actions are split into several distinct commands before the satellite applies them in order to reduce the risk of an accidental activation of the action. Similar to telemetry, telecommands are also archived at the mission control center.

Payload data and its archiving are completely mission dependent. Following confidentiality principles, data should be encrypted all the way between mission, payload controls, and spacecraft. Data should also be encrypted between spacecraft and user terminals without decoding at ground station level.[10]

Missions rely on ground storage as much as possible to keep onboard storage for short-term memory. The reason for this is that storage onboard is much more expensive and unreliable than on the ground. One explanation is due to how space radiation affects the spacecraft memory, which requires expensive memories and redundancies. To put this in perspective, in 2020 the cost of a LEO launch ranged between 1,500 and 30,000 USD/kg.[11]

2.2.1 Satellite Telecommunications

The ground segment and space segment are typically connected via two-way radio links. The connection requires either a line of sight between a particular spacecraft and its ground station or additional satellites to relay data between the ground and space segment. The Institute of Electrical and Electronics Engineers (IEEE) has categorized the Radio Frequency spectrum into bands, many of which are used in space applications.[12] Spectrum allocation occurs at the national level as every country determines who is permitted to transmit on which frequencies. Frequency coordination between nations occurs through the International Telecommunication Union (ITU) Radiocommunication Sector, a division of a United Nations agency that also assists with satellite orbit deconfliction.[13]

---

10 James Pavur, "Whispers Among the Stars," Presentation at DEFCON Safe Mode (2020) https://www.youtube.com/watch?v=ku0Q_Wey4K0.

11 Thomas G. Roberts, "Space Launch to Low Earth Orbit: How Much Does it Cost?" *CSIS Aerospace Security* (2020) https://aerospace.csis.org/data/space-launch-to-low-earth-orbit-how-much-does-it-cost/.

12 NASA, "What Are the Spectrum Band Designators and Bandwidths?" (2018) https://www.nasa.gov/directorates/heo/scan/communications/outreach/funfacts/txt_band_designators.html.

13 ITU, "Space Services Department (SSD)" (2021) https://www.itu.int/en/ITU-R/space/Pages/default.aspx.

The authority of national governments to regulate the airwaves in their territory has important legal ramifications. Satellite operators must obtain and maintain authorization from every national government in which they want to operate. Access to the radio frequency spectrum has been a topic of contention among satellite operators in the recent past, with threats of litigation,[14] actual litigation,[15] protests to government agencies,[16] and requests for regulatory action.[17] This trend of using the legal and regulatory mechanisms to attack and defend the finite resource of radio frequency spectrum seems likely to only increase. This is primarily due to the fact that access to space is becoming less technologically complex and demand for bandwidth is increasing.

Student and amateur-radio satellites tend to use VHF and UHF frequency bands, though there is a trend towards the S-band.[18] Now many LEO satellites operate in the S-band for Telemetry and Telecommand (TC) and X-band for high data-rate downlink.[19] The developing trend is to move TM/TC to X-band and the payload downlink to Ka-band to enable more satellites to transmit data without interference and higher data rates.[20]

Global Navigation Satellite Services (GNSS) such as GPS and Galileo provide users with signals on L-band frequencies.[21] GEO satellites transmit data on a variety of frequencies, typically in the C-, K-, Ku-, and Ka- bands.[22]

Optical communications, the transmission of data using lasers, is emerging as a supplement to traditional radio communications links. Laser

14 Theresa Hitchens, "Iridium Publicly Threatens Lawsuit to Overturn FCC'S Ligado Vote," *Breaking Defense* (2020) https://breakingdefense.com/2020/07/iridium-publicly-threatens-lawsuit-to-overturn-fccs-ligado-vote/.

15 Caleb Henry, "SES Files $1.8 Billion Claim against Intelsat over Splitting C-Band Alliance," *Space News* (2020) https://spacenews.com/ses-files-1-8-billion-claim-against-intelsat-over-splitting-c-band-alliance/.

16 Todd Feathers, "Spacex is Lobbying against Amazon's Internet-Beaming Satellites," *Vice* (2019) https://www.vice.com/en/article/5dmzyx/spacex-is-lobbying-against-amazons-internet-beaming-satellites.

17 Jeff Foust, "Viasat Asks FCC to Perform Environmental Review of Starlink," *Space News* (2020) https://spacenews.com/viasat-asks-fcc-to-perform-environmental-review-of-starlink/.

18 VHF is defined as 30–300 MHz. UHF is defined as 300–3000 MHz. S-band is defined as the 2.5 GHz band. ITU, *Nomenclature of the Frequency and Wavelength Bands used in Telecommunications.* (2015): TABLE 4, https://www.itu.int/dms_pubrec/itu-r/rec/v/R-REC-V.431-8-201508-I!!PDF-E.pdf.

19 X-band is defined nominally as 8.5–10.5 GHz. *Id.*

20 Ka-band is defined nominally as the 30 GHz band. *Id.*

21 The L-band is defined nominally as the 1.5 GHz band. *Id.*

22 The C-band is defined nominally as the 4–6 GHz band. The K-band is defined nominally as the 20 GHz band. The Ku-band is defined nominally as the 11–14 GHz band. *Id.*

communications terminals have low volume, mass, and power requirements, which may make them easier to mass-produce.[23] Optical communications have the potential to increase the efficiency of space-to-space and space-to-ground communications by improving the signal-to-noise ratio and transmitting at higher data rates.[24] Furthermore, a satellite with an optical communications system is able to target a ground station on Earth much more precisely than one with a radio transmitter because optical frequencies' wavelengths are much smaller than radio frequency wavelengths. While it is more difficult for others to passively intercept these transmissions by deploying an antenna in the footprint, a space-based optical transmitter must be pointed at the intended ground station much more precisely than a radio transmitter. At this point, the technology is not yet developed enough for mass production, and it is not likely to completely replace radio communications in the near- or medium-term. However, the technology is viable and has been adopted by enough government and industry partners that a forward-looking approach to space-based cybersecurity must consider the unique opportunities and risks posed by this technology.[25]

2.2.2 Networks

2.2.2.1 *Classical Architecture*

In the traditional architecture, the four entities consisting of user segment, ground station, spacecraft control, and payload control are separate subsystems, with potential for each to have its own internal network.[26] Most of the equipment of each entity is connected to the internal network. Both spacecraft control and payload control are also each connected with at least one ground station.[27] This means that the ground station has at least one piece of

23 Rudolf Saathof et al., "Optical Satellite Communication Space Terminal Technology at TNO," *Proceedings Volume 11180, International Conference on Space Optics – ICSO 2018* (2018) https://www.spiedigitallibrary.org/conference-proceedings-of-spie/11180/111800K/Optical-satellite-communication-space-terminal-technology-at-TNO/10.1117/12.2535939.full.

24 Suzana Sburlan, "Introduction to Optical Communications for Satellites," Keck Institute for Space Studies (2016) https://www.youtube.com/watch?v=zDjuRg5aNf4.

25 NASA, "Low-Cost Transceiver Will Allow First Laser Mass Communication," *NASA Spinoff* (2019) https://spinoff.nasa.gov/Spinoff2019/it_4.html.

26 Consultative Committee for Space Data Systems, *CCSDS Guide for Secure System Interconnection*, Report CCSDS 350.4-G-2 (2019) https://public.ccsds.org/Pubs/350x4g2.pdf.

27 Wilfried Ley, Klaus Wittmann, & Willi Hallmann, *Handbook of Space Technology* (Wiley 2009) 461.

equipment connected to spacecraft control equipment and one piece of equipment connected to payload control equipment (it may be the same device).

Ground stations can use copper or fiber optic cables to interconnect networks. Data can sometimes be transmitted over a dedicated line but more frequently a virtual private network (VPN) or equivalent over the Internet. VPNs are technologies insulating the ground segment networks from the Internet using a layer of cryptography and security protocols. This makes the Internet insulation system a potential entry point for a capable outsider with an Internet connection.

When the user segment offers a service through the Internet, this service is also a privileged entry point for attackers, as it is connected to the ground segment and accessible from anywhere.

2.2.2.2 *Co-location*

When several parts of the ground segment are co-located, this reduces the reliance on the Internet, and may even make the system completely independent if all parts of the ground segment are co-located. This architecture is more protected from a cybersecurity perspective as it removes the Internet as an entry point, but also severely constrains the system. This allows for no reliance on external services, no remote connection with users, and limits to a single antenna location – which reduces opportunities for redundancy.

2.2.2.3 *Ground Station in the Cloud*

Using emerging third-party cloud based ground station services allows for multiple new architectures from the traditional three networks. This external service can provide a full range of services from antenna rental only to a fully integrated service where ground station, mission control, and payload control are all hosted in the same provider's cloud. Some of the hybrids are already covered by our description of the co-located architecture. Proposing satellite communication services allows for historical cloud services providers to be directly interfaced with the satellites and pushes forward their own services for distribution, archiving, or performing machine learning on the data exchanged with space.[28] These are cost attractive opportunities for new functionalities that also come with potential new threat exposures due to the outsourcing of more activities, resources sharing, and multiplying interconnections between

28 AWS, "What is AWS Ground Station?" (2019) https://docs.aws.amazon.com/ground-station/latest/ug/what-is-aws-ground-station.html.

the satellite control and the outside world.[29] Third party ground station services come with an increased attack surface, but also with embedded cybersecurity features that improve auditability and resiliencurthermoremore, shared antenna resources could potentially be leveraged by an attacker for denial of service by booking all visibility slots between the target satellite and the ground stations provider's antennas. Consequences of not being able to communicate with a satellite for too long may cascade up to the loss of the mission. Space awareness may also benefit from analyzing the availability slots of the shared antennas and trying to deduce which satellites are using the service.

2.2.2.4 *Space Networks*

Communication buses inside a satellite constitute internal communication network infrastructures that could be used by attackers to laterally move to compromising other satellite parts. Another potential entry point is the inter satellite links (ISL). Whether there are relay satellites such as EDRS/TDRS or a constellation of satellites each communicating with one another, their routing functionality could potentially be exploited as an entry point. One can imagine a hostile cyber operation spreading from satellite to satellite using these inter-satellite networks.[30] As these new networks develop, extra-care should be taken at the engineering stage as experience from the ground teaches that any kind of interoperability and legacy protocol support constitutes an additional attack surface.

Section 2 described the complexity and characteristics of space missions from main components to their interconnection. Despite – and because of – their importance for States, military forces, commercial entities, and the public society space systems are often targeted by hostile cyber operations. Section 3 addresses these threats and some of their consequences.

3 Space Cyber Threats and Their Consequences

Following the overview of the main components of space missions and how they communicate together in Section 2, Section 3 provides a description of the type of attacks. The section sets off by defining cyber operations and provides real-life examples under Section 3.1. Section 3.2 gives an overview of the

29 Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing v4.0" (2017) https://cloudsecurityalliance.org/artifacts/security-guidance-v4/.

30 Jacob G. Oakley, *Cybersecurity for Space: Protecting the Final Frontier* (Springer 2020).

different entry points for hostile cyber operations to space systems, ranging from hardware to software and their supply chains. Section 3.3 proposes a tool to identify threats and their components, providing the reader the keys to understanding the mitigation strategies that will be the subject of the next section.

3.1 *Type of Operations*

3.1.1 Electronic vs. Cyber Operations (Jamming/Spoofing/Hacking)

Electronic warfare such as jamming and EMP are generally not considered cyberattacks.[31] Defined as attacks leveraging the use of direct energy, these can sometimes be associated with physical attacks, because the electronic warfare radio wave is effective because of its power.[32] On the other hand, cyberattacks are performed at the information level – the cyberattack is effective because of the data it carries.

3.1.2 Systems and Infrastructure Disruptions, Unauthorized Data Collection, and Falsification: Stage of the Operations

Cyberattacks are not a new threat to the space industry, and previous targets span from the ground segment (either through ground stations or space agencies) to the use of radio signals. The following provides examples of hostile cyber operations against space systems.

In 2008, a passenger unintentionally introduced malware to the International Space Station through a USB drive.[33] Satellites used for navigation signals have been targeted, as seen in the Black Sea incident, where the US Maritime administration reported that 20 vessels in the Black Sea area had experienced GPS "spoofing" in which a false signal confused a GPS receiver, potentially misdirecting the ship.[34]

China has also been suspected to be behind satellite related attacks, such as the 2014 hack of a US weather satellite, thereby blocking essential data that was

31 Julian Turner, "The New Battlefield: The Race to Integrate Cyber and Electronic Warfare," *Global Defence Technology* (2021) https://defence.nridigital.com/global_defence_technology_special/the_new_battlefield_the_race_to_integrate_cyber_and_electronic_warfare.

32 Sam Cohen, "Integrating Cyber and Electronic Warfare," AFCEA (2018) https://www.afcea.org/content/integrating-cyber-and-electronic-warfare.

33 Connor Simpson, "Russian Cosmonauts Occasionally Infect the ISS with Malware," *The Atlantic* (2013) https://www.theatlantic.com/international/archive/2013/11/russian-cosmonaut-accidentally-infected-iss-stuxnet/355150/.

34 Dana Goward, "Mass GPS Spoofing Attack in Black Sea?" *Maritime Executive* (2017) https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea.

used for disaster planning and transportation interests.[35] The nature of two attacks on US satellites in 2007 and 2008, which gained control of command over the satellite in 2008, through a ground station in Norway also links China as the perpetrator.[36] Although no damage was done, the attack was alarming. Space agencies themselves can also be targeted as seen with DLR in 2014, which fell victim to a form of Trojan software, enabling hackers to maintain unauthorized access for several months to confidential information without detection.[37] In 2018 hackers gained access to NASA JPL's Deep Space Network array of radio telescopes and many of their systems. A report indicates that the breach was due to a failure to adopt basic "security 101" measures.[38]

After having described space missions, their components and their communications, we will now develop their exposure to cyber-attacks. The next paragraphs present the diverse nature of cyber threats, detail their components, propose a tool to analyze them and visual examples.[39]

3.2 *Main Entry Points*

In a globalized world, a complex space operation uses sub-systems, pieces of hardware, and software from dozens of countries and a fully developed supply chain pool of thousands of companies. Every software system relies on hardware. If the hardware is compromised, so too is the system running it. Starting at an integrated circuit level, it is feasible to embed a backdoor, and stealthiness increases with the scale of the subsystem.

It does not take intent from the supplier to introduce a cybersecurity breach, because each supplier's information system may be attacked, and its production discreetly modified by hackers in order to embed a vulnerability. While nothing guarantees that a backdoor in a chip will indeed be accessible from the board where it is integrated, the threat exists nonetheless. The more

35 Tony Capaccio and Jeff Bliss, "Chinese Military Suspected in Hacker Attacks on U.S. Satellites," *Bloomberg* (2011) https://www.bloomberg.com/news/articles/2011-10-27/chinese-military-suspected-in-hacker-attacks-on-u-s-satellites.

36 Jim Wolf, "China Key Suspect in U.S. Satellite Hacks: Commission," *Reuters* (2011) https://www.reuters.com/article/us-china-usa-satellite-idUSTRE79R4O320111028.

37 Pierluigi Paganini, "German Aerospace Center Hit by Serious Malware-Based Attack," *Cyber Defense Magazine* (2014) https://www.cyberdefensemagazine.com/german-aerospace-center-hit-by-serious-malware-based-attack/.

38 Davey Winder, "Confirmed: NASA Has Been Hacked," *Forbes* (2019) https://www.forbes.com/sites/daveywinder/2019/06/20/confirmed-nasa-has-been-hacked/?sh=210f5129dc62.

39 Consultative Committee for Space Data Systems, *Security Threats Against Space Missions*, Report CCSDS 350.1-G-2 (2015).

advanced the integration level of the compromised subsystem, the more likely the hostile cyber operation will succeed. Nevertheless, suppliers of higher-level subsystems are addressing cybersecurity threats more carefully.

Software also constitutes a potential entry point into a space mission that can be a target in a hostile cyber operation. Unlike hardware, where once a chip is manufactured its design is set, modern spacecraft software is often designed to be updated as needed in support of spacecraft builders, testers, and operators. An example of this at the component level is the Software Defined Radio.[40] This technology's modifiability complicates the software of a space system and makes it a potential entry point for attackers. On the one hand, as it is subject to updates, a vulnerability that is present today may disappear tomorrow if it is identified and closed. On the other hand, a new vulnerability may be introduced by a software update.

There are two paradigms for software as an entry point to the space system. First, there are exploited "bugs," or errors in the software. Simply put, software is a microcosm of the spacecraft, in that it takes an infinite amount of effort to design it correctly.[41] Cyber operators are skilled at identifying flaws and exploiting them to support their objectives. The second paradigm for a hostile cyber operation involves no known flaw in the software itself, but leverages the known behavior of software to render the target operationally ineffective. A classic example of this sort of hostile cyber operation is a denial of service attack.[42]

The supply chain is unquestionably a vector for hostile cyber operations, based on historic examples such as NotPetya and the SolarWinds US government data breach.[43] Outsourcing any element of the supply chain – software or hardware – or support activities, like facilities, maintenance, launch vehicle, and human resources, invites cyber risk.[44] This risk can be avoided if a decision

40 Mamatha Maheshwarappa, Marc Bowyer, & Christopher Bridges, "Software Defined Radio (SDR) Architecture to Support Multi-Satellite Communications," *2015 IEEE Aerospace Conference* (2015) https://ieeexplore.ieee.org/document/7119186.

41 Dave Akin, "Akin's Laws of Spacecraft Design" (n.d.) accessed January 31, 2021, https://spacecraft.ssl.umd.edu/akins_laws.html.

42 Qijun Gu & Peng Liu, "Denial of Service Attacks" (2007) https://s2.ist.psu.edu/paper/ddos-chap-gu-june-07.pdf.

43 Joe Panettieri, "Solarwinds Orion Security Breach: Cyberattack Timeline and Hacking Incident Details," *Channele2e* (2021) https://www.channele2e.com/technology/security/solarwinds-orion-breach-hacking-incident-timeline-and-updated-details/.

44 Paul Ashcroft, "Reducing Outsourcing Cyber Risks," *Today's CPA* (March/April 2018) https://www.tx.cpa/docs/default-source/communications/2018-today's-cpa/marchapril/techissues-march-april2018-today'scpa.pdf.

is made at the strategic level not to outsource anything, and to do everything in-house. This means vertically integrating the designing, building, testing, and operation of both the space and ground segments. SpaceX is notable as having taken this approach more than any other non-government institution in the space industry. However, this method has costs in terms of both time and money that may not be justifiable in all organizations that need to operate satellites. A more middle-of-the-road approach might involve limiting outsourcing to those elements of the supply chain or support work that an institution lacks the knowledge base to execute in-house, conducting security audits, and requiring outsourcing providers to maintain cybersecurity certifications. In short, "Trust, but verify."[45]

3.3 *Characterizing Space Cyber Threats*

One of the issues in computing, and in security in particular, is the visualization of abstract concepts, especially when they have a very broad scope. In "*The Mission as a Tree: A Novel Approach to Identifying Cyber Threats to Satellites"* the authors attempt to resolve this for missions within the scope of their paper. They map the Open Threat Taxonomy to uncrewed spacecraft.[46] This leads to a visualization of cyber threats to space missions that looks similar to a data structure that software developers call a tree. The paper provides a framework for conversations at a high level about the technical characteristics of cyber threats to a space mission. This is a necessary first step to an analysis of the domain from legal and policy perspectives.

The first subtree of the threat tree is the Threat Agents Tree (Figure 3.1). It is populated with all the individuals and institutions who might wish to harm a mission through cyber means and have the capabilities to do such harm. Threat agents need to be identified before any of the other subtrees because their capabilities and limitations will constrain the development of the other subtrees. For example, a British national security satellite like Skynet does not need to worry about commercial competitors' cybersecurity threats, whereas foreign states likely present much more substantive and credible threats to it.

The next subtree is the Threat Target Tree (Figure 3.2). This tree visualizes all the elements of the mission through which a cyber-attack could be introduced.

---

45 Ronald Reagan, "Remarks on Signing the Intermediate-Range Nuclear Forces Treaty," Ronald Reagan Presidential Library & Museum (8 December 1987) https://www.reaganlibrary.gov/archives/speech/remarks-signing-intermediate-range-nuclear-forces-treaty.

46 Sébastien Bonnart et al, "The Mission as a Tree: A Novel Approach to Identifying Cyber Threats to Satellites," International Astronautical Congress 2020: CyberSpace Edition (2020).

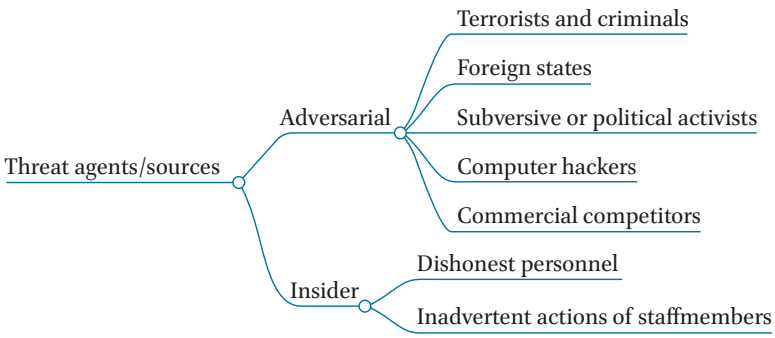


FIGURE 3.1 Illustrative threat agents tree from Bonnart et al., "The mission as a tree"

This includes places where mission- or security-critical data is stored, media by which it is transmitted, and personnel who have the authority to access it. A thorough Threat Target Tree considers hardware, software, process, systems, and human vulnerabilities that the identified Threat Agents have the capability to compromise. This subtree presents unique difficulties because its development requires an honest and self-critical assessment not just of the mission, but of each individual and institution that supports the mission – from the processors in components to nontechnical support staff at the prime contractor to cybersecurity and access control measures in place at the machine shop where mechanical components are fabricated.

The third subtree is the Threat Action Tree (Figure 3.3). This maps out all the ways that a Threat Agent could compromise a Threat Target in the cyber domain. The four most common types of cyber-attacks in general are interruption of connectivity, interception of data, modification of data, and fabrication of data. Each of these actions can be done in different ways, depending on the Threat Target. Threat actions to spacecraft in the cyber domain will be discussed in more detail in the next section.

The Threat Consequences Tree (Figure 3.4) considers the possible effects of each leaf of the Threat Action Tree on the mission. The consequences of cyber attacks to spacecraft will be discussed in more detail in the next section.

Mission planners can quantify the likelihood of a threat agent taking a threat action against each possible threat target for that action, and the probability of any relevant threat consequence arising from that action. This allows mission planners to easily identify what the likely cybersecurity risks to their architectures are and efficiently allocate more resources to mitigate the more likely threats.

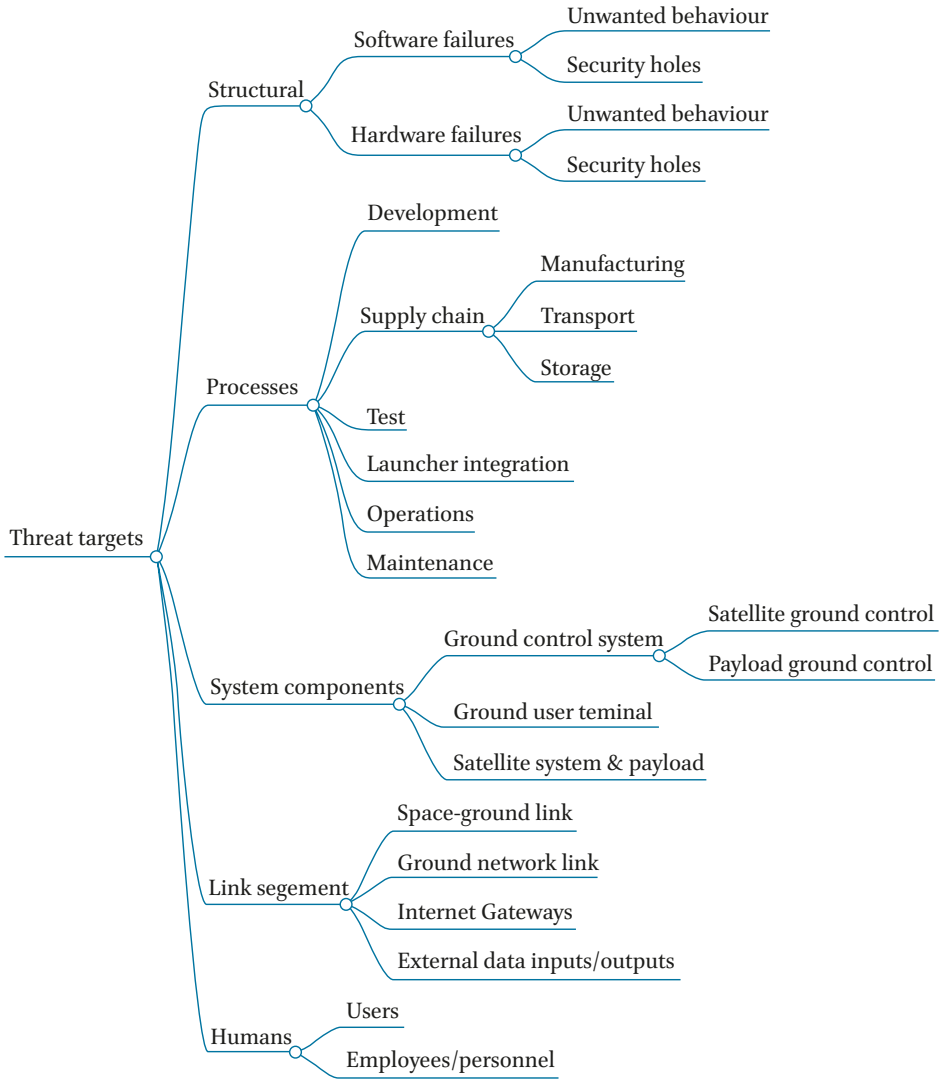


FIGURE 3.2 Threat target tree from Bonnart et al., "The mission as a tree"

The Threat Consequences subtree, however, will likely be the most difficult to quantify, because cyber-attacks have, relative to electronic or kinetic attacks, much more aleatory risk. Unlike mainstream cybersecurity where one would assume that the attacker crafted his action using a copy of the software[47] or hardware, it is currently expected not to be the case for most assets

47 E. Kenneth Hong Fong, David A. Wheeler, & Amy E. Henninger, *State-of-the-Art Resources (SOAR) for Software Vulnerability Detection, Test, and Evaluation* (IDA 2016)

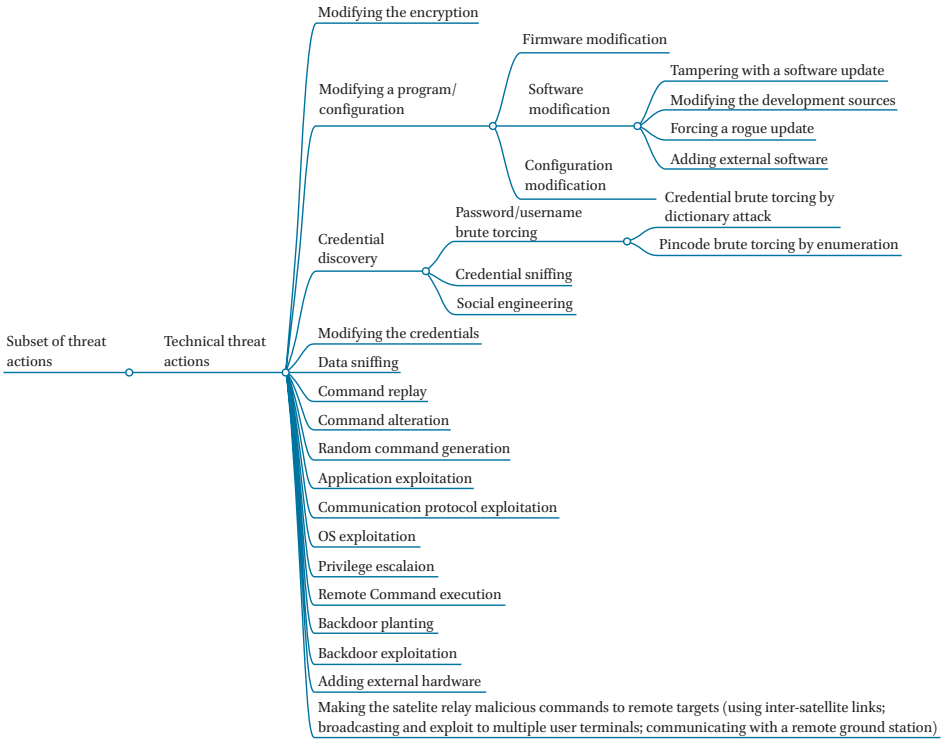


FIGURE 3.3 Illustrative sub-section of a threat action tree from Bonnart et al., "The mission as a tree"

in space. The unknown unknowns make it more difficult for a threat agent to anticipate precisely how their actions will affect their threat target. If a threat agent cannot understand in advance the effects of their attack, it must be that much more complicated for the mission operator to plan for the effects of cyber-attacks. This planning, however, may well be crucial to ensure that the mission can recover from an attack. The expected confidentiality of the hardware and software is presented here as a hypothesis and could be countered by the attacker through the possibility of initial successful ground-based attacks revealing onboard software, hardware designs, and documentation.

This section presented an overview of previous hostile cyber operations against space systems and outlined possible entry points for an attack and

https://www.ida.org/research-and-publications/publications/all/s/st/stateoftheart-resources-soar-for-software-vulnerability-detection-test-and-evaluation-2016.

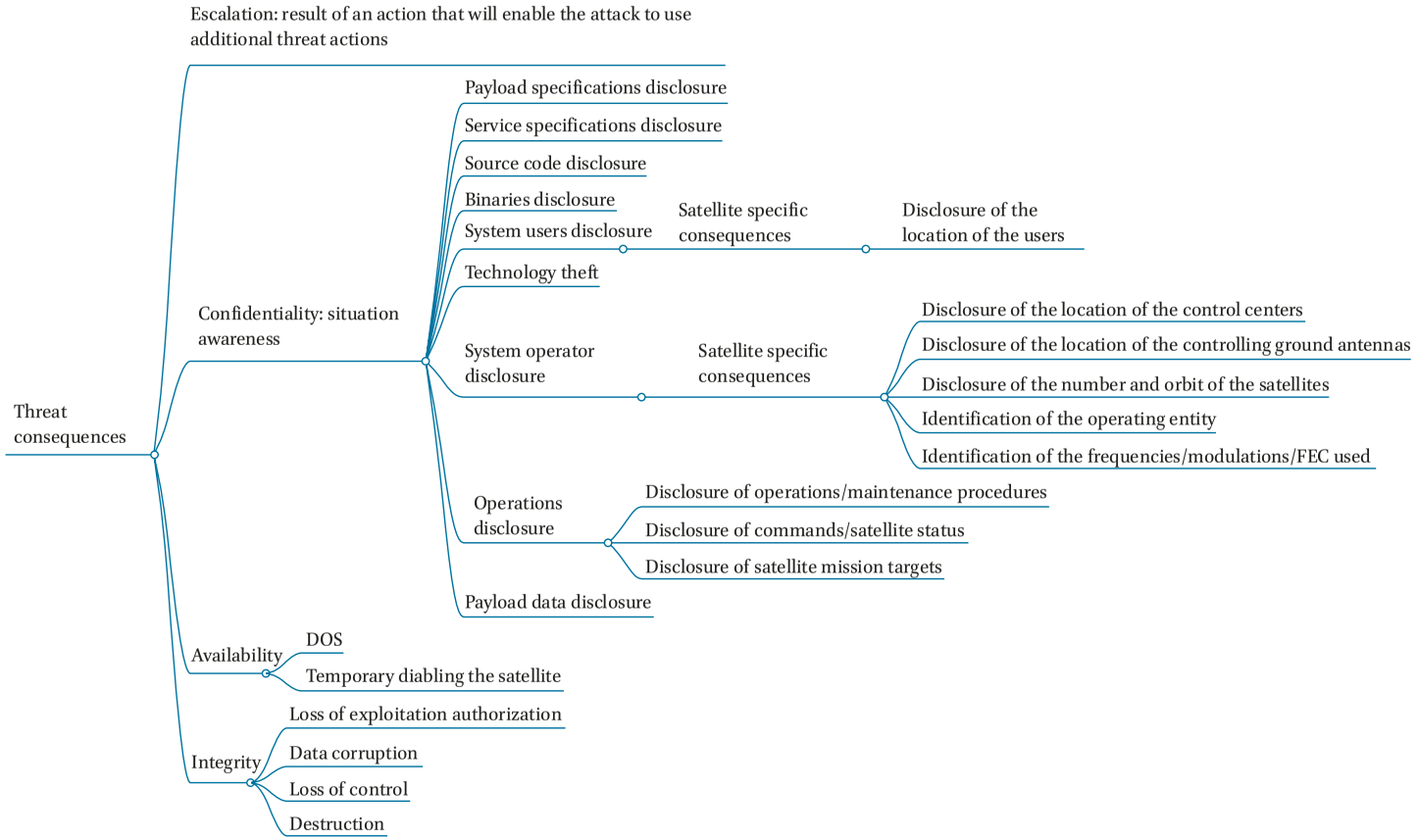


FIGURE 3.4 Illustrative threat consequences tree from Bonnart et al., "The mission as a tree"

concluded by presenting the use of trees in order to inventory and visualize threats.

