**Facoltà di Scienze Politiche, Sociologia, Comunicazione**

**Dipartimento di Scienze Politiche**

DOTTORATO DI RICERCA IN DIRITTO PUBBLICO, COMPARATO E INTERNAZIONALE

**XXXIV Ciclo**

Tesi di Dottorato

# SPACE CYBERSECURITY: THE INTERSECTION BETWEEN SECURITY OF CRITICAL NATIONAL INFRASTRUCTURES AND SUSTAINABILITY OF OUTER SPACE ACTIVITIES

Candidata:
Dott.ssa Laura María de Lourdes Jamschon Mac Garry (*)

Tutor
Chiar.mo Prof. Sergio Marchisio

A.A. 2021/2022

(*) The views expressed in the present thesis are strictly personal and do not necessarily reflect the views of the Argentine Republic.

# PREFACE

## *The dialogue among Ada, Valentina and Eilene: Intertemporal fiction or reality?*

Ada was born in the bosom of a turbulent aristocratic family in the years of the English Romanticism apogee. Her favourite science was mathematics, but she used to meet with great novelists, such as Charles Dickens; and her father himself was a renowned poet. French literature, arithmetic and music were part of her daily education. Mary Somerville, Charles Babbage and Augustus de Morgan were her tutors and governesses in mathematics. The latter was convinced that such hard sciences should remain out of bounds for women, although he accepted one exception: Maria Agnesi, credited as the first woman mathematician.

To the contrary, Valentina was not a British aristocratic lady but a Soviet textile worker. She was proud of who then became her good friend, Yury Alekseyevich Gagarin, the first man in space. She and her girlfriends used to imagine the first woman in space; probably differently from how men used to imagine them... with a lipstick tube attached to their '*yastreb*'.

These two ladies shared the same passion for flying, but certainly not in the same way. Ada was a pilot and Valentina, a cosmonaut. So different, but so similar...aviation is considered to be the cradle of spaceflights...

Eilene: *Your friends have created a lot of trouble for us! Now, I am trying to help my boss to sort out this mess and I am burning the midnight oil studying how to establish an American Administration to defeat those crazy guys in this space race...*

Valentina*: Are you sure you want to waste your time? My friends are too tough! Wouldn't you prefer to join us flying? It's more fun than spending your time studying boring and complicated things that only lawyers understand...*

Ada*: Well, I think Eilene is doing a great job. According to my numbers, she has 93% of chances to be promoted if the bill establishing an American space agency is passed, although the chances of defeating*

*the Soviets are the result of multiplying the variables of time and human resources by the political will, which is measured in binary numbers 0 and 1...*

When Babbage envisaged his Analytical Engine -based on the binary code used by the jacquard loom (an exemplar of this textile manufacturer is exhibited in the Museo Nazionale Scienza e Tecnologia Leonardo da Vinci, in Milan), he did not imagine a lady would develop an extraordinary thing that would change our daily lives.

Eilene*: I don't think this needs be so complicated, Ada. We just have to convince the Americans and the Soviets to cooperate and forget about this race...If we reach this goal we will also avoid another race...the arms race...*

Eilene was a national defence expert, graduated in political sciences but with a long career as a legal advisor in the American Legislative Reference Service. She was well versed in missiles and outer space, but she wanted a peaceful outer space, where States could cooperate without bureaucratic hurdles to use and explore it for the benefit of mankind.

Valentina*: Ok, ladies...I am more interesting in flying. I have to train hard because otherwise I won't be able to cope with zero gravity. I am still trying to get used to digesting my noodles with dried tomato sauce...*

Eilene: *COPUOS is our hope for international cooperation and a system of international space law, where weapons in outer space are forbidden and States can conduct their experiments in peace.*

Ada: *What do you mean by weapons? Does it mean that if I create a programme that changes the velocity of a Soviet satellite or its position and direct it towards the sun until it burns up completely, I would become a fighter?*

Eilene: *Well, it doesn't matter if you are a fighter, that's not a legal concept or at least we should first explain its meaning. The most important thing is whether a State is responsible for space activities, or if it is liable for damage, and if it is accountable to pay compensation to the Soviets for the damage you caused with your space assets.*

Valentina: R*esponsible, liable, accountable...I don't understand, there is no translation into Russian! Anyway, Ada, let me know if you are planning to attack my friends!*

Eilene: *Of course, she won't...we three want outer space for peaceful purposes only!*

Valentina: *For 'peaceful purposes' is enough, Eilene. Don't complicate things as lawyers usually do. Remember I belong to the Air Force and I still dream of flying on a Vostok up to the skies!*

Valentina finally spent three fascinating days appreciating the halo of the Earth from the skies 48 times, before coming back to her beloved Yaroslavl. She experienced the fall of the iron curtain at first hand.

Eilene finally drafted legislation that ultimately became the National Aeronautics and Space Act of 1958 (NASA Act). She was also closely involved in the American Delegation to COPUOS and in the formation and evolution of the International Institute of Space Law (IISL) and the International Academy of Astronautics (IAA).

Ada invented the 'science of operations', what we call today the 'science of computing'. Note G (a part of a comprehensive interpretation of a paper written by Federico Luigi Menabrea on the Babbage's machine) is considered by some to be the first computer programme, and it was written by her. Her notes were published under the title 'Sketches of the Analytical Engine by Charles Babbage', in a number of the Scientific Memoirs of 1843.

Ada Lovelace was born on 10 December 1815 and is considered to be the first computer programmer. Eilene Galloway came into this world on 4 May 1906 and was called the 'grand dame of space' and was one of the space law pioneers. Valentina Tereshkova was born on 6 March 1937 and gained fame after becoming the 'first lady' of space. Three impressive women; so different but so complementary.

In 1843 it was impossible to imagine touching space with your hands, creating a computer programme to have control over a space object, or even less making others lose control over it. The hopes for an international regime to halt these fears are still a challenge. This is the present, but it would not be a reality without a past. Three women made huge steps in the field of hard sciences and space governance, and with them, left traces in history.

In the present research, space cybersecurity combines the passion for computers and outer space that Ada and Valentina experienced, with a legal and political focus –Eilene's passion. The author will have the challenge of conducting holistic research, combining

science, politics and law. This thesis has a multidisciplinary approach in a century where women have gained recognition for their academic endeavours but still struggle for more equality and for the end of stereotypes.

## ABSTRACT

The title of this thesis already conveys the idea that space cybersecurity is addressed in this research taking into consideration two main aspects: first, that space systems are critical infrastructures and thus play an important role in State security and international stability. Second, that space security, space safety and long-term sustainability of outer space activities cannot be disassociated but require a holistic approach.

This thesis focuses on the problem of how international space law applies to space cybersecurity, how international law in general may fill the regulatory gaps and how the international community may address future negotiations. The research is motivated on the need to expand the global space governance taking into account current mechanisms in the United Nations on security in the use of information and communication technologies and in space security, space safety and long-term sustainability of outer space activities.

On the basis of six research questions, this thesis develops the relevant arguments along its six chapters to conclude with a proposal for a resolution of the General Assembly containing principles governing space cyber activities. The proposed normative solution would be negotiated at the Committee on the Peaceful Uses of Outer Space (COPUOS) and considered jointly by the First and Fourth Committees of the General Assembly.

In the course of this research, three main methods were employed: analysis of relevant international law, examination of national positions at relevant multilateral bodies and domestic/intergovernmental legal frameworks; and finally, consideration of teachings of qualified publicists. It is a qualitative study based on a selection of representative State practice and is envisaged as a multidisciplinary approach to the matter, including technological, legal and political aspects.

This thesis concludes with the assessment that international space law and international law in general provide a certain legal ground to regulate space cybersecurity; thus, a set of principles adopted by the General Assembly would provide a preliminary element of guidance in the field. That solution is envisaged as an initial step in a task that needs to be progressive. Throughout this work, several issues connected to the research topic are examined but many of them remained inconclusive, either due to the lack of State practice

or insufficient state of the art. Consequently, certain areas are identified at the end of this study for further research.

# RIASSUNTO

Il titolo di questa tesi fornisce già un'idea del fatto che la cybersecurity spaziale viene affrontata in questa ricerca prendendo in considerazione due aspetti principali: primo, che i sistemi spaziali sono infrastrutture critiche e quindi giocano un ruolo importante nella sicurezza dello Stato e nella stabilità internazionale. Secondo, che la sicurezza spaziale ('security' e 'safety') e la sostenibilità a lungo termine delle attività spaziali non possono essere dissociate ma richiedono un approccio olistico.

Questa tesi si concentra sul problema di come il diritto internazionale dello spazio si applichi alla cybersecurity spaziale, di come il diritto internazionale in genere possa colmare le lacune normative e di come la comunità internazionale possa affrontare i futuri negoziati multilaterali. La ricerca è motivata dalla necessità di espandere la governance spaziale tenendo conto degli attuali meccanismi delle Nazioni Unite sulla sicurezza nell'uso delle tecnologie dell'informazione e della comunicazione; e sulla sicurezza spaziale ('security' e 'safety') e la sostenibilità a lungo termine delle attività nello spazio extra-atmosferico.

Sulla base di sei domande di ricerca, questa tesi sviluppa gli argomenti rilevanti lungo i suoi sei capitoli per concludere con una proposta di risoluzione dell'Assemblea Generale che contiene principi che devono regolare le attività cibernetiche spaziali. La soluzione normativa proposta verrebbe negoziata presso il Comitato delle Nazioni Unite per l'Uso Pacifico dello Spazio Extra-atmosferico (COPUOS) e considerata congiuntamente dal Primo e Quarto Comitato dell'Assemblea Generale.

Nel corso di questa ricerca, sono stati impiegati tre metodi principali: l'analisi del diritto internazionale pertinente, l'indagine delle posizioni nazionali presso gli organismi multilaterali pertinenti e i quadri giuridici nazionali e intergovernativi; e infine, la considerazione degli insegnamenti di pubblicisti qualificati. Si tratta di uno studio qualitativo basato su una selezione di pratiche statali rappresentative ed è previsto un approccio multidisciplinare alla questione, includendo aspetti tecnologici, legali e politici.

Questa tesi si conclude con la valutazione che il diritto internazionale dello spazio e il diritto internazionale in genere forniscono un certo quadro normativo per regolare la cybersecurity spaziale; così, un insieme di principi adottati dall'Assemblea Generale

fornirebbe un primo elemento di orientamento nel campo. Questa soluzione è concepita come un primo passo in un compito che deve essere progressivo. Nel corso di questo lavoro sono state esaminate diverse questioni legate al tema della ricerca, ma molte di esse sono rimaste inconcludenti, sia per la mancanza di pratica statale che per l'insufficiente stato dell'arte. Di conseguenza, alla fine di questo studio vengono identificate alcune aree per ulteriori ricerche.

## ACKNOWLEDGMENTS

A Ph.D. student is a bunch of emotions, life experiences, bright and dark moments, in which the research and learning processes insert and evolve complementing and enriching individual human aspects. Throughout my research, I encountered great mentors who marked me and to whom I owe my most sincere gratitude.

I would first like to thank my supervisor, Professor Sergio Marchisio, whose extensive expertise in multilateral negotiations and space law was an invaluable source of inspiration in my research. I am deeply grateful that he accepted to go along with me in this process, which is a great honour. My research would have not been possible without the openness of the Sapienza University and the support of the Ph.D. coordinator, Professor Fabio Giglioni, the Scientific Committee and the administrative staff. I want to express my sincere gratitude to the whole Sapienza team for welcoming me warmly into this prestigious institution.

When I started my studies, I was posted in Vienna as a member of the Embassy and Permanent Mission of Argentina, whose head was Ambassador Rafael Mariano Grossi – now current Director General of the International Atomic Energy Agency (IAEA). He belongs to the group of those bosses who let you spread your wings, so I am immensely grateful for his support in my academic endeavours.

I also want to thank Minister Felix Menicocci, former Secretary General of CONAE (Comisión Nacional de Actividades Espaciales), with whom I shared many COPUOS sessions. I am particularly grateful to physicist Alberto Ridner, former Manager of Technological Projects at CONAE, for his patient, generous and permanent assistance at every stage of the research project.

I would like to express my sincere gratitude to Professor Maureen Williams, Honorary Chair of the Space Law Committee of the International Law Association (ILA) and Emeritus Researcher at the Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), for her valuable advice, insightful comments and continuous support. Likewise, my appreciation goes for Professor Luis Fernando Castillo Argañarás (University of Buenos Aires and CONICET) for his guidance in difficult moments during my research.

I also want to thank Professor Kai-Uwe Schrogl, President of the International Institute of Space Law (IISL), and Professor Rafael Moro-Aguilar (IISL) for their generosity in sharing with me some materials for the research. Likewise, I am deeply grateful to Professor Bernhard Schmidt-Tedd (IISL) who provided me with the three volumes of the Cologne Commentary on Space Law when I was posted in Vienna.

Simonetta di Pippo is one of the persons that left an important footprint in my space background. She is not only the Director of the Office for Outer Space Affairs but notably a role model for so many women that see STEM as a reserved area for men. I want to thank her for contributing to this thesis by writing the foreword.

Notwithstanding all of the above support for this research, any flaws or errors and/or omissions are solely my own.

Definitely, my father was the main support throughout the whole process. He has always embodied the role model of a gladiator to me and was there in the hardest moments. The immense effort put into this thesis is dedicated to my mother in Heaven and to my father still on Earth.

Laura Jamschon Mac Garry

# FOREWORD

As the Director of the United Nations Office for Outer Space Affairs (OOSA), I am committed to promoting international cooperation in the peaceful use and exploration of outer space and furthering global space governance. Outer space is both an enabler and catalyser of sustainable development. Space applications provide numerous benefits to society, and likewise play a substantive role in national and international security. In this regard, space infrastructure has become a critical asset in the modern world. Such a fact calls for a fit-for-purpose normative regime to keep outer space safe, secure and sustainable for present and future generations.

Since its establishment in 1959, the Committee on the Peaceful Uses of Outer Space (COPUOS) has been the platform that Member States use to develop the normative framework governing outer space activities. The role of the Outer Space Treaty in maintaining international peace and security is crystallised in its preamble and operative part. It is the cornerstone of the legal system governing outer space activities, and was complemented with four subsequent space treaties and other instruments, such as sets of principles and guidelines. Yearly, the General Assembly passes a resolution on international cooperation in the peaceful uses of outer space, which is the result of intensive work at COPUOS contributing to the normative framework in the field.

Although the need for coordination within the United Nations bodies has always been an indispensable ground for efficient work, the need for synergies between the First and Fourth Committees of the General Assembly in space matters has become even more urgent during the last years. Fruitful exchange of views took place in joint meetings on topics that concern the mandates of COPUOS and the Conference on Disarmament. It is clear that endeavours to understand challenges emerging from space activities and efforts to address them in a normative manner call for a comprehensive approach given their dual-use nature.

The integration of information and communications technology (ICT) in spacecraft's operation has opened up several opportunities to advance space activities and explore the final frontier. Today, however, there is an increasing concern about protecting space critical infrastructures from malicious cyber activities to guarantee international peace and stability. In that context, it is of the utmost importance to examine how the existing legal system

applies to emerging challenges and whether additional tools can be developed to strengthen the global governance of outer space.

Laura Jamschon Mac Garry put together here several initiatives carried out by the international community to promote space security, safety and sustainability of outer space activities, and examined them from a diplomatic standpoint building onthe practice in international negotiations. In such a process, she reached the conclusion that space cybersecurity should be addressed in a progressive and holistic manner. While acknowledging that the mandate of COPUOS may need to be reviewed, she argues that the Legal Subcommittee should contribute to the global space governance in this field by proposing a set of principles to be initially discussed within the Legal Subcommittee in the format of a draft General Assembly resolution, which should be submitted to the joint discussion of the First and Fourth Committees.

Whether such innovative proposal might work out is a matter that lies within the political will of Member States –andas such, it belongs to the sphere of space policy that we all expect to enhance.

As an academic work, this thesis provides an overview of important topics on the agenda of COPUOS, and is food for thought for current and future 'space diplomats' on issues that might be on the international agenda in the years to come.

In addition, the story of Ada Lovelace, Valentina Tereshkova and Eilene Galloway described in an original manner in the preface and epilogue of this thesis tells us a story of real women who made huge contributions in the field of computing, space activities and multilateralism. In my role as a champion of the UNOOSA Space4Women project, I am convinced that women empowerment is a necessary premise to achieve the sustainable development goals, and these role models help promoting this aim. Ms Jamschon Mac Garry has begun and concluded her research in a witty manner enhancing the role of women in science and conveying sharply the idea that women are smart enough for hard sciences like computing, tough enough for harsh environments like outer space and skilful enough for negotiations at multilateral bodies. This is an inspiring message that I can only agree with and support.

In sum, this thesis touches upon issues that the UN Secretary-General has labelled as 'areas of international concern' in his recently report entitled 'Our Common Agenda'. These include the protection of civilian infrastructures from cyberattacks; the peaceful, secure and sustainable use of outer space; and gender equality. The driving force of the common agenda is to promote a more inclusive and effective multilateralism to address these core areas within the more overarching goal of peace and security, taking in consideration future generations. Thus, the topic of research in thisthesis appears timely in a context where the UN Secretary-General proposes appointing a Special Envoy for Future Generations and convening a Summit of the Future to seek high-level political agreements on the governance of the global commons.

OOSA Director Simonetta di Pippo

# TABLE OF CONTENTS

## LIST OF FIGURES AND TABLES



## LIST OF ACRONYMS

| | |
|---|---|
| ABM | Anti-Ballistic Missile |
| ADR | Active Debris Removal |
| APT | Advanced Persistent Threats |
| ASAT | Anti-Satellite |
| C2 | Command and Control |
| CBMs | Confidence-Building Measures |
| CD | Conference on Disarmament |
| CI | Critical Infrastructure |
| CIA | Central Intelligence Agency |
| CII | Critical Information Infrastructure |
| CNI | Critical National Infrastructure |
| CoC | Code of Conduct of Space Activities |
| CODUN | Working Party on Global Disarmament and Arms Control |
| CONAE | Comisión Nacional de Actividades Espaciales (Arg.) |
| CONICET | Consejo Nacional de Investigaciones Científicas y Técnicas (Arg.) |
| COPUOS | Committee on the Peaceful Uses of Outer Space |
| COTS | Commercial off-the-Shelf |
| CSI | Critical Space Infrastructure |
| CSIS | Center for Strategic and International Studies |
| ECI | European Critical Infrastructure |

| | |
|---|---|
| ECSL | European Centre for Space Law |
| EEAS | European External Affairs Service |
| EGNOS | European Geostationary Navigation Overlay Service |
| ELDO | European Launcher Development Organisation |
| ESA | European Space Agency |
| ESPI | European Space Policy Institute |
| ESRO | European Space Research Organization |
| EU | European Union |
| EUTELSAT | European Telecommunication Satellite Organization |
| G77 | Group of 77 |
| GEO | Geosynchronous Orbit |
| GGE | Group of Governmental Experts |
| GNSS | Global Navigation Satellite Systems |
| GOVSATCOM | Governmental Satellite Communications |
| GRULAC | Group of Latin American and the Caribbean |
| HCOC | Hague Code of Conduct |
| HEO | High Earth Orbit |
| IADC | Inter-Agency Space Debris Coordination Committee |
| IAA | International Academy of Astronautics |
| ICJ | International Court of Justice |
| ICT | Information and Communications Technology |
| IGY | International Geophysical Year |
| IISL | International Institute of Space Law |
| ILA | International Law Association |
| ILC | International Law Commission |
| INMARSAT | International Maritime Satellite Organization |
| INTERSPUTNIK | Intersputnik International Organization |
| INTELSAT | International Telecommunications Satellite Consortium |
| IRS | Intelligence, Reconnaissance and Surveillance |
| ISS | International Space Station |
| IISL | International Institute of Space Law |
| ITU | International Telecommunication Union |
| LEO | Low Earth Orbit |
| LSC | Legal Subcommittee of COPUOS |
| LTS | Long-Term Sustainability |
| MEO | Medium Earth Orbit |
| NASA | National Aeronautics and Space Administration |
| NATO CCDCOE | North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence |
| NIEO | New International Economic Order |
| NFP | No First Placement of Weapons |
| NOAA | Oceanographic and Atmospheric Administration |
| OBC | On-board Computers |
| OEWG | Open-Ended Working Group |
| OOSA | Office for Outer Space Affairs |
| OPCW | Organisation for the Prohibition of Chemical Weapons |
| PAROS | Prevention of an Arms Race in Outer Space |
| PCA | Permanent Court of Arbitration |
| PCIJ | Permanent Court of International Justice |

| | |
|---|---|
| PPP | Public-Private Partnership |
| PPWT | Treaty on the Prevention of the Placement of Weapons in Outer Space |
| QUESS | Quantum Experiments at Space Scale |
| RF | Radio Frequency |
| RPO | Rendezvous Proximity Operations |
| SALT | Strategic Arms Limitation Talks |
| SATCOM | Satellite Communications |
| SCADA | Supervisory Control and Data Acquisition |
| SDGs | Sustainable Development Goals |
| SDR | Software Defined Radio |
| SSVs | Suborbital Space Vehicles |
| STEM | Science, Technology, Engineering and Mathematics |
| STSC | Scientific and Technical Subcommittee of COPUOS |
| SWG | Sub-working group |
| TCBMs | Transparency and Confidence-Building Measures |
| TEU | Treaty of the European Union |
| TFEU | Treaty of Functioning of the European Union |
| TT&C | Telemetry, Tracking, and Commanding |
| UN | United Nations |
| UNGA | United Nations General Assembly |
| UNIDIR | United Nations Institute for Disarmament Research |
| USCYBERCOM | United States Cyber Command |
| USSR | Union of Soviet Socialist Republics |
| WCED | World Commission on Environment and Development |
| WSIS | World Summit on Information Society |

# CHAPTER 1:
# INTRODUCTION

## 1.1.-RESEARCH TOPIC:

Cyber threats have become a top priority all over the world because they may endanger international peace and security. This is the reason why national policies began to incorporate cyber strategies and multilateral bodies started to allocate efforts to discuss the matter. Definitions on how international law applies to malicious cyber activities are still in an embryonic stage at intergovernmental level due to antagonistic positions and more probably due to misgivings around a limitation of State action. At a doctrinaire level, a lack of agreement among the experts of the most extensive work on 'cyber operations' (the Tallinn Manual) is the major shortcoming to provide conclusive academic input.

In the space field, the IISL set up a working group on cyber law and addressed the topic in the 61st Colloquium in 2018. In the same vein, other significant institutions, such as the ILA and the Chatham House Royal Institute of International Relations addressed issues related to space cybersecurity. However, there is no comprehensive, holistic and multidisciplinary research such as the one proposed in the present thesis.

Existing research on space systems viewed as critical infrastructures is sparse (the Romanian school). Furthermore, space cybersecurity did not receive much attention during the negotiations on the Guidelines on the Long-Term Sustainability of Outer Space Activities (LTS), and the link between space cybersecurity and LTS is controversial for those who might consider that space cybersecurity remains under the remits of the Conference on Disarmament or UNGA First Committee rather than under the mandate of the body that deals with the peaceful uses of outer space (COPUOS).

This research builds upon previous academic work on both security in the use of information and communication technologies (ICTs) and space cybersecurity. Additionally, it inserts the academic research in the political and multilateral context of multilateral

negotiations, notably those related to a) the security in the use of ICTs, b) the elaboration of transparency and confidence-building measures in outer space and c) the consideration of safety, security and sustainability of outer space activities.

The thesis is designed in three levels: first, overview of the general framework (*lex generalis*); second, the examination of the particular framework of space law (*lex specialis*); and third, the identification of gaps and how the general framework might fill those gaps and how the remaining loopholes might be filled or addressed otherwise.

In sum, this thesis combines contents that have not been put together before –here, technology, politics and law will interact with a global mindset as the backdrop.

## 1.2.- OVERVIEW OF THIS THESIS:

This thesis is divided into six chapters that will approach the object of the research from a holistic analysis integrating political, legal and technological aspects. The present chapter is devoted to explaining the interest in the topic, the relevance of the research and the methodology employed. Chapters 2 to 5 are substantially aimed at providing elements to answer the research questions outlined in the next section. Chapters 2 to 4 begin with a section that clarifies the necessary terminology to better understand the whole content. They conclude with a section that summarises the partial conclusions and exposes to what extend they contribute to answering specific research questions.

Chapters 2 and 3 include a section dealing with the characteristics of a) cyberspace and cyber activities (chapter 2) and b) outer space and space activities (chapter 3). The aim of those sections is to explain in a comparative manner their commonalities and differences. There is also another section that is similar in both chapters, which is the section that reviews a selection of cases of malicious cyber activities on Earth (chapter 2) and in outer space (chapter 3).

An additional commonality between chapters 2 and 3 is that they both lay out the available legal framework: in the case of cyberspace, the rules of international law in general that might be applicable to the security in the use of ICTs according to the state of the art (with certain limitations explained in chapter 2). As to outer space, a review of *lex specialis*

consolidated around the five UN space treaties and the International Telecommunication Union (ITU) regime is briefly outlined in chapter 3.

Section 6 of chapter 3 interplays with chapter 2 since it argues that not only do space systems underlie the operation of critical infrastructures, but also that they are critical infrastructures themselves. This is a necessary premise to potentially apply the conclusions – if any– regarding malicious cyber activities targeting critical infrastructures to space systems.

A common denominator between chapters 2 and 5 is the analysis of the regime of responsibility applicable to each domain. While there is no particular regime of responsibility applicable to the security in the use of ICTs, there is a very specific one for outer space activities due to their ultra-hazardous nature. Once again, *lex specialis* (international responsibility for space activities and liability for damage of the space object) and *lex generalis* (State responsibility and responses thereto) are delineated in order to examine how they might complement each other.

Section 8 of chapter 2 goes in tandem with chapter 4. The former deals with the negotiations at the UN of the Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGEs on ICTs) and reviews their recommendations. The latter reviews multilateral mechanisms addressing safety, security and sustainability of outer space matters: namely, the Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities (GGE on TCBMs) and the Working Group on Long-Term Sustainability of Outer Space Activities (Working Group on LTS). Special emphasis is made on linkages, intersections and contradictions between the work in the General Assembly (UNGA) First and Fourth Committees. Chapter 4 adds another element to the political assessment: the role of the Group of the Latin American and the Caribbean (GRULAC) in the negotiation of the LTS Guidelines, the role of Europe in the negotiation of a draft Code of Conduct of Space Activities (CoC); and the role of China and the Russian Federation in space security initiatives, notably the draft Treaty on the Prohibition of Placement of Weapons in Outer Space (PPWT) and the policy of No First Placement of Weapons in Outer Space (NFP).

In stark contrast to the policy and legal approach just described, the first half of chapter 3 addresses technological issues related to space systems and space cybersecurity. Section 4 proposes a classification of malicious space cyber activities and describes each of them, which reveals the link between space cybersecurity and LTS: the creation of space debris and the safety risks associated thereto. In this context, a review of the draft guidelines on space cyber security proposed by the Russian Federation is included also in this chapter.

Chapter 5 recollects the findings of the previous chapters and complements them in order to finally answer all the research questions. It examines general international law and space law and seeks to answer whether they might be applicable to the topic under scrutinity. That chapter examines the lacunae in the legal regime and how they might be filled, for which it proposes an UNGA draft resolution as a preliminary step. The proposal made in this chapter is built upon the practice of UNGA joint meetings explained in section 4.7.3.

Chapter 6 summarises the overall conclusions referring back to the research questions put forward in the first chapter, explains the originality of this thesis, exposes the significance and the limitations of the research and makes recommendations on issues that will require further study and work.

## 1.3.-RESEARCH OBJECTIVES AND RESEARCH QUESTIONS:

The objective of this research is to demonstrate that there are provisions of space and telecommunications law that apply as *lex specialis* to the threats stemming from the convergence of the cyber and space domains. However, those provisions do not fully address the challenges that space cybersecurity poses nowadays. Thus, an additional objective is to identify the aspects that remain unregulated under those regimes; and finally, argue how these gaps might be filled and identify what is left for future negotiations.

These objectives will be achieved by progressively answering or providing elements for answering the following research questions:

1.- Is there a regulatory framework applicable to the convergence of the cyber and space domains?

2.-To what extent can space and telecommunications law be applied to cyber threats against space assets?

3.-Is the extant regulatory framework complete/adequate enough?

- Is cyber damage included in the definition of damage under the liability regime?
- Are cyber activities included in the definition of space activities?
- Is the operating system/software of a space asset an integral part of it?

4.- Which is the competent body to deal with these issues? Is there a need for a joint work encompassing more than a specialised body?

5.- Which is the best way to address cyber threats in the space domain? Why is a binding instrument not –for the time being– the appropriate solution to address the legal lacunae in the field?

6.-How can the regulation of cyber and space security contribute to the long-term sustainability of outer space activities and the governance of outer space?

In this regard, chapter 2 will provide several elements –which together with the progress to be made in chapter 3– will contribute to answerering **research question 1.** In addition, it will provide the necessary background for the future assessment that is required to answer **research questions 4** and **5**.

Chapter 3 will partially answer **research question 1 and 2** and on the basis of those elements, chapter 5 will complete the task of finding answers to both of them. This chapter will also provide elements to answer **research question 6**.

Chapter 4 will complete the analisis to answer **research question 6**. This chapter will also provide some inputs that will be complemented by chapter 5 to answer **research question 5.**

Building upon the elements that will jointly provide chapters 1 to 4, chapter 5 will address **research question 3** and will complete the answers to the remaining research questions.

## 1.4.- METHODS AND METHODOLOGY:

The research for this study was derived from three major methods that will be enumerated below with the explanation of the reasons on which they were employed, as well as their strengths and limitations (methodology).

**a) Analysis of relevant international law:**

International law is by far the most valuable source in this research to determine what is regulated and to what extent the current legal framework lags behind addressing emerging issues related to international peace and security. A significant shortcoming of this source is that it is usually not straightforward. Thus, further clarification is needed taking into consideration the sources enshrined in Article 38(1) of the Statute of the International Court of Justice (ICJ) and the interpretative techniques laid out in Articles 31 and 32 of the Vienna Convention on the Law of the Treaties.