4 Protective Measures to Boost Cyber Resilience of Space Assets

After having described the space environment and space mission's cyber threats, Section 4 shows how they can be analyzed as risks. Section 4.2 addresses the processes of reconstructing a system after a breach and the potential for response through international collaboration. Section 4.3 outlines IT governance frameworks, which is part of corporate governance. These frameworks facilitate means of specifying decisions, rights, and accountability tied to an organization's use of technology. Finally, Section 4.4 proposes technical strategies that an entity can adopt to mitigate the risks, including *inter alia* methods to assure software and to protect its integrity.

4.1 *Impact and Effects of Hostile Cyber Operations*

4.1.1 Long-Term Consequences on the Activities, Relationships, and Environment

Given the ultra-hazardous nature of outer space, every hostile cyber operation can have an impact on space activities. The unforgiving space environment presents a concerning likelihood of increased risk/impact due to constraints on recovery abilities and limitations on resilience. The impact of these operations might have long-term or short-term consequences based on the different nature and purposes of the targeted system and the kind of attack perpetrated against the system/satellite.

In order to define the impact and effects of hostile operations, it is important to estimate the risk related to an event. This is defined by two parameters: the first is the likelihood of the event occurring, while the second is the severity/impact of the event's consequences. By crossing these two parameters, a matrix can be created through which five categories of risk can be identified, namely: 'extreme,' 'major,' 'moderate,' 'minor,' and 'incidental.'

This "heat map" matrix (Figure 3.5) allows for the two-dimensional identification of the potential risk impact that every hostile operation can create.[48]

Assessing space activities allows for a better comprehension of the risk and therefore a better comprehension on how to diminish the impact or the

48 Patchin Curtis & Mark Carey, *Risk Assessment in Practice* (Committee of Sponsoring Organizations of the Treadway Commission, 2012).

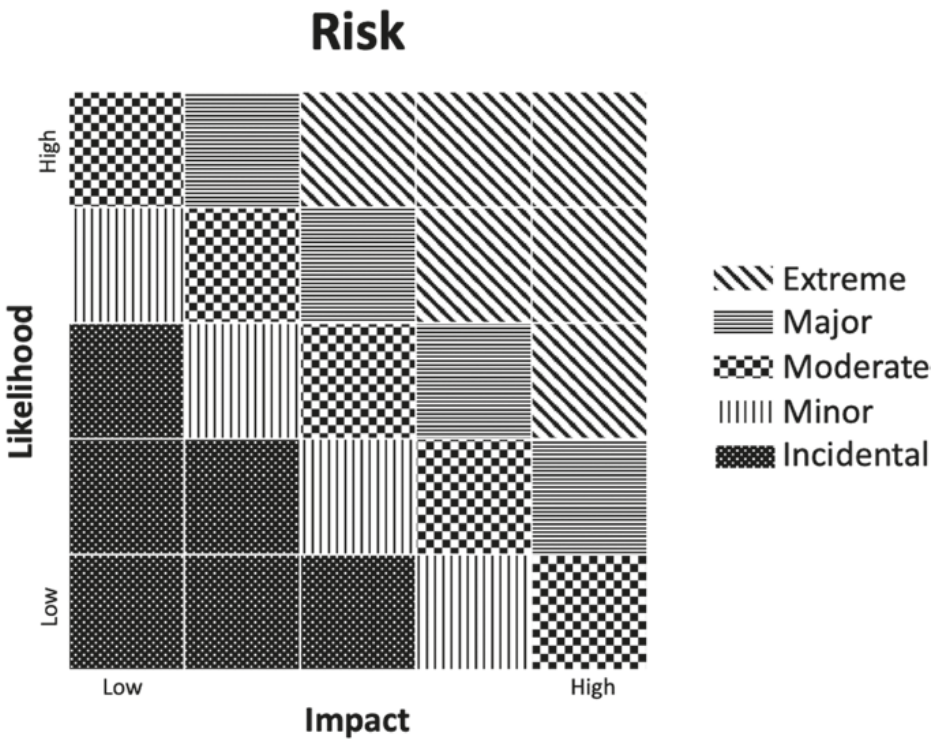


FIGURE 3.5 Illustrative heat-map

likelihood of an event. By doing so, it is possible to create a more stable system that conducts activities in a safer and more resilient structure.

Space capabilities provide a wide range of applications such as earth-observation, communication, exploration, and positioning, navigation, and timing (PNT).

– Earth-observation satellites provide information services based on Earth observation data from orbit. These systems provide land monitoring, emergency management, atmosphere monitoring, maritime environment monitoring, climate change, and security applications. These services can be used both for military and civil purposes. Civilian Earth measurable benefits from Earth Observation activities range from agriculture yields improvement, disaster risk management, famine prevention, water management, weather forecasting, to plane travel time forecasting.
– Communications satellites (SATCOM) relay and amplify radio telecommunications signals. These satellites provide telecommunications, broadcasting, and data communications services over wide areas of the globe.

– Exploration satellites aim to provide information on outer space or on celestial bodies. With the development of new activities planned to be carried out on celestial bodies, a new trend is emerging. The emergence of space mining may boost the space economy and subsequently, the systems may become ideal targets to disrupt another State's or company's activity.
– Positioning, Navigation, and Timing (PNT) satellites aim to provide accurate positioning and timing information. These space-based assets are essential for the performance of everyday life since they are used for precision targeting, tracking, and provision of precise timing that is also vital for the function of economic and banking networks.[49]

With the increasing number of satellites launched in different orbits, and the creation of new constellations, the number of entry points via which attackers may enter has increased. Security-related space infrastructure has suffered a decline of attention over the years, leaving it vulnerable to hostile cyber operations.[50]

The different space applications may lead to different long-term consequences related to hostile cyber operations. When a hostile cyber operation occurs, the targeted victim faces numerous consequences including the appropriation of sensitive information. Earth Observation satellites operated by civilians may possess classified information that should not be disclosed and needs to be protected.

Any kind of interruption of a space activity may cause disastrous outcomes due to the ultra-hazardous environment. The disruption, however, can be partial and non-damaging to any system of the satellite. In this case, the system would be momentarily compromised and would not lead to any major consequences. However, if the system is permanently compromised the launching State would face numerous consequences. This could result in a monetary loss due to the fact that systems need to be replaced. Subsequently, the whole mission could be threatened because it needs to redevelop new technologies to prevent the repetition of such outcomes.

Disruption of a single system can threaten an entire mission and its activities. The interruption of communication during a mission may lead to the loss

49 Antonio Carlo, Lacroix & Zarkan, "The Challenge of Protecting Space-based Assets Against Cyber Threats," International Astronautical Congress 2020: Cyberspace Edition (2020).

50 Alex Mathew, "Cyber Security – How Vulnerable are Satellites to Cyberattacks" *International Journal for Research in Applied Science & Engineering Technology*, v. 7/III (2019): 2427–2430, http://doi.org/10.22214/ijraset.2019.3443.

of control of the space segment and lead to the collision of satellites. The intent of an attack could be to cause a collision between satellites turning the satellite itself into a weapon – also known as an anti-satellite weapon (ASAT).[51] The destruction of a space object would result in the creation of a large amount of space debris making utilisation of the orbit impossible due to the danger that those objects would pose. Collisions of debris larger than 10 cm may result in catastrophes, releasing hazardous debris clouds which can lead to an escalatory chain reaction and potentially make some orbital zones unusable.[52]

4.2 *Reconstructing and Incident Response*

As technology continues to evolve, so do the opportunities and challenges it poses. In particular, the ever-increasing dependence on technologies exposes stakeholders to a whole set of risks associated with cyberattacks. Hostile cyber actors are continuously trying to break into close and highly secure systems while the cyber threat landscape continues to expand and evolve rapidly.[53] To counter these issues, security and defence of the space systems need to be updated and secured. Many governments, companies, and institutions have created *ad hoc* Computer Emergency Response Teams (CERTS) and Computer Security Incident Response Teams (CSIRTS) coordinated by Security Operational Centres (SOCS) in order to pre-empt possible cyber events. However, when these entities do not manage to stop an attack there are different ways to deal with the reconstruction of infrastructure. Attacked entities have to face not only the damage of the attack itself, but also its consequences such as the loss of trust and reputation. The reconstruction of a stronger system should be done by private-public partnerships (PPPS), technical personnel, and lawyers in parallel.

Strong national and international cooperation could lead to the sharing of best practices and unique know-how to prevent, strengthen, and reconstruct a system after a cyber event. Information Sharing and Analysis Centres (ISACS) were created in order to answer this need, to make cyber threat data and best practices more accessible internationally. ISACS also provide a central resource

51 John Pike, "The Military Uses of Outer Space" *SIPRI Yearbook 2002: Armaments, Disarmaments and International Security* (2003): 613–655.

52 Antonio Carlo & Giannakou, "Active Debris Removal: The Legal Challenges and the Way Forward," *Proceedings of the AIDAA XXV Congress of Aeronautics and Astronautics* (2019): 1261–1273.

53 Center for Strategic and International Studies, *Significant Cyber Incidents since 2006* (2020) https://csis-website-prod.s3.amazonaws.com/s3fs-public/201218_Significant_Cyber_Events.pdf.

for gathering information on cyber threats and events to critical infrastructure. Further, constant monitoring of the activities and risk assessment may lead to the reduction of such events. For instance, Estonia entrusted terabytes of information on its citizens to Luxembourg after assessing that this option could prevent cyberattacks directed at gathering this information.[54] Such sharing of data led to so-called cyber diplomacy between two allied countries within the European Union.

Cyber diplomacy drives International Organizations to establish strong cooperation.[55] Such as, in 2003, when the European Union (EU) and the North Atlantic Treaty Organization (NATO) signed the "Berlin Plus" agreement, which established the milestone principle of allowing the European Union the possibility to use NATO forces when necessary. This cooperation was successfully implemented in Macedonia and Bosnia. In 2016 the European Union and NATO signed a Technical Arrangement to facilitate technical info-sharing between CERT-EU and NATO Computer Incident Response Capability (NCIRC) leading to an international cooperation in information sharing.[56] In particular, the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) is now liaising with the European Defence Agency (EDA) by exchanging information on common topics of concern. To construct a strong and resilient system, public and private cooperation and cyber diplomacy are essential together with the establishment of CERTs and SOCs that monitor and organize the cyber operations.

Section 4.1 has outlined the methodologically process of defining and reacting to a cyber risk, including responses from international cooperation ranking from *ad hoc* response teams to international cooperation in EU and NATO. The following part will focus on the internal organisational responses processes in the shape of ICT Governance Strategies.

54 Yuliya Talmazan, "Data Security Meets Diplomacy: Why Estonia is Storing its Data in Luxembourg," *NBC News* (2019) https://www.nbcnews.com/news/world/data-security-meets-diplomacy-why-estonia-storing-its-data-luxembourg-n1018171.

55 Attila Mesterhazy, *NATO-EU Cooperation after Warsaw*, NATO Parliamentary Assembly, Defence and Security Committee Report (2017) https://www.nato-pa.int/download-file?filename=/sites/default/files/2017-11/2017%20-%20163%20DSCTC%2017%20E%20rev%201%20fin%20-%20EU%20AND%20NATO%20COOPERATION%20-%20MESTERHAZY%20REPORT.pdf.

56 NATO, "NATO and the European Union Enhance Cyber Defence Cooperation" (10 February 2016) https://www.nato.int/cps/en/natohq/news_127836.htm.

4.3 *ICT Governance Strategies*

The promotion of an Information and Communications Technology (ICT) governance framework for space-based assets represents a vital step toward improving cyber resilience, reducing the incidence of catastrophic cyber incidents, and conducive to the maintenance of peace and stability across the final frontier. Consequently, existing ICT governance frameworks across the information security and technology profession provides opportunities for individual space enterprises to pick and devise frameworks suited to their individual circumstances.

The application of ICT governance is pertinent in protecting space-based assets against cyber threats from an organizational perspective. This section addresses the preemptive, proactive, and remedial processes in promoting a best-practice approach to cyber-threat intelligence, determining the taxonomy of threats, and in advancing measures conducive to estimating cyber-insurance covers for space assets. Improving ICT governance mechanisms concerning space-related technologies are a vital part in encouraging positive behaviors, improving top-level decision making, reducing the possibility and effects of catastrophic incidents, and enabling better strategic planning vis-a-vis cybersecurity matters.

The significant risk posed by potential cyberattacks against space assets warrant the need for a cybersecurity framework and control structure. ICT governance frameworks help organizations assess and manage the cyber risks across an expanded attack surface.

Specific challenges arise in the application of terrestrial ICT governance framework to space-based technologies and systems. Some of these challenges include: compliance with international treaties, national space laws, the difficulties associated with access to space, the harsh outer space environment, and the difficulty of affecting physical repairs to space-based infrastructure. This is complemented by traditional information security risks posed to ICT infrastructure – including data breaches, cyberattacks, supply chain cybersecurity, and insider threats. Within this context, the tailored application of relevant governance frameworks and standards assumes a vital role in creating a safe and sustainable outer space environment.

4.3.1 Context

ICT governance exists as a subset of corporate governance, which represents a system of directing and controlling the action of the governing organization. ICT governance also ensures that businesses have the proper decision-making

processes and controls in place to balance the interests of all stakeholders.[57] Furthermore, the concept of management can be distinguished from that of governance in several aspects. Management involves the planning, building, and running of activities in alignment with the directions set by the governance body to achieve the enterprise objectives. They are usually established by executives at the highest management level (C-level) and cover all functions and processes to govern and manage the organization at large.

Consequently, the objective of ICT governance seeks to facilitate the means of specifying the decision, rights, and accountability framework tied to an organization's use of technology. The process encourages desirable behaviors in the use of technology and technical systems across both public and private sector organizations.

A codified governance framework takes stakeholders' interests into account, as well as the needs of staff and the processes they follow. Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-upon enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on directions and objects.

The need for an ICT governance framework for space is driven by several realities.[58] First, the notion of continuous expansion, which is when an innovative space sector is contingent upon increased competitive offerings across a variety of space companies. This accounts for the needs and requirements of various stakeholders. This results in customers wanting more secure products and services, investors requesting increased returns, and regulators seeking increased accountability and responsibility.

Second, the realization of size and complexity as traits inherent to the space industry and environment. Noting predictions of future trillion-dollar space-based enterprises, the rise of mega corporations in the outer space domain necessitates the need for standards and guidance. The reason for standards and guidance is to empower executives and managers to implement effective whole-of-organization ICT governance measures.[59]

---

57 "What is IT Governance?" *IT Governance* (2020) https://www.itgovernance.co.uk/it_governance.

58 Deloitte, *Developing an Effective Governance Operating Model – A Guide for Financial Services Boards and Management Teams* (Deloitte, 2013): 2.

59 Deepak Sethi, "The First Trillionaire Will Be Made in Space Mining," *Medium* (11 December 2020) https://medium.com/datadriveninvestor/the-first-trillionaire-will-be-made-in-space-mining-cea665c1b00d.

Third, the emergence of new legislative instruments and regulations concerning outer space applications. Noting the possibility of space companies such as Swarm Technologies conducting activities outside government authorization,[60] both regulatory changes and lapses in governance are likely to continue. This highlights the potential need for executives and managers to extend governance processes deeper into their organizations.

The implementation of an ICT Governance Framework is predicated upon several major elements. First, structure and policy define the decision process, which includes outlining the policies and individual responsibilities to be created.[61] Second, procedure and process specify how decisions are made and what processes exist to propose and approve investments. Third, communication involving the mechanisms involved in communicating ICT investment decisions to the board of directors, employees, and shareholders.

These elements span the formation of a strategic vision for an organization, and coordination between different pieces of ICT-related work and infrastructure. Proper application of an ICT governance framework can result directly in increases to productivity, higher quality product offerings, and improved financial performance. Conversely, poor governance can result in programmatic waste, needless and confusing bureaucracy, diminished overall financial performance governance, and ultimately the demise of an organization.[62]

4.3.2 ICT Governance Frameworks

The notion of a "framework" represents a conceptual structure, defined by the governance of an organization to set out policies, principles, and a model demonstrating ICT governance tasks and activities within the organization.[63] Frameworks embody a top-down approach, identifying the main stakeholders first, along with their needs and appetite for risk. This is followed by identifying the stakeholders who will manage policies on a day-to-day basis. As opposed to a "guideline," frameworks provide for clear controls and policies that need to

60 Loren Gush, "Company that Launched Satellites without Permission Gets New License to Launch More Probes," *The Verge* (4 October 2018) https://www.theverge.com/2018/10/4/17928452/swarm-technologies-spacebees-satellites-spacex-falcon-9-fcc-license.

61 "IT Governance Framework," *CIO Wiki* (2020) https://cio-wiki.org/wiki/IT_Governance_Framework.

62 Australian Public Service Commission, "Building Better Governance' on Australian Government" (12 June 2018) https://www.apsc.gov.au/building-better-governance.

63 "Understanding Guidelines, Frameworks and Standards from a Governance Standpoint," *Spector* (12 September 2019) https://www.spector.ie/blog/understanding-guidelines-frameworks-and-standards-from-a-governance-standpoint/.

be in place to adhere to. Presently, within the cybersecurity industry there exist several ICT governance frameworks of note.

The IT Infrastructure Library (ITIL),[64] developed by the UK Cabinet Office as a library of best-practice processes for IT service management, has been widely adopted around the world. ITIL represents a framework that focuses on and enables ICT services to be managed across their lifecycle. The framework is supported by ISO/IEC 20000:2011, against which independent certification can be achieved, and structured across several areas – including service strategy, service design, service transition, service operation, and continuous service improvement.

COBIT19,[65] an internationally recognized ICT governance control framework that aims to connect business goals to technical goals, assigns objectives and duties to both business and ICT leaders. The framework helps organizations meet contemporary business challenges across regulatory compliance, risk management, in aligning their technology strategy with organizational goals. The underlying rationale of COBIT19 is highlighted within its six core principles, representing a design philosophy: 1) providing stakeholder value; 2) enabling a holistic approach; 3) dynamic governance system; 4) governance distinct from management; 5) tailored to enterprise needs; and 6) covering the enterprise end-to-end.

Val IT[66] is a governance framework utilized to create business value from IT investments. Developed by Information Systems Audit and Control Association (ISACA), the framework is a comprehensive and pragmatic organizing framework that enables the creation of business value from ICT-enabled investments. Val IT integrates a set of practical and proven governance principles, processes, practices and supporting guidelines that help boards and enterprise leaders optimize the realization of value from ICT investments. The framework's main processes encompass value governance, portfolio management, and investment management.

In summary, it must be emphasized that none of the ICT frameworks covered represent a single definitive solution to improving an organizations' cyber resilience. The creation of an ICT framework does not specifically need to derive from one source. Organizations can elect to adopt a tailored approach

64 Stephen Watts, "COBIT vs ITIL: IT Governance Frameworks," *BMC blogs* (15 May 2017) https://www.bmc.com/blogs/cobit-vs-itil-understanding-governance-frameworks/.

65 Kim Lindros, "What Is IT Governance? A Formal Way to Align IT & Business Strategy," *CIO* (1 August 2017) https://www.cio.com/article/2438931/governanceit-governance-definition-and-solutions.html.

66 "VAL IT Framework," *CIO Wiki* (2020) https://cio-wiki.org/wiki/Val_IT_Framework.

in drawing from several frameworks, and their underlying standards to develop their own structure, as suited to the unique requirements and capabilities of each organization.

4.3.3 US Approach to IT Governance in Space

The US government has adopted an interagency process for governance and policy coordination on outer space affairs.[67] This encompasses the Federal Communications Commission (FCC), the Federal Aviation Administration (FAA), the Department of Commerce, NASA, and the Department of Defense. The Executive Branch of the US government has continuously updated and reviewed its authorization and oversight framework for private sector space activities. Consequently, a sectoral approach to information security and cybersecurity matters across each government body would prove to be overly bureaucratic, slow, and unsustainable.

Since 2014, the US federal governance structure for general ICT-based cybersecurity has made strides with the maturation of the National Institute of Standards and Technology (NIST) Risk Management Framework and Cybersecurity Framework. NIST cybersecurity maturity standards and guidelines are best-suited in covering ground-based space infrastructure and assets by assisting organizations in improving their cybersecurity measures and best practices. However, these are not directly applicable to the space domain. While efforts have been made to mold these frameworks for space systems (per the Committee on National Security Systems Instruction – 1253F), uniformity is deficient and updated standards for spacecraft and their associated IoT systems are necessary.

However, overarching governance and policies lack the necessary integration between cybersecurity and the space domain. Governance efforts in the space and cyber domains remain highly siloed, which may limit meaningful progress. Strategy documents covering the improvement of cybersecurity in the space domain include the 2017 National Security Strategy, 2018 National Cyber Strategy, Space Policy Directive-3, and Space Policy Directive-5 (SPD-5).[68] The most relevant is SPD-5, issued by the Trump administration in September 2020, representing a government framework incorporating cybersecurity into

67 Daniel L. Oltrogge & Ian A. Christensen, "Space Governance in the Newspace Era", *Journal of Space Safety Engineering* v. 7, 436 (2020).

68 Presidential Memoranda, "Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems" (4 September 2020) https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/.

all phases of space system development. The intent behind SPD-5 is to develop a culture of prevention, active defense, risk management, and the sharing of best practices.[69] This includes security by design, cybersecurity hygiene practices, supply chain cybersecurity, and the leveraging of widely adopted best practices. However, while SPD-5 serves as a high-level policy direction, it should not be interpreted as a substantive ICT governance framework or standards.

A broader literature analysis highlighting research from Chatham House describes the deficiencies on a global scale in relation to NATO. While the majority of documents addressing cybersecurity issues in space outline policy and governance challenges, few are solution-oriented in reducing cyber risk to space systems concerning human spaceflight vehicles.

In lieu of the development of a structured ICT governance framework by the US government, a threat-based principles approach to managing cybersecurity risks to spacecraft provides an alternate means of addressing this concern. This is predicated upon the application of defense-in-depth (DiD) principles to reduce the risk of cyberattack on a spacecraft. These principles should provide decision-makers, acquisition professionals, program managers, and system designers alike with considerations while acquiring and designing cyber-resilient spacecraft.

4.3.4 Benefits of ICT Governance for Space

The adoption of ICT governance framework covering space-based assets is conducive to boosting organizational cyber resilience. From a general perspective, the clear instructions and established best practice information technology standards advanced play a significant role in improving performance and promoting adaptability and responsiveness to changes in the cyber-threat environment.[70] These organizational and business improvements flow from the potential of ICT governance to address several key information security challenges affecting cybersecurity for outer space assets.

First, a tailored ICT governance framework addresses the unique environmental, technical, and policy challenges associated with outer space, elevating the protection of space-based assets against cyber threats. A framework helps both ordinary employees and senior management understand and

69 Jonathan Blair, "Space Policy Directive-5 Establishes Comprehensive Cybersecurity Policy for Space Systems," LMI Advisors (4 September 2020) https://www.lmiadvisors.com/space-policy-directive-5-establishes-comprehensive-cybersecurity-policy-for-space-systems/.

70 "6 Benefits of Good IT Governance," *O'Reilly* (2021) https://www.oreilly.com/library/view/governance-of-it/9781780171548/19_ch06.xhtml.

communicate about the business risk and threat landscape within which the business operates. This feeds into Business Continuity Management (BCM) in the creation of interdependent contingency planning and response operations documents. These measures help preserve competitive advantages, keep business functions, and enable ICT operations in the event of a cyberattack upon both space-based assets and their ground-based infrastructure.[71]

Second, an adaptable ICT governance framework promotes novel approaches to the identification of cyber threats to satellites. The integration of cyber risk identification standards under a tailored ICT governance framework helps identify, assess, and drive the management of residual risk.[72] Within the outer space context, it is established that malicious actors can be sorted into various categories (Figure 3.1) and summarised into four main groups – including Nation State Actors, Private Economic Actors, Hacktivists/Natural Persons, and International Entities. The integration of ISO/IEC 385000 standards herein is beneficial in recognising the specific interests and scope of activities of each of these actors within the outer space context, and illustrating the different levels of sophistication within their offensive cyber capabilities targeting space-based and ground-based ICT networks for satellites.[73]

4.4 *Technical Strategies*

After having identified governance strategies to cyber threats above, Section 4.4 presents an overview of the technical strategies to be adopted in space systems to mitigate risks related to cyberattacks. A system's security policy combines a series of intended and performed operations with respect to security. Different areas of actions concur to operate and integrate inside a space system maintaining the requested level of security. They are explored in the following paragraphs.

4.4.1 Software Assurance Methods

Software assurance risks are due to accidental design or implementation errors that can provoke failures or worse hazards and accidents. In a space system the exploitations of software vulnerabilities can cause undesirable events or

71 Brahum Herbane et al., "Business Continuity Management: Time for a Strategic Role?" *Long Range Planning,* v. 37/5 (2004): 435.

72 "Cyber Risk Identification," *Cyberwatching.eu* (2021) https://www.cyberwatching.eu/cyber-risk-identification.

73 Australian Cyber Security Centre, "Using a Risk Management Framework" (2021) http://cyber.gov.au/acsc/view-all-content/guidance/applying-risk-based-approach-cyber-security.

system damage that can result in the loss of spacecraft's control, data or even of the mission[25]. Software safety best practices and methodologies compliant with Safety Standards[74] should be performed during the entire software lifecycle. The security by design approach is defined by six phases: 1) identification of requirements; 2) design; 3) implementation; 4) testing and verification; 5) release; and 6) maintenance.

In the first phase, clear security requirements are defined, also with respect to requested levels of security of developed software. System security architecture and design guidelines are specified in the design phase. The attacker's point of view is considered, and threat modelling and mitigation planning is required. In the implementation phase, secure programming practices[75] should be taken into account. The use of a combination of manual and automated tools for code generation, analysis, and testing minimize possible human errors and detect relevant bugs that can lead to vulnerabilities. In the testing and verification phase, diversified vulnerability scanning tools give the overall detection and analysis of vulnerabilities. Penetration testing of the system, manual or automated, should be performed by independent and expert teams and they could be both internal and external (external are suggested). Automated tools give a range of services for identifying and exploiting security weaknesses.[76] Regarding the release and maintenance of software, space missions should be designed to support on-going upgrades of all systems including the space segment in order to prevent attacks based on already known and exploited vulnerabilities.

4.4.2 Software and Firmware Integrity Protections

The integrity of a platform's firmware and software is crucial to ensure the programmed behaviour of a system without malware in the space domain. Attacks on the firmware could affect the device's operations injecting malicious functionality that compromises interoperability within the platform. As suggested by Bailey and his fellow authors, only authenticated updates and proper configuration management must be implemented for all software and firmware residing in any system.[77] The Root of Trust guarantees the security

74 Bryan O'Connor, *"NASA Software Safety Guidebook,"* NASA Technical Standard NASA-GB-8719.13 (2004).

75 Owasp.org, *OWASP Secure Coding Practices-Quick Reference Guide* (2021) https://owasp.org/www-project-secure-coding-practices-quick-reference-guide.

76 Gilberto Najera-Gutierrez et al., *"Web Penetration Testing with Kali Linux: Explore the Methods and Tools of Ethical Hacking with Kali Linux"* (Packt Publishing Ltd, 2018).

77 B. Bailey et al., *Defending Spacecraft in the Cyber Domain* (The Aerospace Corporation 2019).

mechanism of detection, protection, and recovery of firmware code and critical data. A Root of Trust is a source that provides security functions and it is typically the first element in a Chain of Trust. Only authenticated and authorized firmware update mechanisms must be allowed. An updated image is considered authentic if the source and integrity can be successfully verified.[78] The authentication is provided by means of cryptographic signature verification, through a Root of Trust for Update. The authorization is reached by mechanisms that legitimize the update of firmware (that is by the user, managed updates, manual recovery, *etc.*). The spacecraft and the other critical space systems, such as the ground station, should be provided with automatic recovery in such a way that they are able to detect a possible corruption of a firmware image. After detecting the modification, the systems should be able to recover from a backup firmware stored in a secure location.[55]

4.4.3 SIEMs for Logging Onboard Events and Identification and Prevention Systems

In a typical security incident and event management system (SIEM), the event sources are differentiated and cover possible risk interfaces (that is network device, application server, authentication device, *etc.*). The events (for example, logging data) are then normalized and sent to the security management platform, which analyzes them in a window and triggers security alerts to the terminal. The events are also sent to the archival forensic analysis database that maintains the events for a longer period.[25] Both the spacecraft and the ground station should maintain an independent trace of the occurring events. Commands received may be stored and sent to the ground through telemetry and then automatically checked to verify consistency between commands sent and commands received.[54] Experimenting with the creation or adoption of a security information and event management tool for space vehicles is suggested in "Defending Spacecraft in the Cyber Domain."[54] However, not having enough logging data is a limitation in characterizing and attributing cyberattacks. Log management includes guaranteeing the confidentiality, integrity, and availability of logs. To ensure that changes to archived logs are detected (that is, integrity), an option could be integrity checking, which consists of calculating a message digest for each file and storing the message digest securely.[79]

78 Andrew Regenscheid, "Platform Firmware Resiliency Guidelines," NIST Special Publication (SP) 800–193 (Draft) (2017).

79 Karen Kent & Murugiah Souppaya, "Guide to Computer Security Log Management," NIST SP 92 (2006): 1–72.

Analysis of the audit log periodically could be useful to review and report logs for urgent errors and warnings.

Currently, there exist several challenges in collecting, storing and analyzing events in a scalable and smart manner. A challenge to face is that the system should be able to learn from previous incidents, automating the correlations between alerts. Machine learning-based intrusion detection and prevention systems can block the detected anomalies and cyberattacks.

As suggested by Bailey and his fellow authors, intrusion detection systems should implement both signatures (derived from known cyber information and weakness of the system) and machine-learning-based anomaly detection techniques.[51] These systems can rely on different machine learning techniques such as Bayesian Network and Naive Bayes, Decision Tree and Decision Table, Random Forest and Random Tree, and Artificial Neural Network.[80] These algorithms should be trained on datasets that include available and standard space operations. As a result, a new research frontier is applying deep learning techniques to solve the current problems and challenges derived from applying classical machine learning algorithms (for instance diverse nature of datasets, growth in the number of unclassified new malwares, network traffic diversity *etc.*).[81]

4.4.4 Cryptographic Solutions and Crypto-agility

Cryptography is a method of protecting information through the use of algorithms and transformations – allowing for communication even in the presence of adversaries, given proper supporting protocols and management. The correct design and implementation of cryptographic solutions can offer confidentiality, data integrity, and authenticity for mission system data. Information security services, with cryptographic safeguards of sufficient security strength and reliable key management, should be implemented inside mission environments. The decreasing cost for hardware and the increasing interconnection of ground networks are two examples of reduction in attack costs, easing the process of gathering information unless sound cryptographic safeguards are in place. As a result, attackers can potentially create passive or actively malicious

80 Hamed Alqahtani et al., "Cyber Intrusion Detection Using Machine Learning Classification Techniques," *International Conference on Computing Science, Communication and Security* (Springer 2020): 121–131.