**b) Examination of national positions at relevant multilateral bodies/negotiating mechanisms, and domestic and intergovernmental legal frameworks:**

The research is based on a strong conviction that a multilateral solution is the best answer to global challenges. Hence, it is not possible to envisage a multilateral solution without a clear understanding of how States conceive malicious cyber activities and space threats. Furthermore, this source is necessary to understand possible alliances and like-minded groups in a negotiation. Analysis of national positions encompasses statements at the relevant international fora, documents containing strategies or policies, domestic law and position papers.

There are a few limitations of this method: on the one hand, national positions might vary from time to time depending on internal political factors or on the result of allies'

influence. On the other hand, not all the meetings at the UN (particularly working or experts' groups) are recorded and made available to the public. Therefore, it is important to recall that this research is based only on documentable open source materials.

**c) Assessment of the teachings of qualified publicists:**

Documents of the International Law Commission (ILC), articles in journals and specialised literature, commentaries and other materials from main think tanks, such as the ILA, the IISL, the Chatham House Royal Institute of International Relations and the European Space Policy Institute (ESPI) or outcome documents/proceedings of relevant conferences or workshops are taken into consideration and examined. Publicists provide a valuable source for reflection when the other two methods do not offer a clear picture. This triangulation of methods is a necessary premise to the holistic approach that is pursued in this thesis and offers an analysis in different levels: a) regulatory, b) deliberative and a) academic.

The present research is a qualitative study of State behaviours and national positions in negotiations within multilateral bodies. It prioritises a selection of relevant (for the purposes set out in the objectives section) cases and actors, instead of engaging in a quantitative collection of data. In fact, cases were selected on the basis of particular elements that deserved to be enhanced or because of their paradigm-changing nature. As to States, focus is on national/group positions of: the United States (one of the main space powers), Japan (an Asiatic country with a pro-American position in the topics at stake), China (an Asiatic country with a pro-Russian position in the topics at stake), the Russian Federation (initiator of the cyber and space weaponisation debates at the UN), India (a fast consolidating Asiatic space power), the European Union (EU) (the only block of States with its own well-developed space policy and own flagship programmes), France (a leading space power within the EU), the United Kingdom (with new post-Brexit negotiating autonomy and member of the European Space Agency), Brazil (an active player in the LTS debate and a booster of the participation of the GRULAC) and South Africa (a representative of the G77 that played a key role chairing the Working Group on LTS).

One shortcoming of this qualitative research is that it required a continuous follow-up and update of the outcomes of negotiations during the three years of research. However,

for a research problem based on a 'how' question (how international space law applies to space cybersecurity, how international law in general may fill the gaps and how the international community might address the topic future negotiations), it proved to be the most appropriate.

# CHAPTER 2:
# CYBERSECURITY AND INTERNATIONAL LAW

## 2.1.-INTRODUCTION:

Cyber threats are no more a concern of the future but a reality in the present days. Reports on cyberattacks, cyber intrusions and cybercrimes have drastically surged in the last decade. The fear that forthcoming elections would be manipulated, that satellites could be hijacked and put out of orbit, that sensitive databases could be leaked or that personal photos or videos might be stolen and go viral is no longer a remote possibility.

Technological tools are quite widespread and accessible, and the return of a malicious cyber activity may range from mere economic profit to military advantage, both at little cost. Malicious cyber activities may take the form of minor intrusions or of severe destructive actions that threaten the regular exercise of individual and State rights alike.

The individual rights that might be endangered through cyber means include most notably the right to property and the rights to honour and privacy. Even if that seems to remain in the domestic domain, State Parties to international instruments, such as the Convention on Cybercrime, assume obligations to prevent such crimes, to enact proper legislation and to cooperate in the investigation and prosecution of guilty individuals.

Moreover, there is another aspect of cybersecurity that goes far beyond the sphere of individual rights and touches upon issues of national security and international stability. In this second case, the rights that might be endangered are those that emanate from statehood, such as the right to non-interference in the internal affairs, the right to sovereignty over national territory and the right against the use of force. The regular exercise of and respect for all these rights have a crucial impact on the maintenance of international peace and security, the primary purpose of the UN Charter system.

However, the threats to international peace and security that the drafters of the UN Charter envisioned were utterly different from the threats that cybersecurity poses nowadays.

The growing interconnectivity of the current world has sown the seeds to the increasing vulnerability that States face today.[1] Thus, domestic measures to address such threats are pressing and are high priority, particularly for those States that have become an information society, or borrowing the words of Daniel Kuehl, an 'omni-linked' society.[2]

The more developed a country is, the more it depends on the Internet and the more interconnected its information and communications become. Information dependence affects military, political, economic and social resources,[3] so do threats related to malicious access to information systems. The assumption mentioned above and the tendency of States to incorporate cyber domain into national military strategies has led some authors to predict that malicious cyber activities will be an increasingly important aspect of conflicts in the future.[4]

All these factors have awakened great interest in the international community and triggered extensive debates both at the governmental and academic level on how better to address legal challenges that cyber threats pose to national and international security. As part of the discussions, it is possible to distinguish between two main paradigms: the applicability of existing international law or creating a *lex specialis*.

In-between, there is a hybrid solution that combines the complementarity of the existing international regime with additional rules, norms, principles or measures of confidence-building and responsible State behaviour. A preliminary assessment of the current status of the discussions seems to confirm that the international community is moving in this direction. However, it is not clear to what extent current international law is applicable and which kind of instrument is best suited to complement it.

Although the topic has been on the agenda of UNGA First Committee since 1998, positions are not ripe enough to draw conclusions. While stances at that time were polarised, the work within the UN has demonstrated that States are sometimes prone to breach

---

[1] See DELIBASIS, D., *State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century,* in 'Peace Conflict and Development: An Interdisciplinary Journal', Vol. 8, 2006, p. 5.
[2] KUEHL, D., *Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age*, in 'International Law Studies', Vol. 76, 2002, pp. 40-41.
[3] See BOWMAN, M., *Is International Law Ready for the Information Age?*, in 'Fordham International Law Journal', Vol. 19, 1995, p. 1938.
[4] See BOOTHBY, W., *Some Legal Challenges Posed by Remote Attack*, in 'International Review of the Red Cross', Vol. 94, 2012, p. 581.

differences as much as possible in the interest of moving forward in the field of ICTs in the context of international security. Efforts towards consensus are quite slow and sometimes even fragile. Nonetheless, there is a growing awareness that the topic is of the utmost importance.

The aim of this chapter is to review the state of the art and assess the results of negotiations at the multilateral level regarding the legal approach to malicious cyber activities within the international security dimension. Part of this assessment includes the identification of elements that deserve further study, positions that are difficult to reconcile in the short term and prospects for future work.

To that purpose, the present chapter is divided into nine sections. After this introductory section, the second one is devoted to the clarification of the lexicon that will be employed along the following sections. To better assess the particularities of malicious cyber activities, the third section accounts for some characteristics of cyberspace and cyber activities. A selection of iconic cases that have contributed to raising awareness of the potential consequences of malicious cyber activities is contained in section 4. The remaining sections review international law issues from a cyber perspective: the legal qualification of malicious cyber activities (section 5), State responsibility and attribution (section 6) and legal responses (section 7).

It is not possible to finalise a study on legal challenges to the use of ICTs in the context of international security without examining regulatory prospects. To that aim, section 8 offers a review of the valuable work of the GGEs on ICTs and the open-ended working group on the topic (OEWG), and provides an insight into national positions in the field. The final sub-section lays out the opinions of scholars regarding whether there is a need for a new instrument and if such endeavour is desirable or feasible.

The final remarks will attempt to convey an assessment regarding the work of the group of experts of the Tallinn Manual and share views on what may be expected at a multilateral and intergovernmental level.

Elements of the research carried out in the framework of this chapter are contained in the following publication: JAMSCHON MAC GARRY, L., *Actividades Cibernéticas y Seguridad*

*Internacional: Hacia un Régimen de Normas de Comportamiento Estatal Responsable y Medidas de Fomento de la Confianza,* in 'Revista Electrónica Instituto de Investigaciones Jurídicas y Sociales A. L. Gioja', No. 26, 2021.

## 2.2.-TERMINOLOGY:

In the legal realm, it is of the utmost importance to adopt a precise lexicon because terminological imprecision can lead to a wrong application of the governing regime. Therefore, this section will aim to clarify the meaning of certain concepts that are employed when it comes to the use of ICTs in the context of international security. Finally, it will assess why a consensual definition for some concepts could help further future work on the matter.

**a) Cyberspace**:

At the outset, it is necessary to understand better what cyberspace is. According to general knowledge, the simplest way is to define it as the domain where digital activities develop and are carried out. However, the concept is more intricate than it seems at first sight. Daniel Kuehl proposed both a simple and a more technical definition. The more technical definition considered cyberspace as 'that place where electronic systems such as computer networks, telecommunications systems, and devices that exert their influence through or in the electromagnetic spectrum connect and interact'.[5] The simpler version is 'the physical environment where computer network attacks take place'.[6]

The International Telecommunication Union has developed a guide for national cyber strategies where the term 'cyberspace' is used 'to describe systems and services connected either directly to or indirectly to the Internet, telecommunications and computer networks'.[7]

Some States have defined the concept of cyberspace in their domestic cyber strategies. This is the case of Argentina that defined it as 'the global and dynamic domain comprised of information technology infrastructures, including the Internet, networks and

[5] KUEHL, D., *Information Operations*, cit. note 2, p. 39.
[6] Ibid., p. 40.
[7] ITU Cybersecurity National Strategy Guide, September 2011, p. 5.

information and telecommunication systems, among others'.[8] A similar definition is provided by the American Department of Defense: 'A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers'.[9] However, a presidential directive of the United States defined 'cyberspace' as follows: 'the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems and embedded processors and controllers in critical industries'.[10] The difference between this definition and the preceding one is that the former defined cyberspace in terms of a domain, while the latter did not. In a similar approach, New Zealand answered the question of what cyberspace is, as follows: 'The global network of interdependent information technology infrastructures, telecommunication networks and computer processing systems in which online communication takes place'.[11] Returning to the 'domain-based' definition, the Italian National Strategic Framework for Cyberspace Security defined it as 'a man-made domain essentially composed of Information and Communications Technology (ICT) nodes and networks, hosting and processing an ever-increasing wealth of data of strategic importance for States, firms, and citizens alike, and for all political, social and economic decision-makers'.[12]

The glossary of the Tallinn Manual (for the origin of this academic work, see section 2.4 below) adopted a different type of definition, which has no reference to a domain but to an 'environment': 'The environment formed by physical and non-physical components characterized by the use of computers and the electro-magnetic spectrum to store, modify, and exchange data using computer networks'.[13]

[8] Cyber Space Strategy of the Argentine Republic (2019), Government Secretary of Modernisation, Resolution 829/2019 (free translation).
[9] See DOD Dictionary of Military and Associated Terms, as of May 2019, p 57, available at .https://www.jcs.mil/(last accessed on 11 August 2021).
[10] National Security Presidential Directive 54/ Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), 8 January 2008, available at https://irp.fas.org/ (last accessed on 11 August 2021).
[11] Cyber Security Strategy of New Zealand (2015), available at the ITU Repository: https://www.itu.int/ (last accessed on 11 August 2021).
[12] National Strategic Framework for Cyberspace Security, December 2013 (Italy), available at the ITU Repository: https://www.itu.int/ (last accessed on 11 August 2021).
[13] SCHMITT, M. (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare,* New York, 2013. See the glossary of technical terms ('*Tallinn Manual*').

A final comment deserves the qualification of cyberspace made by the North Atlantic Treaty Organization (NATO) in the Warsaw Summit (2016) as a domain of operations like the air, land, and sea.[14]

It would be a challenging endeavour to review every definition here. States could take the opportunity to exchange views on this concept and elaborate on a definition that addresses essential elements that should be included. This thesis considers that a consensus definition should include at least the following ideas: 1) cyberspace is a concept that applies to the conduction of cyber activities –either malicious or not; 2) cyberspace not only comprises the group of networks and systems but also the infrastructures where they exist and operate, 3) a clear definition regarding the inclusion or exclusion of electromagnetic communications and 4) cyberspace is critical to socio-economic development.

**b) 'information operations', 'cyber operations', 'cyberattacks' and 'computer network attacks':**

Now, turning the attention to other concepts related to ICTs in the context of international security, it is useful to refer to the terms that the literature tends to employ interchangeably for designating malicious cyber activities. The most frequent are 'information operations', 'cyber operations', 'cyberattacks' and 'computer network attacks'. However, before that, it is necessary to make a preliminary comment on the distinction between 'information' and 'cyber', which should precede any conceptual discussion in the matter.

The qualifier 'cyber' is probably more familiar to the reader because this is the term that is colloquially used and thus is more entrenched in society for daily references to anything connected with the digital era. However, it is remarkable that upon a thorough analysis of national positions and intergovernmental discussions, this differentiation seems to be more an upcoming political issue rather than a matter of style. In effect, it is possible to deduce a clear explanation from the national submission of the United Kingdom in response to the invitation of the General Assembly to provide views on issues related to

[14] Warsaw Summit Communiqué issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016, para. 70, available at https://www.nato.int/ (last accessed on 11 August 2021).

information security. On several opportunities since 2013, that delegation steadily expressed its preference for the term 'cybersecurity' instead of 'information security' since that State considered that the latter 'is used by some countries and organizations as part of a doctrine that regards information itself as a threat'.[15] France expressed similar misgivings in 2014.[16]

As already mentioned, concerns about this terminology have arisen lately. In effect, it is appropriate to underscore that 'information security' is the terminology that the Russian Federation proposed originally in 1998. The General Assembly put the topic on its agenda by Resolution 53/70, adopted without a vote.[17] This is also the terminology used in the Russian National Security Strategy entitled 'Information Security Doctrine of the Russian Federation'[18] and is also the terminology used in the Chinese strategy, entitled 'The National Medium- and Long-Term Program for Science and Technology Development (2006-2020)'.[19] Similarly, this is the language adopted in the proposal for an 'International Code of Conduct for Information Security'[20] and the wording used in the first report of the GEE on ICTs.[21]

At a regional level, 'cybersecurity' is the term employed in the 2004 'Comprehensive Inter-American Cybersecurity Strategy'.[22] To the contrary, the term 'information security' was employed in the Information Security Strategy 2016-2020 of the European Union Agency for Network and Information Security (ENISA).[23] However, it is noteworthy that

---

[15] See Developments in the Field of Information and Telecommunications in the Context of International Security, UN. Doc. A/68/156, 16 July 2013, p. 15. See also the submissions in 2015, 2016 and 2017: UN Doc. A/70/172, 22 July 2015, p. 14; UN Doc. A/71/172, 19 July 2016, p. 23; UN Doc. A/72/315, 11 August 2017, p. 25.

[16] Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/69/112/Add.1, 18 September 2014, France, p. 3.

[17] United Nations General Assembly, Resolution 53/70, 4 December 1998, A/RES/53/70.

[18] Information Security Doctrine of the Russian Federation (2008). English text available at the ITU Repository: https://www.itu.int/ (last accessed on 11 August 2021).

[19] The National Medium- and Long-Term Program for Science and Technology Development (2006-2020). English text available at the ITU Repository: https://www.itu.int/ (last accessed on 11 August 2021).

[20] International Code of Conduct for Information Security (China, the Russian Federation, Tajikistan and Uzbekistan), reproduced in Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, UN Doc. A/66/359, 14 September 2011.

[21] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/65/201, 30 July 2010.

[22] Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity, OAS General Assembly Res. AG/RES. 2004 (XXXIV-O/04), 8 June 2004.

[23] ENISA Strategy 1016-2020, January 2016, available at https://www.enisa.europa.eu/ (last accessed on 11 August 2021).

the 2016 Network and Information Systems (NIS) Directive of the European Union preferred to use 'security of the network and information systems'[24] and that the new Cybersecurity Strategy of the European Union 2020-2025 employs –as its title makes it clear– 'cybersecurity'.[25] In the same line, several European States adopted national strategies on 'cybersecurity', such as Austria, Estonia, Italy and France.

As already depicted, there is no unanimity concerning the concept that is at the core of this chapter. In this thesis, the term 'cybersecurity' is considered and employed as an umbrella concept applying to security in the use of ICTs and cybercrime. While the former is generally the UN language for dealing with national and international security matters relating to malicious cyber activities, the latter is the term used to address criminal activities connected to cyber threats.

Having clarified this preliminary issue, it is possible to shift to the distinction among 'cyberattacks', 'cyber operations' and 'computer network attacks', as already advanced.

The level of intensity of damage, disruption or interference of a malicious cyber activity should determine the language that will be used. In the cyber domain, activities may range from simple disruptive incidents or information exploitation (information theft) to attacks that cause injury, damage or even death. The encompassing concept that the literature tends to use for all of them is 'cyber operations'.

Kuehl defined 'information operations' as 'actions taken to affect adversary information and information systems while defending own information systems'.[26] Drawing from a definition adopted by the United States National Military Strategy for Cyberspace Operations,[27] Duncan Hollis defined 'information operations' as 'the use of information technology, such as computer network attacks or psychological operations, to influence, disrupt, corrupt, usurp or defend information systems and the infrastructure they support'.[28]

---

[24] Parliament and Council Directive (EU) 2016/1148 of 6 July 2016 concerning Measures for a High Common Level of Security of Network and Information Systems across the Union, OJ L 194/1.
[25] Commission Communication (EU), The EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final, 16 December 2020.
[26] KUEHL, D., *Information Operations*, cit. note 2, p. 36.
[27] United States National Military Strategy for Cyberspace Operations (NMS-CO), December 2006, available at https://www.hsdl.org/ (last accessed on 11 August 2021).
[28] HOLLIS, D., *Why States Need an International Law for Information Operations*, in 'Lewis and Clark Law Review', Vol. 11, 2007, p. 1023.

For that author, information operations may focus on affecting the entire adversary, not just its military force.[29] Stephen Cox used the terms 'information operations' and 'information warfare' alternatively as synonyms.[30]

Jay Kesan and Carol Hayes included under 'computer network operations' not only attacks but also actions relating to defence and exploitation.[31] Michael Schmitt considered that 'computer network attacks' are a form of new warfare denominated 'information operations'.[32] His definition of 'computer network attacks' was 'operations to disrupt, deny, degrade or destroy information resident in computers and computer networks or the computer and the networks themselves'.[33] Furthermore, he considered 'cyberattacks' a more restricted category applicable to 'particularly egregious hostile cyber operations that allow for the most robust of state responses'[34] and contended that the violent characterisation does not qualify the act but the consequences thereof.[35]

While Kuehl adopted the same definition of 'computer network attacks' of Schmitt (taken from the Joint Information Operations Policy),[36] he also attached importance to the intent of the attacker.[37] A similar approach based on the intent was proposed by Herbert Lin, who included in his definition of 'cyberattack' the subjective element of deliberation as follows: 'the use of deliberate actions and operations – perhaps over an extended period of

[29] Ibid., p 1034.
[30] COX, S., *Confronting Threats Through Unconventional Means: Offensive Information Warfare as Covert Alternative to Preemptive War,* in 'Houston Law Review', Vol. 42, 2005, p. 886. It is important to point out that this author makes a clear distinction between computer network attacks and electronic warfare.
[31] See KESAN, J. AND HAYES, C., *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, in 'Harvard Journal of Law and Technology', Vol. 25, 2012, p. 453.
[32] SCHMITT, M., *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, in 'Columbia Journal of Transnational Law', Vol. 37, 1999, p. 890.
[33] SCHMITT, M., *Wired Warfare: Computer Network Attack and the Jus in Bello*, in 'International Review of the Red Cross', Vol. 84, 2002, p. 367. It should be underscored that the origin of this definition may be traced back to the Joint Doctrine for Information Operations (1998) which reads: '[o]perations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves'. The Joint Information Operations Policy sets forth a joint doctrine to govern the activities and performance of the Armed Forces of the United States in joint operations and provides the doctrinal basis for US military coordination with other US Government departments and agencies during operations and for US military involvement in multinational operations.
[34] SCHMITT, M. AND VIHUL, L., *The Nature of International Cyber Norms*, CCDCOE, Tallinn Paper No. 5, Special Expanded Issue 2014, p. 7, available at https://ccdcoe.org/ (last accessed on 11 August 2021).
[35] See SCHMITT, M., *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, in 'Harvard International Law Journal Online', Vol. 54, 2012, p. 26.
[36] KUEHL, D., *Information Operations*, cit. note 2, p. 44.
[37] Ibid., p. 45.

time – to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and (or) programs resident in or transiting these systems or networks'.[38]

The Tallinn Manual defined the term 'cyber operation' in its glossary as 'the employment of cyber capabilities to achieve objectives in or through cyberspace',[39] and 'cyberattack' as follows: 'A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects'.[40] That academic work built upon the definition of 'attack' enshrined in Article 49 of the Additional Protocol I to the Geneva Conventions. Pursuant to that provision, 'attacks' are 'acts of violence against the adversary, whether in offence or defence'.[41]

From the above, it is apparent that there is not yet a uniform language in the literature. Regarding the term 'cyberattacks', there appears to be agreement that there has to be injury, death, damage or destruction. However, scholars are not yet conclusive regarding loss of functionality. The international community should further discuss that aspect and also reach an agreement on the requirement of intent and duration for a cyberattack to be considered as such, and whether a definition including language that is linked to warfare is desirable for the more encompassing term 'cyber operations'.

From the concepts just reviewed, this thesis will only employ 'cyberattacks' for destructive and permanent disruptive malicious cyber activities.

**c) 'cyber war', 'information warfare', 'cyber weapons' and 'digital data warfare':**

A part of the literature goes even further and employs explicit warfare terminology. Thus, expressions such as 'cyber war' or 'information warfare' and 'cyber weapons' tend to become entrenched in the lexicon referred to international peace and security. Initially, the term used in case of hostilities was 'war'; however, this concept was overcome and replaced

---

[38] LIN, H., *Offensive Cyber Operations and the Use of Force*, in 'Journal of National Security Law and Policy', Vol. 4, 2010, p. 63.
[39] *Tallinn Manual*, cit. note 13. See the glossary of technical terms.
[40] Ibid., Rule 30. See also Rule 92 of SCHMITT, M. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge, 2017 ('*Tallinn Manual 2.0*').
[41] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), adopted on 8 June 1977, and entered into force on 7 December 1978, 1125 UNTS 3.

by 'armed conflict'. Indeed, after the Second World War, large scale hostilities were increasingly referred to as 'armed conflicts' instead of 'wars'. A classical definition of 'war' was famously coined by Lassa Oppenheim as 'the contention between two or more States through their armed forces to overpower each other and impose such conditions of peace as the victor phases'.[42] Yoram Dinstein suggested that 'war' is 'a hostile interaction between two or more States, either in a technical or in a material sense'.[43] It should also be recalled that the Prussian military theorist Carl von Clausewitz had characterised the 'war' as 'an act of policy' and as 'a pulsation of violence'.[44] For its part, the commentary to the Additional Protocol II to the Geneva Conventions provided a definition of 'armed conflict' in the following terms: 'an armed conflict is the existence of open hostilities between armed forces which are organized to a greater or lesser degree'.[45]

As Richard Aldrich pointed out, there is no universal definition of 'information warfare'.[46] However, it is possible to point at some elements to elucidate its meaning, such as those provided by Schmitt and Kuehl. They defined 'information warfare' as a subset of information operations 'conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries'.[47] Susan Brenner defined 'cyber warfare' as 'the conduct of military operations by virtual means'.[48] Todd Morth differentiated between 'information warfare' and 'netwar'. He defined the fomer as a State activity with an incapacitating effect on an information network, and the latter as 'a method of organising combatants into networks'.[49]

---

[42] OPPENHEIM, L., *International Law*, quoted in DINSTEIN, Y., *War, Aggression and Self-Defence,* Cambridge, 2005, p. 5.
[43] DINSTEIN, Y., *War, Aggression and Self-Defence*, cit. note 42, p. 15.
[44] VON CLAUSEWITZ, C., *On War*, New York, 2007, p. 28.
[45] ICRC Commentary on Protocol Additional to the Geneva Conventions of 12 August 1949, 1987, para. 4341.
[46] See ALDRICH, R., *The International Legal Implications of Information Warfare*, in 'Airpower Journal', Vol. 10, No. 3, 1996, p. 102.
[47] SCHMITT, M., *Wired Warfare*, cit. note 33, pp. 365-366; KUEHL, D., *Information Operations*, cit. note **2**, p. 36. See also SCHMITT, M., *Computer Network Attack and the Use of Force*, cit. note 32, p. 890.
[48] BRENNER, S., *At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare*, in 'The Journal of Criminal Law and Criminology', Vol. 97, 2007, p. 401.
[49] MORTH, T., *Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter',* in 'Case Western Reserve Journal of International Law', Vol. 30, 1998, pp. 571 and 574.

For his part, Daniel Silver used the expression 'digital data warfare' and offered a definition that did not expressly refer to a conflict: 'the covert introduction of malicious computer code into a computer system or network to achieve an objective'.[50]

A future agreement on the terminology should take into consideration some issues relating to express warfare language: firstly, it has a limited scope in terms of context and actors involved. Secondly, this language connects directly with the application of *jus ad bellum* and *jus in bello* regimes, which will deserve a contingent governmental discussion and consensus on how it is applied, an issue that still needs to be settled. Thirdly, such language also limits the competent forum where possible regulatory rules, principles, norms or measures might be discussed. Finally, it should be borne in mind that the fundamental purpose of the UN Charter to mantain international peace and security goes beyond the prohibition of war. Due to these shortcomings, this thesis will avoid employing this language for its own conclusions.

**d) Cyber weapons:**

When it comes to cyber war, the concept of 'weapons' necessarily comes implicitly or explicitly into the scene. In this regard, taking elements from different definitions, weapons are considered devices used or designed[51] to cause deaths, injuries or damage[52] for offensive or defensive purposes.[53] Academic commentators like William Boothby considered that a computer used to cause death, injury, damage or destruction to another party to an armed conflict becomes a weapon or means of warfare.[54] Another example of this line of thought is Dinstein. That author was of the view that a computer can become a weapon if it is directed to attack an adversary.[55] In the same line, Russell Buchan focused on the effects-

[50] SILVER, D., *Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter*, in 'International Law Studies', Vol. 76, 2002, p. 77.
[51] See GARNER, B. (ed), *Black's Law Dictionary*, St. Paul, 2009, p. 717. It reads: '[…] instrument used or designed to be used to injure or kill someone'.
[52] See WALKNER, P., *Organizing for Cyberspace Operations: Selected Issues*, in 'International Law Studies', Vol. 89, 2013, p. 345.
[53] See INTOCCIA, G. AND MOORE, J., *Communications Technology, Warfare, and the Law: Is the Network a Weapon System?*, in 'Houston Journal of International Law', Vol. 28, 2006, p. 480.
[54] See BOOTHBY, W., *Some Legal Challenges*, cit. note 4, p. 587.
[55] See DINSTEIN, Y., *Computer Network Attacks and Self-Defense*, in 'International Law Studies', Vol. 76, 2002, p. 102.

based approach developed by Ian Brownlie, where the physical damage is more important than the instrument itself to qualify as a weapon.[56]

Neither Article 36 of Additional Protocol I to the Geneva Conventions nor its commentary clarified the meaning of 'weapon'. This void gives flexibility to States to define it domestically, as Duncan Blake and Joseph Imburgia acknowledged. In the words of those authors, 'each State bears the onus to determine whether a space or cyberspace capability qualifies as a weapon, means or method of warfare'.[57] However, as already illustrated by the opinions referred above, the qualification of a particular instrument as a weapon is less significant than its effects.

The Tallinn Manual crafted a definition of 'cyber weapons' as follows: 'cyber weapons are cyber means of warfare that are by design, use, or intended use capable of causing either i) injury to, or death of, persons; or ii) damage to, or destruction of objects, that is, causing the consequences required for the qualification of a cyber operation as an attack'.[58]

Brenner differentiated three types of cyber weapons: i) weapons of mass destruction, such as those that may –for instance– disable a computer system running a nuclear plant causing a devastating explosion, ii) weapons of mass distraction (for instance, programmes that announce the contamination of water systems leading to general panic, and iii) weapons of mass disruption (for instance, an attack that causes the shutting down of a grid the same day every week, undermining social confidence in the infrastructure).[59] Bradley Raboin provided a different classification of cyber weapons: i) denial of service (coordination and use of numerous pre-infected computers working in unison to disable a targeted computer network or service), ii) malicious software or malware (disruption of normal computer functions through a back door for a remote attacker to take control of the computer), iii) logic bombs (dormant threats causing severe damage only once activated), iv) IP spoofing (access with a concealed identity) and v) Trojan horses (remote unauthorised access to the

[56] See BUCHAN, R., *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions*?, in 'Journal of Conflict and Security Law', Vol. 17, 2012, p. 217.
[57] BLAKE, D. AND IMBURGIA, J., *'Bloodless Weapons'? The Need to Conduct Legal Review of Certain Capabilities and the Implications of Defining Them as 'Weapons'*, in 'Air Force Law Review', Vol. 66, 2010, p. 173.
[58] *Tallinn Manual*, cit. note 13, Rule 41, commentary, para 2. See also *Tallinn Manual 2.0,* cit. note 40, Rule 103, commentary, para. 2.
[59] BRENNER, S., *At Light Speed*, cit. note 48, pp. 390 ff.

computer).[60] Cox only included in his list of cyber weapons viruses, worms, and logic bombs.[61] A more expanded version was proposed by Christopher Joyner and Catherine Lotrionte, who included sniffer, trap doors, spanning and IP spoofing as cyber weapons.[62]

The discussion on the term 'weapon' deadlocked the Conference on Disarmament for decades, and this is one of the main reasons why progress has not been made in other fields, such as the prevention of an arms race in outer space (PAROS). The Russian Federation proposed a definition of 'cyber weapons' when that delegation brought the topic of information security to the attention of the General Assembly, but without success.[63] Therefore, any future work dealing with malicious cyber activities should avoid getting trapped into terminological discussions that *a priori* would not move forward, such as the inclusion of a concept of 'cyber weapon'.