81 A.M. Aleesa et al., "Review of Intrusion Detection Systems Based on Deep Learning Techniques: Coherent Taxonomy, Challenges, Motivations, Recommendations, Substantial Analysis and Future Directions," *Neural Computing and Applications,* v. 32/14 (2020): 9827–9858.

ground stations that target mission information and communications. The Consultative Committee for Space Data Systems (CCSDS) also suggests that cryptographic algorithms and protocols can be utilized by civilian space missions to avoid loss of data or total mission loss, providing their systems and operations with the required communications protections.[82] In cryptography, however, the discovery of algorithm weaknesses, and the retirement of algorithms or other constructions, is inevitable. Other technical priorities, such as performance, are also considerations. Moreover, the phenomenon of quantum computation casts traditional or "classical" cryptographic algorithms in a new light, with some cryptosystems widely considered vulnerable[83] to sufficiently powerful quantum computers. For all these reasons, "crypto-agility" is emerging as an important requirement and valuable process inside any organization responsible for maintaining a system (or part of one) that relies on cryptography to protect missions. It is also worth noting that crypto-agility represents an important and challenging consideration for long missions, where security methods may have to remain robust for extended periods. Companies should plan and design capacity that allows them to quickly update cryptographic methods without significant change to information systems, to retain regulatory compliance, reduce the likelihood of errors in new implementations, and mitigate security risks.[84]

Section 4 has focused on the identification of risk for space systems and its responses. As has been illustrated, an all-around response is necessary in order to be protected against hostile cyber operations. These responses range from the creation of incident response teams, international cooperation, internal IT governance policies, and technology strategies that can be adopted into a space system in order to mitigate hostile cyber operations.

5 Application and Enforcement of the Law

The following sections of the chapter focus on the legal aftermath of a cyber operation. Section 5 deals with the public international law perspectives from an already established set of treaties and principles. It will therefore focus on

82 Consultative Committee for Space Data Systems, *CCSDS Cryptographic Algorithms. Recommendation for Space Data System Practices* (2019).

83 Vasileios Mavroeidis et al., "The Impact of Quantum Computing on Present Cryptography," arXiv preprint arXiv:1804.00200 (2018).

84 Lily Chen et al., "Report on Post-quantum Cryptography," v. 12 (US Department of Commerce, National Institute of Standards and Technology 2016).

State-to-State hostile cyber operations. Section 5.1 starts by outlining the main challenges of applying principles of international law to the novel threat that hostile cyber operations pose to States. This is followed by an investigation of the source of a cyber attack and the challenges relating to legal attribution under Section 5.2, from locating the source of the attack to the political willingness of States to publicly acknowledge State attribution of a hostile cyber operation. Whereas part A and B outline the challenges to the application of public international law to cyber operations, part C provides a practical example of how the rules under *jus ad bello* and *jus in bello* regarding collateral damages can be applied to cyber operations against space systems.

5.1 *The Context of Hostile Cyber Operations in International Law*

The intricate dematerialized domain of cyber operations poses challenges to the application of international law. After decades of world-wide development of cyber capabilities and the completion of countless hostile operations at the trans-national level, the international community is still struggling to create a proper regulatory framework for these types of activities. The reason behind this impasse is two-fold. First, the cyber domain's technical aspects hinder the conventional understanding and application of international law. Secondly, there is a certain reluctance – *rectius*, a lack of political will – by States with strong cyber capabilities to develop an international framework against hostile cyber operations.

5.1.1 Legal Responses to Cyber Issues

From a technical perspective, it is possible to identify two elements that are particularly problematic for the application of international law to cyber operations: 1) the constant evolution of technological capabilities, which poses a serious risk of obsolescence to any codification attempt; and 2) the issue of identifying the original source of cyber activities which can represent an obstacle to the application of the attributability principle.[85]

Due to the increased complexity when applied to the cyber world, attribution needs some further insights. Simply put, the issue of attribution from a legal perspective can be described in the following terms. Every system of law is based on a basic principle: whoever breaches a legal obligation is responsible for the consequences caused by that breach. However, in order to hold the wrongdoer responsible, the breach needs to be attributed to the wrongdoer

85 For an analysis of the issue of attribution from a non-legal perspective see below at Section 5.2.

through sufficient evidence that identifies that party as the cause of such breach.

Transposed in the realm of international cyber operations, this basic legal principle entails that any time a party conducts a hostile cyber operation against a foreign party, the latter cannot respond unless it is able to identify with evidence the source of the operation. This is true irrespective of the target's nature, whether it is private assets or public infrastructure. For civilian law enforcement authorities and governmental entities, attribution is an essential and necessary condition to further legal action.

From a practical perspective, attributing a cross-border cyber offense to a specific foreign party poses certain difficulties. The first layer of challenges comes from the specifics of cyber operations, which, as described in Section 5.2 can be performed from remote locations while concealing the operator's identity and remaining undetected for an extended period. The collection of digital evidence in foreign jurisdictions is an additional layer of challenges as it requires a transnational investigation.[86] In such cases, access to evidence entails the collaboration of the State where the source of the attack is located.[87]

Such collaboration is usually achieved by signing Mutual Legal Assistance Treaties (MLATs). MLATs are agreements between two or more countries to provide assistance on criminal legal matters.[88] However, even assuming that MLATs cover all States involved in a transnational cyber investigation, enforcing such treaties requires expertise and resources that are not accessible to all States. Developing nations may lack the capacity to adequately investigate and prosecute cybercrimes or assist in cross-border investigations, even if they have the willingness to comply.[89]

---

86 There are different actors that provide assistance in cross-border cybercrime investigations with the aim of facilitating collaborative efforts among international parties. Such actors are national criminal justice agencies, regional agencies, such as the European Union Agency for Law Enforcement Cooperation (Europol) promoting law enforcement cooperation in the European Union, and Eurojust promoting judicial cooperation in the European Union, and international agencies, such as INTERPOL (i.e., International Criminal Police Organization). For more information on the role and function of these actors see UNODC, "Who Conducts Cybercrime Investigation?" (n.d.) https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/who-conducts-cybercrime-investigations.html.

87 Dorothy Denning et al., *Internet Besieged: Countering Cyberspace Scofflaws* (ACM Press, 1998).

88 A good example of how MLATs work is provided by the EU, whose Member States collaborate under Council Act 2000/C 197/01 of 29 May 2000 and who also has signed MLATs with the US and Japan.

89 Alexandra Perloff-Giles, "Transnational Cyber Offenses: Overcoming Jurisdictional Challenges," *The Yale Journal of International Law*, v. 43/191 (2018): 207. See also: Jan

Moreover, collecting evidence is not enough. Legislative and adjudicative jurisdiction are established when the perpetrator is identified and a judgment is entered against the defendant. However, there is still the problem of extradition of foreign citizens. This issue requires either a treaty signed between the two States involved or a diplomatic agreement to extradite the wrongdoer. As a result, cyber operators conduct their activities in a domain dominated by little real threat of international legal liability.[90]

A possible solution to this situation could be a broadly ratified international agreement, harmonizing domestic regulations on cyber activities and providing a tool for facilitated cooperation among States. The first step in that direction was taken with the adoption of the Convention on Cybercrime, or the Budapest Convention, under the Council of Europe's auspices.[91] The Convention entered into force on 1 July 2004 and is open for signature by the member States and the non-member States that have participated in its elaboration and accession by other non-member States. The purpose of the Convention is to create a common policy aimed at protecting society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international cooperation. To this end, it contains different provisions on facilitating the detection, investigation, and prosecution of hostile cyber operations at both domestic and international levels. Furthermore, the Convention provides arrangements for fast and reliable international cooperation.[92]

Despite the positive result achieved with the Budapest Convention[93] and its considerable number of ratifications (65 as of January 2021),[94] the Convention is not beyond reproach. There is a reservation mechanism embedded in the Convention that allows different States to opt-out of some of its provisions. Moreover, missing definitions of key terms or using vague ones has lessened the efficacy of its provisions. Finally, the absence of enforcement mechanisms opens the door to inconsistencies in its implementation.[95]

Kleijssen et al., "Cybercrime, Evidence and Territoriality: Issues and Options," *Netherlands Yearbook of International Law 2016* (2016): 147 *et seg*.

90 Perloff-Giles, *Transnational Cyber Offenses*, 208.

91 Council of Europe, *Budapest Convention on Cybercrime*, ETS No. 185 (adopted in Budapest on 23 November 2001).

92 *Id.*, especially Art. 11 *et seq.*, but also Arts. 29 and 30.

93 For a recent account on the impact of this instrument see Council of Europe, *The Budapest Convention on Cybercrime: Benefits and Impact in Practice*, T-CY(2020)16 (13 July 2020).

94 See the list provided by the official website of the Budapest Convention, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=C0kA8O8d.

95 For more on the skepticism over the Budapest Convention see Allison Peters et al., "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime,"

In parallel to the Budapest Convention, which is mainly the expression of like-minded Western States, there have also been other regional efforts to promote international agreements on hostile cyber activities. Examples are the 2002 *Asia-Pacific Economic Cooperation* (APEC) *Cybersecurity Strategy* and the subsequent 2005 APEC *Strategy to Ensure a Trusted, Secure and Sustainable Online Environment*, which aim at promoting information and network security, harmonising frameworks for securing transactions and communications, and combating cybercrime. The 2005 *Economic Community of West African States* (ECOWAS) *Directive on Fighting Cybercrime* is another example, which provides an interesting legal framework with substantive and procedural norms against cybercrimes, as well as the 2014 *African Union Convention on Cybersecurity and Personal Data Protection*, whose aim is to address the need for harmonized legislation in the area of cybersecurity.

5.1.2 Legal and Political Responses in State-to-State Cyber Relations

The practical dynamics related to the application of the attribution principle, in terms of investigation and collection of evidence, apply in equal terms when the transnational cyber offense is undertaken by private individuals or by national governments. As US Deputy Secretary of Defense William Lynn stated in 2010, "Whereas a missile comes with a return address, a computer virus generally does not."[96] Thus, attributing a malicious activity to a State can be a politically sensitive matter. Public statements of attribution have been met with suspicion, confusion, and a request for greater transparency about the investigation and its evidential basis.[97] A possible solution can be the creation of an international independent investigation authority. A joint attribution mechanism overseen by an international authority would greatly improve States' individual and collective ability to decide who is responsible for an attack and decide how to respond. This would go a long way towards solving the problem of monitoring and enforcement.[98]

Journal of National Law and Security, v.10/3 (2020); and Perloff-Giles, *Transnational Cyber Offenses*, 217.

96 William J. Lynn, "Defending a New Domain – The Pentagon's Cyberstrategy" (2010) https://archive.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx.

97 John Davis II et al., *Stateless Attribution – Toward International Accountability in Cyber Space* (RAND 2017): v. Moreover, it is necessary to demonstrate that the hacker was acting as an organ of the state in order to consider the cyber-attack as an act of the state under international law. *See* International Law Committee, *Responsibility of States for Internationally Wrongful Acts*, annex to General Assembly resolution 56/83 of 12 December 2001, and corrected by document A/56/49(Vol. I)/Corr.4, Arts. 4, 5 and 8.

98 Mette Eilstrup-Sangiovanni, "Why the World Needs an International Cyberwar Convention," *Philosophy & Technology*, v. 31/3 (2018): 400.

Once a hostile cyber operation is legitimately attributed to a State actor, the victim State has the possibility to put in place a legal response. However, such possibility revolves around the question: can a State-sponsored malicious cyber act constitute a breach of an international obligation?

The reason why this question is so important is that exercising the so-called "right to respond" entails an underlying breach of international law and it is only based on such breach that it is possible to determine the legal reaction available to the victim-State. When it comes to cyber operations the precise nature of a breach often remains unclear.[99] The main reason for this uncertainty lies in the absence of a proper international cyber law framework setting precise obligations on States' operations in the cyber domain. Therefore, it is often hard to determine which obligations have been breached. In this context, a possible solution is to resort to the general principles of international law, such as the prohibition to violate the sovereignty of another State, the duty of due diligence, and the obligation of causing no-harm (or, in case of telecommunication activities, no harmful interference).[100] They are all relevant concepts that can be used by a State to claim that a malicious cyber act of another State violated an international obligation. As a matter of fact, the link between these concepts and cyber operations has been at the centre of the work of the International Group of Experts that prepared the Tallinn Manual 2.0,[101] the most relevant non-governmental guide (sponsored by the NATO CCD COE) on how existing international law applies to cyber activities. Assuming that a State-sponsored malicious cyber act constituted a violation of a general principle of international law, how can the victim State legally respond?

According to the literature on the matter, even if a hostile cyber operation was legitimately attributed to a State and it was demonstrated that such conduct breached an international obligation, the crucial factor to consider is the impact of such an operation on the victim State.[102] The legal response

---

99 See the examples and analysis of this aspect carried by Harriet Moynihan, "The Application of International Law to State Cyberattacks Sovereignty and Non-intervention" (Chatham House Research Paper, Dec. 2019): 4.

100 On the intersection between cyber operations and telecommunication activities *see* Ingo Baumann, "GNSS Cybersecurity Threats: An International Law Perspective," *Inside GNSS* (3 June 2019) https://insidegnss.com/gnss-cybersecurity-threats-an-international-law-perspective/.

101 Michael Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017).

102 *See*, in particular, Eric Talbot Jensen, "The Tallinn Manual 2.0: Highlights and Insights," *Georgetown Journal of International Law*, v. 48 (2017): 735 *et seq*. *See also* W. Stahl, "The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity," *Georgia Journal of International and Comparative Law*,

available to the latter depends on the harm it suffered. Obviously, it is not easy to determine how large was the scale of a hostile cyber operation after it hit the targeted State, but the response, in any case, has to be necessary and proportional. In other terms, the scale and effects of such operations define how the victim State can legally respond, from simple diplomatic measures to retaliation or counter-attacks. As a matter of fact, the choice of the most adequate reaction from the victim State is connected to the long-standing debate surrounding the definitional threshold of an armed attack according to international humanitarian law.[103] In general, it can be said that a hostile cyber operation must amount to a "use of force" under Article 2(4) of the UN Charter for the victim State to resolve to respond with the use of (defensive) force.

In the end, legal responses to hostile cyber operations in State-to-State relations are still a grey area of law. Considering the accelerating use of the cyber domain for malicious activities, there is pressure to find a solution at the international level. The current geopolitical climate, however, is slowing this process. In particular, technologically advanced States are generally skeptical of the idea of constraining their cyber activities with tight rules, as these rules can be ineffective against States that do not share the same commitment to the "rule of law." Viewing international law as asymmetrically disadvantageous, these States prefer to rely on self-help such as offensive tools and credible warnings, rather than international law, to safeguard their cyberspace.[104]

The result is that hostile cyber operations can still be conducted today in a "favorable" legal context. Both technical and political elements play a role in rendering the situation legally unsustainable. Vagueness and uncertainty leave more freedom to all actors, but also create the basis for tensions and conflicts, which render the cyber domain more "unstable" for all involved. Without certainty of the penalty, any system of law is inefficient, as its function is to dissuade and deter individuals from committing rogue actions. For this reason, building confidence among States on the measures necessary to repress vicious uses of the cyber world can bring great benefits to all, both in terms of

---

v. 40 (2011): 247 *et seq*. For a diverging opinion, stating that hostile cyber activities "may be undertaken, just as espionage is, without sanction from the international community," see G. Brown et al., "The Customary International Law of Cyberspace," *Strategic Studies Quarterly*, v. 6/3 (2012): 138.

103 Michael Schmitt, "'Attack' as a Term of Art in International Law: The Cyber Operations Context," *Proceedings of the 4th International Conference on Cyber Conflict* (2012): 283.

104 Yuwal Shany et al., "An International Attribution Mechanism for Hostile Cyber Operations," *International Law Studies*, v. 96 (2020): 217.

international security and in terms of safety of operations, especially the ones highly dependent on cyber technologies, like outer space activities.

The first step in that direction is a well-functioning attribution mechanism which, as underlined above, represents the basic and main problem when dealing with hostile cyber operations.[105] Thus, the next section goes on to look at the problems surrounding the detection of a hostile cyber operation's source.

5.2 *Source of Hostile Cyber Operations*

The lack of recognized standards of proof for attributing cyber activities in international law increases the uncertainty about the actor's identity.[106] Hence, the victim of a hostile cyber operation faces a double jeopardy, namely the breach itself and the legal system's gaps to make the situation stop, to execute self-defense operations, and to obtain reparation.[107]

Detecting a hostile cyber operation is the first step of attribution. When we consider the source of a cyber operation, it is meaningful to map the system architecture including the infrastructure and networks. In the realm of cyberspace, interconnected systems increase the impact of hostile cyber operations. As described in Section 2.1.1, pieces of hardware, software, and memory interact with other components. They can be vectors of a hostile operation through the two-way radio links connecting the ground and space segment or through the chips embedded in space systems. The configuration of such a hostile operation is continually evolving. As stated by Joseph Nye: "It is far safer to send electrons than agents through customs and immigration controls."[108] Therefore, knowing where data and lines of codes are, is extensively challenging as they can be duplicated, transferred, and stored in multiple locations.

5.2.1 Techniques of Attribution: Localization and Identification

After detecting an attack against a space object, identifying its source in cyberspace is difficult, but attributing the operation to one or several actors is even more challenging.[109] Identifying the perpetrators of a malicious cyber operation requires certain key indicators to localize the direct source of the

105 Beyza Unal, "Responsible Behaviour in Outer Space Protects Everyone," Chatham House (5 March 2021).

106 Nicholas Tsagourias, "Cyber attacks, Self-defence and the Problem of Attribution," *Journal of Conflict & Security Law* (2012): 235.

107 Erik M. Mudrinich, "Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem," *Air Force Law Review*, v. 68 (2012): 172.

108 Joseph S. Nye, Jr, *Cyber Power* (Harvard Kennedy School 2010): 12.

109 Carlo, Lacroix & Zarkan, "The Challenge of Protecting Space-based Assets against Cyber Threats," 5.

activity, whether it is a machine or a human operator. While the perpetrator of an operation is necessarily located within a State's jurisdiction, relying on a geographical origin is not sufficient to attribute an operation in cyberspace. The reason for this is the fact that attacks can be delayed or be performed through a big amount of multiple networks, routers, or servers and through many jurisdictions.

Despite being faced with many challenges in cyberspace, States are starting to discuss individual solutions to address cyber issues with the risk of fragmenting the international normative and legal framework.[110] Such a strategy will soon reach its limit. In *Information Warfare and International Law*, the authors rightfully describe that "electrons may flow through networks freely across international borders, but the authority of agents of national governments does not."[111] International cooperation and the development of a global governance system for cyber activities are keys to increasing cyber awareness and being able to prosecute cybercriminals.

There is a very small possibility that a cyber hostile operation can be attributed just after an incident occurred.[112] Prudence requires the avoidance of political tensions and misinterpretations, which makes the willingness to want to prove attribution difficult. The ground segment uses integrated computer networks scattered across the world to send and receive data from satellites, control them, and monitor their parameters. Hence the ground segment is an ideal and vulnerable target to hostile cyber operations.

Satellites do not only use the air as a communication medium over the surface of the Earth. At any time, satellites are in radio visibility of a multitude of States and potential malicious orbiting spacecraft used as cyber-threat vectors. When located in MEO or in LEO, satellites are not constantly communicating with their mission's ground segment, which increases the risk of undetected interactions with a threat actor. The difficulty of detecting and attributing a malicious act increases when its source is located in outer space, especially if the radiofrequency medium is used as a point of entry. Therefore, the

110 Kerstin Vignard, "Launch Event: Joint Initiative on the Digitalization of Conflict," Academy of International Humanitarian Law and Human Rights (October 29, 2020) https://www.youtube.com/watch?v=KbKU5FRnYv8.

111 Lawrence T. Greenberg, Seymour E. Goodman, & Kevin J. Soo Hoo, *Information Warfare and International Law*, (National Defense University Press 1998): 23.

112 Duncan B. Hollis, "Why States Need an International Law for Information Operations," *Lewis & Clark Law Review*, v. 11 (2007): 1031–1032; and Duncan B. Hollis, "An e-SOS for Cyberspace," *Harvard International Law Journal,* Vol. 52 (2011): 392.

perpetrators of an attack may not only mask their positioning on the ground or spoof their IP address, but also be located anywhere on Earth.[113]

Besides geography, other elements can also be used to determine the source of an operation, such as the type of operation and its estimated cost, how disruptive it is, the type of target and collateral damages, as well as the time of the attack. Some authors have used methodical analysis of an operation premise to trace back threat agentsand sources by considering the ecosystem of hostile cyber operations to include on the one hand adversarial actors and on the other hand insider actors.[114] Other authors do not only consider the identity of the threat agents, but also the type of services affected and the impact of the operation.[115] Determining the motivations and objectives of the threat agent, as well as the methods and techniques they used is essential to trace the malicious operation back to its source.[116] Additionally, establishing the causes of the breach, the services affected, and the impact of the event is important for assessing the objectives and motivations of the perpetrators. Altogether, these elements are evidence for a State to trace back who could be behind the operation committed within its territory, jurisdiction, or against one or several of its nationals.

Actors' unwillingness to reveal they have suffered from a breach in their system, makes it both difficult to understand what is responsible State behavior when using digital technologies[117] and which cyber operations, if any, qualify as use of force under the Charter of the United Nations.[118] As a result, a persistent and disruptive operation in cyberspace that threatens international peace, security, and harms an actor's interests may never be acknowledged in order to prevent the creation of a precedent.

Even though in most cases, when committing hostile cyber operations, groups such as terrorists or hacktivists will claim responsibility for it,[119] the

113 David Wheeler & Gregory Larsen, *Techniques for Cyber Attack Attribution* (Institute for Defense Analyses 2003): 43.

114 Sébastien Bonnart et al., "The Mission as a Tree: A Novel Approach to Identifying Cyber Threats to Satellites."

115 Keith Harrison, & Gregory White, "A Taxonomy of Cyber Events Affecting Communities" *44th Hawaii International Conference System Sciences* (2011).

116 Herbert Lin, "Attribution of Malicious Cyber Incidents," Aegis Paper Series No. 1607 (Hoover Institution 2016): 2.

117 Lora Saalman, ed., *Integrating Cybersecurity and Critical Infrastructure: National, Regional and International Approaches* SIPRI (2018): 2 https://www.sipri.org/sites/default/files/2018-04/integrating_cybersecurity_0.pdf.

118 Charter of the United Nations, Art. 2(4) (1945).

119 Lee Jarvis, Stuart MacDonald, & Thomas M. Chen, *Terrorism Online: Politics, Law and Technology* (Routledge, 2016): 175.

author of a hostile operation does not always claim credit for it as "cyber conflict remains in the grey area between war and peace."[120] Tracking a hostile cyber operation is tough as the author of an hostile operation can conceal its identity or steal another user's identity.[121] Cyber weapons are easily accessible to non-governmental actors and the more open and spread an infrastructure is, the more vulnerable it becomes. Therefore, localization is more challenging as the characteristics of the operations change. For instance, time is shortened so distances do not count as much in outer space as it is the case for operations on the ground, sea, or air space.[122]

However, identifying the category and the State of origin of the threat agent is the first step to attribute a malicious cyber operation to a specific public or private actor. Not all cyber-attacks threaten national security. As identified in *The Challenge of Protecting Space-based Assets against Cyber Threats*, agents can be private entities acting against their competitors or more generally, natural persons perpetrating "an attack with a political aim or wanting to demonstrate an ability to make such a manoeuvre."[123] When identified, agents must be held responsible so the activities they carry out in cyberspace are compliant with their legal obligations.

5.2.2 Responsibility of State Actors and Non-state Actors: The Question of the Positive Obligations

In *The Mission as a Tree*, Bonnart and his fellow authors make a distinction between adversarial and insider agents and sources.[124] Among them are terrorists and criminals, foreign states, subversive or political activists, computer hackers, commercial competitors, dishonest personal, or inadvertent actions of staff members.

Three categories of perpetrators can be identified depending on the nature of the actors: natural persons, private economic actors, and Nation State actors. In *Cyberconflicts and National Security*, Schneier suggests that a common feature of hostile cyber operations is the use of "the same weaponry" and the

120 David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (Scribe Publications Pty Ltd, 2018): xi.

121 Martin Motte, *La mesure de la force* (Tallandier, 2018): 350.

122 Brett Williams, "Forward Defence Postures in Developing Cybersecurity Capabilities| #CSGlobal20 | s06e35," *CYBERSEC Forum*, (12 October 2020) https://www.youtube.com/watch?v=TOToVVRAWDY.

123 Carlo, Lacroix & Zarkan, "The Challenge of Protecting Space-based Assets against Cyber Threats," 5.

124 Bonnart et al., "The Mission as a Tree," 4.

exploitation of "the same vulnerabilities," whoever the perpetrator may be.[125] In other words, not all attacks are an act of war executed by another State or military force. Natural persons, acting either as a part of a group or operating on their own, can be motivated by criminal intent[126] and use cyberspace to commit espionage, subversion, fraud, and sabotage,[127] as well as personal data breaches.[128]

The reason for an attack could also be political. Often called 'hacktivism,' the most common types of operations are "virtual sit-ins and blockades, automated email bombs, web hacks and computer break-ins, and computer viruses and worms."[129] These operations can qualify as offensive. They are often executed with the aim of getting the attention of the media for their cause or disrupting normal operations of actors or activities they frown upon. Another way of "hackting" would be to collect a target's documents, policy statements, and discussions about the activities or actors they are willing to act against. It appears that some individuals are also committing hostile cyber operations on behalf of a bigger entity such as a company, to take down a competitor, a group, or a State.[130]

Also, private economic actors, including in the space sector, are less likely to disclose cybersecurity incidents and data breaches they suffered from, as they might subsequently suffer from a negative impact both economically and in reputationally. To some extent, the devastating effects of hostile cyber operations involving private economic actors have an impact on national security. The recent SolarWinds case is the perfect example of how a hostile cyber operation carried out against Fortune 500 and smaller companies can become a

125 Bruce Schneier, "Cyberconflicts and National Security," *UN Chronicle* (n.d.) https://www.un.org/en/chronicle/article/cyberconflicts-and-national-security.

126 "Deloitte Puts the Spotlight on the Cost of Cyber-Crime Operations in New Threat Study", Deloitte (2018) https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-announces-new-cyber-threat-study-on-criminal-operational-cost.html.

127 Olivier Kempf, "Cybersécurité et Résilience : Les Grandes Oubliées des Territoires," Fondation pour la Recherche Stratégique, Note de la FRS n°39/2020 (2020) https://www.frstrategie.org/publications/notes/cybersecurite-resilience-grandes-oubliees-territoires-2020.

128 Bob Gibbs, "Potential PII Compromise of NASA Servers, Internal Memo," NASA HQ (2018) http://spaceref.com/news/viewsr.html?pid=52074.

129 Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla & David Ronfeldt (RAND Corporation (2001)): 263.

130 Carlo, Lacroix, & Zarkan, "The Challenge of Protecting Space-based Assets against Cyber Threats," 5.

national issue.[131] However, private economic actors cannot be responsible for protecting the national security interests of their State.

In *The Spectrum of National Responsibility for Cyberattacks*, Healey points out that finding who is responsible for a hostile cyber operation is more important than the technical attribution. Healey suggests a political approach involving nations' responsibility "for major attacks from their national territory or citizens,"[132] including when said nation ignored or prohibited the operation.[133] The author considers that nations "unable to stop or investigate attacks coming from its cyberterritory" or "having an insecure national information infrastructure" contribute to the lack of security of their national cyberspace, even in a passive way.[134]

Strictly speaking, network infrastructure and devices are located within the boundaries of a nation's sovereign territory. Hence the country is responsible for building a cooperative and robust framework to address hostile cyber operations within their sovereign territory, especially if they travel through multiple jurisdictions. In *Internet Besieged: Countering Cyberspace Scofflaws*, the authors state that tracing the source of an operation requires "the cooperation of every system administrator, and network service provider on the path."[135]

When addressing the question of attribution of conduct to Nation-State actors, it has been suggested that "the activity of a State is nothing but the activity of individuals that the law imputes to the State."[136] Hence, operations led or supervised by State organs and entities subordinated to a State are

131 Christopher Bing & Joseph Menn, "After Big Hack of US Government, Biden Enlists 'World Class' Cybersecurity Team," *Reuters* (January 2021), https://www.reuters.com/article/us-usa-biden-cyber-idUSKBN29R18I; Brad Smith, "A Moment of Reckoning: The Need for a Strong and Global Cybersecurity Response," *Microsoft Blog* (December 2020), https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/; Lily Hay Newman, "The SolarWinds Hackers Used Tactics Other Groups Will Copy," *Wired* (January 2021), https://www.wired.com/story/solarwinds-hacker-methods-copycats/; and Martin Untersinger, "L'affaire SolarWinds, une des opérations de cyberespionnage « les plus sophistiquées de la décennie »" *Pixels, Le Monde*, (January 2021), https://www.lemonde.fr/pixels/article/2021/01/27/la-compromission-de-solarwinds-une-des-affaires-de-cyberespionnage-les-plus-longues-et-les-plus-sophistiquees-de-la-decennie_6067777_4408996.html.

132 Jason Healey, "The Spectrum of National Responsibility for Cyberattacks," *The Brown Journal of World Affairs*, v. 18, no. 1 (2011): 57.

133 *Id.* at 59–60.

134 *Id.* at 62–63.

135 Denning et al., "Internet Besieged," 35.

136 Dionosio Anzilotti, *Cours de droit international* (Panthéon Assas, 1929–1999): 469.

attributable to this State.[137] In the context of a hostile cyber operation, the victim has to prove that the operation meets all the criteria under international law that permit attribution of behaviour to a State, one of them being the control over the operation, whether it is an "effective control"[138] or an "overall control" approach.[139] Not every cyber operation coming from computing systems located within a State's territory may be considered as having been launched from this State. However, sovereignty over cyberspace is at the core of the attribution issue. States should not allow their territory to be used for malicious activities against space systems.[140] "If such activities are carried out anyway, the control exercised by a State over its territory [does not mean] that [a] State necessarily knew, or ought to have known, of any unlawful act perpetrated therein, nor yet that it necessarily knew, or should have known, the authors."[141] However, a State could be expected to act as a reasonable and prudent actor by being aware of the cyber and space infrastructure developed within their jurisdiction by their nationals and therefore, should work on national strategies to address vulnerabilities.

Generally speaking, even though some States developed special legal provisions and a policy strategy addressing cyber threats,[142] the attribution challenge requires strong global cyber policies to trace the trail of a malicious operation. In *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, Shackleford and his fellow authors argue that transit States whose territory is used for the transit of cyber operations, have due diligence obligations when the State's infrastructure was not initially set up for malicious purposes.[143] Due diligence is a principle of international law requiring states to prevent their territory from being used to harm other

137 Djamchid Momtaz, "Part III. The Sources of International Responsibility, Ch.19.1 Attribution of Conduct to the State: State Organs and Entities Empowered to Exercise Elements of Governmental Authority," in *The Law of International Responsibility*, ed. James Crawford, Alain Pellet et al., (2010): 238.

138 *Nicaragua v. United States of America*, I.C.J. 1984, para. 99.

139 *The Prosecutor v. Dusko Tadić*, IT-94-1-AR72, ICTY Appeals Chamber, Decision, 2 October 1995, para. 120 and Scott J. Shackelford & Richard B. Andres, "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem," *Georgetown Journal of International Law*, v. 42 (2011): 971–1017.

140 *Case of the Corfu Channel* (*United Kingdom of Great Britain and Northern Ireland v. Albania*), 1949 I.C.J. Reports 1949, p. 244.

141 *Id.*

142 UNIDIR, Cyber Policy Portal (n.d.) https://unidir.org/cpp/en/.

143 Scott J. Shackelford, Scott Russell, & Andreas Kuehn, "Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors," *Chicago Journal of International Law*, v.17 (2016): 1.

States, following the Latin maxim: *sic utere tuo ut alienum non laedas* ('Use your own property in such a way that you do not injure other people's').[144] In the Case of the S.S. Lotus before the Permanent Court of International Justice in 1927, Justice Moore declared: "[i]t is well settled that a State is bound to use due diligence to prevent the commission within its dominions of criminal acts against another nation or its people."[145]

The International Group of Experts working on the Tallinn Manual 2.0 also discussed the issue. They observed that transit States must comply with due diligence requirements when they are aware of a hostile cyber operation that would reach the "requisite threshold of harm" if they are able to take measures to make it cease.[146] The latter condition makes sense regarding the existing technological differences between developed and less-developed States. The former condition however seems to weaken the whole global infrastructure as States can argue that they did not know such an operation was being carried out or considered the operation did not reach the threshold.