The concluding remark of this section is that there should be some agreement on the terminology to be used in a future endeavour regarding the security in the use of ICTs. The use of language and definitions that implicitly or explicitly refer to war, weapons, adversaries or conflicts bring about several limitations that would only delay future work on the matter. For that reason, this thesis will employ the expression 'malicious cyber activities' to circumvent those limitations.

## 2.3.-CHARACTERISTICS OF CYBERSPACE AND CYBER ACTIVITIES:

The examination of the characteristics of cyberspace and cyber activities is a necessary preliminary exercise to comprehend the particular nature of the use of ICTs in the context of international security. This task will help draw differences and find similarities

[60] See RABOIN, R., *Corresponding Evolution: International Law and the Emergence of Cyber Warfare,* in 'Journal of the National Association of Administrative Law Judiciary ', Vol. 31, 2011, pp. 611-616.
[61] See COX, S., *Confronting Threats*, cit. note 30, pp. 888-889.
[62] See JOYNER, C. AND LOTRIONTE, C., *Information Warfare as International Coercion: Elements of a Legal Framework*, in 'European Journal of International Law', Vol. 12, 2001, pp. 837-838.
[63] Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/54/213, 10 August 1999, para. 15: 'information weapon' was defined as 'Means and methods used with a view to damaging another State's information resources, processes and systems; use of information to the detriment of a State's defence, administrative, political, social, economic or other vital systems, and the mass manipulation of a State's population with a view to destabilising society and the State').

with other domains, and provide guidance to explain why the governance of malicious cyber activities is a challenging endeavour.

**a) Cyberspace as a global commons:**

When this chapter referred to the concept of cyberspace above, it reviewed specific definitions that described cyberspace as 'global'. This adjective is the starting point of the qualification of cyberspace as a global commons. This conception is favoured by the assessment that 'cyberspace has eroded the connection between territory and sovereignty'.[64] Not only did the American Department of Defense consider cyberspace along international waters and air (beyond national airspace), space and cyberspace as a global commons,[65] but so did the NATO Allied Command Transformation.[66]

A global commons is by definition a domain over which no State has sovereignty. However, in the Strategy for Cooperation in Cyberspace, China made explicit references to 'sovereignty in cyberspace', defined as 'the right to independently choose their development path, network management method, and Internet public policy, as well as to equally participate in international cyberspace governance'.[67] For its part, with a similar view, the Russian Federation made a critical step in 2019 by passing legislation to have 'sovereign Internet', in force since 31 October 2019. This law enables the country to disconnect itself from the rest of the Internet.

The fact that cyberspace is a man-made creation with a physical infrastructure is a feature that the Chatham House Royal Institute underscored as a challenge in the qualification of cyberspace as a global commons. However, the experts from that institution

---

[64] SHACKELFORD, S., *From Nuclear War to Net War: Analogising Cyber Attacks in International Law*, in 'Berkeley Journal of International Law', Vol. 27, 2009, p. 214.
[65] See Strategy for Homeland Defense and Civil Support of the United States (2005), Department of Defense, p. 12.
[66] NATO, *Assured access to the common globals, Findings and Recommendations*, April 2011, p. 4, available at https://www.act.nato.int/ (last accessed on 11 August 2021). It reads: 'Cyberspace is not owned or controlled by any single entity or sovereign state, and it is potentially accessible to all actors with the requisite technological capabilities'). The NATO Allied Command Transformation is one of two Strategic Commands at the head of NATO's military command structure. The other one is the Allied Command Operations, which is responsible for the planning and execution of all NATO military operations.
[67] International Strategy of Cooperation on Cyberspace of China (2017), English translation available at https://www.fmprc.gov.cn/ (last accessed on 11 August 2021).

agreed that it would be useful to label it as such.[68] This apparent dichotomy between global commons and jurisdiction is clearly explained by Gerald Stang, who affirmed that most security specialists include cyberspace in the category of global commons, although this one is particular since it is not a physical domain; only the nodes of Internet are physical and exist within States and thus are subject to their control and national law.[69] A different argument is laid out by Scott Shackelford, who regarded cyberspace as a global commons but considered that such fact would not impede a State to regulate *activities* that impact upon its territory.[70] Another opinion supporting this view is represented by the argument made by Johann-Christoph Woltag, who asserted that cyberspace should not be qualified as a new space that exists devoid of State authority and regulation under international law but 'as a new kind of social and public sphere'.[71] In that regard, he pointed at the territorial jurisdiction and concluded that the State where the networks and systems are located has territorial jurisdiction.[72]

On the opposing side, authors like Sean Kanuck disagree with the qualification of cyberspace as a global commons. His argument is based on the fact that its underlying physical resources remain subject to private property rights and that it is not possible to identify legitimate users and exclude illegitimate ones in cyberspace.[73] Neither the report of the GEE on ICTs nor the Tallinn Manual referred to the global commons feature; however, both concluded that States have jurisdiction over ICT infrastructure within their territories.[74] Nevertheless, the latter made clear that States may not claim sovereignty over cyberspace *per se*.[75]

---

[68] *Making the Connection: The Future of Cyber and Space*, International Security Workshop Summary-Chatham House Royal Institute, 24 January 2013, p. 4, available at www.chathamhouse.org (last accessed on 11 August 2021).
[69] STANG, G., *Global Commons: Between Cooperation and Competition*, European Union Institute for Security Studies, April 2013, pp. 1 and 3, available at https://www.iss.europa.eu/ (last accessed on 11 August 2021).
[70] See SHACKELFORD, S., *From Nuclear War to Net War*, cit. note 64, pp. 211-212.
[71] WOLTAG, J., *Computer Network Operations below the Level of Armed Force',* in 'European Society of International Law Conference', Paper Series 1, 2011, p. 12.
[72] Ibid., p. 16.
[73] See KANUCK, S., *Sovereign Discourse on Cyber Conflict Under International Law,* in 'Texas Law Review', Vol. 88, 2010, p. 1579.
[74] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98, 24 June 2013, para. 20; *Tallinn Manual*, cit. note 13, Rule 2.
[75] *Tallinn Manual*, cit. note 13, Rule 1.

Another point that deserves a brief mention here is the existence of a current of opinion that regards Internet as the common heritage of mankind. One of the representatives of this line of thought is Antonio Segura-Serrano.[76] Close to that view is Anthony D'Amato, who speculated that Internet would increasingly be valued as a precious resource, as 'the heritage of mankind'.[77]

At this juncture, it is possible to conclude that due to the *sui generis* nature of cyberspace, it is necessary to draw a distinction between sovereignty *over* and *in* cyberspace. As long as the cyber domain remains considered a global commons, sovereignty *over* cyberspace is ruled out. Sovereignty *in* cyberspace is legally possible through the exercise of a certain type of jurisdiction over cyber activities or the underlying infrastructure within a State territory. The next chapter will explain how this characteristic also applies to the outer space domain.

**b) Dual-use of ICTs:**

The activities carried out in cyberspace are either of civil or military character. They use the same technology and infrastructure; however, they differ in the purpose of their use and the level of confidentiality. Scholars and governmental experts unanimously agree on this characteristic. In effect, the GEE on ICTs confirmed this assessment in its 2013 report[78] and the Tallinn Manual dedicated Rule 39 to dual-use objects.

As pointed out by some academic commentators, this characteristic brings about severe difficulties in controlling the proliferation of destructive cyber tools.[79] Such threats – where control of proliferation becomes impracticable– make cooperation between the government and the private sector a critical need.[80] Another significant aspect derived from this characteristic is the definition of what peaceful purposes are. Furthermore, the Tallinn

[76] See SEGURA-SERRANO, A., *Internet Regulation and the Role of International Law',* in BONGDANDY, A. AND WOFLRUM (eds), *Max Planck Yearbook of United Nations Law*, Vol. 10, Leiden-Boston, 2006, p. 260.
[77] D'AMATO, A., *International Law, Cybernetics and Cyberspace*, in 'International Law Studies', Vol. 76, 2002, p. 69.
[78] UN Doc. A/68/98, cit. note 74, para. 5.
[79] See MORTH, T., *Considering Our Position*, cit. note 49, p. 582.
[80] See DELIBASIS, D., *State Use of Force in Cyberspace for Self-Defence*, cit. note 1, p. 25.

Manual admitted that cyberspace is a feasible warfare theatre and that dual-use objects are military objects.[81]

In short, dual-use technologies increase international tensions emerging from distrust and misperception; thus, they pose a threat to international stability and are a challenge to governance.

**c) Anonymity of cyber activities:**

This aspect is a well-established feature that makes malicious cyber activities appealing for criminals and States alike. Additionally, this characteristic lies at the core of the so-called 'attribution problem'; namely, the difficulty in pinpointing the attacker.[82] The anonymity advantage makes malicious cyber activities an attractive instrument for offenders, particularly for terrorists,[83] and an ideal tool for States that prefer to hide behind civilian groups within their borders.[84] Anonymity, coupled with the speed in which the attack materialises contributes to complicating attribution.[85] Michael Glennon postulated that 'the possibility of concealment of the perpetrator is backed into the structure of the Internet and cannot feasibly be eliminated'.[86] For its part, Christopher Lentz clarified that the location of the server that launched the attack only demonstrates that a territory was used as 'a launch pad',[87] but it does not necessarily –and virtually in most of the cases does not– determine the identity of the aggressor, nor its location. This is the reason why malicious cyber activities reduce the potential costs of getting caught[88] and –paraphrasing Cox– prevent honour jeopardising.[89]

---

[81] *Tallinn Manual*, cit. note 13, Rule 39, commentary, para. 1.
[82] See WILLIAMS, R., *(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action*, in 'The George Washington Law Review', Vol. 79, 2011, p. 1183.
[83] See ROBBAT, M., *Resolving the Legal Issues Concerning the Use of Information Warfare in the International Forum: The Reach of the Existing Legal Framework, and the Creation of a New Paradigm*, in 'Journal of Science & Technology Law', Vol. 6, 2000. See also UN Doc. A/68/98, cit. note 74, para. 7.
[84] See SHACKELFORD, S., *From Nuclear War to Net War*, cit. note 64, p. 232.
[85] See TSAGOURIAS, N., *Cyber Attacks, Self-Defence and the Problem of Attribution*, in 'Journal of Conflict and Security Law', Vol. 17, 2012, p. 233.
[86] GLENNON, M., *The Road Ahead: Gaps, Leaks and Drips',* in 'International Law Studies', Vol. 89, 2013, pp. 382-383.
[87] LENTZ, C., *A State's Duty to Prevent and Respond to Cyberterrorist Acts,* in 'Chicago Journal of International Law', Vol. 10, 2010, p. 811.
[88] FIDLER, D., *Tinker, Tailor, Soldier, Duqu: Why Cyber espionage is more Dangerous than You Think,* in 'International Journal of Critical Infrastructure Protection', Vol. 5, 2012, p. 29.
[89] COX, S., *Confronting Threats*, cit. note 30, p. 891.

It is noteworthy that the Five Eyes alliance (the United States, Canada, Australia, New Zealand and the United Kingdom) initiated a strategy of public naming and shaming.[90] Although this policy might be a means of political pressure, it is doubtful how helpful it is for the legal purposes of attribution unless a shared understanding within the international community is reached in that regard.

Despite the problems that anonymity brings about in terms of attribution, it should be underscored that in the field of human rights anonymity plays an important role in a democratic society. In effect, as acknowledged by the Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye: 'Encryption and anonymity provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks'.[91] Hence, restrictions must be only limited in accordance with the principles of legality, necessity, proportionality and legitimacy of the objective.[92]

In sum, it is safe to conclude that anonymity and the problem of attribution are two sides of the same coin. Even if cyber experts may identify the server, they might not identify the attacker; thus, the possibility of attributing the malicious cyber activity is limited or remote at the existing technology development.

**d) Geographical ubiquity of cyber activities:**

This characteristic is linked to the possibility of accessing systems or networks remotely. Since cyberspace eliminates the need for physical proximity of the hacker, it 'creates the potential for increased differentiation between the point of origin and the point of occurrence of the attack'.[93]

---

[90] See for instance, United States Department of Justice, *U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations*, 4 October 2018, available at https://www.justice.gov/ (last accessed on 11 August 2021); Government of the United Kingdom, *UK and Allies Reveal Global Scale of Chinese Cyber Campaign*, 20 December 2018, available at https://www.gov.uk/ (last accessed on 11 August 2021); United States Department of Justice, *Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information*, 20 December 2018, available at https://www.justice.gov/ (last accessed on 11 August 2021).

[91] Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, UN Doc. HRC/29/32, 22 May 2015, para. 16.

[92] Ibid. para. 56.

[93] BRENNER, S., *At Light Speed*, cit. note 48, p. 414.

The cyber world poses unique challenges to legal practitioners and governments alike since it is tremendously easy to section and present a malicious cyber attack as coming from one or several different States, even when the owners of the computers involved are unaware of that. This conduct is commonplace in multi-stage malicious cyber activities that use computers located in different places as stepping stones. Ubiquity often makes it difficult to determine not only who is the perpetrator but when a malicious cyber activity begins,[94] how fast it spreads and where (in the words of Gary Brown, 'time and geography offer a few limits to cyber operations').[95]

One additional advantage derived from this characteristic is that the attacker undertakes the malicious cyber activity without putting at risk its personal security or integrity. Hence, malicious cyber activities become a preferred tool in case of an armed conflict where the adversary presents a clear military superiority.

**e) Low cost and wide accessibility:**

No less important is the fact that the necessary expertise and equipment to gain unauthorised cyber access are widely available at a low cost.[96] This is an aspect that some authors enhanced when it comes to military advantage.[97] A computer and some basic knowledge are enough to unleash a military confrontation, as the legendary 'War Games' illustrated in a film shot by John Badham during the Cold War years. In that movie, fiction showed how a teenager might be able to penetrate the Pentagon systems and activate the nuclear alerts as if there were a threat coming from the Soviet Union. More recently, a competence in the United States showed in practice that children might be able to hack a voting system without great difficulty.[98] For those curious about this, there are tutorials on

[94] See BARKHAM, J., *Information Warfare and International Law on the Use of Force,* in 'New York University Journal of International Law and Politics', Vol. 34, 2001, p. 64.
[95] See BROWN, G., *International Law applies to Cyber Warfare! Now, What*?, in 'Southwestern Law Review', Vol. 46, 2017, p. 358.
[96] See JOHNSON, P., *Is It Time for a Treaty on Information Warfare?*, in 'International Law Studies', Vol. 76, 2002, p. 441.
[97] See for instance COX, S., *Confronting Threats*, cit. note 30, p. 909; CONDRON, S., *Getting It Right: Protecting American Critical Infrastructure in Cyberspace*, in 'Harvard Journal of Law and Technology', Vol. 20, 2007, p. 404.
[98] See LEE, D., *Los Niños que lograron hackear el Sistema Electoral de los Estados Unidos*, 13 August 2018, available at https://www.bbc.com/ (last accessed on 11 August 2021)

the Internet, and for the specialists, there is Defcon, the conference to improve hacking capabilities.[99]

Thus, low cost and wide accessibility play in conjunction and the latter is a consequence of global digitalisation. Digitalisation supports and accelerates the accomplishment of the sustainable development goals set by the international community at the UN, but there are associated risks with it: the more digitalised a society, the more vulnerable it becomes. Hence, States need to redouble efforts to develop strategies to guarantee broad access to digital tools while avoiding their use for malicious purposes.