However, hostile cyber operations can be very complex, the lines of code sent from a system to another are not always recognizable, and only become intelligible and operational when reaching their target. For instance, Stuxnet was activated only on the Iranian systems it targeted.[147] In this case, identifying the transit of a hostile cyber operation becomes almost impossible for less technology-advanced States. In the *Tallinn Manual 2.0*, a transit State's due diligence obligation is reduced to prevent any disproportionate burdens on these less technology-advanced States.[148]

The Public International Law regime may apply to hostile cyber operations against satellites if States take measures to hold other parties accountable and deepen their collaboration to encourage responsible behavior in both outer space and cyberspace. By acknowledging the existing security issues and identifying the potential threats to space systems and ground segments, States could bridge the legal gaps and provide more clarity to prevent disastrous situations that would more likely involve collateral victims.

---

144 "Sic utere tuo ut alienum non laedas," *Oxford Reference* (n.d.) https://www.oxfordreference.com/view/10.1093/oi/authority.20110803100504563.

145 *Case of the S.S. Lotus* (*France v. Turkey*), 1927 PCIJ Series A, No. 10. Justice Moore at 88, referencing the US Supreme Court case of United States v. Arjona, 120 US 479 (1887).

146 Schmitt, ed., *Tallinn Manual 2.0*, 33–34.

147 Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown Publishers, 2014).

148 Schmitt, ed., *Tallinn Manual 2.0*, 33–34.

5.3 *Collateral Victims*

Section 5.3 will examine the legal boundaries that exist for target precision for a hostile cyber operation when it comes to collateral victims. It will provide an overview of what collateral damages could be in a cyber operation against a space system, and then apply the rules under *jus ad bellum* followed by *jus in bello*. In this regard, it is noted that the application of international law, including *jus ad bellum* and *jus in bello*, to a hostile cyber activity is a legal grey area as outlined in Section 5.1.2. Without state practice or opinion, this section is instead largely guided by the international experts of the *Tallinn Manual 2.0*, noting that this a non-binding document.

Collateral damage can cause both direct and indirect effects.[149] Direct effects are 'the immediate, first order consequences (of a cyber attack), unaltered by intervening events or mechanisms.' Indirect effects are those that are 'delayed and/or displaced second-, third-, and higher-order consequences of action, created through intermediate events or mechanisms.'[150]

As outlined in Section 4.1 above, the space domain supports much of the world's critical infrastructure. Many of these systems are interlinked and serve several purposes. This is why hacking a weather satellite can have widespread effects ranging from blocking signals that disaster relief relies on to causing implications for our financial services. The existence of interlinked systems creates an increased threat consequence for collateral damage when satellites are used as a vector for an attack. The *Tallinn Manual 2.0* exemplifies collateral damage in scenarios where a cyber operation targets a military object through civilian communication cables, satellite, or other infrastructure causing harm to the infrastructure through different forms: both due to the transit and also because of the cyberattack itself.[151]

The question regarding collateral victims in peacetime, is whether a cyber operation may fall under *jus ad bellum.* These are the rules found in the UN Charter primarily under Article 2(4) regarding the prohibition of the use of force and Article 51 regarding the right to self-defense in response to an armed attack. In a cyber context, the question is, whether a hostile cyber operation can be qualified as an 'use of force' or 'armed attack.' Several States consider that it is possible for a cyber operation to meet this threshold, however, there is not an agreement about when that threshold is passed as it will depend on the

149 *Id.* at 472.

150 *Id. quoting* Joint Chiefs of Staff, Joint publication 3–60 and Joint Targeting 1–10 (2007).

151 Schmitt*, Tallinn Manual 2.0,* 471.

specific circumstances of the case and its consequences.[152] Without an agreed threshold there is no clarity, leaving any evaluation uncertain. This makes it difficult to evaluate whether a victim that is a direct or indirect target of a hostile cyber operation can claim that this operation broke the prohibition on the use of force. Furthermore, it also makes it difficult to determine whether the effects are severe enough for it to justify self-defense. Where most States do not address the specific circumstances, the Dutch Minister of Defence, Ank Bijleveld gave an example of a hostile cyber operation that could reach the use of force threshold through an attack that targets the entire Dutch financial system.[153] To make this scenario more concrete, a hostile state may be interested in attacking another state's GNSS for the purpose of impeding their transportation system. If this also affected financial services that rely on this signal, the Dutch may, according to their Minister of Defence's previous statement, support the application of international law. However, in general States have not given very clear statements. The *Tallinn Manual 2.0* highlights factors that should be included when assessing whether a non-destructive cyber operation reaches the use of force threshold, including severity, directness, immediacy, invasiveness, measurability of effects, military character of the operation, degree of State involvement, presumptive legality, prevailing political environment, identity of the attacker, and nature of the target.[154]

For wartime operations, *jus in bello* or International Humanitarian Law are the rules of the law of armed conflict. Collateral damage refers to the incidental loss of civilian life, injury to civilians, or damage to civilian objects.[155] In itself, collateral damage is not unlawful under *jus in bello,* but there are certain restrictions. These restrictions include, among others, the principle of distinction, which ensures that attacks are directed at legitimate military objectives, and minimize the collateral damage.[156] The restrictions also include the principle of proportionality, which insists that the military advantage to be gained from attacking a target outweighs the anticipated incidental civilian loss of life

152 Micheal Schmitt, "France's Major Statement on International Law and Cyber: An Assessment" *Just Security* (September 2019) https://www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/.

153 Ank Bijkeveld, "Keynote Address by the Minister of Defence, Ms. Ank Bijleveld, Marking the First Anniversary of the Tallinn Manual 2.0 on the 20th of June 2018" (2018) https://english.defensie.nl/downloads/speeches/2018/06/21/keynote-address-by-the-minister-of-defence-ms.-ank-bijleveld-marking-the-first-anniversary-of-the-tallinn-manual-2.0-on-the-20th-of-june-2018.

154 Schmitt*, Tallinn Manual 2.0,* 331–337.

155 *Id.* at *472.*

156 Articles 48 and 52(2) of the Additional Protocol I (1977) to the Geneva Conventions (1949).

and property.[157] The dual nature of information and communications infrastructure means that the implementation of *jus in bello* rules is challenging in cyberspace, and France, Germany and the United States have stated that a careful individual assessment should be applied in determining whether for example a civilian computer can be considered a military objective.[158]

Compliance with efforts to reduce the spread of malicious code can be used to determine how a cyber- attack conforms to the law of armed conflict. Collateral damage can be more difficult to estimate in cyber than regular warfare because of the interconnectedness of the systems. The spread of malicious code can be constrained by limiting the targets to the geography of the target's physical location, limiting the code to attack a certain function in a bigger system, be it a business, government, or other groups.[159]

Malware control examples include a "kill switch," as used for the Wannacry ransomware, that was able to be shut down through registration of an URL that the code was set to search.[160] Stoned and Morris Worm checked to see whether the target was already infected and if it was, the code would not re-infect it.[161] The code can also be limited to deliver the payload on a specific date, for example the Jerusalem virus that was triggered on any Friday 13th or the Michelangelo virus that deleted important data on March 6th.[162] The Stuxnet code was one of the most tightly controlled malware codes. The code limitations were achieved by developing a code that only targeted the control system used by the Iranian nuclear refinement centrifuges. In addition, the code deleted itself from infected USB drives after three infections and deleted itself after 21 days off of non-targeted systems.[163] However, these control

157 Article 51(5)(b) of the Additional Protocol I (1977) to the Geneva Conventions (1949).

158 "Military Objectives – International Cyber Law: Interactive Toolkit" (2021) *Cyberlaw.Ccdcoe.Org*. https://cyberlaw.ccdcoe.org/wiki/Military_objectives#cite_note-14. French Ministry of Armed Forces (Ministère de la Défense). "International Law Applied to Operations in Cyberspace," Délégation à l'information et à la communication de la défense. (2019).

159 Robert Fanelli & Gregory Conti, "A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context oof Lawful Armed Conflict," *4th International Conference on Cyber Conflict* (Tallinn: NATO CCD COE 2012): 6.

160 Lily Newman, "How An Accidental 'Kill Switch' Slowed Friday's Massive Ransomware Attack", *Wired* (2017) https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/.

161 David Raymond et al., "A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons," *5th International Conference on Cyber Conflict* (Tallinn: NATO CCD COE 2013): 5.

162 *Id* at 7.

163 *Id* at 8.

mechanisms were not completely functional. Stuxnet ended up infecting computer systems in Azerbaijan, Indonesia, India, Pakistan, and the United States. It has been claimed that Stuxnet created collateral damage to an Indian INSAT-4B Satellite although this has not been proven.[164]

The ability to control malware is only as good as the intelligence informing its development. Just as kinetic weapons should not be used without sufficient intelligence regarding the target, cyber weapons should not be used unless intelligence is available to adequately limit potential damage to non-target systems.

6 Private International Law Aftermath of the Hostile Cyber Operation

Section 6 will examine and analyze the private international aspects of a hostile cyber operation, which covers hostile cyber operations incidents where the perpetrators and victims are non-state actors. For example, a cyber operation could be covered by the contractual provisions or excluded by cross-waivers, which will be explored in Section 6.1. Disputes relating to a breach can be solved either through private arbitration or in Court. The former will be explored in Section 6.2, and the latter in Section 6.3 that will address the challenges relating to establishing jurisdiction in cases relating to unlawful cyber operations. Finally, Section 6.4 explores how private actors can protect themselves through insurance. An examination of the field of space and cyber insurance will be conducted, with a particular focus on its ability to help shape minimum requirements for risk mitigations.

6.1 *Contract Terms and Cross Waivers*

While dealing with the aftermath of hostile cyber operations is usually a reactive endeavor, there are legal mechanisms set in place from a proactive approach. The benefit of approaching the aftermath of hostile cyber operations from a proactive approach is that, in the context of space and cyber law, it provides the benefit of clarifying each party's responsibility and liability for certain events. Waivers of liability are a legal mechanism used in lieu of satellite contract arbitration when there is a satellite loss due to a launch failure or defective

164 Jeffrey Carr, "Did the Stuxnet Worm Kill India's INSAT-4B Satellite?" *Forbes* (2010) https://www.forbes.com/sites/firewall/2010/09/29/did-the-stuxnet-worm-kill-indias-insat-4b-satellite/?sh=3f0db2a7127d.

satellite in orbit.[165] When it comes to commercial satellite contracts there is no shortage of reciprocal waivers, also known as cross-waivers. Reciprocal waivers are customary in launch services, satellite purchase contracts, and related sub-contracts. For instance, both the United States and France have a comprehensive liability waiver regime in place to cover launches. The purpose of the reciprocal waiver of claims is twofold. First, reciprocal waivers limit the number of possible claims from the launch.[166] Second, these waivers eliminate the need for the parties to obtain property and casualty insurance to protect themselves against such claims. Moreover, cross-waivers are an efficient way to enable and promote private space companies to engage in high investment and high-risk scenarios.[167]

The most famous example of a cross-waiver is the liability arrangement applicable to inter-party damage aboard the International Space Station (ISS). Through this arrangement, except for gross negligence or willful misconduct, international activities on the ISS can function free from legal disputes that may arise from third parties. While the ISS is an exceptional case because of the intergovernmental agreements, it presents a promising sign that when issues of third-party liability rise it may be possible to adapt cross-waivers to the private enterprise side of the space industry.[168] This section continues by examining cross waivers in specific organizations, NASA and ESA, respectively.

In the United States provisions for cross-waivers are embedded in the Commercial Space Launch Act of 1984 (CSLA).[169] As a prerequisite to the launch license, the CSLA requires a US licensed launch provider to execute a waiver of liability when launching US government payloads. As a result, each party waives claims against and releases from liability the other party, its contractor, and subcontractors involved in the launch.[170] Moreover, each party assumes the risk and financial responsibility for loss or damage to the satellite. This is similar to what is embedded in the National Aeronautics and Space Act of 1958 that created NASA (which was later modified by the Commercial Space Launch Act of 1984 to allow civilian use of NASA systems in launching space vehicles).[171] As stated in the US Code of Federal Regulations, each Party agrees

165 Pamela L. Meredith and Marshall M Lammers, *Commercial Satellite Contract Arbitration: Special Legal Considerations* (2013): 423.

166 Commercial Space Launch Act Amendments of 1988, 100 Pub. L. 657 (1988).

167 Ingo Baumann and Lesley Jane Smith, *Contracting for Space: An Overview Of Contract Practice in The European Space Sector* (Ashgate Publishing Group 2011): 63.

168 *Id.*

169 Commercial Space Launch Act Amendments of 1984, 98 Pub. L. 575 (1984).

170 Meredith and Lammers, *Commercial Satellite Contract Arbitration*, 423.

171 National Aeronautics and Space Act, 85 Pub.L. 568 (1958).

to a cross-waiver of liability pursuant to which each Party waives all claims against any damage arising out of Protected Space Operations.[172] "Protected Space Operations" meaning all launch or transfer vehicle activities and payload activities on Earth, in outer space, or transit between Earth and outer space in implementation of an agreement for launch services. Due to how integrated cybersecurity operations are with space operations, it can be argued that even though cybersecurity provisions are not explicitly stated here, this section of the code does cover damages from cyberattacks.

Similar to NASA, ESA has embedded provisions regarding cross-waiver liability within their General Clauses and Conditions (GCC). One main difference is that with ESA the GCC only relates to damages of goods or to the staff. Moreover, similar to NASA, cybersecurity provisions are not explicitly mentioned in the GCC. However, while ESA is not subject to national or EU laws, there are provisions regarding personal data protection. ESA has adopted a Personal Data Protection Policy in line with the EU's General Data Protection Regulation.[173] This Personal Data Protection Policy, adopted by the ESA Council in 2017, established governance and operations necessary for the effective personal data protection. Unfortunately, as a result, it is unlikely that contracts between NASA or ESA with private companies will include provisions for claims for the type of cyberattacks the previous sections have outlined. Moreover, even with legal mechanisms in place, the space industry is still vulnerable to damages in the form of hostile cyber operations and cybersecurity breaches. The next section looks at how space companies and the legal system handles damages in the cyber context.

6.2 *International Commercial Arbitration*

International commercial arbitration involves contracts between sophisticated business parties in different countries. Companies doing business across borders regularly turn to international arbitration to resolve their disputes and aerospace companies are no exception. As stated in *Houston, We Have an Arbitration,* arbitration is well suited for aerospace companies because the "results that are quick, less intrusive, can be decided by people with expert-level knowledge of the subject matter, and can be resolved outside of the

172 14 C.F.R. § 1266.104 (2021).

173 Marco Ferrazzani and Ilaria Ziliolo, "ESA Facing Cybersecurity Issues," Presentation, University of Genoa (2018). https://www.eu-space.eu/images/2018/document/Slides/Slides-Ferrazzani-Zilioli.pdf. The EU's General Data Protect Regulation not only places obligations within the EU, but it can impose obligations onto organizations located anywhere if they collect data related to people in the EU.

public eye."[174] These characteristics are particularly relevant for an aerospace company because arbitration can provide added protection for its intellectual property and reputation. The reason for this is because arbitration provides confidentiality. From a civil procedural perspective, discovery is more limited than in the courts, which protects companies from inadvertently disclosing other sensitive intellectual property not related to the dispute at hand. As a result, the closed system of arbitration provides substantially more protection than public litigation in a national court.

6.3 *Prescriptive Jurisdiction vs Long-Arm Jurisdiction*

Cybercrime jurisdiction is established by factors such as the nationality of the offender, the nationality of the victim, and the impacts of the cybercrime on the interests and security of the state as long as there exists "a 'sufficient connection' or 'genuine link' between the hostile cyber operation and the state exercising jurisdiction."[175] This section offers a brief overview of the types of jurisdictional matters in the cybersecurity context, as well as the nuances that come into play from the inherent nature of cyberattacks.

The use of prescriptive jurisdiction under international law is largely inadequate for governing the modern challenge of cyberterrorism.[176] This is unsurprising given that these jurisdictional theories were formulated long before the creation of the Internet. Moreover, the Internet's borderless nature and the techniques used by cyberterrorists make it pointless to apply traditional notions of jurisdiction such as territoriality to hostile cyber operations. However, out of the classical theories of prescriptive jurisdiction under international law – territoriality, nationality, passive personality, protection, and universality – the protective principle is best suited to reduce the number of conflicting jurisdictional claims and mitigate international discord found in hostile cyber operations.[177] One reason why the protective principle works well in the case of hostile cyber operations is that applying the principle provides nations with the stronger capacity to prosecute cyber criminals outside their

174 W. Carson Bennett, "Houston, We Have an Arbitration: International Arbitration's Role In Resolving Commercial Aerospace Disputes," *Pepperdine Dispute Resolution Law Journal* v.19/1 (2019).

175 UNODC, "Cybercrime Module 7 Key Issues: Sovereignty and Jurisdiction" (2019) https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/sovereignty-and-jurisdiction.html.

176 Paul N. Stockton & Michele Golabek-Goldman, "Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat," *Stanford Law and Policy Review,* v. 25 (2021): 230.

177 *Id.*

jurisdiction when the attacks occur. In addition, there is a judicial precedent that provides strong support for applying the protective principle to hostile cyber operations that will be addressed later in this section.

Articles 7 and 8 of the 1935 Harvard Draft Convention on Jurisdiction with Respect to Crime described the principle as conferring jurisdiction on a nation "with respect to any crime committed outside [the nation's] territory by an alien against the security, territorial integrity or political independence of that State."[178] The protective principle is grounded on the axiom that every nation is entitled to defend itself from hostile attacks.[179] As a result, in the context of hostile cyber operations, the application of the protective principle can provide nations with the authority to preventively prosecute and apprehend individuals outside the sovereign State's jurisdiction when hostile cyber operations take place. Under international law, this unique technique makes the protective doctrine the only jurisdictional basis that authorizes extraterritorial jurisdiction over potentially dangerous crimes that threaten a state's security.

The *United States v. Yousef*[180] is an example that depicts judicial precedents providing strong support for extending the protective principle. In this manner, it can also be used to prosecute cyberterrorists. In what has been described as one of the most "seminal cases involving terrorism," the court held that it did not exceed the US government's authority to exercise jurisdiction over a terrorist whose conduct occurred outside the United States.[181] In a similar case, the *United States v. Reumayr*,[182] the court exercised extraterritorial jurisdiction over Canadian defendants who attempted to detonate the TransAlaska Oil Pipeline based on the protective principle. Both these cases illustrate how hostile cyber operations may fall under the purview of protective jurisdiction.

While the protective principle is arguably the best legal mechanism to prosecute those who engage in hostile cyber operations, it is not all-encompassing to address some of the jurisdictional nuance present when dealing with hostile cyber operations. For instance, if a cyberattack is planned to happen in more than one country simultaneously, then a problem arises when trying to

178 "Draft Convention on Jurisdiction with Respect to Crime," *American Journal of International Law*, v29(S1) (1935): 439–442.

179 Stockton & Golabek-Goldman, "Prosecuting Cyberterrorists," 230.

180 927 F. Supp. 673 (S.D.N.Y. 1996).

181 Stockton & Golabek-Goldman, "Prosecuting Cyberterrorists," 254.

182 530 F. Supp. 2d 1210 (2008).

determine which country can exercise the protective principle. With the number of hostile cyber operations increasing globally, it is imperative that the legal community takes proactive steps in the form of treaties or guidelines to address this inevitable issue.[183]

Moreover, multinational companies traditionally faced challenges when attempting to enforce cybersecurity claims against employees due to the employees being located in foreign jurisdictions. Traditionally, a Court is able to exercise personal jurisdiction over an out-of-state defendant based on the connection the defendant has with the state where the act was committed.[184] This is referred to as long-arm jurisdiction. However, establishing what "connection" the out-of-state defendant has with the state where the crime has been committed has been difficult in terms of cybercrimes. The case of *MacDermid, Inc. v. Deiter*[185] made it possible for the Court to establish long-arm jurisdiction in cases of cybercrime occurring outside US borders.[186] MacDermid, a company located in Connecticut, sued an employee named Deiter who worked remotely in Canada for the misuse of a computer and misappropriation of trade secrets. Based on Connecticut's long-arm statute, the Court held that they could exercise jurisdiction over Deiter, because she knew MacDermid's computer servers were located in Connecticut when she knowingly accessed the files. The Connecticut long-arm statute permitted the exercise of jurisdiction over anyone who uses a computer or a computer network located within the state.

However, as previously stated, a hostile cyber operation on space operations or data storage across multiple sovereignties and jurisdictions adds another level of complexity to a complex subject. This daunting reality along with the evolving techniques and technology used to initiate a hostile cyber operation is why, in the context of cybersecurity, there needs to be a proactive approach similar to the protective principle instead of reactive when dealing with the legal ramifications of cyberattacks.

183 Rob Sobers, "134 Cybersecurity Statistics and Trends For 2021," *Varonis* (2021) https://www.varonis.com/blog/cybersecurity-statistics/.

184 "Long-Arm Statute," *LII / Legal Information Institute* (accessed 20 January 2021) https://www.law.cornell.edu/wex/long-arm_statute.

185 2012 WL 6684580 (2nd Cir. 2012).

186 Shawn Tuma, "What is the Proper Jurisdiction for an International Computer Fraud Lawsuit?" *Business Cyber Risk* (2013) https://shawnetuma.com/2013/01/12/what-is-the-proper-jurisdiction-for-an-international-computer-fraud-lawsuit/.

6.4 *Space and Cyber Insurance*

6.4.1 Liability Convention and Insurance

The next section provides a brief yet detailed overview of the global cybersecurity insurance within the space industry. The insurance market related to space activities represents a critical factor in the exploration and utilization of outer space. Specifically, the insurance market provides coverage of the risks to which a spacecraft is exposed during its lifecycle.[187] The need for space insurance is due, in part, to the obligations set upon spacefaring Nations by the international space treaties. These obligations involve aspects of national liability for public and private activities beyond the atmosphere. The general framework developed at the international level frames the issue of liability by means, principally, of Article VII of the Outer Space Treaty (1967) and the Liability Convention (1972). For both treaties the issue is focused on what is the basis of fault and who would be liable to pay damages caused by space objects. However, the treaties are silent with regards to the extent insurance might (have to) cover a potential liability compensation. Instead, this aspect is left to national regulations to determine the appropriate insurance required from the private operator.[188] Moreover, the problem lies in the fact that liability is triggered by damage being caused by another space object as opposed to a non-physical cyberattack.

The four main insurance products related to the space market are: pre-launch insurance, launch insurance, orbital insurance, and third-party liability insurance. Space assets like satellites are most vulnerable to cyber-attacks during their operational phase. However, cyber-attacks are rarely included in orbital insurance policies.[189] The exclusion of cyber-attacks represents a growing concern for stakeholders because it represents a crucial gap for the space insurance market. This is unfortunate because the United States and Europe have the most advanced cybersecurity markets in the world. In 2016 the US and Europe accounted for $3 billion and $300 million, respectively, of $3.5 billion in global cyber-insurance premium.[190] In the satellite context, a 2019 report issued by the insurance company AXA XL stated that 43% of GEO satellites

187 M. Zajac, "Overview of Space Insurance," *Risques*, v. 111/1 (2017): 42–46.

188 Armel Kerrest de Rozavel and Frans G. von der Dunk, "Liability and Insurance in the Context of National Authorization," in *National Space Legislation in Europe: Issues of Authorisation of Private Space Activities in the Light of Developments in European Space Cooperation*, ed. Frans G. von der Dunk (Martinus Nijhoff, 2011): 125–61.

189 For more on this see Andrea Capurso & McLee Kerolle, "How to Estimate Insurance Coverage for Cybersecurity Protection for Satellites: A Case Study," International Astronautical Congress 2020: Cyberspace Edition (2020).

190 Nir Kshetri, "The Economics of Cyber-Insurance," *IT Professional* v.20/6(2018): 9–14.

are insured on orbit and 25% of GEO operators buy little or no in-orbit insurance beyond their first year in space.[191] As for LEO, only 6% of satellites have orbital insurance. Overall, the market is looking at 86% of the active satellites being uninsured while operating in outer space.[192] For insurers that do provide cybersecurity insurance, it is for first-party insurance and third-party insurance. First-party cybersecurity insurance focuses on compensating or mitigating the costs of the policyholder.[193] While third-party insurance covers the business and people that are found to be "responsible" for a breach.

Unfortunately, cybersecurity insurance cannot be analyzed in a straightforward manner due to the lack of standardization of the cybersecurity insurance market and the high uncertainty in pricing cybersecurity risks. According to a survey by Marsh & McLennan, 49% of policyholders said that they had "insufficient knowledge" about their cyber risk exposures to assess the type and coverage of insurances they need.[194] This insufficient knowledge highlights the lack of standardization of the cybersecurity insurance market. If there was standardization then policyholders would have a clear understanding of their cyber risk exposures, as well as the amount of coverage based on the situation, to determine the type of coverage required.

Due to the sensitivity of classified data regarding satellite coverage, it is difficult to estimate the costs of cyberattacks. Satellite coverage data is not only scarce to the public, but to the insurers as well. As a result, it also becomes difficult for companies to measure the nature and extent of cyber-related exposure in order to make decisions as to what coverages for how much to purchase. Insurers tend to be conservative and overcharge for cyber risk coverage because of the uncertainty in pricing cyber risk coverage.

As stated above, in order to increase the number of insured satellites in orbit, a crucial role must be played by national legislation which can impose insurance requirements on private operators in order to obtain and maintain the necessary licenses. Many spacefaring nations have put in place such mechanisms. However, the focus has been traditionally brought on third-party liability insurance, leaving product insurance often overlooked.

---

191 AXA XL, "Space Insurance Update" (2019) https://iuai.org/IUAI/Study_Groups/Space_Risks/Public/Study_Groups/Space_Risk.aspx.

192 *Id.*

193 "What is Cybersecurity Insurance," *Cyberinsureone* (2021) https://cyberinsureone.com/faq/what-is-cyber-security-insurance/.

194 Kshetri, "The Economics of Cyber-Insurance."

6.4.2 Minimum Requirements for Risk Mitigations (the Notion of Prudent and Reasonable Actor): Insurance Aspects

Cyber insurance works as a redistribution of risk. Insurance companies can incentivize their clients to implement *ex-ante* actions creating a more secure system, as well as offer *ex-post* remedial support. The former, which is the focus of this section, asks what role insurance companies can have in influencing cybersecurity governance. Some scholars believe that insurance has the potential to spread minimum requirements for cyber risk mitigation, thereby creating a common reference point for prudent and reasonable cyber-secure behavior.[195] This idea is tied to a liberal theory of governance that de-emphasizes state responsibility.[196]

The idea is that insurance companies can influence cybersecurity practice by, for instance, including compliance to security standards as a requirement for coverage.[197] As mentioned in Section 4.3 there are different standards that companies can rely on to mitigate their exposure to cyber threats. However, there is no consensus of what constitutes minimum standards for cybersecurity. Because the cyber insurance market is not a widespread and standardized market it cannot currently create a widespread cybersecurity implementation. With no standardized form, content or vocabulary for cyber insurance policies, they are "the wild west of insurance policies."[198]

In order to perform the risk calculations, insurance companies will have to boost their technical capabilities. This can be done by either hiring experts or partnering with companies that have those capabilities. In addition, as the market grows, the information from the claims will contribute to the generation of information about the nature and extent of cyberattacks in general. Insurance companies can also gather information about breaches when assessing premiums. If the companies are not forthcoming, providers can deny coverage.[199] Creating an obligation to disclose can create transparency and make it easier

195 Bruce Schneier, "Insurance and the Computer Industry," *Communications of the ACM,* v. 44/3 (2001): 114; and Scott J. Shackelford, "Should Your Firm Invest in Cyber Risk Insurance?" *Business Horizons,* v. 55/4 (2012): 349–356.

196 Daniel Woods & Tyler Moore, "Does Insurance Have a Future in Governing Cybersecurity?" *IEEE Security & Privacy*, v. 18/1 (2020): 21.

197 Shauhin A. Talesh, "Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as 'Compliance Managers' for Businesses," *Law & Social Inquiry,* v. 43/2 (2018): 13.

198 Ericka Chickowski, "10 Things IT Probably Doesn't Know About Cyber Insurance," *Dark Reading* (2021) https://www.darkreading.com/operations/10-things-it-probably-doesnt-know-about-cyber-insurance/d/d-id/1316862.

199 Scott J. Shackelford, "Should Your Firm Invest in Cyber Risk Insurance?", 353.

for insurers to calculate premiums in the future. Such obligations may not only stem from insurers, but also from governments.

These are potential opportunities that the market may leverage, but in their research Woods and Moore show there is little evidence that insurance companies are currently providing a strong form of governance.[200] The little research that exists on the topic indicates that in practice, insurance companies are not performing the assumed health checks of the companies before extending coverage.[201] Instead, insurers are relying more on *ex-post* remedies such as incident response after a breach. Such products are popular because the insurers lessen the cost of a claim they would otherwise have to cover. Moreover, the benefits of risk mitigation are more difficult to observe, although it could prevent the breach from happening at all.[202] It is also exactly these technological complexities that might bar insurance companies from having the same effect on markets, such as safety measures for property insurance. It is more difficult to measure a software product's effectiveness at reducing losses than, for instance, a manufacturer of fire doors. In addition, underwriters find it difficult to analyze the risks because they lack data about cyber operations. Only a few breaches are reported and those that are quickly become outdated because of the rapid technological development.[203] Unknown vulnerabilities will have an effect on the policy coverage and premiums.[204]

Another way of influencing cybersecurity best practice is by adding surcharges to companies for using old operating systems and providing monetary incentives to reduce premiums for secure cyber behavior – similar to safe driving discounts. Currently, there is no widely accepted discount for cybersecurity reduction fees and insurance companies tend to prefer a holistic risk assessment.[205] Insurers are focusing more on organizational procedures than technical controls, meaning that they rarely include basic security procedures in the contract.

---

200 Woods & Moore, "Does Insurance Have a Future in Governing Cybersecurity?", 23.

201 Sasha Romanosky et al. "Content Analysis of Cyber Insurance Policies: How Do Carriers Write Policies and Price Cyber Risk?", *Journal of Cybersecurity,* v. 5/1 (2019): 10–11 and Daniel Woods et al., "Mapping the Coverage of Security Controls in Cyber Insurance Proposal Forms," *Journal of Internet Services and Applications,* v. 8 /1 (2017): 9.

202 Woods & Moore, "Does Insurance Have a Future in Governing Cybersecurity?", 24.

203 Nicole Perlroth & Elizabeth A. Harris, "Cyberattack Insurance: A Challenge for Business", *New York Times* (8 June 2014) https://www.nytimes.com/2014/06/09/business/cyberattack-insurance-a-challenge-for-business.html.

204 Meland, Tondel & Solhaug, "Mitigating Risk with Cyberinsurance", 39.

205 Woods & Moore, "Does Insurance Have a Future in Governing Cybersecurity?", 24.

Even if insurance companies succeed in creating a standardized risk approach, companies will still need to pay attention to their security. The risk of relying too heavily on insurance to provide all the tools necessary to stay cyber secure is that they neglect other cybersecurity investments. To only adapt to the insurance company's risk indicators might not sufficiently protect the insured from breaches. As threats are constantly evolving, it is important that both insurers and companies innovate in their response to the dynamics of cybercrime. A secure solution will balance prevention, detection and recovery.[206]

Most standards will not have to be space-specific, meaning that the space industry can benefit from more broad cybersecurity standards. Cybersecurity insurance in itself is a relatively new market, but cybersecurity coverage for satellite systems is not a widely spread product and in fact favored to be excluded by insurers.[207] Insurance companies are taking to include cyber war risk exclusions in their policies, but the lack of rules on international attribution for States engaging in cyber conflicts makes it uncertain how such exclusions would hold up in court.[208] In order for this industry to take off, it will require a willingness from insurance companies to accept the risks involved. If cybersecurity is included in the insurance coverage, it could either see a market forming that is stand-alone or as part of a broader product. A stand-alone product will ensure technical expertise. Moreover, it will ensure that attention is kept on cybersecurity awareness and the generation of knowledge. The challenge for the market to take off is that there is a trend for space companies not to insure their satellites. In order for cybersecurity insurance to be attractive, it requires a balance between the assessment of the threat and the price of premiums. This balance can be achieved by gathering more actuarial data that will enable better risk assessment. Providing *ex-ante* services, such as support from security professionals after a cyber operation, will enable the insurers to understand the risks better. In addition, more data could be collected during the claims processes if the insurers request a forensic investigation.[209] A market with a specialized insurance product that gathers actuarial data has the

206 Mark Camillo, "Cyber Risk and the Changing Role of Insurance", *Journal of Cyber Policy,* v.2/1 (2017): 55.

207 Kerolle and Capurso, "How to Estimate Insurance Coverage for Cybersecurity Protection for Satellites", 4.

208 Daniel Woods & Jessica Weinkle, "Insruance definitions of Cyber War", *The Geneva Papers on Risk Insurance – Issues and Practice*, 45 (2020): 653.

209 Daniel Woods & Andrew Simpson, "Policy Measures and Cyber Insurance: A Framework", *Journal of Cyber Policy,* v. 2/2 (2017): 211.

potential to support the establishment of minimum requirements for cyber risk management in the future. Due to the economic self-interest of insurance companies in setting standards and deciding whether they are met, regulators should also play a role in the development of minimum standards whilst insurers can provide additional guidance and promotion of their adherence.[210] In such a scenario cyber insurance would not only function as risk transfer but would also support avoidance and mitigation elements.[211]

7 Conclusion

This chapter has provided an overview of cyber threats against space systems from the attack to the aftermath. It has done so by using the diverse background of the authors to provide an all-around tour: from the technical structure of satellite systems, the entry points and characterization of threats to responses at entity level through IT governance, technical strategies, contractual clauses and insurance to the challenges of international responses in a public international law fora. The chapter reflects the complexity of mitigating threats from both a technical and legal perspective. showing that keeping a satellite system cyber secure is a task for all types of stakeholders, from both the public and the private sector, to continually work on as the threats evolve.

---

210 Jan Martin Lemnitzer, "Why Cybersecurity Insurance Should be Regulated and Compulsory", *Journal of Cyber Policy* (2021): 8–9.

211 Ulrik Franke, "The Cyber Insurance Market in Sweden", *Computers & Security,* v. 68 (2017): 130.

Appendix 4

IV

D. Jha, N. P. Mantı, A. Carlo, L. C. Zarkan, P. Breda, and A. Jha. Safeguarding the Final Frontier: Analyzing the Legal and Technical Challenges to Mega-Constellations. *Journal of Space Safety Engineering*, 9(4):636–643, 2022

Journal of Space Safety Engineering 9 (2022) 636–643

Contents lists available at ScienceDirect

Journal of Space Safety Engineering

journal homepage: www.elsevier.com/locate/jsse

Safeguarding the final frontier: Analyzing the legal and technical challenges to mega-constellations

Devanshu Jha[a,*], Nebile Pelin MANTI[b], Antonio Carlo[c], Laetitia Caesari Zarkan[d], Paola Breda[e], Antara Jha[f]

[a] MVJ College of Engineering, Bangalore, India
[b] Istanbul University, Faculty of Law, PIL Dept., Istanbul, Turkey
[c] Tallinn University of Technology, Estonia
[d] University of Luxembourg, Luxembourg City, Luxembourg
[e] Bundeswehr University of Munich, Neubiberg, Germany
[f] National Forensic Sciences University, Gandhinagar, Gujarat, India

ARTICLE INFO

Article history:
Received 14 May 2022
Received in revised form 22 August 2022
Accepted 23 August 2022
Available online 10 September 2022

ABSTRACT

Satellites are becoming more interconnected and are just as cyber-vulnerable as any other technology. Mega-constellations of satellites launched into Low Earth Orbit (LEO) spark a myriad of longstanding concerns from different stakeholders, including traditional satellite operators and astronomers, as well as the growing number of activists involved in the protection of the space environment. Space cyber security involves the study of data security related to transmission networks. It includes signal processing between control segments, orbital objects and their onboard systems, and a component of cybernetics. This paper aims to elaborate on the concept of cyber safety for mega-constellations, intended as mitigation of cybersecurity risks and their avoidance through policy amendments and technology advancements.

Introduction

When analyzing the commercial sector for space applications, most of the LEO activities included remote sensing satellites for Earth observation and human activities, with a smaller percentage allocated to communication services [1]. NewSpace applications allow the development and the launch of swarms of satellites, CubeSats and nanosatellites (to name only a few possibilities) for Earth Observation and integrated applications at a lower cost, but at the same time with lower reliability. “A satellite constellation is a group of artificial satellites working together as a system", while “a mega-constellation is a group of large constellations, with hundreds or thousands of individual satellites” [50]. This poses challenges for collision avoidance manoeuvres. As an example, in April 2020 two satellites from mega-constellations (SpaceX’s Starlink and OneWeb) came to a dangerous close approach [2]. This incident highlights the necessity for collision avoidance systems and, more broadly, a stronger space traffic management framework.

An advantage of using LEO is that the communication latency for the uplink/downlink operations is significantly reduced compared to a Geostationary Earth Orbit (GEO) which is a huge advantage, especially for 5G global internet service. This provides a competitive edge for internet-dependent markets. However, a single satellite in LEO can only cover a portion of the Earth in less than a 20-minute timeframe, implying that a larger number of satellites are needed in the constellation to cover the Earth’s surface than in GEO. Furthermore, because of the constantly changing topology and high mobility, network management becomes more complex, raising the dilemma of how to reliably transmit information in the ground-to-satellite and satellite-to-satellite segments [3].

To the current date (2021), the following mega-constellations are known: Starlink (SpaceX), One Web, Kuiper (Amazon), Telesat (Canada), Hongyan and Hongyun (CNSA), Sphere (ROSCOSMOS). Satellites belonging to (mega-)constellations are redundant, contributing to LEO congestion, and leading to an increased risk of collision. About 3% of the Starlink satellites are already out of service and no longer manoeuvrable, which leads to the creation of space debris. [49] For instance, a significant event raising the concern of a future congested LEO was the Chinese launch of a direct-ascent Anti-Satellite (ASAT) weapon in January 2007, which struck a Chinese weather satellite in LEO [4,5]. This caused the second-largest creation of space debris in history at an altitude of 850 km

* Corresponding author.
E-mail addresses: devanshu.jha7@gmail.com (D. Jha), np_manti@yahoo.com (N.P. MANTI), ancarl@taltech.ee (A. Carlo), laetitia.zarkan@uni.lu (L.C. Zarkan), paola.breda@unibw.de (P. Breda), ajha646@gmail.com (A. Jha).

https://doi.org/10.1016/j.jsse.2022.08.006

in LEO. According to NASA, the Orbital Debris Program Office estimated that around 30% of the debris larger than 10 cm would stay in orbit until 2035 [66].

Therefore, another risk foreseen for mega-constellations in LEO is the increasing number of orbital debris, strictly connected to orbit congestion [6, 7]. Satellites in LEO can have a limited lifetime of several decades after the end of service, if sufficient atmospheric drag is present at the operational orbit. For higher altitudes (starting from 500 km [8]), drag devices for spacecraft self-disposal should be used when possible. A dead satellite in space could harm an operative asset because it cannot be controlled to perform collision avoidance manoeuvres. This happened during the first satellite collision back in 2009 in which an inactive Russian satellite (Cosmos 2251) collided with an active communication satellite operated by Iridium [9]. A de-orbiting plan should be integrated into each asset to prevent unsafe environmental conditions in space when reaching the end-of-life. An additional risk associated with CubeSats, and nanosats is that such assets are not easily trackable from Earth telescopes [10]. A Kessler effect [11] deriving from an uncontrolled amount of both small space assets and orbital debris in LEO would make the use and exploration of outer space difficult.

Cyber capabilities can have very harmful consequences for space assets at relatively low costs. Moreover, due to the difficulty to attribute cyber activities, both States and non-States actors can now access such cyber capabilities and carry out more hostile operations against all types of space infrastructure, whether on the ground or in outer space [12]. Cyber hostile operations in space are carried out by breaching the ground control system or intercepting signals from satellites and attacking sensors, actuators, or other electronic devices [13]. In the first case, the use of cloud-based ground services (like Amazon Web Services or Microsoft's Azure Cloud Services) has increased the cyber risk. In the second case, remote sensors are vulnerable to attacks because the used communication protocols based on TCP/IP models are accessible via the internet. For a satellite-to-satellite attack, it is essential to have close proximity or a line of sight with the target asset [13]. Preliminary actions can be taken following the line of the Committee on National Security Systems (CNSS) Policy 12 [14] (or CNSSP-12), which aims to incorporate security standards into land and space programs during the design process, rather than trying to bring security after launching the asset.

The fundamental question which is addressed in this work is what can be done to ensure the safety of the assets in space, from both the technical and the legal perspectives. As an example, at the international level, the European Space Agency (ESA) has recently established a cyber training range at the European Space Security and Education Centre (ESEC) in Belgium [15]. The range provides training and testing for its employees and partners and aims to develop knowledge in awareness, detection, investigation, response, and forensics to counter cyber hostile operations specific to space systems. This paper suggests potential technologies which can help to increase the safety of space assets.

On the other hand, a legal framework for mega-constellations must be developed considering the gravity of actions taken by actors, such as States, non-governmental organizations (NGOs) or individuals, against the safety and security of space systems. The current legal framework under the International Telecommunication Union (ITU) will be discussed, as well as how the process of orbit/spectrum allocation works, and how public and private space actors decide which orbit or frequency will be used to not interfere with the activities of other actors. Legal obligations to collisions and failures, including liability regimes, are developed. Cyber interferences causing collisions and failures are therefore relevant for this study. This work identifies liability for space debris as a critical legal aspect concerning mega-constellations. New legal questions arise either through collisions or failures (through cyber interference or attacks), and mega-constellations in orbit carry the potential to cause an increase in space debris.

Legal framework for cyber secure mega constellations

Mega-constellations attempt to provide worldwide internet connectivity, with low latency and high capacity. Their revolutionary influence on global internet access raises the danger of cyber-attacks on both the platforms and the assets. In this section, a legal framework for the management of mega-constellations is provided.

Definition and legality of the mega-constellations

A satellite mega-constellation is a group of several hundreds and thousands of artificial satellites, orbiting around the Earth and working together as a system. With the advent of mega-constellations of satellites, one of the emerging legal issues is the cyber safety of the system and the development of a legal framework for the sustainable and secure use of outer space, mega-constellations, related technologies, and services. These require a delicate balance between law and ingenuity; the deployment of satellites by different entities raises concerns as to space safety, due to the increasing number of satellite mega-constellations causing congestion in LEO [16], and could escalate risks of in-orbit satellite collisions and has negative effects upon the core principle of customary international law in outer space, the 'freedom of access [17]. Spacecrafts, including vital communications and navigation satellites, have been considered safe from physical aggression or attack. On the other hand, satellites are increasingly vulnerable to cyber-attacks in the space domain.

There is not a definition of mega-constellations in the existing space treaties. These systems present new challenges to the existing norms and national and international regulatory regimes governing space activities. As procedures and regulations vary in different countries, how to govern mega-constellations without creating legal fragmentation becomes a challenge to be discussed at the international level. Large constellations are defined as any satellite constellation that is at least an order of magnitude larger than the first-generation constellations like Iridium (66 satellites), Globalstar (48 satellites), and Orbcomm (31 satellites), with a maximum number of 500 satellites [18]. A mega-constellation of satellites is a network of satellites in LEO, working as one interconnected system for global communication coverage and to provide navigation and communication services [19]. The legal regime governing outer space activities was established by the 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space (shortly the Outer Space Treaty or OST) [20]. However, OST does not include the terms "constellation" or "mega-constellation", and satellite mega-constellations are considered space objects, like all other satellites. Nevertheless, satellite mega-constellations are raising new legal questions, as to the future regulatory challenges of the services they will provide and related aspects.

The OST is the main framework to regulate the deployment of mega-constellations and the services provided by conducting outer space activities. Article I of the OST embodies three basic rights: the right to free access, the right to free exploration and the right to free use. As a result, other than for peaceful purposes and uses, the deployment and operability of mega-constellations cannot be restricted under the OST system, and harmful interference cannot be restricted directly but initiates the consultation process as per Art IX, accordingly, diplomatic dialogues to warn or complain about, however, this process cannot directly avoid or grant substantive rights, similar to the harmful contamination, which is also regulated within the OST Art. IX. Another aspect is whether satellite constellations could cause national appropriation of space giv-

ing their extension in space and time. Under Article II of the OST, the "*outer space (…) is not subject to national appropriation by claim of sovereignty (…) by means of use, by means of occupation, or, indeed, by any other means". As underlined by many scholars, there is no lawful, permitted means which will legitimize the national appropriation of outer space, with the highlight on the expression on "by any other means," meaning the listing of actions is not exhaustive and to prevent any loopholes, and makes it clear that outer space cannot be brought under the sovereign domain of any State, and that no State may claim exclusive rights in these areas, by* use of any orbit [53]. Article III of the OST states that "*States Parties to the Treaty shall carry on activities in the exploration and use of outer space (…) in accordance with international law (…), in the interest of maintaining international peace and security and promoting international cooperation and understanding*". Any action carried out by the mega constellation in outer space should comply with universally acknowledged principles in space law as to peaceful uses and decisions of international organisations as to safe conduct in space to avoid any harm in the orbit. As an example, in September 2019 the European Space Agency had to perform evasive manoeuvres on one of its satellites to avoid a collision with a mega-constellation of SpaceX [55].

Another important aspect to be assessed is the legality of the prevention of harmful interference. Since the early 2000s, a growing number of detrimental interferences have arisen intending to disrupt or block the receipt of signals, affecting communication satellites [56]. In some cases, harmful interferences have targeted "radio navigation-satellite service" signals used by civil aviation and threatened the international air traffic with dire consequences including the potential loss of life.

The International Telecommunication Union (ITU) [21] is responsible for administering and organizing this cutting-edge technology, as well as determining how the orbit/spectrum distribution procedure works. ITU has numerous functions relating to satellites and telecommunications including the assignment of the orbital slots to satellites stationed in the GEO orbit. ITU Regulations prohibit intentional interference (jamming) with satellite signals based on reciprocity [54], accordingly, under ITU regulations all member States are under obligation to respect ITU regulatory regime and not to cause harmful interference as per ITU Constitution Art. 6.1 [61], 45 [62] and 48 [63]; and pursuant to the ITU Radio Regulations Art. 15.1.1 [64] and 15.2.2 [65], all ITU Member States are under an obligation not to use unnecessary transmission power that might cause interference. The worldwide technical standards for the use, assignment and allocation of radio frequencies and technical standards are codified under ITU regulatory regime. The ITU frequency allocation system [22] ensures equitable access to outer space and avoidance of harmful interference in the conduct of space activities, defining harmful interference as *"(…) an interference with a radio signal that endangers the functioning of a radio service (or) seriously degrades, obstructs or repeatedly interrupts a radio communication service operating in accordance with ITU Radio Regulations* [23]*"*.

Under the ITU Constitution [24], all member states are responsible for enforcing and respecting the ITU regulatory system, and any interference with, or deliberate jamming of a signal is a breach of the ITU regulatory regime. The interference with, or intentional jamming of a signal will not only violate the principle of international recognition under the ITU Radio Regulations [25] but will also constitute interference with another user's rights, regulated under Article 6 and Article 45 of the ITU Constitution. The ITU Radio Regulations provide under Article 15.1§1 that *"all Stations are forbidden to carry out unnecessary transmissions of superfluous false or misleading signals"* and Article 15.1§2 that *"transmitting stations shall radiate only as much power as is necessary to ensure a satisfactory service"*. It is therefore difficult to identify whether the signal attenuation and spoofing are caused by cyber operations, as this identification requires identification of the right IP address to find the original attacker at the time when cyber operations started with intangible targets and weapons.

Rule 63/1 of the Tallinn Manual [26] defines that *"the prohibition of harmful interference by a State with the wireless cyber communications and services of another State is based on Article 45(1) of the ITU Constitution*". The latter reports that *"all stations, whatever their purpose, must be established and operated in such a manner as not to cause harmful interference to the radio services or communications of other Member States"*. In 2013, the ITU started a process of drawing up a memorandum of cooperation (MoC) with administrations and organizations that can monitor the use of spectrum allocated to satellite services to assist in performing measurements related to cases of harmful interference. In 2018 ITU published the 'Harmful Interference To Satellite Systems' document [56], which provides a non-exhaustive list of actions and ongoing initiatives to combat harmful interferences [57].

A final point of discussion in this paragraph is the role of national frameworks for space safety. The term 'Security' is related to the maintenance of peace and stability, while 'Safety' is the combination of measures precluding risks and protecting space systems during normal operations [27]. Space safety refers to space mission hazards and relevant risk avoidance and mitigation measures. The space mission hazards include threats to human life, loss of space systems, and pollution of the Earth's environment [28]. Satellites depend on cyber technology including software, hardware and other digital components, and any threat to a satellite's control system or available bandwidth poses a direct challenge to national critical assets [29]. An active national framework attempting to define space safety is given by the US [30], having two regulatory bodies: the US Federal Communications Commission (FCC), and the Space Information Analysis and Sharing Center (Space-ISAC). The latter is a public-private partnership aimed at the cyber protection of satellites. Nonetheless, the National Cybersecurity Federally Funded Research and Development Centers (in short, FFRDC) report that space and cybersecurity policies are not yet prepared for the challenges created by the meshing of space and cyberspace [58]. More than 3,000 functioning satellites provide integrated data for power grids, shipping and delivery services, automobile navigation, banking, and broadcasting. Such systems, however, are also used in the military for communications, missile warning, and weather forecasting. Mega-constellations are usually made of SmallSats, which are not yet fully categorised internationally. For example, NASA classifies SmallSats based on size and mass (less or equal to 180 kg). The SmallSats market has expanded with an average of 23 % per year between 2009 and 2018, due to the use of SmallSats for large and mega-constellations [59]. The main advantage of using SmallSats LEO of less than 1000 km is the crossing of the Van Allen radiation belts is prevented. In this belt, the spacecraft is subjected to high radiation causing a stronger degradation of the solar panels and the electronics. The longer the spacecraft resides in this region, the higher the damage. Therefore, SmallSats show fewer requirements in terms of electronics shielding from highly charged particle interference and their use for mega-constellations is justified. The market foresees rapid growth for the next few years.

In the next section, an overview of the technical standards required for the safety and cybersecurity of the assets in mega-constellations is presented.

Technical standards for cyber safety of mega-constellations

The 'attribution problem' is a key difficulty for cyber activity, acts connected to downlink and uplink operations (ground-satellite) [65]. In reality, an attack may be launched from almost

anywhere along the process of conveying a signal, which is split into packages that take separate paths to a recipient. A scenario involving an attack within the satellite-satellite segment instead is purely hypothetical, and no such assault has been proven [13]. An offensive satellite would necessitate the use of sensors and actuators that are not typically carried on the satellite itself. One option would be to use satellite awareness sensors from which the offensive satellite may obtain information about the victim satellite via local proximity sensors or a third-party system. Electromagnetic Pulse Actuators and Radio Frequency Actuators could be potentially used to generate a power system failure and a GPS spoofing respectively [13]. A recent work developed for satellite communications (SATCOM) and Global Navigation Satellite Systems (GNSS) provided the following solution [31]**:** a multi-layer satellite system topology with a cross-layer design of multi-path routing and a communication protocol stack. Advancements have been achieved in the past few years toward the use of higher carrier frequencies, including the higher frequency bands X- through Ka. Their benefits (especially for CubeSats [32]) include the use of a reduced antenna aperture while maintaining consistent gain.

Larger data rates are much easier to achieve at higher frequencies since the data transfer rate is related to transmission bandwidth, which is more readily available at higher frequencies. However, Ku/Ka bands are mostly useful for satellite-to-satellite communications for spacecraft weighing more than 200 kg. Cell phones have caused significant congestion in lower RF frequencies, notably in S-band. Advanced programming, such as the CCSDS Low-density parity-check code (LDPC) family with various code types, is a good technique for offering bandwidth and power tradeoffs with high-order modulation to fulfil high data rate requirements for CubeSat missions. Small spacecraft have also demonstrated lasercom (laser communication) technologies, such as the Optical Communications and Sensor Demonstration (OCSD) mission launched in 2017 and successfully transfer data. A potential technology which could reduce the risk of a cyberattack is the Quantum Key Distribution (QKD) as a new cryptographic primitive for establishing a private encryption key between two parties [33]. Satellite QKD can be used to enable global coverage and QKD protocols, already proven on ground facilities, could be extended to GEO. A promising architecture for cybersecurity in space is the Zero-Trust Architecture, based on the idea of a 'never trust, always verify' policy [34]. It delivers a "Layer 7" threat protection and makes the management of user access easier. This architecture is made up of the network's most essential and valuable data, assets, applications, and services (DAAS). Knowing who the users are, what apps they use, and how they connect would allow them to implement a policy that assures safe data access, which is accomplished by building a segmentation gateway (a next-generation firewall) to ensure that only known, allowed traffic or legitimate applications have access to it. Blockchain technologies [35] in space and cybersecurity has also the potential to address numerous critical security and trust issues in the space sector. Blockchain is a subset or type of Distributed Ledger Technology (DLT) that includes cryptographically linked "blocks" (transactions) and a "chain" where each block is time stamped and placed in chronological order.

The advantage of this technology is that it is decentralized, traceable and data tempering (deliberately modifying data through unauthorized channels) is difficult. The disadvantages linked to this technology are the limitations around performance and scalability, the lack of privacy and some minor security vulnerabilities. An interesting report from HDI Global Specialty SE from 2021 [36] shows that the backbone of cyber-resilient spacecraft is a robust Intrusion Detection System (IDS), which continuously monitors telemetry, and the command sequences, operating states, flight software configuration, etc. If severe rules are violated or a high threshold is crossed in response to a threat, the spacecraft's Intrusion Prevention System (IPS) will take automatic actions. The IPS and the ground should be capable of returning critical systems to a known cyber-safe mode, shutting down all non-essential systems and represtinating a healthy system configuration. The cyber-safe mode shall be stored in the asset's memory board, shall not be modifiable and shall be controlled by hardware.

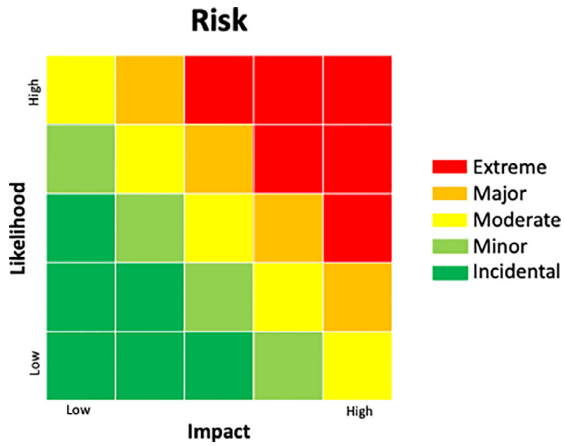


Fig. 1. Risk matrix.

To conclude, promising technologies are emerging to ensure standards in communications for the satellite-satellite segment and for uplink/downlink when using SmallSats and CubeSats for mega-constellations. If these standards are applied, the safety of the asset against cybersecurity attacks can be improved as well.

Shared risks and shared responsibilities

Monitoring risks

Defining cyber risks for satellite mega-constellations is becoming complicated. To begin with, the terminology is important as the terms vulnerability, threat, and risk are not referring to the same type of problems. A vulnerability is a weakness in an asset that an adversary could exploit, while a threat requires an adversary to have the motivation, resources, and intent to exploit this vulnerability. And finally, the resulting risk is the potential for the loss or damage of the asset when an adversary actively exploits the vulnerability [37]. This can be visualized thanks to the auxiliary of a risk heat map (Fig. 1). The horizontal axis shows the impact of an event, while the vertical axis shows the likelihood of an event. The risk matrix is general, but in this work, it is applied primarily to cyber security risks. A colour matrix can be created, which identifies the risk areas in five main categories, namely: "extreme", "major", "moderate", "minor" and "incidental". The incidental category coloured in green indicates no action is needed while the extreme category coloured in red indicates that immediate action is needed to contrast an event. This matrix allows to monitor and identify the necessary countermeasures, also known as risk mitigations.

To ensure business continuity and resilience for an organization, it is essential to define an adaptive system. McCormick stated that an adaptive system is *"characterized by how aggressively it adapts to the unexpected"* [38], therefore systems are required to be designed to learn continuously from their environment. It is essential to keep in mind that cyber, space and any other essential system need to be autonomous and disconnected from the rest of the public system in order to prevent any kind of intrusion. This can be

Table 1
Table of risks affecting mega-constellations. Grey rows: categorization of cyber risks according to NASIC*.

Category	Risks	Mitigation
Space Segment*	Command intrusion, payload control, service denial, malware, loss of satellite control	Encryption, onboard authentication of uplinked commands, robust Intrusion Detection System (IDS), on-board logging for cross-validation
User segment*	Spoofing, service denial, malware	Encryption, cyberattack resilience testing before launch
Link segment*	Command intrusion, spoofing, replay	RF communications, encryption
Ground segment*	Hacking, hijacking, malware	Avoid cloud-based services, train personnel, onboard logging for cross-validation
Supply chain	Breach in hardware/software provided by multiple vendors, deliberate installation of hidden back doors	Global cybersecurity standards among vendors, supply chain risk management
Space weather	Solar activity, cosmic radiation	Pre-warning systems on ground and spaceborne (ESA and NASA), electromagnetic shielding
In-space operations	Collision, congested orbits	Active collision avoidance devices, AI algorithms, Space Traffic Management authority
End-of-life	Debris, collision	De-orbiting, atmospheric re-entry

done thanks to the creation of Information and Communications Technology (ICT) systems that are independent and not connected to the internet. Accreditation of all systems, public and/or classified, is also a good practice in order to have a well-defined list of the systems and to protect them from possible intrusions and attacks. In case of an event, the accreditation helps to identify the possible weak link that leads to the breach.

Satellite mega-constellations are multi-domain, multi-sectoral, multi-asset systems [39]. Mega-constellations are enabled by technology miniaturization and require a coordinated effort to face the technological limits in spacecraft operations and space traffic. As their importance is increasing, so the threat actors targeting space systems via cyberattacks are. As the attacks are increasing, the research and intelligence on the vulnerabilities of space systems are also becoming more sophisticated, detailed, and accessible. While the list of cyber threat actors is expanding for space, States are trying to increase awareness of vulnerabilities and adversary capabilities. The National Air and Space Intelligence Center (NASIC) identified the cyber threats and cyber risks into four categories: the space segment, the user segment, the link segment, and the ground segment [40]. An additional key point of access for a potential cyberattack is also provided by the supply chain, because satellites require multiple manufacturers and a system integrator to make all subsystems function as one. For military satellites using advanced encryption methods with a well-protected ground infrastructure, the risk of a cyberattack is already mitigated. The main risks associated with these categories are listed in Table 1, using a grey background. Monitoring risks effectively starts with an effective cyber resilient posture design. In order to achieve and maintain cybersecurity, space systems should be designed to continuously monitor, anticipate and adapt to the situation, to mitigate cyber activities that could manipulate, deny, degrade, disrupt, destroy, surveil, or eavesdrop on space operations [41].

Space-weather conditions can also provide a risk, as reported in Table 1. For instance, excessive radiation doses aboard a spacecraft in LEO can cause electronic component damage and/or solar panel degradation. Globally, ESA and NASA are working alongside to offer a pre-warning system based on in-space and Earth monitoring of solar activity, with the goal of minimizing the impacts of bad space weather on both spacecraft and Earth [42].

In-space operations and end-of-life are also connected with risks. According to the Union of Concerned Scientists (UCS) [43] which keeps the records of the operational satellites, there are 6,542 satellites, out of which 3,372 satellites are active and 3,170 satellites are inactive, as recorded by 1st January 2021; and there are 8,840 satellites, out of which 6,200 are active satellites and 2,640 are inactive satellites by August 11, 2022 [48]. The overall number is presumed to rise to over 100,000 by the end of the decade. Despite the use of collision avoidance maneuvers, Artificial Intelligence (AI) can be a fundamental technology to detect a collision risk in advance and to activate a collision avoidance maneuver from the spacecraft itself, instead of being initiated by ground control. Additionally, with the aim of guaranteeing the safety of the space environment, an analogy with the aeronautical regulations could help to draw the basic line to define a Space Traffic Management authority to deal with the congested traffic in LEO.

Responsibility

Space is a strategic domain, and some satellites are part of a nation's critical infrastructure. Cyberattacks and cyber threats to the satellite have national security implications, and commercial actors, therefore, have to know the consequences their satellite can bring to national security. The OST envisages direct responsibility of States for their national space activities in Article VI: it obligates an "*appropriate State*" to "ensure *authorization and continuing supervision*" over space activities of non-governmental entities, without defining any of these concepts. Non-interference is a general principle of international law and an inherent right of national sovereignty. "*Interference*" is not defined in international space law, however, OST signatories define "interference" for purposes of outer space activities. In the sense of OST, the prevention of harmful interference is understood as any harmful interference with space activities and the environment, not directly in the cyber sense [52]. Avoiding harmful interference, under Article IX of the OST, does not regulate notion explicitly, but *calls on nations to avoid "harmful interference with the activities of other State Parties in the…use of outer space" and to "undertake appropriate international consultations before proceeding with any such activity or experiment"* [51]. The Liability Convention contemplates physical damage caused by a space object. Under the state responsibility provisions established under Article VI of the OST, if harmful interference is attributable to a governmental entity or harmful interference attributable to a non-governmental entity, a fundamental question arises. Has the involved State taken all required measures to prevent or stop this interference? If the State has not taken all required measures it is responsible for the harmful interference.

The customary law rule of prohibition of the use of force, under Art. 2(4) of the UN Charter requires States to "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations". According to the UN Charter "force" is understood as conventional "armed force", since the Charter was written after World War II, and other than States there was no other power or entity to endanger international peace and security with armed activity. Under the UN Charter, the right to self-defence is regulated in Art. 51 as: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs

against a Member of the United Nations". However, even if the use of force is justified under Article 51, the use of force must be consistent with the long-accepted principles that constitute the basis of the law of armed conflicts, namely military necessity; proportionality; target distinction (discrimination); and minimizing unnecessary suffering (humanity). However, responsibility for use of force can be reconsidered in case a cyber operation constitutes the use of force if its scale and effects are comparable to non-cyber operations rising to the level of armed use of force in terms of Art. 2(4) of the UN Charter. In case it is not possible to define a threshold, several factors can be used to assess whether a cyber operation can be qualified as "use of force", including the severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement and presumptive legality. For a proper assessment, these factors must be evaluated on a case-by-case basis. If a cyber operation is to be considered as a 'use of force' under these parameters, the threat of such an operation will also be illegal under international law.

In case of satellite signal interference or jamming, Member States are obligated to comply with ITU provisions and cooperate with other States to eliminate harmful interference, through bilateral negotiations. In case the negotiations remain inconclusive, the affected State can pursue arbitration. As an example, the U.S.-German ROSAT X-Ray satellite hack in 1998 [44] was released with a cyber hostile operation to the ground control system in Goddard Space Flight Centre in Maryland, and hackers changed the aim of the satellite's solar panels, directing them to the sun, resulting in the batteries burning and the satellite being lost and hitting Earth in 2011 [45]. With the framework ruling the responsibility of States, risk mitigation can rely upon this definition to ensure the safe operation of space assets. Under the OST regime, it is important to understand the scope of responsibility and liability regimes. While the Art. VI regulates the international responsibility of states for national activities in space to be in conformity with the treaty, liability of launching State(s) for damage towards other states or their nationals or property is regulated under Article VII of the OST. In terms of Art. VII, the term launching State(s) covers, not only the State where the satellite is launched, and as per Art. VII, States that launches or procures the launch or from whose territory or facility and object is launched. And the launching State has jurisdiction and control over the spacecraft, and must regulate, authorise, and supervise, and is responsible for, the activities of commercial operators.[60]

Risk mitigation requires taking into consideration the particularities of satellites. After launching a satellite, hardware maintenance hardware is not possible without bringing the satellite back for servicing and updates. Satellite components are also using different technologies, produced by different quality standards, different manufacturers, and in different countries. Moreover, satellites don't have one entry point and need to communicate with ground stations. The intricate architecture of space, ground and RF/optical interfaces potentially causes a unique vulnerability in each access point, which can be a start for a cyberattack.