**f) Asymmetry of benefits:**

This characteristic is closely linked to the previous one. Malicious cyber activities bring several advantages to States and non-State actors that do not have the 'economic or military supremacy of the adversary'.[100] An easily accessible harmful tool is the 'weapon of the weak', in the words of Oona Hathaway.[101] With one hacker, a State might put at risk critical infrastructure and paralyse the regular provision of essential services of another in the blink of an eye and with a small budget.

Like the previous characteristic, this one also creates a 'cyber regulatory dilemma' because, on the one hand, States that are very much dependent on computer systems will be willing to limit the capacity that other States have to interfere and damage those systems but, on the other hand, a strict regulatory regime would curtail their own capabilities to defend and hack others. This dilemma provides some arguments to explain why there is little and slow progress in the governance of security in the use of ICTs.

**g) Unpredictable damage:**

As previously submitted, malicious cyber activities encompass a wide range of threats, from mere inconvenience or exploitation to physical destruction or even death. However, this differentiation is not easily predictable in practice. The cyber domain makes it almost impossible to distinguish between a code that may be used to steal data or destroy

[99] For more information, visit: https://www.defcon.org/
[100] See SEGURA-SERRANO, A., *Internet Regulation*, cit. note 76, p. 222.
[101] HATHAWAY, O., *The Law of Cyber-Attack*, in 'California Law Review', Vol. 100, 2012, p. 842.

it.[102] The same software may allow a hacker to gain access to a computer for the purpose of surveillance or theft and information destruction. These factors explain why Bowman considered that 'the threats of cyberspace are less coherent, less tangible, and certainly less foreseeable than military confrontation'.[103]

A critical factor that contributes to this characteristic is the speed in which the effects of a malicious cyber activity develop and spread. As explained by Dimitrios Delibasis, hackers start causing severe damage immediately after making unauthorised access to a certain information system,[104] which means that in many cases damage is instantaneous. However, the initial damage or inconvenience might be the starting point of a series of disturbing effects that may affect a whole network system of a critical infrastructure, causing severe consequences in the provision of electricity, water or other essential State services.

The unpredictable damage complicates the scenario of allowed responses, which need to be decided upon the legal qualification of the activity. Some authors have argued that the difficulty in the assessment of damage restricts the possibilities of preventive measures,[105] which makes the defence of the targeted State even more difficult. Further complicating things is the fact that the hacker might upgrade the payload of certain malware for exploitation in real-time and lead to a destructive action, even after the initial qualification of the malicious cyber activity.[106]

As a concluding remark of this section, it is appropriate to underscore that some of the characteristics described above are not exclusive to cyberspace and cyber activities, which is a relatively young area of study. This is encouraging because it allows for gathering experience from other domains to serve as guidance in the cyber field. This point will be taken up and developed in subsequent chapters. The less encouraging conclusion of this section is that the particular characteristics constitute a challenge for policy-makers and contribute to the difficulties in reaching consensus on a governing regime at an international level.

---

[102] See BROWN, G. AND POELLET, K., *The Customary International Law of Cyberspace*?, in 'Strategic Studies Quarterly', Vol. 6, No. 3, 2012, p. 135.
[103] BOWMAN, M., *Is International Law Ready for the Information Age*, cit. note 3, p. 1943.
[104] See DELIBASIS, D., *State Use of Force in Cyberspace for Self-Defence*, cit. note 1, p. 21.
[105] See BARKHAM, J., *Information Warfare*, cit. note 94, pp. 81 and 83.
[106] See LIN, H., *Offensive Cyber Operations*, cit. note 38, p. 79.

## 2.4.- OVERVIEW OF ICONIC CASES OF MALICIOUS CYBER ACTIVITIES

A preliminary caveat is necessary to note at the outset of this section: malicious cyber activities are commonplace nowadays; therefore, the scope of this section is limited to accounting for a selection of cases based on a particular feature that made them a 'paradigm-changer'. This section serves a double purpose: on the one hand, it seeks to highlight that cyber threats go back long before the last two decades, mistakenly considered to be the genesis of cybersecurity. On the other hand, this selection of cases will depict the multiplicity of actors, targets, and contexts that might be involved.

### a) 1982 the Soviet pipeline:

It was not until 2004 when an operation of the Central Intelligence Agency (CIA) came to light allegedly to sabotage the economy of the Soviet Union in 1982. Purportedly, it could have triggered an enormous explosion in a Siberian natural gas pipeline during the last years of the Cold War. Thomas Reed, a former American Air Force Secretary during the Reagan Administration, published a book in 2004 where he disclosed that the CIA had filtered software that would make the pipeline explode.[107]

The economic backdrop of this story was the strategic interest in East-West trade. A document from the CIA held that Moscow needed the cooperation of Western Europe in building new pipelines for the delivery of natural gas, which in turn would ease economic problems.[108] This document further explained that the malicious cyber activity was supposed to be a response to the Soviet intelligence that allegedly had sought to clandestinely obtain technical and scientific knowledge from the West. The Special Assistant to the American Secretary of Defense Gus Weiss contended in an article entitled 'The Farewell Dossier', that

[107] See HOFFMAN, D., *Reagan Approved Plan to Sabotage Soviets*, 27 February 2004, available at https://www.washingtonpost.com/ (last accessed on 11 August 2021); RUSSELL, A., *CIA plot led to huge blast in Siberian gas pipeline*, 28 February 2004, available at https://www.telegraph.co.uk/ (last accessed on 11 August 2021).

[108] See Director of Central Intelligence, *The Soviet Gas Pipeline in Perspective*, 21 September 1982, available at https://www.cia.gov/ (last accessed on 11 August 2021)

French intelligence would have discovered the Soviet manoeuvres to get software secretly from the West to update the pipeline to export gas to Western countries.[109]

Some authors manifested that the facts of this account are controversial.[110] Vasily Pchelintsev, a Russian official at that time denied the story in the Russian media in 2004 and contradicted the findings of the book by Reed, explaining that the only explosion that took place about 50 kilometers from the city of Tobolsk, in the Tyumen region in April 1982 was due to a failure in the construction of the pipeline.[111] Additionally, some academic commentators argued that the lack of Soviet reports in the media about the alleged intrusion in 1982 and the technological capacity of the United States to hide malware made the story of this malicious cyber activity implausible.[112]

Regardless of the debate around this story, which is far beyond the scope of this study, the alleged facts reveal how geopolitics, economic interests and technological capabilities interact and play an essential role in the background of malicious cyber activities. Besides, the fact that this case went public in 2004 (three years before the case of Estonia) demonstrates that the topic was already well-rooted in the media at that time.

**b) 1999 war in Yugoslavia:**

During the war in the former Yugoslavia, a variety of allied computer systems, such as those relating NATO website and its e-mail account was targeted via a denial of service (an overload of electronic traffic) as a response to the Operation Allied Force.

Some authors considered this case as 'the first cyberwar';[113]others, 'the first broad-scale Internet war'.[114] However, some media reports considered that the United States

[109] See WEISS, G., *The Farewell Dossier*, 1996, available at https://www.cia.gov/ (last accessed on 11 August 2021).
[110] See RID, T., *Think Again: cyberwar*, 27 February 2012, available at https://foreignpolicy.com/ (last accessed on 11 August 2021).
[111] See MEDETSKY, A., *KGB Veteran Denies CIA Caused '82 Blast*, 18 March 2004, available at http://oldtmt.vedomosti.ru/ (last accessed on 11 August 2021).
[112] See RID, T., *Cyberwar and Peace: Hacking Can Reduce Real-World Violence*, 2013, p. 79, available at https://ridt.co/ (last accessed on 11 August 2021).
[113] See SEGURA-SERRANO, A., *Internet Regulation*, cit. note 76, p. 222.
[114] See GEERS, K., *Cyberspace and the Changing Nature of Warfare*, Tallinn, CCDCOE, Keynote Speech, available at https://ccdcoe.org/ (last accessed on 11 August 2021).

withheld a reaction to avoid an escalation into the 'first world cyberwar'.[115] An unclassified document of the American Department of Defense described the importance of holding the critical nodes of the Serbian air defence system at risk by way of an 'electronic warfare'.[116] Media reports argued that President Clinton had authorised the CIA to destabilise Milosevic and that within possible measures, cyber reactions were included.[117] However, some reports contended that the plans to target banks were shelved after a document from the American Department of Defense explained the legal implications of a 'cyberwar'.[118] That document is said to be the first legal opinion on the application of already existing international law to malicious cyber activities. It was already in 1999, around a decade before the initial discussions of the Tallinn Manual, when the United States already made clear its national position on a regulatory framework for cyber threats: 'there seems to be no particularly good reason to support negotiations for new treaty obligations in most of the areas of international law that are directly relevant to information operations'.[119]

As follows on from the above, this is a relevant study case since it demonstrates that malicious cyber activities may be part of a conventional conflict employing kinetic means. In such circumstances, cyber harm became under the more general umbrella of the use of force in the framework of an armed conflict.

### c) Estonia 2007 and Georgia 2008

Malicious cyber activities in Estonia have been labelled as 'the WWI' (Web War I).[120] At that time, tensions between Georgia and the Russian Federation were exacerbated due to the relocation of a Soviet Red Army memorial from a prominent location in Tallinn to a military cemetery on the outskirts of the city. According to some reports, the Russians

---

[115] See BORGER, J., *Pentagon Kept the Lid on Cyberwar in Kosovo,* 9 November 1999, available at https://www.theguardian.com/ (last accessed on 11 August 2021).
[116] See Report to Congress - Kosovo Operation Allied Force, available at https://archive.org/ (last accessed on 11 August 2021).
[117] See article entitled *Sources: CIA gets go-ahead to destabilize Yugoslavia*, 24 May 1999, available at www.edition.cnn.com/ (last accessed on 11 August 2021); GRAHAM, B., *Military Grappling with Rules for Cyber Warfare*, 8 November 1999, available at http://www.washingtonpost.com/ (last accessed on 11 August 2021).
[118] Assessment of International Legal Issues in Information Operations, Department of Defense, Office of General Counsel, p. 50, available at https://fas.org/ (last accessed on 11 August 2021).
[119] Ibid.
[120] See article entitled *War in the fifth domain. Are the Mouse and Keyboard the New Weapons of Conflict?*, 1 July 2010, available at https://www.economist.com/ (last accessed on 11 August 2021).

considered the memorial as a symbol of the liberation of Estonia from the Nazis, while the Estonians considered it a symbol of the oppression.[121]

Malicious cyber activities targeted daily newspapers, TV stations, Internet service providers, universities, hospitals and banks; more than a million computers were hijacked.[122] The most important bank of Estonia was shut down for one day (with the ensuing economic consequences that this means) and the members of Parliament remained without email access for several days.[123] Altogether, these malicious cyber activities mostly involved a distributed denial of service (DDOS) rather than the destruction of information.

It turned out that the computers utilised by the hackers were located in the United States, yet the owners were unaware of that.[124] Even if these malicious cyber activities caused severe interference and economic loss, Article 5 of the NATO Charter was not activated.[125] However, it paved the way for the future position of that organisation that expressly agreed in the Wales Summit (2014) that a State may invoke this provision to activate the right to collective self-defence in case of a cyberattack.[126]

The case of Estonia is emblematic because the target was an 'information system's society';[127] namely, a highly interconnected, communicated and technologically advanced society, which earned the country the nickname of 'E-stonia'.[128] These circumstances made Estonia a 'milestone and a symbol'[129] or a 'hotshot in cybersecurity'.[130]

---

[121] See RAIN, O., *Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective,* Tallinn, CCDCOE, available at https://ccdcoe.org/ (last accessed on 11 August 2021).
[122] See HOLLIS, D., *Why States Need an International Law*, cit. note 28, p. 1025.
[123] See HINKLE, K., *Countermeasures in the Cyber Context: One More Thing to Worry About*, in 'Yale Journal of International Law Online', Fall 2011, p. 13.
[124] See WOLTAG, J., *Computer Network Operations*, cit. note 71, p. 4.
[125] See TIKK, E., KASKA, K. AND VIHUL, L., *International Cyber Incidents: Legal Considerations*, Tallinn, 2010, pp. 24-25, available at https://ccdcoe.org/ (last accessed on 11 August 2021).
[126] Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 5 September 2014, para. 72, available at https://www.nato.int/ (last accessed on 11 August 2021).
[127] TIKK, E., KASKA, K. AND VIHUL, L., *International Cyber Incidents*, cit. note 125, p. 16.
[128] See MANSEL, T., *How Estonia became E-stonia*, 16 May 2013, available at https://www.bbc.com/ (last accessed on 11 August 2021).
[129] Terms used by Jaan Priisalu, senior researcher at Tallinn's NATO Cooperative Cyber Defence Centre of Excellence in an article entitled *Estonia's reaction to cyber attacks influenced global security policy,* 25 April 2017, available at https://news.err.ee/ (last accessed on 21 July 201).
[130] MCGUINNESS, D., *How a Cyber Attack Transformed Estonia,* 27 April 2017, available at https://www.bbc.com/ (last accessed on 11 August 2021).

These facts laid the ground for the future of the country as the building stone of the Tallinn Manual. Its first edition (2013) was a study of the law governing cyber warfare. A second version was released under the name of Tallinn Manual 2.0, which extended the study to operations during peacetime. As described in its introduction, that academic work was produced at the core of the Cooperative Cyber Defence Centre of Excellence (CCDCOE), under the aegis of NATO,[131] created shortly after the referred malicious cyber activity. The aim was to create a non-binding document applying existing law to 'cyber warfare'.[132] Schmitt, the Director of the project, described the Manual as a set of rules adopted unanimously by the Group of Experts, which are meant to reflect customary international law.[133]

A twin case took place in Georgia the year after the events in Estonia. Not only were the governmental and media servers targeted but also financial, educational and business servers were affected in a second phase. Noteworthily, Georgia, unlike Estonia, was not considered an 'information society'. Hollis described that malicious cyber activity as 'the first case in history of a coordinated cyberspace domain attack synchronized with major combat actions in the other war fighting domains (consisting of Land, Air, Sea, and Space)'.[134]

There are lessons to be learnt from these cases as well: Estonia demonstrated that economic loss is a common effect that malicious cyber activities bring about. Regarding Georgia, it has similarities with the Yugoslavian case in that malicious cyber activities were carried out in both cases in the context of a conflict; the difference was that in Georgia the target was a single State whereas in Yugoslavia, the target was NATO.