An effective risk management framework starts with determining the asset (physical and virtual) that can be most attractive to hackers and the vulnerabilities of it and how to defend and protect it. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) helps to define the Risk Management Framework (RMF), which is the framework already used by several governments for cybersecurity. The five elements of the NIST Cybersecurity Framework include identification, protection, detection, response, recovery [46]. These actions all take place at the same time to build the basis for other key parts of high-profile cybersecurity risk management to be developed. Additionally, the United States Department of Defense (DoD) launched the Cybersecurity Maturity Model Certification (CMMC) program to assess defense contractors' cybersecurity skills, readiness, and sophistication. It is seen as another exemplary example of effective cybersecurity activity [47]. The CMMC is another successful example of how cybersecurity risks can be managed to preserve the safety of the asset in space.

Conclusions

Mega-constellations of satellites are creating a sophisticated network in LEO, resulting in new technical and legal challenges, among which cybersecurity is one of the most important. Mega-constellations change and will continue to change the outlook of satellite communications, as they are easy to deploy and use. Potential technologies were proposed in this work to diminish the risks of cybersecurity attacks and to guarantee the safety of the assets in space. Additionally, to protect space assets and their supporting infrastructure from cyber threats and to ensure continuity of space operations for both government and commercial space industry, a legal definition of mega-constellations and the responsibility associated to the mitigation of risks was revisited in this work.

For future efforts to regulate this area, international and national authorities have to take into consideration many variables. First of all, the harmful threshold is a measure of the vulnerability of a system to interference. To develop more rebust and sresilient systems, even against low intensity attacks, standardisation bears a great importance, therefore, the regulations provided by ITU must be followed with care by national authorities, and as mentioned, the lack of supervision may cause some private actors to escape from the process and these may create risks in orbit.

Successful examples of national frameworks or institutes have to be collected and followed to develop a guideline for the future missions and in order to design a legal contextualization for space activities involving mega-constellations.

CREDIT author statement

Devanshu Jha: Conceptualization, Methodology, Software
Nebile Pelin MANTI.: Writing- Original draft preparation.
Antonio Carlo: Writing- Reviewing and Editing,
Laetitia Caesari Zarkan: Supervision.
Paola Breda: Visualization, Investigation.
Antara Jha: Articulate law of ITU, Cyber law, Space law.:

Declarations of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Types of Orbits, ESA official Website, 30 March 2020 (Available at: https://www.esa.int/Enabling_Support/Space_Transportation/Types_of_orbits)
[2] Joey Roulette, OneWeb, SpaceX satellites dodged a potential collision in orbit, 'Red alerts' of a potential disaster were sent to the companies, in The Verge, April 9, 2021. (Available at: https://www.theverge.com/2021/4/9/22374262/oneweb-spacex-satellites-dodged-potential-collision-orbit-space-force)
[3] Low earth orbit (LEO) mega-constellations - satellite and terrestrial integrated communication networks. Xin Yang, University of Surrey, PhD Thesis, Nov. 2020, (https://doi.org/10.15126/thesis.00850382).
[4] Phillip C. Saunders and Charles D. Lutes, "China's ASAT Test: Motivations and Implications," Institute for National Strategic Studies, Special Report, June 2007, (Available at: https://apps.dtic.mil/sti/citations/ADA517485)
[5] Brian Weeden, '2007 Chinese anti-satellite test', Secure World Foundation, Fact Sheet, 23 Nov. 2010, (Available at: https://swfound.org/media/205391/chinese_asat_fact_sheet_updated_2012.pdf); Nivedita Raju, "A Proposal for a Ban on Destructive Anti-Satellite Testing: A Role for the European Union", EU Non-Proliferation and Disarmament Consortium, Non-Proliferation and Disarmament Papers, No. 74, April 2021, p. 4

[6] Mega-Constellations Pose Massive Risks to Shared Space Access, Viasat, Inc., March 30, 2021. (Available at: https://www.fiercewireless.com/sponsored/mega-constellations-pose-massive-risks-to-shared-space-access)

[7] Kieran O'Brien, Sweeping Up Space: The End-of-Life Solution, *in* Astroscale, July 6th, 2021. (Available at: https://astroscale.com/sweeping-up-space-the-end-of-life-solution/)

[8] Abdul Majid, Muhammad Naeem Owais, Muhammad Nauman Qureshi, Aerodynamic Drag Computation of Lower Earth Orbit (LEO) Satellites, J. Space Technol. 8 (1) (July 2018) 82–89.

[9] Brian Weeden, 2009 Iridium-Cosmos Collision Fact Sheet, 2012. (Available at: https://swfound.org/media/6575/swf_iridium_cosmos_collision_fact_sheet_updated_2012.pdf)

[10] Identification and Tracking Systems, (Chapter 13) *in* State Of Art Of The Small Spacecraft Technology, (Available at: https://www.nasa.gov/smallsat-institute/sst-soa-2020/identification-and-tracking-systems)

[11] Donald J. Kessler, Burton G. Cour-Palais, Collision frequency of artificial satellites: The creation of a debris belt, J. Geophys. Res. 83 (A6) (1978) 2637–2646.

[12] Antonio Carlo, Lisa Lacroix, Laetitia Zarkan, The challenge of protecting space-based assets against cyber threats, IAC (2020) 5.

[13] Gregory Falco, When Satellites Attack: Satellite-to-Satellite Cyber Attack, in Defense and Resilience, Published Online on Nov 2, 2020, (DOI: https://doi.org/10.2514/6.2020-4014), (pp.1-9), (p.2); G. Falco, "The Vacuum of Space Cyber Security", in 2018 AIAA SPACE and Astronautics Forum and Exposition, 2018, p. 5275.

[14] Critical Infrastructure Protection in the Information Age dated October 16, 2001. In 2001, under E.O. 13231, the President redesignated the NSTISSC as CNSS. Cybersecurity Policy For Space Systems Used To Support National Security Missions (*CNSS Policy 12*), by CNSS, Released on 02/06/2018, p.-18. (Available at: https://www.cnss.gov/CNSS/issuances/Policies.cfm)

[15] ESA Education Training Centre, more details (Available at: https://www.esa.int/About_Us/Corporate_news/ESA_ESEC)

[16] Lauren Grush, As Satellite Constellations Grow Larger, Nasa Is Worried About Orbital Debris, September 28, 2018, (Available at: https://www.theverge.com/2018/9/28/17906158/nasa-spacex-oneweb-satellite-large-constellations-orbital-debris).

[17] The Emerging Customary Law of Space, (Available at: https://core.ac.uk/download/pdf/72829832.pdf).

[18] The Impacts of Large Constellations of Satellites, Space Domain Awareness Project No. 1319JAPM, JASON Program Office, The MITRE Corporation, November 16, 2020, (Available at: https://www.nsf.gov/news/special_reports/jasonreportconstellations/JSR202H_The_Impacts_of_Large_Constellations_of_Satellites_508.pdf).

[19] Eytan Tepper, Jean-Frédéric Morin, The Mega Disruption: Satellite Constellations and Space-based Internet, CIGI Paper, August 31, 2020. (Available at: https://www.cigionline.org/articles/mega-disruption-satellite-constellations-and-space-based-internet).

[20] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, A/RES/2222(XXI), 19 Dec. 1966; (Available at: https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html).

[21] ITU: Available at: https://mpo.cz/en/guidepost/for-the-media/press-releases/the-oldest-organization-of-the-un-system–the-international-telecommunication-union-celebrates-150th-anniversary–158129/).

[22] ITU-R: Managing the radio-frequency spectrum for the world, December 2019; (Available at: https://www.itu.int/en/mediacentre/backgrounders/Pages/itu-r-managing-the-radio-frequency-spectrum-for-the-world.aspx).

[23] ITU Radio Regulations, Art. 1.169. http://www.spacenews.com/article/military-space/35948military-satellite-communications-panel-ties-us-troop-rotationsto #.Ue254RZsWR8

[24] Constitution of the International Telecommunication Union, Concluded in Geneva on 22/12/1992, (Available at: https://www.itu.int/council/pd/constitution.html)

[25] ITU Radio Regulations, Art. 8.1.

[26] Harmful Interference To Satellite Systems, (https://www.itu.int/dms_pub/itu-r/md/15/wrs18/c/R15-WRS18-C-0005!!PDF-E.pdf)

[27] Safety Design for Space Systems, Gary E. Musgrave Ph.D, Axel Larsen, Tommaso Sgobba (Eds.), IAASS, Elsevier, 2009, p.3.

[28] Webster Unabridged Dictionary, (Available at: https://unabridged.merriam-webster.com/)

[29] Beyza Unal, Cybersecurity of NATO's Space-based Strategic Assets, Chatham House, International Security Department, July 2019, p.2.

[30] William E. Paulson, Smallsats and Mega-Constellations for U.S. National Security: Some Legal Aspects, (Available at: https://escholarship.mcgill.ca/downloads/jw827h66v?locale=en).

[31] Cyber security with radio frequency interferences mitigation study for satellite systems, (https://doi.org/10.1117/12.2224632 DOI: 10.1109/ACCESS.2020.2966045)

[32] Small Spacecraft Technology State of the Art, NASA/TP–2015–216648/REV1, (Available at: https://www.nasa.gov/smallsat-institute/sst-soa-2020/communications)

[33] R. Bedington, J.M. Arrazola, A Ling, Progress in satellite quantum key distribution, Quantum Inf. 3 (2017) 30 https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecturehttps://www.juniper.net/content/dam/www/assets/white-papers/us/en/security/the-rise-of-zero-trust.pdf, doi:10.1038/s41534-017-0031-5. The Rise Of Zero Trust: Separating the Reality from the Myths; White Paper by Juniper Networks, 2019; (Available at.

[34] P. Bansal, R. Panchal, S. Bassi and A. Kumar, "Blockchain for Cybersecurity: (10.1109/CSNT48778.2020.9115738).

[35] Luke Shadboldt, Technical Study, Satellite Cyberattacks and Security, July 2021, pp. 13-15; (Available at: https://www.hdi-specialty.com/downloads/_Global/HDIS209_Satellite%20Cyberattack_whitepaper_V8_05JULY21.pdf)

[36] Richard. Bejtlich, SANS Confuses Threats with Vulnerabilities, TaoSecurity Blog (2005) 26 January(Available at https://taosecurity.blogspot.com/2005/01/sans-confuses-threats-with.html .

[37] G. Frank McCormick, "Adaptive Controls", CSI Document 04-232-1245, Rev. 1.0, Appendix E, October 2004. Cybersecurity Principles for Space Systems, (Available at: https://www.federalregister.gov/documents/2020/09/10/2020-20150/cybersecurity-principles-for-space-systems).

[38] S. Soesanto, Terra Calling: Defending and Securing the Space Economy, Center for Security Studies (CSS), ETH Zürich, 2021 (Available at https://css.ethz.ch/en/publications/risk-and-resilience-reports.html .

[39] Competing in Space, The National Air And Space Intelligence Center (NASIC), January 23, 2019, p.19. (Available at: https://www.nasic.af.mil/About-Us/Fact-Sheets/Article/1738710/competing-in-space/)

[40] Cybersecurity Principles for Space Systems, A Presidential Document by the Executive Office of the President on 09/10/2020, (Citation code 85 FR 12345); (Available at: https://www.federalregister.gov/documents/2020/09/10/2020-20150/cybersecurity-principles-for-space-systems).

[41] The SSA Space Weather Service Network, ESA 2020, (Available at: https://swe.ssa.esa.int/current-space-weather)

[42] UCS Satellite Database, Updated on May 1, 2021, (Available at: https://www.ucsusa.org/resources/satellite-database)

[43] NASA Computers Hacked By Intruders, in Via Satellite, December 1, 2008. (Available at: https://www.satellitetoday.com/government-military/2008/12/01/nasa-computers-hacked-by-intruders)

[44] Denise Chow, German Satellite Fell to Earth Over Indian Ocean's Bay of Bengal, in Space.com, October 25, 2011. (Available at: https://www.space.com/13385-dead-german-satellite-earth-fall-indian-ocean.html)

[45] What are the 5 Domains for the NIST Cybersecurity Framework?, September 9, 2020 (Available at: https://www.scasecurity.com/nist-security-framework/)

[46] Office of the Under Secretary of Defense for Acquisition & Sustainment Cyber Security Maturity Model Certification, (Available at: https://www.acq.osd.mil/cmmc/faq.html); CYBER SECURITY & SPECIALTY CONSULTANTS, COMPLIANCE & CERTIFICATION (Available at: https://cyberssc.com/cmmc).

[47] Space Environment Statistics, ESA, Last updated on August 11, 2022, (Available at: https://sdup.esoc.esa.int/discosweb/statistics/)

[48] Phys, About 3% of Starlink satellites have failed so far, October 26, 2020 (Available at: https://phys.org/news/2020-10-starlink-satellites.html)

[49] Matt Williams, About 3% of Starlinks Have Failed So Far, October 24, 2020, https://www.universetoday.com/148514/about-3-of-starlinks-have-failed-so-far/; Denise Chow, SpaceX says up to 40 Starlink satellites lost to geomagnetic storm, Feb. 10, 2022, https://www.nbcnews.com/science/space/spacex-says-40-starlink-satellites-lost-geomagnetic-storm-rcna15516

[50] Definition of the large constellations and mega constellations: The Impacts of Large Constellations of Satellites, by Gordon Long, JSR-20-2H, JASON, The MITRE Corporation, November 2020 (Updated: January 21, 2021), p.11. https://bit.ly/3c6GLDZ

[51] OST Art. IX

[52] International Space Law: United Nations Instruments, United Nations Office For Outer Space Affairs, May 2017, p.7

[53] Christopher D. Johnson, The Legal Status of MegaLEO Constellations and Concerns About Appropriation of Large Swaths of Earth Orbit, in: J. Pelton (Ed.), Handbook of Small Satellites, Springer, Cham, 2020, p. 5, doi:10.1007/978-3-030-20707-6_95-1. https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties.html.

[54] Sarah M. Mountin, The Legality and Implications of Intentional Interference with Commercial Communication Satellite Signals, 90 INT'L L, STUD 101 (2014) 101–197.

[55] ESA spacecraft dodges large constellation, ESA Website, 03/09/2019, https://www.esa.int/Space_Safety/ESA_spacecraft_dodges_large_constellation.

[56] Christopher M. Petras, The Use of Force in Response to Cyber-Attack on Commercial Space Systems - Reexamining Self-Defense in Outer Space in Light of the Convergence of U.S. Military and Commercial Space Activities, in J. Air L. & Com., 2002; S.E. Nicol; G. Walton; L.D. Westbrook; D.A. Wynn, Future satellite communications to military aircraft,Volume 12, Issue 1, February 2000, pp. 15–26; Major William C. Ashmore, Impact Of Alleged Russian Cyber Attacks, U.S. Army,School of Advanced Military Studies, United States Army Command and General Staff College, Fort Leavenworth, Kansas, AY 08/09, May 2009; Harmful interference to satellite systems, ITU-R WRS18 Contribution 5, Space Services Department, 2018-10-03, https://www.itu.int/md/R15-WRS18-C-0005/en .

[57] *Ibid*. Art.4.A non-exhaustive list of these ongoing initiatives is described in detail, including the titles: Extension and use of the international monitoring system (IMS) related to space services; Promotion of exchange of experiences, cooperation, joint organization and participation in related fora; Provisions of technical and regulatory assistance to ITU members; Recommendation on access procedures for fixed-satellite service occasional use, transmissions to GSO space stations in the 4/6 GHz and 11-12/13/14 GHz FSS bands (ITU-R S.2049, December 2013); Recommendation on Carrier ID (ITU-R S.2062-0, September 2014); New Recommendation on Detection and Resolution of radio frequency interference to Earth exploration-satellite service (passive) sensors (ITU-R RS 2106-0, July 2017); New Report on Measurement Techniques and New Technologies for Satellite Monitoring. (Report. ITU-R SM.2424-0, June 2018); De-

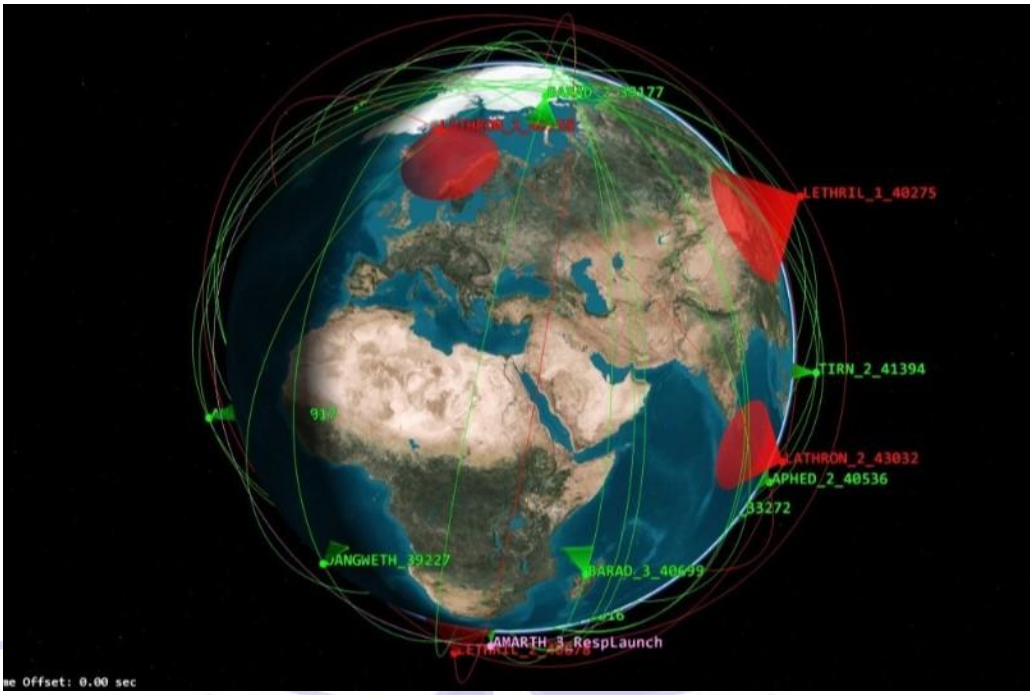
velopment of Working Document towards a Preliminary Draft New Rec. ITU-R SM.[APP10] on reporting harmful interference in Support of Appendix 10; Implementation of a Satellite Interference Reporting and Resolution System (SIRRS)
[58] Colin Clark, US Must Improve Cyber Protection For Sats: Aerospace Corp, November 07, 2019; https://breakingdefense.com/2019/11/us-must-improve-cyber-protection-for-sats-aerospace/;
[59] Maxime Puteaux and Alexandre Najjar, Analysis: Are smallsats entering the maturity stage?, in SpaceNews, August 6, 2019; https://spacenews.com/analysis-are-smallsats-entering-the-maturity-stage/.
[60] Article VI of the Outer Space Treaty states that "the activities of non-governmental entities shall require authorization and continuing supervision." It is important to note that the Article VI is not self-executing, meaning that it is not enforceable until the domestic implemetation legislation as to is enacted. Therefore, private actors may operate in outer space, even without authorization or supervision, and the national and other regulatory agencies may not rely on Article VI to attempt to deny private actors access to space.
[61] ITU Constitution Article 6.1: "The Member States are bound to abide by the provisions of this Constitution, the Convention and the Administrative Regulations in all telecommunication offices and stations established or operated by them which engage in international services or which are capable of causing harmful interference to radio services of other countries….."
[62] ITU Constitution Article 45: "All stations, ….. must be established and operated in such a manner as not to cause harmful interference to the radio services or communications of other Member States or of recognized operating agencies, or of other duly authorized operating agencies which carry on a radio service, and which operate in accordance with the provisions of the Radio Regulations."
[63] ITU Constitution Article 48: Though military radio installations are generally exempt from the ITU regime, yet "these installations must, so far as possible, observe statutory provisions relative …… to the measures to be taken to prevent harmful interference……."
[64] ITU Radio Regulations Article 15.1 § 1 : All stations are forbidden to carry out unnecessary transmissions, or the transmission of superfluous signals, or the transmission of false or misleading signals, or the transmission of signals without identification …
[65] ITU Radio Regulations Article 15.2 § 2 :Transmitting stations shall radiate only as much power as is necessary to ensure a satisfactory service.
[66] Lewis Dartnell, What is space junk and why is it a big problem?, in BBC Sky At Night Magazine, April 15, 2022; https://www.skyatnightmagazine.com/space-missions/space-junk/

Appendix 5

V

A. Salmeri and A. Carlo. Security-by-Design Approaches for Critical Infrastructure: Mapping the Landscape of Cyber and Space Law. *NATO Legal Gazette*, 42(1):97–113, 2021[1]

[1]Reprinted from the NATO Legal Gazette, issue 42 (December 2021). The NATO Legal Gazette is produced and published by Headquarters Supreme Allied Commander Transformation (HQ SACT). The NATO Legal Gazette is not a formal NATO document and does not represent the official opinions or positions of NATO or individual nations unless specifically stated. The NATO Legal Gazette is an information and knowledge management initiative, focused on improving the understanding of complex issues and facilitating information sharing. HQ SACT does not endorse or guarantee the accuracy of its content. All authors are responsible for their own content. Any further publication, distribution, or use of all or parts from these articles are required to remain compliant with the rights of the copyright holder. Absent specific permission, the NATO Legal Gazette cannot be sold, republished, or reproduced for commercial or promotional purposes.



Source : https://ac.nato.int Photo based on screenshot from AGI

Security-by-Design Approaches for Critical Infrastructure: Mapping the Landscape of Cyber and Space Law[1]

by Avv. Antonino Salmeri, Adv. LL.M[2] and Mr. Antonio Carlo[3]

Introduction

After more than half a century of space activities, scientific and technological progress has led to the blossoming of new technologies that have deeply impacted both civil and military spheres. Since the launch of the first artificial satellite, the cyber and space domains have gradually become

[1] **DISCLAIMER**: The views expressed in this article are solely those of the authors and may not necessarily represent the views of NATO, Allied Command Operations, or Allied Command Transformation, or of their affiliated organizations.

[2] Doctoral Researcher in Space Law at the University of Luxembourg and registered attorney at the Italian BAR, antonino.salmeri@uni.lu

[3] PhD Candidate at Tallinn University of Technology, ancarl@taltech.ee

two faces of the same coin and now one could not exist without the other. The strengthening of relations between these two domains holds the potential to bring disruptive changes to both environments, as showcased by the 'big data' phenomenon as well as by the emergence of cyber-attacks as a new category of threats. In recent years, the space sector has witnessed a new, fourth industrial revolution[4] resulting in the development of new emerging disruptive technologies (EDTs) and breakthroughs like artificial intelligence. The development of these new technologies further influenced the interconnection between the cyber and space domains and ultimately led to their "democratisation", with a multitude of public and private actors currently conducting activities in these fields. On the one hand, the interrelations between cyber and space allow for their mutual support in terms of defence and resilience. On the other one, the close interconnection of the cyber and space domains has aggravated the threat that EDTs pose to their respective critical infrastructure. This context is further complicated by the legal status of outer space as enshrined in Articles I and II of the Outer Space Treaty (OST)[5], as well as by the fragmented nature of international law, which pose additional challenges to the effective enforcement of existing national and international regulations. In this situation, the dependence of North Atlantic Treaty Organization's (NATO) military operations on cyber and space technologies exposes the organization to new types of vulnerabilities. In light of the critical strategic importance of cyberspace and outer space for warfare, security-by-design approaches in the early stages of their conjunct development are not only desirable but indispensable. As part of this process, particular attention should be given to cyber cooperation as an indispensable tool for the mitigation of cyber threats. Ultimately, given the ultra-hazardous nature of space activities, security concepts should extend beyond cyber security to cyber defence and eventually also cyber resilience.

Building on the above premises, this article evaluates and analyses the interrelations between outer space and emerging cyber technologies from the legal and policy viewpoints. Throughout the analysis, particular attention is given to what role could be played by organisations like NATO for the peaceful, sustainable and strategic use of these interconnected domains.

---

[4] Also known as Industry 4.0. It refers to the correlation of physical assets and advanced digital technologies. K. Schwab, *The Fourth Industrial Revolution* (Penguin 2017).

[5] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, entered into force 10 October 1967, 610 U.N.T.S. 205 (hereinafter referred to as "OST").

The context: targets and threats

Over the years, modern Western states have created a model of society that is characterised by a high quality of life, meaning the possibility of accessing a set of 'basic' services and opportunities that are made available to each citizen to express their attitude and fulfil their needs. From this perspective, the quality of life is defined by, for example, energy supply services, health protection, the transport system, the banking system and in recent years, space and cyber activities. Therefore, it is important to better understand the real dependence of society on those infrastructures that allow the provision of services that characterise the quality of life. These infrastructures have been called 'critical' and the need to protect their existence and correct functionality is synonymous with the need to safeguard the quality of life. To this end, critical infrastructure can be defined as "an asset, system or part thereof located in [a state] which is essential for the maintenance of vital societal functions […] and the disruption or destruction of which would have a significant impact in a [state] as a result of the failure to maintain them".[6] Critical infrastructure has therefore become a natural target of malicious attacks, as the impact produced is relatively high compared to the effort needed to generate the event itself.

For these reasons, critical infrastructure has become increasingly vulnerable to the rise of EDTs. As mentioned, EDTs include those technologies that are cutting-edge and that have potential opportunities in the Information and communications technology (ICT) sector.[7] For instance, in October 2019, the NATO Defence Ministers identified eight EDTs in the areas of data, quantum, artificial intelligence (AI)[8], autonomy, space, hypersonic, biotechnology, and materials.[9] These areas tend to be extremely broad and have significant

[6] Council Directive (EC) 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.
[7] NATO, 'NATO Advisory Group of Emerging and Disruptive Technologies' (Annual Report 2020). https://www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/210303-EDT-adv-grp-annual-report-2020.pdf accessed April 2021.
[8] The first definition of AI appeared in 1956 during a workshop on AI at Dartmouth University. Since then, many definitions have followed. John McCarthy, also known as the father of AI, defined AI as "the science and engineering of making intelligent machines". LIAO Matthew, *Ethics of Artificial Intelligence* (Oxford University Press 2020) 3.
[9] NATO Science & Technology Organization, 'Science & Technology Trends 2020-2040: Exploring the S&T Edge' https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf accessed April 2021.

overlaps. In this context, data, AI, autonomy, space and hypersonics are regarded as 'disruptive' while developments in quantum, biotechnology and materials are seen as 'emergent' as they still require more time to mature.[10] The development of new EDTs has led to the rise of new threats. The growing sophistication of the tools and techniques available to malicious actors, combined with the increasing digitisation, has resulted in new challenges to security. These threats can be classified as kinetic and non-kinetic. Kinetic threats are those that attempt to strike directly or detonate a weapon near a satellite or other space stations.[11] Non-kinetic threats involve weapons that have physical effects on space systems without any physical contact such as in electronic and cyber warfare.[12] Since this article explores the connections between the cyber and space domains, the present analysis will focus mainly on non-kinetic threats, particularly in the cyber field. In this respect, while cyberattacks are not a new threat to the space industry, malicious cyber actors have become much more sophisticated. These cyber actors usually stem from one of the following four categories:[13] nation state actor, private economic actor, hacktivists/natural persons and international entities.[14] These actors can either be the instigator of an attack, responsible for the attack, the victim or collateral victim of the attack. As technology continues to evolve, so do the opportunities and challenges it poses. In particular, the ever-increasing dependence on technologies exposes us to a whole set of risks associated with cyberattacks. Hostile cyber actors are continuously trying to break into close and highly secure systems while the cyber threat landscape continues to expand and evolve rapidly. To counter these issues, space systems' security and defence need to be constantly updated, secured, and monitored. Many governments, companies, and international organisations have created ad hoc Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) coordinated by Security Operational

[10] They are expected to mature in a timeframe of 20 years, *supra* nota 9.
[11] A. Carlo, L. Lacroix, L. Zarkan, 'The challenge of protecting space-based assets against cyber threats' (71st International Astronautical Congress 2020).
[12] A. Carlo, N. Veazoglou, 'ASAT Weapons: Enhancing NATO's Operational Capabilities in the Emerging Space Dependent Era' (6th International Conference Modelling and Simulation for Autonomous Systems 2019).
[13] P. Wallace, R. J. Schroth, W. H. DeLone Cybersecurity Regulation and Private Litigation Involving Corporations and their Directors and Officers: A Legal Perspective (Kogod Cybersecurity Center. Kogod School of Business, American University 2015).
[14] Supra note 11.

Centres (SOCs) in order to pre-empt and, if necessary, confront possible cyber events.[15]

The cyber domain is vast and presents different subcategories such as cyber-security, cyber-crime, cyber-terrorism, cyber-sabotage, cyber-attack, cyber-war, information warfare, cyber-espionage, etc. These are just some of the terms denoting the criminal use of the cyber network. They go hand in hand with the evolution of these phenomena and with the legislative developments that attempt to regulate them while it becomes increasingly difficult to cope with the protection of critical infrastructure, or the complexity deriving from the combination of Information and Communication Technology (ICT) with the key management systems of the functions of modern companies.[16] The online market now offers highly specialised products and services to commit criminal activities and / or carry out cyber threats (crime-as-a service), modifying the more traditional and hierarchical forms of organised criminal groups, in favour of networks characterised by fluidity, changeability and transience.[17] These networks are formed on the basis of limited actions and projects that are limited in time and objectives, thanks to the work of professional freelance cyber-criminals who sell their skills and tools (malware, zero-day exploits, or access to botnets) to criminal and terrorist groups. Furthermore, the growing specialisation of cybercriminals exponentially increases the offensive capabilities of other traditional criminals who do not possess this technological know-how. There are various organised underground markets (with sellers, buyers and intermediaries) implemented through online forums and characterised by different degrees of accessibility and technology. For instance, 80-90% are cyber-criminals with basic skills who essentially sell financial or counterfeit goods, while 10-20% make up highly qualified individuals who sell products and sophisticated tools, suitable for targeting individuals, companies, organisations, government bodies, etc.[18] This market can be further divided into single 'cyber-professionals' or those structured in small groups (70%), criminal organisations (20%), cyber-terrorists (5%), cyber-criminals hired by government agencies (4%), and activists (1%).[19] Although this is a global

[15] Samuele De Tomas Colatin, 'National Cybersecurity Organisation: Italy', in National Cybersecurity Governance Series (CCD-COE 2020).
[16] Schmitt N. Michael, Brian T. O'Donnell, *Computer Network Attack and International Law* (Naval War College 2002) (hereinafter referred to as "CNAIL").
[17] European Cybercrime Centre, *The Internet Organised Crime Threat Assessment* (Europol 2014).
[18] Stefan Fafinski, *Computer Misuse. Response, Regulation and the Law.* (Routledge 2013).
[19] ibid.

market, the most prominent cybercriminals that conduct malware attacks come from China, Latin America, and Eastern Europe. Russia, Romania, Lithuania, Ukraine and other Eastern European countries feature more prominently for those targeting financial institutions.[20] Vietnam is most known for threats related to e-commerce, and the United States of America (a more recent trend) for financial crimes.[21] In total, 1670 cyber-attacks were carried out in 2019 – an increase of 7.6% from 2018 and 91.2% compared to 2014.[22] Today, cyber-crime is the main cause of attack, while malware is the most used medium.[23]

The overall landscape seems to be heading towards the creation of a new generation of sophisticated criminal cyber-organisations, with larger and more specialised dimensions. These are transformations that will have consequences on traditional organised criminal groups, terrorist groups and activist groups, while the recruitment of freelance cyber-criminals will be replaced by the birth of structured and solid joint ventures, and with the development of internal cyber resources within criminal groups. The greatest risk is posed by the possibility of a significant convergence of criminal interests with a wider exchange of skills and services between these groups.[24] The trends that can be deduced from the current developments of cybercrime shows an increase in more sophisticated and multipurpose attacks, in the number and types of attacks, but also in the number of targets and victims and the related economic damage.