### d) 2010 Stuxnet in Iran

Stuxnet has been considered 'the world first digital weapon'.[135] Stuxnet was a cyber worm delivered by a USB memory stick that manipulated the speed of the centrifuges of the

---

[131] See the official website: https://ccdcoe.org/about-us/
[132] *Tallinn Manual*, cit. note 13, p. 16.
[133] SCHMITT, M., *International Law in Cyberspace: The Koh Speech*, cit. note 35, p. 15.
[134] HOLLIS, D., *Cyberwar Case Study: Georgia 2008*, in 'Small Wars Journal', 2011, p. 2. See also the description in the media: 'it was the first time a known cyber-attack had coincided with a shooting war' in MARKOFF, J., *Before the Gunfire, Cyber-Attacks,* 12 August 2008, available at https://www.nytimes.com/ (last accessed on 11 August 2021).
[135] See SETTER, K., *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*, 11 March 2014, available at https://www.wired.com/ (last accessed on 11 August 2021). See also FILDES, J., *Stuxnet Virus Targets and Spread*

nuclear reactor that enriched uranium at Natanz plant in Iran. This intrusion caused the centrifuges to switch back and forth to the point of damaging them. Despite the destructive effects, Iran did not invoque its right to self-defence. In effect, the particular advantage that such malicious cyber activities have over kinetic attacks is that they can achieve goals without causing loss of life or injury to civilians that traditional means of war are likely to inflict.[136]

Inspectors of the International Atomic Energy Agency informed that during the week starting on 16 November 2010, Iran had stopped feeding uranium into the Natanz centrifuges,[137] which could be an indication of a significant breakdown.[138]

This was considered the first destructive malicious cyber activity; in other terms, what some considered to be the first 'cyberattack'. The particular characteristics of this case led some to consider it as a 'game-changer' because it targeted zero-day (unknown) vulnerabilities in an inadvertently way; it laid the grounds for creating future malware (which indeed happened); and it targeted a critical national infrastructure.[139] In effect, Stuxnet became the first malware with such a level of sophistication.[140] This malicious cyber activity raised awareness on the capacity a malware has to circumvent the systems designed for real-time data collection, control, and monitoring of critical infrastructure, including power plants, oil and gas pipelines, refineries and water systems (usually designated by the acronym SCADA, i.e. supervisory control and data acquisition). Such malicious cyber activities may cause, *inter alia,* nuclear explosions, floods, wreak havoc in traffic, shut down power grids or blow up gas pipelines.

This case also marked a milestone in international debate and the adoption of national positions. In 2011 the United States published its International Strategy for

---

*Revealed*, 15 February 2011, available at https://www.bbc.com/ (last accessed on 11 August 2021). It reads: 'Stuxnet …was the first-known virus specifically designed to target real-world infrastructure'.

[136] See FARWELL, J. AND ROHOZINSKI, R., *Stuxnet and the Future of Cyber War*, in 'Survival', Vol. 53, No 1, 2011, p. 34. See also: LANGER, R., *Stuxnet und die Folgen*, Munich, 2017, p. 24, available at https://www.langner.com/ (last accessed on 11 August 2021).

[137] See International Atomic Energy Agency Report, GOV/2010/62, 23 November 2010.

[138] See FARWELL, J. AND ROHOZINSKI, R., *Stuxnet and the Future of Cyber War*, cit. note 136, p. 29. See also: ALBRIGH, D., STRICKER, J. AND WALROND, C., *IAEA Iran Safeguards Report: Shutdown of Enrichment at Natans Result of Stuxnet Virus?*, ISIS Report, 23 November 2010, available at http://isis-online.org/ (last accessed on 11 August 2021).

[139] See DENNING, D., *Stuxnet: What has Changed?*, in 'Future Internet', Vol. 2, 2012, p. 672; PORTEOUS, H., *The Stuxnet Worm: just Another Computer Attack or a Game Changer?*, Publication No. 2010-81-E Ottawa, Canada, Library of Parliament (2010), available at http://publications.gc.ca/ (last accessed on 11 August 2021).

[140] DENNING, D., *Stuxnet: what has changed?*, cit. note 139, p. 674.

Cyberspace declaring that '[w]e reserve the right to use all necessary means –diplomatic, informational, military, and economic– as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests'.[141] This statement was an apparent reference to the application of the right to self-defence under Article 51 of the UN Charter.

It cannot be ruled out that this precedent might have influenced the work of the Tallinn Manual group of experts, which included a complete section on the use of self-defence against malicious cyber activities considered armed attacks. Incidentally, three weeks after the release of the first draft of the Tallinn Manual, the State Department Legal Adviser Harold Koh made public the American position on how international law applies to cyberspace (including the right to self-defence) at a conference sponsored by the United States Cyber Command (USCYBERCOM).[142] It is timely to recall that declarations of State officials can convey traces of *opinio juris* in the formation of customary law.[143]

**e) 2015 Ukrainian Power Grid:**

This case took place in the framework of a serious bilateral crisis accelerated by the annexation of Crimea by the Russian Federation in 2014. In December 2015, hackers took control of a few power plants in Ukraine and stopped them for several hours with an unprecedented degree of sophistication and planning. Ukraine and some other States blamed the Russian Federation, explaining that the malicious cyber activity was a retaliation for the attacks on the Crimean power sub-stations conducted by pro-Ukrainian activists after the nationalisation of Ukrainian-owned energy companies.

There are some particularities of this case: firstly, not only did the hackers take control of the power grid, but they also prevented operators to re-gain access and restore the

[141] See International Strategy for Cyberspace of the United States (2011), p 14, available at https://obamawhitehouse.archives.gov/ (last accessed on 11 August 2021).
[142] See SCHMITT, M., *International Law in Cyberspace: The Koh Speech*, cit. note 35, p. 14; KOH, H., *International Law in Cyberspace*, in 'Harvard International Law Journal' , Vol. 54, 2012, question 4, p. 4.
[143] On this point, see VÄLJATAGA, A., *Tracing Opinio Juris in National Cyber Security Strategy Documents*, Tallinn, 2018, p. 4, available at https://ccdcoe.org/ (last accessed on 11 August 2021).

system.[144] Secondly, this malicious cyber activity was unique since it was the first one that targeted a civilian and not a military infrastructure.[145]

Ukraine suffered another malicious cyber activity in 2016, and –as Ben Buchanan explained– the difference between both of them was that the latter employed artificial intelligence for the automated commands.[146]

### f) 2018 the Organisation for the Prohibition of Chemical Weapons (OPCW)

This case was the first time that a non-military international governmental organisation was the intended target. The government of the Netherlands (host State of the OPCW) disrupted an attempted malicious cyber activity to undermine the integrity of the organisation by a group of hackers pertaining to the Russian military intelligence team.[147] Allegedly, the hackers had travelled with diplomatic passports to the Netherlands; that is the reason why they were not prosecuted in The Hague but sent back to the Russian Federation.[148]

Upon this precedent, for the first time the European Union applied restrictive measures against four Russian individuals for the attempted malicious cyber activity directed against the OPCW.[149] Such measures are part of the European diplomatic response against malicious cyber activities (the so called 'diplomatic toolbox' of the EU),[150] which comprises

---

[144] LEE, R., ASSANTE, M. AND CONWAY, T., *Analysis of the Cyber Attack on the Ukrainian Power Grid*, 18 March 2016, p. 20, available at https://ics.sans.org/ (last accessed on 11 August 2021).
[145] Ibid.
[146] See article entitled *Transcript: Tech Expert Ben Buchanan talks with Michael Morell on 'Intelligence Matters'*, 19 February 2020, available at https://www.cbsnews.com/ (last accessed on 11 August 2021).
[147] Government of the Netherlands, 'Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW', 4 October 2010, available at https://www.government.nl/ (last accessed on 11 August 2021).
[148] See article entitled *How the Dutch foiled Russian 'cyber-attack' on OPCW*, 4 October 2018, available at https://www.bbc.com/ (last accessed on 11 August 2021).
[149] Council (EU) Implementing Regulation 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 246/4. Similar restrictive measures were applied to Chinese individuals and entities for the malicious cyber activities publicly known as 'WannaCry' and 'NotPetya', as well as 'Operation Cloud Hopper' on 30 July 2020.
[150] Council (EU) Draft Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Toolbox'), 9916/17, 7 June 2017.

prohibitions to enter or transit the territory and freeze assets (this toolbox also encourages third States to apply similar measures).[151]

In a nutshell, the cases reviewed above marked a turning point in the study of malicious cyber activities for different reasons that were just explained. Remarkably, some facts remain controversial as to their existence, and their qualification under international law is unclear probably due to the difficulties in the identification of the hacker and the intent. None of the victim States has yet alleged that another State had violated international law by the cyber use of force. Therefore, practice in this field does not provide elements that may assist States in the legal qualification of malicious cyber activities. The next section will provide an insight into the work done in the academic field to elucidate the legal questions that these cases left open.

## 2.5.-LEGAL QUALIFICATION OF MALICIOUS CYBER ACTIVITIES UNDER INTERNATIONAL LAW:

The specialised literature has suggested that malicious cyber activities may be classified under the existing legal framework in a) intervention, b) uses of force and c) armed attacks. These three categories are identified on the basis of the provisions of the UN Charter and the complementary system of international law. For a better analysis of whether a special legal regime is required to address malicious cyber activities, it is indispensable to firstly review extant international law to assess its adequateness, lacunae and shortcomings. For such purposes, this section will review the state of the art in the qualification of malicious cyber activities in the already mentioned three categories.

[151] Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 129 I/13, Articles 5, 6 and 9; Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 129 I/1.

### 2.5.1.- INTERVENTION:

The fact that certain malicious cyber activities may fall outside the *jus ad bellum* regime does not lead to the conclusion that they fall outside the scope of other rules of international law, such as the principle of non-intervention.[152]

As a starting point, it has to be clarified that while all uses of force are coercive *per se* and thus breach the non-intervention obligation,[153] not all interventions infringe upon the prohibition on the use of force. According to the findings of the International Court of Justice (ICJ) in the Nicaragua case, the element of coercion defines and forms the very essence of the prohibition of intervention.[154] Coercion affects matters in which a State freely decides on the basis of the principle of State sovereignty (including political, economic and cultural issues). In addition, the ICJ argued in the Lotus case that a State may not exercise its power in any form in the territory of another.[155] The primary State's attribute protected by the obligation of non-intervention is the territorial sovereignty –an essential foundation of international relations, as pointed out by the ICJ in the Corfu Channel case.[156] It should be noted that some legal experts differentiate between sovereignty as a rule and as a principle. In the former case, sovereignty is a primary rule of international law that might be violated, whereas in the latter case it is only a principle that underpins other primary rules, like non-intervention and the prohibition on the use of force.[157]

Non-intervention is a bedrock principle, which is already accepted as a rule of customary international law.[158] While the UN Charter does not explicitly incorporate this

---

[152] See GRIMAL, F. AND SUNDARAM, J., *Cyber-Warfare and Autonomous Self-Defense*, in 'Journal on the Use of Force and International Law', 2017, p 11. See *Tallinn Manual*, cit. note 13, Rule 10, commentary, para. 6.
[153] See JIMENEZ DE ARECHAGA, E., *International Law in the Past Third of a Century*, Recueil des Cours, Alphen aan den Rijn, 1978, p. 113 ('The threat or the use of force represents the most obvious and extreme form of intervention').
[154] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America),* Judgement, [1986] ICJ Reports 14, 27 June 1986, ('*Nicaragua*'), para. 205. See also *Tallinn Manual*, cit. note 13, Rule 10, commentary, para. 8.
[155] *SS 'Lotus' (France v. Turkey),* PCIJ (Ser. A) No. 10, 7 September 1927 ('*Lotus*'), p. 18.
[156] *Corfu Channel (United Kingdom v Albania),* Judgment, [1949], ICJ Reports 4, 9 April 1949 ('*Corfu Channel*'), p. 35. See also SHAW, M., *International Law,* Cambridge, 2015, p. 352 ('[t]he principle whereby a state is deemed to exercise exclusive power over its territory can be regarded as a fundamental axiom of classical international law').
[157] SVANTESSON, D., AZZOPARDI, R., BONYTHON, W. et al., *The Developing Concept of Sovereignty. Considerations for Defence Operations in Cyberspace and Outer Space*, June 2021, p. 28 ff, available at https://research.bond.edu.au/ (last accessed on 19 October 2021).
[158] *Nicaragua*, cit. note 154, para. 202.

principle, it may be regarded as implicit in it.[159] The concept of 'non-intervention' was captured explicitly in UNGA Resolution 2131 (XX) on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty,[160] which condemns not only armed intervention, but all other forms of interference, and declares that intervention threatens international peace and security. Five years later, UNGA Resolution 2625 (XXV),[161] which was adopted without a vote, proclaimed non-intervention as a principle.

Non-intervention has traditionally been connected to State sovereignty in terms of territorial sovereignty. This approach makes unlawful intervention arise only where the physical territory of a State has been violated by another State or by non-State actors, if such activities are attributable to a State. Section 2.2 already explained that cyberspace is generally considered a domain over which no State can exercise territorial control; however, States may exercise sovereign prerogatives over any cyber infrastructure located in their territories, as well as over activities associated with that cyber infrastructure.

When the previous section outlined the case of Estonia, it underscored that one of the main consequences that such malicious cyber activities brought about was the impact on the Estonian economy. Since economic force is not considered to be encompassed in the prohibition of Article 2(4) of the UN Charter, the literature has supported the idea of considering the malicious cyber activities that cause such effects under the prohibition of non-intervention, as long as the element of coercion is verifiable.[162]

In sum, the non-intervention principle might provide a possible legal source applicable to malicious cyber activities when they do not meet the threshold of the use of force enshrined in Article 2(4) of the UN Charter.[163]

---

[159] See JIMENEZ DE ARECHAGA, E., *International Law*, cit. note 153, p. 112. He contends that the prohibition on the UN to intervene enshrined in Article 2(7) has to be read as extending to individual member States.
[160] United Nations General Assembly, Resolution 2131 (XX), 21 December 1965, A/RES/2131 (XX).
[161] United Nations General Assembly, Resolution 2625 (XXV), 24 October 1970, A/RES/2625 (XXV).
[162] UNGA Resolution 2625 reads: 'No State may use or encourage the use of economic [...] measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights [...]'.
[163] See WOLTAG, J., *Computer Network Operations*, cit. note 71, p. 3.