A first trend regards theft and manipulation of sensitive data.[25] Sensitive data is an asset that is increasingly abused by cybercriminals to perpetrate their criminal activities. The increasing digitisation of information and the increase in the collection, processing and storage of data (resulting from the growth of cloud services, hosting, Internet of Things) increases the risk associated with intrusions or identity theft. The abuse of this data ranges from the traditional fraud scheme (of credit cards or bank credentials), to extortion or cyber-

[20] Centre for Strategic and International Studies, 'Significant Cyber Incident' https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents accessed April 2021.
[21] A. Antonielli et al, *Rapporto Clusit 2020: sulla sicurezza ITC in Italia* (CLUSIT 2020).
[22] ibid.
[23] ibid.
[24] CNAIL, supra note 16.
[25] European Union Agency for Cybersecurity, *Physical Manipulation/Damage/Theft/Loss: From January 2019 to April 2020* (ENISA Threat Landscape 2020).

espionage (industrial / government).[26] In addition, 'crime as a service' allows for the purchase of clean data resold in blocks and customised to the needs of the buyer(s). In this context, there is an increase in intrusions within the infrastructures of logistics and transport companies, often perpetrated to facilitate traditional criminal activities. Some analysts further suggest that the increasing introduction of automated systems that are managed remotely will result in more attention being paid to crime and related attempts to use systems for illicit purposes.[27]

A second trend concerns counterfeiting activities.[28] The varied illegal markets on the Surface Web and the Deep Web will lead to the almost exclusive placement of the sale of counterfeit products online, increasingly targeted at the current and future needs of consumers: from toothpastes to detergents, from medicines to vaccines, from medical equipment to professional services in general, there will be more and more counterfeits. This has already resulted in increasingly sophisticated illegal marketplaces, accurate replicas of legal websites to deceive potential buyers.[29]

A third trend includes cryptocurrencies and money laundering.[30] Cryptocurrencies, most prominently Bitcoin, are an expanding payment system caused by a growing number of companies offering e-commerce services and Bitcoin-ATMs. On the one hand, this type of currency exposes those who use it to the risk of having their e-wallets or 'exchanges' (the entities that convert cryptocurrency into 'fiat' currency) violated. On the other hand, it could facilitate criminal activities. The possibility of carrying out monetary exchanges protected by a pseudonym and outside of the controls of traditional financial circuits, creates greater possibilities for the development of illicit trade of material or professional services (including 'crime as a service'), with both online and offline exchanges. In addition, 'niche' cryptocurrencies, unlike traditional ones, offer even greater security and, above all, anonymity, and have proven to be even more efficient in covering up criminal activities.[31]

---

[26] European Union Agency for Cybersecurity, Cyber Espionage: From January 2019 to April 2020 (ENISA Threat Landscape 2020).
[27] J.B. Hill, N.E. Marion, *Introduction to Cybercrime* (Praeger 2016).
[28] Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA [2019] OJ L123/18.
[29] CNAIL, supra note 16.
[30] R. Houben, A. Snyers, *Cryptocurrencies and Blockchain: Legal context and implications for financial crime, money laundering and tax evasion*, (European Parliament 2018).
[31] M-H Maras, *Computer Forensics* (Jones & Bartlett 2014).

The growing specialisation of cybercriminals goes hand in hand with the creation of a network of increasingly differentiated and personalised services for criminal activities by actors without specific IT skills.[32] For example, it has become comparatively easy to not only acquire (for sale or rent) packages of malware, especially banking Trojans and Zero-day exploits, but also receive tutorials and online advice for their implementation at a reasonable price: in 2013, exploit kits cost between $1,000 and $2,000, and could be rented for $200 to $600 per week or $600 to $1,200 per month. It is also possible to access Botnet to facilitate the implementation of distributed 'Denial of Service' attacks aimed at compromising the functionality of different types of online services (banking, e-commerce, etc.).[33] Botnets can also be used to send spam and phishing emails, or to anonymise attacks and fraud on the web.[34]

These trends underline the objectives of recent cyber threats, especially if considering developments in ICT, namely the 'Internet of Things', the 'Internet of Everything' and 'Bring Your Own Device' (BYOD). Due to these, more and more people will be connected to the network of their companies or institutions, making the systems more prone to large-scale attacks. For example, combinations of malware that can infect computers and mobile devices are spreading as a result of the increasing use of smartphones to authenticate online services. Similarly, fake apps, service applications, games, etc., which contain misleading malware, are becoming more and more widespread.[35]

Legal Shortcomings

The development of international space law dates back to the late 1950s. Even before the Sputnik satellite was launched on 4 October 1957, the entire international community worried about the results of a possible expansion of the rivalry between superpowers in outer space. They expressed the idea that space constituted a dimension beyond the sovereignty of states, not susceptible to appropriation, where terrestrial rivalries could not be translated: a *res communis* characterised by a substantial freedom of passage,

---

[32] SIMARGL, *"Nexus of Cyberspace Actors" in Work Package 3: Legal, Social Sciences and Humanities Aspects of the SIMARGL Toolkit to Detect and Counter Malware and Stegomalware* (European Commission 2019).
[33] Supra note 30.
[34] European Union Agency for Cybersecurity, 'Botnets', https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/botnets accessed April 2021.
[35] U. Kohl, A. Charlesworth, *Information Technology Law* (Routledge 2016).

similarly to what is established for the high seas.[36] While involving the overflight of the territory of numerous states, the launch of the first satellite did not cause any protest from the underlying countries, which never claimed their sovereignty could extend to the space covered by the satellite's orbits. The passage into space therefore appeared free from the first moment as long as it was conducted 'for peaceful purposes'.[37] Between 1958 and today, space was the subject of several resolutions by the United Nations General Assembly. During the XIII session of the UN General Assembly (UNGA), on 13 December 1958, 'questions on the peaceful use of Outer Space' were discussed: during the debate, almost all states used the term 'peaceful' as opposed to 'military'.[38] The General Assembly, underlining the innovative nature of activities in space, stigmatised the need for international cooperation so that the exploration and use of space were preserved "solely for peaceful purposes."[39] For this purpose, the UNGA established a Committee on Peaceful Uses of Outer Space (COPUOS),[40] a political body further composed of two sub-committees: scientific and legal. The mandate of COPUOS is to promote international cooperation in space and develop its regulations through a series of recommendations for the consideration of the UNGA.[41] Following, UNGA Resolution 1472 (XIV) of 13 December 1959 introduced the principle that the peaceful use of space and its exploration should be directed for the sake of humanity and the progress of all states.[42] To complement that, UNGA Resolution 1721 A (XVI), adopted unanimously by the General Assembly in 1961, established that Outer Space and celestial bodies are open to the exploration and to the use of all states, in accordance with international law, and are not subject to national appropriation.[43] These resolutions have been the first legal documents addressing outer space and have defined a regulatory framework based on programmatic principles expressing the desire to maintain international peace and security, but deliberately leaving the normative content to be attributed to each of these terms undefined.[44] It was believed

[36] P.M. Martin *Droit des Activités Spatiales* (Masson 1992).
[37] F. Francioni, F. Pocar, *Il regime Internazionale dello Spazio* (Giuffré 1993).
[38] Institute of Air and Space Law, *Air and Space Law* (vol. XL 2015).
[39] M. Cervino, B. Corradini, S. Davolio "Is the 'Peaceful Use' of Outer Space Being Ruled Out?", 19 Space Policy 231-237.
[40] UNGA Res 1348 (XIII), (13 December 1958)
[41] Sergio Marchisio,) "Il ruolo del Comitato delle Nazioni Unite sugli usi pacifici dello spazio extra-atmosferico (Copuos)" in P.A. Pillitu (ed) *Scritti in onore di Giorgio Badiali*, (Aracne 2007).
[42] UNGA Res 1472 (XIV) (13 December 1959).
[43] UNGA Res 1721 (XVI) (20 December 1961).
[44] M. Gestri, "Portata e limiti del principio dell'uso pacifico nel diritto dello spazio", in F. Francioni, F. Pocar (eds) "Il regime internazionale dello spazio" (Giuffré 1993).

that they could be specified later, taking into account political and technological developments.

On 10 October 1967, the "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies", also known as the Outer Space Treaty,[45] entered into force providing the foundational basis of international space law. This treaty regulates the exploration and use of the space domain, including the moon and other celestial bodies, by states. The treaty notes that space is free to be explored by all states and is not subject to national claims of sovereignty.[46] It prohibits the deployment of nuclear weapons in space,[47] although strategic and geopolitical competition has always been a driving force for space exploration. It should be noted that the treaty does not place a legal ban on the placement of conventional weapons in space, and anti-satellite weapons have been successfully tested by the United States, USSR and China.[48] The treaty was approved by the UNGA in 1963 and signed in 1967 in the USSR, United States and the United Kingdom. As of June 2020, 110 countries are parties to the treaty, while another 23 signed the treaty but did not ratify it.[49] Four other treaties have been negotiated and drafted by the United Nations Commission on the Peaceful Use of Outer Space, namely the 1968 Astronaut Rescue Agreement[50], the 1972 Space Liability Convention (LIAB),[51] the 1975 Convention on registration of objects launched into space[52] and the 1979 Treaty on the Moon.[53] As briefly showed, the current framework regulating human activity in outer space dates back to a historical period in which the concept and use of space itself was different from that of today. This makes this framework less adequate to regulate and protect cyberspace activities,

[45] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, entered into force 10 October 1967, 610 U.N.T.S. 205 (hereinafter referred to as "OST").
[46] ibid Article I.
[47] Ibid Article IV.
[48] Supra note 12.
[49] ibid.
[50] Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space (entered into force 3 December 1968) 672 U.N.T.S. 119 (hereinafter referred to as "Rescue Agreement").
[51] Convention on International Liability for Damage Caused by Space Objects (entered into force 9 October 1973, 961 U.N.T.S. 187 (hereinafter referred to as "LIAB").
[52] Convention on Registration of Objects Launched into Outer Space (entered into force 15 September 1976) 1023 U.N.T.S. 15 (hereafter referred to as "Registration Convention").
[53] Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (entered into force 11 July 1984) 1363 U.N.T.S. 3 (hereinafter referred to as "Moon Treaty").

requiring an increasingly urgent update and integration with the strategic and economic issues at stake.

From a strategic-military point of view, space proves to be a vital sector for defence and security, the importance of which is becoming increasingly clear for many countries. Faced with an ever less distant and increasingly indispensable space for citizens' lives, the European institutions have recognised its importance in supporting their policies, for industrial, economic and political reasons, and for security and defence purposes.[54] The recognition of the duality of EU-ESA cooperation programmes has even led to the assumption of a different interpretation of the latter's mandate, in a sense more suited to the expansion of intrinsically dual-space products.[55] Following the innovations introduced by the Lisbon Treaty,[56] which attributes explicit competence to the Union in Space matters, albeit in accordance with its own Member States, an architecture of relations between the two international organisations has also been established, consolidating their independence and specifying the terms of their partnership.[57] This does not, however, exclude the possibility that their relationship may not evolve towards greater integration in the future. From a strictly political-diplomatic and strategic perspective, space appears as a stage for relations between states and an economic, political, military and cultural centre of gravity, in which a growing number of players are making their way. The space dominance of the United States therefore seems to be threatened on the one hand by the expansion of Russian and European Space activities, and on the other by the growth of space activities in emerging countries. These are determined to use their political-diplomatic and symbolic potential and acquire technologies capable of accelerating their economic development. Among these, China poses a particular challenge, due to a lack of transparency and reliability, especially following the anti-satellite test of 2007, and the lack of separation between its civil and military space activities.[58]

---

[54] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions EU Space Industrial Policy Releasing the Potential for Economic Growth in the Space Sector, COM/2013/0108.
[55] European Commission, 'EU funding for Dual Use: Guide for Regions and SMEs' (Enterprise and Industry 2014).
[56] EU Treaty (Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community).
[57] ibid.
[58] Supra note 12.

These aspects underline a series of shortcomings in the current regulation of space activities when integrated with cyber operations. One of them concerns the risks of an uncontrolled transfer of technology. Establishing a framework for the export of space products and technologies is particularly critical and, in some cases, may require a sacrifice of commercial interests for the benefit of states' national security. At the same time, it is important to establish a balanced framework. As demonstrated by the case of the United States International Traffic in Arms Regulation (ITAR),[59] which is currently under review, where too strict frameworks may pose significant obstacles to the transfer of technology between countries cooperating on space projects. Further shortcomings affecting the suitability of international space law to regulate and address cyber-threats are the notions of damage, space object and space activities. Under Article VII OST, damage caused by a space-object triggers international liability: "each State Party from whose territory or facility an object is launched is internationally liable for damage to another State Party to the Treaty."[60] According to LIAB, damage means the "loss of life, personal injury or other impairment of health; or loss of or damage to property of States or of persons, natural or juridical, or property of international intergovernmental organizations".[61] The question is therefore whether electronic damage, impeding the correct functioning of a given space infrastructure, qualifies as compensable damage under international space law. Further to that, to be compensated, damage needs to be caused by a space object.[62] The LIAB defines this term as including "component parts of a space object as well as its launch vehicle and parts thereof".[63] Therefore, the question is whether electronic communications constitute or not 'component parts' of Internet of Things satellites. Lastly, the lack of a definition of space-activities raises the question whether the use of satellites for malicious cyber operations qualifies as illegal use of space in breach of Articles I, III, IV and IX of OST.

In addition to this, both cyber and space normative systems are also addressed in general public law, as well as in various domestic legal frameworks.[64] In this complex multi-level context, and in light of the rapid evolution of cyber and space activities, developing precise laws and policies

[59] 22 CFR §§121-130.
[60] Article VII OST, supra note 5.
[61] Article I LIAB, supra note 51.
[62] ibid.
[63] ibid.
[64] A. Carlo, 'Cyber Threats to Space Communications: Space and Cyberspace Policies' in *Outer Space and Cyber Space: Similarities, Interrelations and Legal Perspectives* (Springer & European Space Policy Institute 2021).

that would perfectly address all the relevant issues may very well be a vain attempt. Hence, the abovementioned shortcomings could be addressed through evolutionary interpretation of general principles and international harmonisation of policies.

Policy Approaches

For NATO, cyber challenges play an increasingly critical role, as an alliance is 'only as strong as its weakest link', especially in the cyber space and on policy areas that require a high degree of cooperation and communication. In recent years, the number of actors involved in cyberattacks has increased. Identifying the perpetrator and/or the victim of the attack is essential and international cooperation is required. In the space sector, and particularly for projects related to the development of observation capabilities, two actors cooperating internationally are of particular note: France, through the Centre national d'études spatiales (CNES), and more recently Italy, through the Agenzia Spaziale Italiana (ASI).[65] The signing of the first agreement[66] with the European Space Agency (ESA) is also recent, which opens up cooperation on space technology in areas such as astrophysics, satellite engineering, environmental monitoring, the prevention of natural disasters, and telecommunications. Last but not least, there is the question of the use and security of the management information systems of all related tools. In 2019, ESA launched the 'Funding & support of Space-based services for cyber security' project, aimed at companies that develop innovative products and services in the ITC field. In particular, the project focuses on initiatives, based on satellites that can mitigate the risks to cyber security and increase the resilience of existing services, infrastructures and operations.[67] In addition, products are sought that improve end-to-end cyber security of space-based applications. The key areas of the project "are transport (sea, land and air, including autonomous vehicles); energy, utilities and critical infrastructures; finances and, public safety".[68]

---

[65] Agenzia Spaziale Italiana "Galileo: il nuovo programma europeo di navigazione in Mediaplanet, Space" Il Sole 24 ore, 3.

[66] European Commission and European Space Agency sign agreement to support innovation in the space sector, https://ec.europa.eu/growth/news/european-commission-and-european-space-agency-sign-agreement-support-innovation-space-sector_en accessed April 2021.

[67] ESA, "Funding & support of Space-based services for cyber security", in Business Applications (2019).

[68] F. Bussoletti, "Spazio: ESA guarda alle aziende per migliorare la cyber security", in Difesa & Sicurezza (2019).

In the past decade, the United States has developed various strategy documents covering the improvement of cybersecurity in the space domain, including the 2017 National Security Strategy,[69] 2018 National Cyber Strategy,[70] Space Policy Directive-3,[71] and Space Policy Directive-5 (SPD-5). [72] The latter directive is the most relevant, as it promotes the development of a government framework that incorporates cybersecurity into all phases of space systems.[73] This directive aims to increase cyber protections for critical space infrastructure. The SPD-5 requests space operators to consider developing a culture of prevention, active defence, and sharing of best practices. This is done by "safeguarding command, control, and telemetry links using effective and validated authentication or encryption measures" and by adopting cybersecurity "hygiene practices, physical security for automated information systems, and intrusion detection methodologies".[74] Moreover, SPD-5 encourages operators to share information, best practices and analysis through the Space Information Sharing and Analysis Centre (S-ISAC).[75]

The sharing of best practices and unique know-how to prevent, strengthen, and reconstruct a system following a cyber-event can only be achieved through strong national and international cooperation. To guarantee strong and efficient sharing of information, ISACs have been established to make data on cyber threats and events, as well as best practices to counter them, more accessible internationally. In this sense, ISACs provide a central resource for gathering information on cyber threats and events related to critical infrastructure.[76] Leveraging on this role of ISACs, constant monitoring of the activities and risk assessment may lead to the reduction of such events. Strong cooperation between different international organisations is fundamental to build a resilient cyber and space

[69] United States, "National Security Strategy of the United States of America" (The White House 2017).
[70] United States, "National Cyber Strategy of the United States if America" (The White House 2018).
[71] United States, "Space Policy Directive-3, National Space Traffic Management Policy" (The White House 2018).
[72] United States, "Space Policy Directive-5, Cybersecurity Policy for Space Systems" (The White House 2020).
[73] ibid.
[74] Executive Office of the President, (2020) Space Policy Directive-5: Cybersecurity Principles for Space Systems, FR Doc. 2020-20150.
[75] Supra note 11.
[76] ITU, "Guide to developing a National Cybersecurity strategy. Strategic Engagement in Cybersecurity" (Geneve 2018).

infrastructure.[77] In 2003, the European Union (EU) and NATO signed the Berlin Plus Agreement[78], which allows for the EU to use NATO forces if and when necessary. Based on the same principle of cooperation, in 2016, the EU and NATO signed a Technical Arrangement to facilitate technical info-sharing between the European CERT and the NATO Computer Incident Response Capability.[79] Currently, the NATO Cooperative Cyber Defence Centre of Excellence[80] is liaising with the European Defence Agency by exchanging information on common topics of concern.

In 2020, the UK proposed a draft UN resolution calling for a "global discussion on what would constitute responsible behaviour in space"[81] following wide-ranging consultations with international actors. As Foreign Secretary Dominic Raab stated, "a new approach is urgently needed to increase trust and confidence between countries operating in space to prevent an arms race or a conflict that could have catastrophic consequences".[82] To construct a strong and resilient system, public and private cooperation, cyber diplomacy, as well as the establishment of CERTs and SOCs that monitor and organise cyber operations, are essential.

Conclusion

Current satellite capabilities allow the management of ever greater portions of civilian and military critical infrastructure management systems through IT systems. However, computer systems are susceptible to attacks by cybercriminals (individual or organised) at national and, especially, transnational level, which requires the coordination of actions against such criminals. In addition, distinguishing 'non-military' from 'military' roles has become more challenging in the cyber and space domains, as many dual-use technologies can be used for both civil and military purposes.[83] This makes it

[77] B. Boutros-Ghali, "International Cooperation in Space for Security Enhancement" (10 Space Policy 265-276).
[78] EU-NATO Berlin Plus Agreement, 16 December 2002. https://www.nato.int/cps/en/natolive/official_texts_19544.htm accessed April 2021.
[79] NATO, 'NATO and the European Union enhance cyber defence cooperation' (10 February 2016) https://www.nato.int/cps/en/natohq/news_127836.htm accessed April 2021.
[80] P. Meyer, "Outer Space and Cyberspace. A tale of Two Security Realms", in Osula A.M, Roigas H (eds), *International Cyber Norms: Legal, Policy & Industries Perspectives*, Tallinn, NATO CCD-COE, 115-169.
[81] UK 'UK push for landmark UN resolution to agree responsible behaviour in space' (26 August 2020) https://www.gov.uk/government/news/uk-push-for-landmark-un-resolution-to-agree-responsible-behaviour-in-space accessed April 2021.
[82] ibid.
[83] Caroline Baylon, 'Challenges at the Intersection of Cyber Security and Space Security' in

more difficult to define key terminology, contributing to a lack and inadequacy of internationally agreed definitions. In turn, this lack has impeded the development of multilateral arms control agreements and has discouraged cooperation, fostering an "ambiguity of intent" and adding to the cycle of escalation.[84] Dual-use technologies also mean that a complete ban on certain technologies and the implementation of adequate measures to verify compliance are often impractical. This further adds to existing difficulties in reaching arms control agreements. Moreover, due to this dual-use aspect, it has become more challenging to determine whether a country engages in military activities beyond its civilian programme. As Caroline Baylon states, this "has a direct impact on ambiguity of intent surrounding countries' actions and thus further stimulates the escalatory cycle".[85]

As a matter of security, the regulation of space and cyber always requires a strong involvement of states seeking autonomy and strategic independence. This need for independence is by all means a new 'stake' in international relations, insofar as it represents an attribute of power and is the subject of negotiation. This is exemplified by Europe's path towards the acquisition of independent access to space and of an autonomous satellite navigation system. Here, too, some questions still remain unanswered. It remains to be clarified what use should be made of Galileo's encrypted positioning signal, how the 2004 Agreement for compatibility with GPS[86] will be implemented, and how to solve the problem of overlapping frequencies with the Chinese Beidou system. As for access to space, it will be necessary to understand how to face the increasingly aggressive competition in the international launcher market, and how to ensure the effectiveness of the liability discipline.

In this context, there are two particularly pressing issues that should be addressed immediately: the verification and implementation of the assets that are adopted in this area, and the implementation of the current perspectives for coordinating the cybersecurity policies of satellite communication systems. Both space and cyber activities have their own national and international regulatory framework which, although often lacking with respect to the demands that gradually arise and poorly integrated into the international arena, forms the basis for desirable future developments. What is missing is the

Country and International Institution Perspectives (Chatham House 2014).

[84] ibid. p.8

[85] ibid. p.10

[86] Agreement on the Promotion, Provision and Use of Galileo and GPS Satellite-Based Navigation Systems and Related Applications [2011] OJ L348/3.

overall vision: a formal coordination between the two areas in terms of policies and assets that has not yet been achieved. A first step in this direction can be seen in the UK draft proposal to the UN on responsible behaviour in space. This has created a new movement to develop more responsible and sustainable space international policies. However, international cooperation is only as strong as the need to exchange and share particular benefits. This cooperation is put at risk with many private businesses entering the space market, creating competition that may ultimately result in less cooperation between state actors. Analysts and specialists in their respective fields and in international politics have highlighted the interconnections between space and IT activities, finding various replies in national programmatic documents and guidelines, but not in a univocal nor uniform and coordinated way among the global players. Therefore, the development of close relationship between space and cyber policies and diplomacy emerges as necessary tool to preserve and strengthen their continuing relevance in the future.[87]

***

[87] Attila Mesterhazy, NATO-*EU Cooperation after Warsaw*, (NATO Parliamentary Assembly, Defence and Security Committee Report 2017).

Appendix 6

VI

A. Carlo. Cyber Threats to Space Communications: Space and Cyberspace Policies. *Studies in Space Policy*, A. Froehlich (eds), 33(1):55–66, 2021

Chapter 4
Cyber Threats to Space Communications: Space and Cyberspace Policies

Antonio Carlo

Abstract Throughout the last decades, modern society has become increasingly dependent on new technological and digital domains. The strengthening of relations between the space and cyber domains holds the potential to bring disruptive changes. National and international guidelines and recommendations constitute the framework within which the coordinating bodies of both areas advance at national as well as international levels. This article aims to provide an overview of the interconnection between the cyber and the outer space domain from a policy standpoint.

4.1 Interconnections

In 1921, General Giulio Douhet affirmed that air, as the third domain of warfare, would upset the balance of the land and sea domains, undermining the importance of borders between States.[1] Similarly, today, the rise of the space and of cyberspace domains has made borders between States even more intangible.

In the twenty-first century, internet and satellite communications play a vital role in everyday life, considering for instance smartphones and applications that require geographical positioning.[2] Each second, millions of often sensitive data set travel via the internet (or even intranets), allowing for communication through satellite systems, both as agents (satellite internet) and as objects (digital satellite management via intranet systems).

[1]Douhet G. "Il Dominio dell'Aria e altri scritti" (2002) Aeronautica Militare, Ufficio Storico.

[2]Agenzia Spaziale Italiana, "Galileo: Il nuovo programma europeo di navigazione" (2008) Space. Alla scoperta del settore spaziale, supplemento a Il Sole 24 ore, December 2008, p. 3, available at http://doc.mediaplanet.com/projects/papers/Space.pdf.

A. Carlo (✉)
TalTech—Tallinn University of Technology, Tallinn, Estonia
e-mail: ancarl@taltech.ee

A. Froehlich (ed.), *Outer Space and Cyber Space*, Studies in Space Policy 33,
https://doi.org/10.1007/978-3-030-80023-9_4

This means that virtually all critical infrastructure depends on satellite systems. Telecommunications, air and sea transport, financial systems, online banking, military communications and defence systems, scientific monitoring, as well as smart grids[3] are all tied to space infrastructure. The latter includes satellites, ground stations and their interconnections to other terrestrial systems.

Today, nearly 1200 satellites operate in outer space on behalf of 60 states or commercial consortia, whose services are used by users from all around the world. The use of cyberspace is even more extensive, with more than three billion users and an estimated exponential growth.[4]

All of this has resulted in the development of an ever-closer interconnection between two domains, otherwise distinct, namely cyber and space. This continuous linkage is followed by the maturation of an increasing interest in creating legal and political solutions and laws able to regulate and protect these areas which is based on the growing dependence of human activities on these systems, especially with regards to critical infrastructures such as communications. The communication sector alone is in continuous expansion due to its democratisation which has led to the exponential increase of private operators.

Since the launch of Sputnik I, the first Soviet artificial satellite, on 4 October 1957, nations all around the world have gradually begun to increase their presence in outer space to ensure the development of civil, scientific and military applications, and, above all, the implementation of civil and military telecommunications. National and international guidelines and recommendations constitute the framework within which the coordinating bodies of both areas advance at national as well as international level.

Today's satellite capabilities enable the management of increasing portions of civil and military critical infrastructure through IT systems. However, these systems can become the target of cybercriminal actions (whether individual or organised) on a national and transnational level, hence requiring the coordination of law enforcement actions against them. Throughout the past decades, the cyberspace and outer space domains have gained increasing importance in the civil and military environment resulting in them now being recognised as the 4th and 5th domain of warfare respectively. This recognition showcases not only the interest but also the past, present and future investments of private, public and international organisations.

Moreover, both outer space and cyberspace can be considered as "common goods", as recognised in various ways by the international community, making them both domains that cannot be subject to national appropriation.[5] For example, the international treaties on outer space state that the use of outer space «must be

[3]Meloni A., Atzori L. "The role of Satellite Communications in the Smart Grid" (2017) In: IEEE Wireless Communications, 2(2), pp. 50–56.

[4]Meyer P. "Outer Space and Cyberspace. A tale of Two Security Realms" (2016) In: Osula A.M., Roigas H. (eds.), International Cyber Norms: Legal, Policy & Industries perspectives, Tallin, NATO CCD-COE, p. 158.

[5]Meyer P. "Outer Space and Cyberspace. A tale of Two Security Realms" (2016) cit., p. 158.

carried out to the advantage and in the interest of all countries […] and must be the province of all mankind».[6] Similarly, the Declaration of Principles adopted by the World Summit on the Information Society (WSIS) in 2005 describes «a people-centred, inclusive and development-oriented information society, where everyone can create, access, use and share information and knowledge».[7]

4.2 Militarisation

The current regulatory framework concerning human activity in outer space dates back to a historical period when the concept and use of outer space substantially differed from today's. This has resulted in an inadequacy to regulate and protect such activities, requiring increasingly urgent modernisation and integration due to the economic issues at stake.

Even before the launch of Sputnik I, the entire international community was concerned about the results of a possible extension of the rivalry between superpowers in outer space. It therefore expressed the idea that space constituted a dimension beyond the sovereignty of states that would not be susceptible to appropriation, a dimension where terrestrial rivalries could not be translated: a *res communis* characterised by a substantial freedom of passage, similarly to that established for the high seas.[8]

The launch of the first satellite, while involving the overflight of the territory of numerous states, did not elicit any protest from any country. Outer space passage therefore appeared free at first, regardless of the purposes of this passage, as long as it was used "for peaceful purposes".

On 13 December 1958, the XIII General Assembly of the United Nations discussed the "peaceful use of outer space issues", during which almost all States used the term "peaceful" as opposed to "military". Emphasising the absolutely innovative nature of outer space activities, the General Assembly stressed the need for international cooperation as long as the exploration and use of space were aimed "exclusively at peaceful purposes".[9] Hence, in 1958, an ad hoc Committee on the Peaceful Uses of Outer Space (COPUOS) was established. This political body was to be composed of two subcommittees, both established in 1961: the Scientific and Technical Subcommittee and the Legal Subcommittee. The purpose of COPUOS

[6]Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, entered into force Oct. 10, 1967, Art. I, 18 U.S.T. 2410, 610 U.N.T.S. 205.

[7]Edmon H., Elder L., Perazzini B. "Connecting ICYs to Development" (2014) London, Anthem, pp. 92–95.

[8]Borrini F. "La componente spaziale nella difesa, Soveria Mannelli" (2006) Rubbettino, pp. 21–25.

[9]Boutros-Ghali B. "International Cooperation in Space for Security Enhancement" (1994) In: Space Policy 10 (4), pp. 265–276.

was the development of international cooperation on space matters and the formulation of its regulations, proposing them to the General Assembly for final approval.

Resolution 1472 (XIV) approved on 13 December 1959, introduced the principle that the peaceful use of space and its exploration should be used for the good of humankind and the progress of all States.[10] On the other hand, resolution 1721 A (XVI),[11] adopted unanimously by the General Assembly in 1961, established that outer space and celestial bodies would be open to exploration and use by all States, in accordance with international law and, above all, that these would not be subject to national appropriation.[12]

These resolutions laid out a general legal framework based on programmatic principles that expressed the desire to maintain international peace and security, but deliberately left the normative content undefined. It was believed that this content could be specified later, taking into account political and technological developments. In fact, it would be the historical-political evolution in the relationship between superpowers which, in the absence of a clear and unambiguous definition, determined its current content and interpretation.

Between 1958 and 2008, outer space was the subject of several United Nations General Assembly Resolutions. More than 50 of them were in relation to international cooperation on the peaceful uses of outer space aimed at avoiding an arms race.[13] Four additional treaties on aerospace law were negotiated and drafted by COPUOS: the 1968 Astronaut Rescue Agreement, the 1972 Space Liability Convention, the 1975 Convention on the Registration of Objects Launched into Space, and the 1979 Treaty on the Moon Convention. However, no legal prohibition evolved on the placement of conventional weapons in outer space, resulting in the successful testing of anti-satellite weapons by the United States, the former Soviet Union, and China.[14]

Moreover, one of the most remarkable developments in the field of outer space law has been the adoption of national space legislation. Even countries with very limited outer space activities have developed national policies, considering the

[10]G.A. Resolution 1472 (XIV), U.N., 14th Sess., International Co-operation in the Peaceful Uses of Outer Space (12 December 1959). Available at https://www.unoosa.org/pdf/gares/ARES_14_1472E.pdf.

[11]G.A. Resolution 1721 (XVI), U.N., 16th Sess., International Co-operation in the Peaceful Uses of Outer Space (20 December 1961). Available at https://www.unoosa.org/pdf/gares/ARES_16_1721E.pdf.

[12]Janokwitsch P. "The Background and History of Space Law" (2015) In: Von der Dunk F., Tronchetti F. Handbook of Space Law, Cheltenham-Northampton, Elgar, pp. 12–44.

[13]Chesterman S., Malone D.M., Villalpano S., "The Oxford Handbook of United Nations Treaties" (2019) Oxford, Oxford University, pp. 186–194.

[14]Association aéronautique et astronautique de France (3AF) Strategy and International Affairs Commission—Writers' Group "The Militarization and Weaponization of Space: Towards a European Space Deterrent" (2008) In: Space Policy, 24 (2), pp. 61–66.

development and the adoption of national space legislation in the future.[15] Reasons behind this phenomenon include the security of foreign investment, self-positioning as an attractive location for launching space objects and the regulation of domestic space activities.[16]

However, national space legislation tends to differ between States. This is due to the specific needs of each State as well as a range of practical considerations. Such diversity has not been welcomed as it has created confusion and uncertainty about the law applicable to outer space activities. On the one hand, this can lead to inconsistent behaviour by space actors licensed by different national authorities. On the other hand, it may lead to opportunities where private operators apply for a license to conduct outer space activities in those countries that offer the most favourable legislative environment.[17]

However, space technologies can be used for both civil and military purposes. This dual-use aspect has implied a total ban on the use of certain technologies and the impracticality of implementing appropriate measures to verify compliance. This has led to difficulties in reaching arms control agreements. In addition, dual-use technologies make it more difficult to ascertain whether a State is developing a military programme in addition to its civil activities or not, directly affecting the ambiguity of intent surrounding States' actions and thus further stimulating the escalation of political tension.[18]

In practice, the militarisation of outer space involves the placement and development of military weapons and technology in space. As previously stated, the first exploration of space in the mid-twentieth century was at least partly motivated by military ambitions, with the United States and the Soviet Union using this as an opportunity to demonstrate their ballistic missile and other relevant military technologies. Since then, outer space has been used as an operational location for military spacecraft including imaging and communications satellites, as well as intercontinental ballistic missiles that are launched on a sub-orbital flight trajectory. As of 2019, known deployments of weapons stationed in space include only space station armaments and guns such as the TP-82 Cosmonaut survival gun (for post-landing and pre-recovery uses).[19]

At the same time, the exploitation of cyberspace for offensive purposes remains scarce when compared to the overwhelming prevalence of its civil uses.[20] Although initially intended for military purposes, it is the civil use of cyberspace, particularly

[15]Esterhazy D. "The Role of the Space Industry in Building Capacity in Emerging Space Nations" (2009) In: Advances in Space Research, 44(9), pp. 1055–1057.

[16]Marbae I. "National Space law" (2015) In: Von der Dunk F., Tronchetti F. Handbook of Space Law, cit., pp. 45–57.

[17]Rosanelli R. "Le attività spaziali nelle politiche di sicurezza e difesa" (2011) Roma, Nuova Cultura—IAI. Available at http://www.iai.it/sites/default/files/iaiq_01.pdf.

[18]Divis D.A. "Military Role Emerges for Galileo" (2002) in GPS World, 13(5), pp. 10–17.

[19]Wong W., Fergusson J., Fergusson J.G. "Military Space Power. A Guide to the Issue" (2010) New York, Praeger.

[20]Meyer P. "Outer Space and Cyberspace. A tale of Two Security Realms" (2016) cit., p. 158.

the internet, that harbours the most criminal activities today. Especially sabotage and espionage have resulted in a new type of conflict namely cyber warfare.[21]

Once again, it is worth reiterating what is expressed in the WSIS Declaration of Principles which highlights the need that «the information society should respect peace», underlining that in a «global culture of cyberspace, security must be promoted, developed and implemented in collaboration with all stakeholders».

In fact, both the use of outer space and cyberspace pose serious challenges to the monitoring and verification of the actions and behaviours of the actors involved. Although a large-scale effort exists to monitor outer space, which is operated mainly by the US military space surveillance network, this is primarily aimed at tracking space debris to avoid collisions. Quite different from this effort is the monitoring of space assets in orbit. It can be argued that in outer space as well as in cyberspace, difficulties exist in verifying compliance with restrictions and in identifying behaviours that violate these restrictions as defined by current agreements.[22]

4.3 Lack of Shared Definitions

As a consequence of many dual-use technologies, the distinction between civil and military purposes is becoming increasingly blurry in both cyber and space.[23] This phenomenon makes it more difficult to define key terminology (particularly war-related terminology) within cyber and outer space, contributing to the lack of or an inadequacy of internationally agreed definitions. This lack also impedes the development of multilateral arms control agreements and discourages cooperation, fostering ambiguity of intent and perceived threats that encourages conflict escalation.

Outer space is a strategic and multidimensional sector and a crossroads for political, strategic, military and economic interests. The picture that emerges, from a legal standpoint, is that of a conventional discipline that has been drawn up in relatively recent times, in which, even if consolidated in the future, grey areas and blurred borders will mostly likely continue to persist.[24]

---

[21]Rajagopalan R.P "Electronic and Cyber Warfare in Outer Space" (2019) Geneve, UNIDIR.

[22]Meyer P. "Outer Space and Cyberspace. A tale of Two Security Realms" (2016) cit., p. 158.

[23]Betza U. "Cybersecurity of NATO's Space-based Strategic Assets" (2019) London, Chatham House. Available at https://www.chathamhouse.org/2019/07/cybersecurity-natos-space-based-strategic-assets.

[24]Brachet G., Deloffre B. "Space for Defence: A European Vision" (2006) In: Space Policy, 22 (2), pp. 92–99; Brachet G. (2004) From Initial Ideas to a European Plan: GMES as an Exemplar of European Space Strategy, in Space Policy, 20 (1), pp. 7–15; Brand S. (2010) Brazil Emerges: A Space Agency With an Eye on Earth, in Tonic Blog. Available at http://www.tonic.com/article/brazil-emerges-a-spaceagency-with-an-eye-on-earth/; Braun F. (2011) Brazil-China Cooperation in Space, in China Digital Times, 10 February. Available at http://chinadigitaltimes.net/2005/01/frank-braun-brazilchina-cooperation-in-space/; Brighel M. (2009) Sicral 1B—le ambizioni spaziali italiane, in Rivista Aeronautica, 85 (3), pp. 84–89.

However, issues such as ambiguity regarding the exact definition of "peaceful purposes" or the absence of a precise delimitation of outer space have led to the adoption of functional solutions. Still, the general nature of the principle of "peaceful purposes" has allowed for the establishment of standards in a high-tech sector characterised by continuous and unstoppable innovation. The lack of stringent limits is therefore not necessarily a negative element but allows for unparalleled flexibility, thus avoiding the risk of rapid obsolescence of definitions. On the other hand, despite a shift in interpretation of some of the principles noted in the outer space treaties, a *status quo* persists due to the general obligation to respect international law and the Charter of the United Nations, particularly concerning the conduct of States in international relations.[25]

From a strategic-military point of view, outer space is proving to be a vital sector for defence and security, as actors are becoming increasingly conscious of the integral part these domains play in military planning and crisis response. As outer space has become increasingly indispensable to the lives of citizens, European institutions have recognised its importance in supporting their policies not only for industrial, economic and political reasons but also for security and defence purposes. The recognition of the significance of cooperation programmes between the European Union (EU) and the European Space Agency (ESA) has even led to a different interpretation of the latter's mandate due to the intrinsically dual-space aspect of space services.

The Lisbon Treaty,[26] which entered into force in 2009, explicitly attributed competence to the EU in space matters albeit together with its member states. It also outlined the vital partnership between the EU and ESA noting, however, their respective independence. From a strictly political-diplomatic and strategic perspective, outer space appears as a centre of gravity for economic, political, military and cultural cooperation between States.[27]

The space dominance of the United States therefore seems to be threatened on the one hand by the expansion of Russian and European space activities, and on the other, by the growth of space activities in emerging countries such as China, India and Japan.[28] The latter are determined to use their political, diplomatic and symbolic potential, but also to acquire technologies capable of accelerating their economic development. Among these, China poses a particular challenge due to a lack of transparency and reliability, especially following the anti-satellite test in 2007. Furthermore, the lack of separation between Beijing's civil and military space activities also brings into question the risks of uncontrolled transfer of technology.

---

[25]UN, Report of the Committee on the Peaceful Uses of Outer Space, New York, UN, 2003.

[26]European Union, Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, 13 December 2007, 2007/C 306/01. Available at: https://www.refworld.org/docid/476258d32.html.

[27]Bini A "Export Control of Space Items: Preserving Europe's Advantage" (2007) In: Space Policy, 23 (2), pp. 70–72.

[28]Harvey B, Smid H, Pirard T "Emerging Space Powers: The New Space Programs of Asia" (2010) the Middle East and South-America, Praxis.

Establishing export controls of space products and technologies is particularly critical and requires a sacrifice in commercial interest for the benefit of States' national security. However, it is important to establish balanced controls, as evidenced by the case of the US International Traffic in Arms Regulations, which is currently under review, and due to barriers to the transfer of technology between countries participating in cooperative projects.[29]

Ultimately, outer space emerges as an issue of sovereignty and requires a strong involvement of states, assuring autonomy and strategic independence.[30] Space thus arises as a new "stake" in international relations, as it represents an attribute of power and, concurrently, forms an object of negotiation.[31] This is demonstrated by Europe's path towards acquiring independent access to outer space and an autonomous satellite navigation system.[32] Here, too, some questions remain unanswered: For instance, it remains to be clarified how the encrypted positioning signal of Galileo[33] should be used, how the 2004 agreement for compatibility with GPS will be implemented, and how to solve the problem of frequency overlap with the Chinese Beidou system.[34] As far as access to space is concerned, it will be necessary to understand how to face the increasingly aggressive competition in the international launcher market, taking into account the strong government backing of the US industry, and how to ensure the effectiveness of liability management at the international level.

4.4 A Security Affair

The combination of outer space and cyber space policies is based on a simple first-order syllogism:

Cyber systems are subject to attack.

Satellite telecommunications are managed through cyber systems.

Satellite telecommunications are subject to cyber-attacks.

---

[29]Moltz J.C "The Changing Dynamics for the Twenty-First-Century Space Power" (2019) in Journal of Strategic Security, 12(1), pp. 15–43.

[30]Boucher M "Is Canadian Sovereignty at Risk by a Lack of an Indigenous Satellite Launch Capability?" (2011) In Space Ref Canada, 4 January 2011. Available at http://spaceref.ca/national-security/is-canadian-sovereignty-at-risk-by-a-lackof-satellite-launching-capability.html.

[31]Braunschvig D, Garwin R.L, Marwell J.C "Space Diplomacy" (2003) in Foreign Affairs, 82 (4), pp. 156–164.

[32]Bujon de l'Estang F, de Montluc B "Making Space the Key to Security and Defence Capabilities in Europe: What Needs to Be Done" (2006) in Space Policy, 22 (2), pp. 75–78.

[33]Agenzia spaziale italiana "Galileo: il nuovo programma europeo di navigazione" (2008) cit.

[34]Dinerman T "China and Galileo" (2006) Continued, in The Space Review, 21 August. Available at http://www.thespacereview.com/article/685/1; Dinerman T (2009) Galileo and the Chinese: One Thing After Another, in The Space Review, 9 February. Available at http://www.thespacereview.com/article/1307/1.

Therefore, it is important to further explore the use and security of the management information system of all instruments operating in outer space, most importantly satellites. In fact, all technologies related to satellites and other space assets must be regularly updated remotely from Earth. These connections, although protected, could still be attacked and "hacked", giving hackers the ability to access all of the target's systems.[35]

Furthermore, space is changing from a selective environment, managed by wealthy States and the academic world with adequate resources, to one where market forces dominate. Today's technologies bring space capabilities within the reach of nations, international organisations, companies and individuals. Moreover, assets that until a few years ago were owned only by government security agencies, are now in the public domain and are available for purchase on the market.[36]

Cyber-attacks to space infrastructures may include jamming (communications disruption), spoofing (data manipulation), and offensive hacks on communication networks. Other malicious actions could be directed against control systems or mission packages, as well as against ground infrastructure such as satellite control centres.[37] Potential sources of threats further include state offensives, military actions, organised crime seeking large financial returns, terrorist groups seeking to advance their causes, and individuals or groups of hackers seeking personal visibility.[38]

In 2019, ESA launched the project "Funding and support of Space-based services for cyber security", aimed at companies developing innovative products and services in the field of Information and Communications Technology (ITC). This project focuses on satellite-based initiatives to mitigate cybersecurity risks and increase the resilience of existing services, infrastructure and operations. In addition, products that improve end-to-end cybersecurity of space applications are sought. Key project areas are transportation (sea, land, and air, including autonomous vehicles), energy, utilities, critical infrastructure, finance and public safety.[39]

In 2017, the International Group of Experts prepared the Tallinn Manual 2.0,[40] the most relevant non-governmental guide on how existing international law applies

[35]Betza U. "Cybersecurity of NATO's Space-based Strategic Assets" (2019) cit.

[36]Livingstone D., Lewis P. "Space, the Final Frontier for Cybersecurity?" (2016) Chatham House, London. Available at https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf.

[37]Carlo A., Veazoglou N. "ASAT Weapones: Enhancing NATO's Operational Capabilities in the Emerging Space Dependent Era" (2019) MESAS 2019, Palermo, Italy. In: Mazal J., Fagiolini A., Vasik P. Modelling and Simulation for Autonomous Systems. 6th International Conference, MESAS 2019, Palermo, Italy.

[38]Rajagopalan R.P. "Electronic and Cyber Warfare in Outer Space" (2019) cit., pp. 6–8.

[39]Duquerroy L. "Cyber Security and Space Based Services" (2019) ESA. Available at https://business.esa.int/sites/default/files/Cybersecurity%20and%20Space%20based%20service_Webinar_Slides.pdf.

[40]Schmitt, M. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations" (2017) In Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press.

to cyber activities. The Tallinn Manual established which acts of States violate the general principles of international law in the context of cyberspace. For instance, according to the Tallinn Manual 2.0, a cyber-operation may qualify as "use of force" amounting to an aggression if it entails the necessary scale and effects—a notion used by the International Court of Justice to qualify certain actions as an armed attack. Furthermore, independent projects are currently underway to develop manuals that will further expand on how international laws apply to not only cyberspace but also military space operations.

Although space and cyberspace are two distinct domains, they are closely interlinked and co-dependent: For instance, outer space operations enable a range of operations in the cyberspace just as control segments of systems in outer space require the use of cyber. Ongoing discussions outside the formal multilateral channels are providing ideas and best practices for the implementation of new policies in both domains. While the International Telecommunication Union has affirmed its competence in cyber questions and has developed a reference guide for States to support the development of national cybersecurity strategies, States have not yet come to an agreement on an international regulatory framework for cyber activities. Similarly, wider questions on outer space may also remain unanswered until either States formally agree to a framework of rules or an armed conflict evolves in outer space. This may further indicate that such hostilities will occur in the medium to long-term at the juncture between outer space and cyberspace.

4.5 Policy and Assets Implementation

In 2014, the National Institute of Standards and Technology (NIST) published the Risk Management Framework and the Cybersecurity Framework providing a policy framework for ITC. Even though the NIST cybersecurity maturity standards and guidelines are not directly applicable to the space domain, these are best suited to covering ground-based space infrastructure and assets by assisting organisations in improving their cybersecurity measures and best practices. While efforts have been made to adjust these frameworks to space systems,[41] standards for spacecraft and their associated IoT systems need to be addressed in the near future.

Governance efforts in the space and cyber domains remain highly siloed which has limited meaningful progress. In the past decade, the US has developed various strategy documents covering the improvement of cybersecurity in the space domain, including the 2017 National Security Strategy, 2018 National Cyber Strategy, Space Policy Directive-3, and Space Policy Directive-5 (SPD-5). The latter directive, issued by the Trump administration in September 2020, is the more relevant, representing a government framework that incorporates cybersecurity into

[41]See for instance the 1253F framework by the Committee on National Security Systems Instruction.

all phases of space systems. This directive aims to increase cyber protections for critical US space infrastructure, such as global communications, navigation, and national security applications.

The SPD-5 aims to develop a culture of prevention, active defence, risk management, and the sharing of best practices to establish cybersecurity protocol. This includes «cybersecurity hygiene practices, physical security for automated information systems, and intrusion detection methodologies».[42] Moreover, SPD-5 encourages public and private space operators to share information, best practices and analysis through the Space Information Sharing and Analysis Centre (S-ISAC) operated by the National Cybersecurity Centre (NCC). Even though SPD-5 serves as a high-level policy directive, it should not be understood as a substantive IT governance framework or standard. Therefore, there are urgent issues that need to be addressed immediately, namely the verification and implementation of the assets being adopted in this area and the implementation of the current outlook for the coordination of cybersecurity policies for satellite communication systems.[43]

Both space and cyber activities have their own national and international regulatory frameworks which form the basis for promising future developments, even though these may often be lacking (with respect to the demands that gradually arise) and, above all, are poorly integrated into the international arena.[44] What seems to be absent is an overall vision: A formal coordination between the two areas in terms of policies and assets has not yet been achieved.[45] While analysts and specialists in their cyber and space fields have highlighted the interconnections between outer space and IT activities, pointing to various documents and national policy guidelines, they lack a unified voice and coordination.[46] In fact, both outer space and cyberspace have not yet been the object of strict international regulations aimed at preserving their initially peaceful character.[47] The absence or, at least, the limitation of policy interventions in this regard, constitutes an area of development for all states and supranational institutions, given the widespread recognition of their increasing vulnerability to attacks.[48]

[42]Executive Office of the President "Space Policy Directive-5: Cybersecurity Principles for Space Systems" (2020) 09 September. Available at https://www.federalregister.gov/documents/2020/09/10/2020-20150/cybersecurity-principles-for-space-systems.

[43]Ertan A., Floyd K., Pernik P., Steens T. "Cyber Threats and NATO 2030: Horizon Scanning and Analysis" (2020) Tallin, NATO CCD-COE.

[44]ITU "Guide to developing a National Cybersecurity strategy. Strategic Engagement in Cybersecurity" (2018) Geneve, ITU.

[45]European Union Agencies for Cybersecurity "Good Practices in Innovation under National Cyber Security Systems" (2019) Candia, ENISA.

[46]Falco G. "Cybersecurity Principles for Space Systems" (2018) in Journal of Aerospace Information's Systems, 16 (2), pp. 1–10.

[47]Goh Meishan G. "Dispute settlement in international space law" (2007) Leiden-Boston, Nijhoff.

[48]Meyer P. "Outer Space and Cyberspace. A tale of Two Security Realms" (2016) cit., p. 159.

It will have to be observed how the interconnections between elements in cyber and outer space further develop, both in their domain and beyond. Gaining this understanding will be essential to better grasp how these elements interact with each other and how their resilience can be ensured.

Antonio Carlo is currently working at NATO HQ. He is also a PhD candidate at the Tallinn University of Technology specialising in space and cyber, particularly in defence and telecommunication.

Curriculum Vitae

1. Personal data

Name	Antonio Carlo
Date and place of birth	22.08.1992, Rome, Italy
Nationality	Italian

2. Contact information

Address	Tallinn University of Technology, School of Information Technologies, Ehitajate tee 5, 19086 Tallinn, Estonia
E-mail	antonio.carlo@taltech.ee

3. Education

2020–2024	Tallinn University of Technology, School of Information Technologies, PhD studies
2020–2021	Università degli Studi di Roma "La Sapienza", Faculty of Political Science, Master's degree in Geopolitica e Sicurezza Globale, MASII *110/110*
2017–2018	Università degli Studi di Roma "La Sapienza", Faculty of Political Science, Master's degree in Political Science, MA *110/110*
2016–2018	Pontifical Institute for Arabic and Islamic Studies, Postgraduate Foundation Diploma in Arabic and Islamic Studies, *cum laude*
2014–2016	Università degli Studi di Roma "La Sapienza", Faculty of Political Science, Master's degree in International Relations, MA *110/110 cum laude*
2011–2014	LUISS, Faculty of Political Science, Bachelor's degree in Political Science, BSc

4. Language competence

Arabic	intermediate
English	fluent
French	intermediate
German	beginner
Italian	native
Spanish	intermediate

5. Professional employment

Since 2022	EuroFighter Jagdflugzeug GmbH
2020–2022	North Atlantic Treaty Organization, NATO HQ
2019–2020	Deloitte Risk Advisory S.r.l., Cyber Security
2018–2019	European Commission, DG GROW
2017–2018	European Space Agency

6. Defended theses

- 2021, Le dinamiche dell'islam radicale: l'IS, MASII, Università degli Studi di Roma "La Sapienza", Faculty of Political Science
- 2018, I Servizi e la Costituzione, Prof. Dr. Paolo Mezzanotte, MA, Università degli Studi di Roma "La Sapienza", Faculty of Political Science
- 2018, 'Umar b. al-Ḥaṭṭāb: L'uomo e il Califfo, Prof. Dr. Don Valentino Cottini, Pontifical Institute for Arabic and Islamic Studies
- 2016, La rappresentanza politica e il mandato parlamentare nell'esperienza Cecoslovacca, MA, supervisor Prof. Dr. Fulco Lanchester, Prof. Dr. Giulia Caravale, Università degli Studi di Roma "La Sapienza", Faculty of Political Science
- 2014, Luigi Romersa: Biografia di un inviato di Guerra, BA, supervisor Prof. Dr. Vera Capperucci, Università Luiss Guido Carli, Faculty of Political Science

7. Field of research[2]

- 2.7 Law
- 4.6 Computer Science
- 4.7 Information and Communication Technologies

8. Scientific work

1. A. Carlo and P. Breda. Impact of Space Systems Capabilities and Their Role as Critical Infrastructure. *International Journal of Critical Infrastructure Protection*, 45(100680), 2024
2. A. Carlo, N. P. Mantı, B. A. S. W. Am, F. Casamassima, N. Boschetti, P. Breda, and T. Rahloff. The Importance of Cybersecurity Frameworks to Regulate Emergent AI Technologies for Space Application. *Journal of Space Safety Engineering*, 10(4):474–482, 2023
3. P. Breda, A. Adbin, R. Markova, D. Jha, A. Carlo, and N. P. Mantı. An extended review on cyber vulnerabilities of AI technologies in space applications: Technological challenges and international governance of AI. *Journal of Space Safety Engineering*, 10(4):447–458, 2023
4. A. Carlo, N. P. Mantı, P. Breda, M. R. de Beaumont, and D. Jha. Towards a Resilient Cyber Architecture for Space Infrastructures: Mitigating the New Attack Vectors. In IAC, editor, *International Astronautical Congress*, volume D5,4,5,x78079, 2023
5. S. Bonnart, A. Capurso, A. Carlo, T. F. Dethlefsen, M. Kerolle, J. Lim, A. Pickard, A. Russo, and L. C. Zarkan. Cybersecurity Threats to Space: From Conception to the After-maths. In Space Law in a Networked World. *Brill | Nijhoff*, P.J. Blount, M. Hofmann (eds), 19(1):39–101, 2023
6. A. Carlo and N. Boschetti. Modelling the Impact of Space Situational Awareness Disruption on the European and Arctic Security Landscape. In J. Mazal, A. Fagiolini, P. Vašík, A. Bruzzone, S. Pickl, V. Neumann, P. Stodola, and S. L. Storto, editors, *Modelling and Simulation for Autonomous Systems*, volume 13866, 2023

[2]Estonian Research Information System (ETIS) field of research

7. K. Nyman-Metcalf, H. Mölder, A. Kasper, and A. Carlo. *Survey on "Space as NATO's fifth military environment international law and dual-use space systems in this context"*. Ministry of Foreign Affairs, 2022

8. G. Falco, W. Henry, M. Aliberti, B. Bailey, M. Bailly, S. Bonnart, N. Boschetti, M. Bottarelli, Byerly, J. Brule, A. Carlo, G. D. Rossi, G. Epiphaniou, M. Fetrow, D. Floreani, N. G. Gordon, D. Greaves, B. Jackson, G. Jones, R. Keen, S. Larson, D. Logsdon, T. Mail-lart, K. Pasay, N. P. Mantii, C. Maple, D. Marsili, E. M. Miller, J. Sigholm, J. Slay, C. Smethurst, J. D. Trujillo, N. Tsamis, A. Viswanathan, C. White, E. Wong, M. Young, and M. Wallen. An International Technical Standard for Commercial Space System Cybersecurity - A Call to Action. In ASCEND, editor, Methods and Considerations for Cyber Protection of Space Assets, 2022

9. A. Carlo, F. Casamassima, G. Costella, and A. Salmeri. Going Green, Staying Strong: An Operational Roadmap for "NATO Climate" Legal and Policy Tools. *NATO Legal Gazette*, 43(1):47–58, 2022

10. A. Carlo, N. P. Mantıa, B. Aswam, F. Casamassima, N. Boschetti, P. Breda, and T. Rahloff. Understanding Space Vulnerabilities: Developing Technical and Legal Frameworks for AI and Cybersecurity in the Spatial Field. In IAC, editor, *International Astronau-tical Congress*, volume D5,4,7,x704606, 2022

11. A. Carlo and F. Casamassima. Going Digital, Staying Secure: Cyber ERM Activities in a Post-Pandemic Setup. In IAC, editor, *International Astronautical Congress*, volume D6,4,9,x70417, 2022

12. M. Lecas, A. Carlo, J. Mendoza, N. Moraitis, G. Leterre, B. G. Gonzalez, T. Owen, D. Raghu, G. Rotola, A. Salmieri, and M. Das. This Is Our Space: Contributions from the Young Generations for Sustainable Space Activities. In IAC, editor, *International Astronautical Congress*, volume E3,4,10,x68775, 2022

13. P. Breda, A. Adbin, R. Markova, D. Jha, A. Carlo, and N. P. Mantı. Cyber Vulnerabilities and Risks of AI Technologies in Space Applications. In IAC, editor, *International Astronautical Congress*, volume D5,4,1,x70380, 2022

14. N. P. Mantı, A. Carlo, R. Markova, D. Jha, P. Breda, A. Abdin, and N. Boschetti. AI Systems to Ensure Cyber Security in Space. In IAC, editor, *International Astronautical Congress*, volume D5,4,2,x70423, 2022

15. D. Jha, N. P. Mantı, A. Carlo, L. C. Zarkan, P. Breda, and A. Jha. Safeguarding the Final Frontier: Analyzing the Legal and Technical Challenges to Mega-Constellations. *Journal of Space Safety Engineering*, 9(4):636–643, 2022

16. D. Jha, P. Breda, A. Carlo, L. Zarkan, D. Stefoudi, and N. P. Mantı. Safeguarding the Final Frontier: Analyzing the Legal and Technical Challenges to Mega-Constellations, Managing Risk in Space. In IAASS, editor, *International Association for the Advancement of Space Safety Conference Managing Risk in Space*, 2021

17. E. Mayerick, A. Pickard, T. Rahloff, S. Bonnart, A. Carlo, and K. Thangavelm. Ground Station as a Service: A Space Cybersecurity Analysis. In IAC, editor, *International Astronautical Congress*, volume D5,4,5,x66555, 2021

18. A. Carlo and F. Casamassima. Space Industry: Applications and Implications of Digital Transformation. In IAC, editor, *International Astronautical Congress*, volume D5,2,9,x65506, 2021

19. A. Carlo and F. Casamassima. Securing Outer Space through Cyber: Risks and Countermeasures. In IAC, editor, *International Astronautical Congress*, volume D5,4,3, x64939, 2021

20. L. Cesari, A. Carlo, T. Dethlefsen, N. Manti, D. Stefoudi, and L. Roux. Space as NATO's Operational Domain:The Case of the Cyber Threats against GNSS. In IAC, editor, *International Astronautical Congress*, volume E9,2,7,x66298, 2021

21. A. Carlo and L. Roux. Emerging Technologies and Space. In J. Mazal, A. Fagiolini, P. Vasik, M. Turi, A. Bruzzone, S. Pickl, V. Neumann, and P. Stodola, editors, *Modelling and Simulation for Autonomous Systems*, volume 13207, 2022

22. A. Salmeri and A. Carlo. Security-by-Design Approaches for Critical Infrastructure: Mapping the Landscape of Cyber and Space Law. *NATO Legal Gazette*, 42(1):97–113, 2021

23. A. Carlo and A. Salmeri. Legal Solutions for the Peaceful, Sustainable and Strategic Utilization of Lunar Resources. *NATO Legal Gazette*, 42(1):165–177, 2021

24. A. Carlo. Cyber Threats to Space Communications: Space and Cyberspace Policies. *Studies in Space Policy*, A. Froehlich (eds), 33(1):55–66, 2021

25. A. Carlo and N. Perucica. Artificial Intelligence: Walking the Line between Military Deterrence and Interstate Cooperation. In USSTRATCOM, editor, *6th Annual U.S. Strategic Command Academic Alliance Conference and Workshop*, 2021

26. A. Carlo. Artificial Intelligence in the Defence Sector. In J. Mazal, A. Fagiolini, P. Vasik, and M. Turi, editors, *Modelling and Simulation for Autonomous Systems*, volume 12619, 2021

27. A. Carlo, L. Lacroix, and L. Zarkan. The Challenge of Protecting Space-based Assets against Cyber Threats. In IAC, editor, *International Astronautical Congress*, volume E9,2.D5.4,11, 2020

28. A. Carlo and N. Veazoglou. ASAT Weapons: Enhancing NATO's Operational Capabilities in the Emerging Space Dependent Era. In J. Mazal, A. Fagiolini, and P. Vasik, editors, *Modelling and Simulation for Autonomous Systems*, volume 11995, 2020

29. A. Carlo and N. Giannakou. Active Debris Removal: The Legal Challenges and the Way Forward. In AIDAA, editor, *XXV International Congress of Aeronautics and Astronautics*, 2021

30. A. Carlo and G. Petrovici. Legal Challenges of Space 4.0: The framework conditions of legal certainty among States, International Organisations and Private Actors in the changing landscape of space activities. In IAC, editor, *International Astronautical Congress*, volume E7,1,8,x46219, 2018

Elulookirjeldus

1. Isikuandmed

Nimi	Antonio Carlo
Sünniaeg ja -koht	22.08.1992, Rooma, Itaalia
Kodakondsus	Itaalia

2. Kontaktandmed

Aadress	Tallinna Tehnikaülikool, infotehnoloogia teaduskond, Ehitajate tee 5, 19086 Tallinn, Estonia
E-post	antonio.carlo@taltech.ee

3. Haridus

2020–2024	Tallinna Tehnikaülikool, infotehnoloogia teaduskond, doktoriõpe
2020–2021	Rooma La Sapienza Ülikool, riigiteaduste teaduskond, magistrikraad geopoliitikas ja globaalses turvalisuses, MASII *110/110*
2017–2018	Rooma La Sapienza Ülikool, riigiteaduste teaduskond, magistrikraad politoloogias, MA *110/110*
2016–2018	Paavstlik araabia ja islami uuringute instituut, Aspirantuuri sihtasutuse diplom araabia ja islami uuringutes, *cum laude*
2014–2016	Rooma La Sapienza Ülikool, riigiteaduste teaduskond, magistrikraad rahvusvahelistes suhetes, MA *110/110 cum laude*
2011–2014	LUISS, riigiteaduste teaduskond, bakalaureusekraad politoloogias, BSc

4. Keelteoskus

Araabia keel	vahepealne
Inglise keel	kõrgtase
Prantsuse keel	vahepealne
Saksa keel	algaja
Itaalia keel	emakeel
Hispaania keel	vahepealne

5. Teenistuskäik

Alates 2022	EuroFighter Jagdflugzeug GmbH
2020–2022	North Atlantic Treaty Organization, NATO HQ
2019–2020	Deloitte Risk Advisory S.r.l., Cyber Security
2018–2019	European Commission, DG GROW
2017–2018	European Space Agency

6. Kaitstud lõputööd

Kaitstud lõputööde loetelu on toodud ingliskeelses elulookirjelduses.

7. Teadustöö põhisuunad

- 2.7 Õigusteadus
- 4.6 Arvutiteadused
- 4.7 Info- ja kommunikatsioonitehnoloogia

8. Teadustegevus
Teadusartiklite, konverentsiteeside ja konverentsiettekannete loetelu on toodud ingliskeelse elulookirjelduse juures.

ISSN 2585-6901 (PDF)
ISBN 978-9916-80-161-1 (PDF)