### 2.5.2.- USE OF FORCE

A differentiation of malicious cyber activities needs to be drawn to avoid erasing the distinction between acts of force and acts of coercion, as posited by Jason Barkham.[164] The prohibition on the use of force stems not only from Article 2(4) of the UN Charter but also from general international law, as acknowledged by the jurisprudence of the ICJ[165] and the doctrine alike.[166] In this regard, both norms (customary and treaty-based) retain their existence despite their identical content.[167] The literature has considered that Article 2(4) of the UN Charter embodies this prohibition in a flexible manner since the wording 'or in any manner' extends the possibility of applying this prohibition to other forms of use of force that might not be captured by violations of the territorial integrity or political independence.[168]

The UN Charter employs the word 'force' in many provisions and also in the preamble. In some provisions, it is preceded by the word 'armed' (for instance in the preamble[169] and in Articles 41[170] and 46[171]). Taking into consideration different rules of interpretation, the prevailing view in the literature is that the use of force in the UN Charter encompasses only the use of military force[172] or armed force.[173] The support for such an

---

[164] See BARKHAM, J., *Information Warfare*, cit. note 94, p. 111.
[165] See *Nicaragua*, cit. note 154, paras. 187-190, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory,* Advisory opinion, [2004] ICJ Reports 136, 9 July 2004, *('The Wall')*, para. 87.
[166] See SHAW, M., *International Law,* cit. note 156, p. 814; SIMMA, B., *The Charter of the United Nations. A Commentary*, Oxford, 2012, p. 133; DÖRR, O., *Use of Force, Prohibition of,* in Max Planck Encyclopedia of Public International Law, August 2019, available at https://opil.ouplaw.com/ (last accessed on 11 August 2021); GRAY, C., *The Use of Force and the International Legal Order*, in EVANS, M. (ed.), *International Law*, Oxford, 2003, p. 591, p. 86; *Tallinn Manual*, cit. note 13, Rule 10, commentary, para. 1.
[167] See *Nicaragua*, cit. note 154, para. 178.
[168] See SIMMA, B. (ed), *The Charter of the United Nations,* cit note. 166, p. 123 (para. 36).
[169] United Nations, *Charter of the United Nations*, signed on 26 June 1945, and entered into force on 24 October 1945. The relevant part reads: '[…] to ensure, by the acceptance of principles and the institution of methods, that armed force shall not be used, save in the common interest'.
[170] Article 41 of the UN Charter reads: 'The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations'.
[171] Article 46 of the UN Charter reads: 'Plans for the application of armed force shall be made by the Security Council with the assistance of the Military Staff Committee'.
[172] See ANTOLIN-JENKINS, V., *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places*, in 'Naval Law Review', Vol. 51, 2005, p. 153; BLAKE, D. AND IMBURGIA, J., *'Bloodless Weapons'?*, cit. note 57, p. 185; SIMMA, B., *The Charter of the United Nations*, cit. note 166, pp. 118-119.
[173] SIMMA, B. (ed). *The Charter of the United Nations,* cit note. 166, p. 117; RUYS, T., *'Armed attack' and Article 51 of the UN Chater. Evolution in Customary Law and Practice*, New York, 2010, p. 55; JIMENEZ DE ARECHAGA, E., *International Law*, cit. note 153, pp. 88-89.

assertion is to be found in the preamble of the UN Charter, which provides that the primary purpose of the organisation is to maintain international peace and security and to save future generations from the scourge of war.

Although some authors are of the view that this prohibition may cover non-military force as well, Judge Bruno Simma considered in his commentary to Article 2(4) that an extensive interpretation of the use of force is acceptable only within the narrowest possible limits.[174] He explained that a broad interpretation of this provision extends the prohibition to indirect force, which refers to the participation of one State in the use of force by another State. In effect, the Declaration on Principles of International Law Friendly Relations incorporated indirect force in two paragraphs dealing with the prohibition on the use of force.[175] It establishes that States have to refrain from organising or encouraging the organisation of irregular forces or armed bands including mercenaries, for incursion into the territory of another State. It also provides that States have to refrain from organising, instigating, assisting or participating in acts of civil strife or terrorist acts in another State or acquiescing in organised activities within its territory directed towards the commission of such acts, when such acts involve a threat or use of force. The jurisprudence of the ICJ went in the same direction considering indirect force to be encompassed in the prohibition on the use of force. In effect, in the Nicaragua case the ICJ concluded that the arming and training of the contras could undoubtedly be said to involve the threat or use of force against Nicaragua (unlike the mere supply of funds to the contras).[176] Some academic commentators construed analogies based on the conclusions of the ICJ in the Nicaragua case and emphasised that providing destructive malware and training to use it against a State would violate the prohibition on the use of force.[177] The previous conclusion would be supported by Marco Roscini if such malware is used to conduct malicious cyber activities amounting to a use of force.[178]

---

[174] SIMMA, B. (ed). *The Charter of the United Nations,* cit note. 166, p. 119.
[175] A/RES/2625 (XXV), cit. note 161.
[176] See *Nicaragua*, cit. note 154, para. 228.
[177] See SCHMITT, M. AND WATTS, S., *Beyond State-Centrism: International Law and Non- State Actors in Cyberspace*, in 'Journal of Conflict & Security Law', 2016, p. 13; *Tallinn Manual*, cit. note 13, Rule 11, commentary, para. 4 and Rule 11, commentary, para. 4.
[178] ROSCINI, M., *Cyber Operations and the Use of Force in International Law,* Oxford, 2014, p. 67.

There is no 'bright-line rule' for the qualification of a malicious cyber activity as a use of force.[179] The Tallinn Manual proposed in the commentary to Rule 11 a list of criteria for assessing whether a 'cyber operation' is a use of force.[180] These criteria are, *inter alia*: severity (activities that impinge on national interests or that cause severe damage, injury or death can easier qualify as use of force), immediacy (if the harmful consequences are immediate, States are more prone to consider a malicious cyber activity a use of force), directness (if the link between cause and effect is clear, it is easier to qualify the malicious cyber activity as a use of force), invasiveness (the more secure a State is, the higher the chances are that it considers a malicious cyber activity that has penetrated its systems a use of force), measurability (the more apparent and quantifiable the harmful consequences are, the easier for a State to qualify a malicious cyber activity as a use of force), military character (since military force is more connected with the concept of use of force, it is easier to assess a use of force when there is military involvement), State involvement (the more precise the nexus between a malicious cyber activity and a State, the more likely States will consider it a use of force) and presumptive legality (if there is no prohibition of a particular activity, States will more likely consider it legal).[181]

In 1963, Brownlie considered that the use of chemical and biological weapons could be considered a use of force even if there was no kinetic effect; the fact that they were employed for destruction of people and property was the determining factor to him.[182] Building upon that argument, authors like Cox suggested that even if malicious cyber activities do not comprise physical force, they might come under the application of Article 2(4) of the UN Charter.[183] Supporters of this argument resorted to an analysis by analogy of the *consequences* of kinetic attacks (physical damage),[184] the so-called 'kinetic equivalence doctrine'.[185] Thus, a malicious cyber activity would qualify as a use of force if it proximately results in death, injury or *significant* destruction.[186] To sustain this position, it has been argued

[179] See SILVER, D., *Computer Network Attack,* cit. note 50, p. 75.
[180] *Tallinn Manual*, cit. note 13, Rule 11, para. 9.
[181] *Tallinn Manual*, cit. note 13, Rule 11, commentary, para. 9; *Tallinn Manual 2.0,* cit. note 40, Rule 69, commentary, para. 9.
[182] This reference is made in MORTH, T., *Considering Our Position*, cit. note 49, p. 591.
[183] See COX, S., *Confronting Threats*, cit. note 30, p. 900.
[184] See SCHMITT, M., *Cyber Operations and the Jus Ad Bellum Revisited*, in 'Villanova Law Review', Vol. 56, 2011, p. 573; BUCHAN, R., *Cyber Attacks*, cit. note 56, p. 212.
[185] See ROSCINI, M., *Cyber Operations and the Use of Force*, cit. note 178, p. 45.
[186] See KOH, H., *International Law*, cit. note 142, pp. 3-4 (question 3). Note that the Tallinn Manual comments that 'acts that injure or kill persons or damage or destroy objects are *unambiguously* uses of force', Rule 11, commentary, para. 8.

that if the definition of use of force remains static, then the prohibition on the use of force gradually would become less effective.[187]

The ICJ in the Advisory Opinion on the Legality of the Threat or Use of Force also took into consideration the destructive capacity of nuclear weapons, i.e. the capacity to cause human suffering and the ability to cause damage to generations to come.[188]

However, even in such cases where there are no destructive effects but only disruptive ones, some authors considered that there might be a use of force involved when the target is a critical infrastructure. In this line, Roscini argued that *disruptive* malicious cyber activities against critical infrastructures would fall under the scope of Article 2(4), if they are significant enough to affect State security taking into consideration factors such as seriousness, duration, sophistication and reliance of the victim State on those infrastructures.[189] In such cases, the effects of disruption might be tantamount to destruction arising out from armed force.[190] Roscini's argument, however, should be contrasted with the assessment made by Roberto Ago in the sense that duration, magnitude and purposes would be irrelevant in the case of a conduct that violates Article 2(4).[191]

Although the consequence-based approach is the one that received more support in the cyber field,[192] it should be recalled that the UN Charter generally adopted an instrument-based approach in its text.[193] Thus, as pointed out by Morth, malicious cyber activities challenge an international legal system that defines warfare in terms of physical violence.[194]

The consequence-based approach is not free from criticism though. Some academic commentators considered that under this approach, the applicable regime would then

---

187 See BARKHAM, J., *Information Warfare*, cit. note 94, p. 73.
188 See *Legality of the Threat or Use of Nuclear Weapons,* Advisory Opinion*,* [1996] ICJ Reports 126*,* 8 July 1996 *('Nuclear Weapons'*), paras 35 and 36.
189 See ROSCINI, M., *Cyber Operations and the Use of Force*, cit. note 178, pp. 55 and 58.
190 Ibid., p. 62.
191 Addendum - Eighth Report on State responsibility by Mr. Roberto Ago, Special Rapporteur - The Internationally Wrongful Act of the State, Source of International Responsibility (part 1), UN Doc. A/CN.4/318/Add.5-7, 1980, p. 41. In the same line, see RUYS, T., '*Armed attack' and Article 51 of the UN Chater,* cit. note 173, p. 57: 'Article 2(4) constitutes a comprehensive ban against all uses or threats of force, regardless of their impact and gravity'.
192 ROSCINI, M., *Cyber Operations and the Use of Force*, cit. note 178, pp. 47-50.
193 See SCHMITT, M., *Cyber Operations and the Jus Ad Bellum Revisited*, cit. note 184, p. 587; SCHMITT, M., *Computer Network Attack and the Use of Force*, cit. note 32*,* p. 909.
194 See MORTH, T., *Considering Our Position*, cit. note 49, p. 584.

become more reactive than proactive because effects must materialise to justify an appropriate response.[195] Other authors argued that the legal system would become anachronistic with this approach because of its resulting inability to protect States from malicious cyber activities that do not cause physical damage.[196] Some even contended that such an approach would oversee the role that intention plays in malicious cyber activities, in particular the destructive intention that the hacker had.[197] Even further, Janne Valo suggested that under a consequence-based approach, a malicious cyber activity with extreme economic consequences might modify the customary rule on the prohibition of use of force as to include those types of force.[198] Vida Antolin-Jenkins warned against such a possibility by arguing that the incorporation of malicious cyber activities against critical economic infrastructure into the definition of use of force cannot be done without excluding other economic policies that were excluded from that definition.[199]

From the above, it is clear that the qualification of a malicious cyber activity as a use of force is far from established. The criteria provided in the Tallinn Manual are weak and provide little assistance: State involvement and immediacy are criteria that are difficult to elucidate in the case of malicious cyber activities due to their intrinsic characteristics, as explained in section 2.3. In effect, State involvement is inherently linked to the attribution problem that will be further explained in section 2.6 below, and immediacy hardly suits the unpredictability of effects. Directness does not suit the concept of indirect force described above. Furthermore, the last criterion (presumptive legality) is controversial since the alleged principle that 'whatever is not explicitly prohibited by international law is permitted' is far from being a generally accepted one (see chapter 5, section 5.4).[200]

---

[195] Ibid., p. 585.
[196] See BUCHAN, R., *Cyber Attacks*, cit. note 56, p. 213.
[197] See SHARP, W., *Cyberspace and the Use of Force*, Virginia, 1999, p. 102: 'any state activity in cyberspace that intentionally cause[s] *any* destructive effect within the sovereign territory of another state is an unlawful use of force'. See also SILVER, D., *Computer Network Attack*, cit. note 50, p. 83.
[198] See VALO, J., *Cyber Attacks and the Use of Force in International Law*, Master Thesis, University of Helsinki, January 2014, p 44, available at https://helda.helsinki.fi/ (last accessed on 11 August 2021). See also SEGURA-SERRANO, A., *Internet Regulation*, cit. note 76, pp. 224-225.
[199] See ANTOLIN-JENKINS, V., *Defining the Parameters of Cyberwar Operations,* cit. note 172, p. 135.
[200] This principle dates back to the Lotus judgment of the PCIJ. It was resumed by the ICJ in the Nuclear Weapons Advisory Opinion and the Kosovo Advisory Opinion. For a critical view, see the Declaration of Simma to the Kosovo Advisory Opinion, where he considered it obsolete and qualified the view of the majority as an 'anachronistic, extremely consensualist vision of international law' (*Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo*, Advisory opinion, Judgement, [2010] ICJ Reports 403, 22 July 2010 ('*Kosovo*'), Declaration of Simma, para. 3.

Without prejudice of this criticism, the other proposed criteria might provide some guidance to ease the difficult task of determining whether a malicious cyber activity qualifies as a use of force. Undoubtedly, this issue deserves more analysis and a discussion at the governmental level. While it is generally accepted that international law –in particular the UN Charter– is applicable and essential to maintain peace and stability in the cyber environment, further work and guidance are needed to elucidate which malicious cyber activities constitute a use of force in the cyber domain.

### 2.5.3.-ARMED ATTACK

Armed attacks are a sub-category of uses of force. This means that all armed attacks are uses of force, but not all uses of force are armed attacks. Therefore, some authors referred to a gap between uses of force and armed attacks, which becomes a source of uncertainty as to the applicable law and the lawful response.[201] However, it is important to note here that this view is not uniform: as advanced in section 2.4, the United States considers that any unlawful use of force is an armed attack triggering the right to self-defence.[202]

Although the UN Charter introduced the concept of 'armed attack' in Article 51, neither that instrument nor any other international treaty defined this concept.[203] 'Attacks' are defined in international law as 'acts of violence against the adversary'.[204] According to the ordinary meaning, 'armed' means 'involving the use of a weapon' and a weapon is an instrument used or designed to be used to injure or kill someone.[205] The preceding concept includes *any* element or instrument used to cause injury or death, regardless of the instrument. This assumption was made clear by the ICJ in the Nuclear Weapons Advisory Opinion[206] and can also be derived from paragraph 3(b) of General Assembly Resolution 3314 (XXIX), which regarded aggression the use of *any* weapons.[207] For his part, Dinstein considered that

[201] See SCHMITT, M. AND WATTS, S., *Beyond State-Centrism*, cit. note 177, p. 14; DINSTEIN, Y., *Cyber War and International Law: Concluding Remarks at the 2012 War Naval College International Law Conference*, in 'International Law Studies', Vol. 89, 2013, p. 100; Blake and Imburgia pointed at the narrower scope of the use of force in relation to an armed attack: see BLAKE, D. AND IMBURGIA, J., '*Bloodless Weapons'?*, cit. note 57, p. 187.
[202] See *Tallinn Manual*, cit. note 13, Rule 11, commentary, para. 7; *Tallinn Manual 2.0,* cit. note 40, Rule 69, commentary, para. 7.
[203] See *Nicaragua*, cit. note 154, para. 176.
[204] Protocol I, cit. note 41, Article 49.
[205] See GARNER, B. (ed), *Black's Law Dictionary*, cit. note 51, p. 717.
[206] *Nuclear Weapons*, cit. note 188, para. 39.
[207] United Nations General Assembly, Resolution 3314 (XXIX), 14 December 1974, A/RES/3314 (XXIX). See Article 3(b): 'Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State'.

an armed attack can be carried out with conventional, primitive or sophisticated ordnance (and made particularly reference to electronic attacks) –what counts are the consequential effects.[208] In the same line, Karl Zemanek considered that 'it is neither the designation of a device, nor its normal use, which make it a weapon but the intent with which it is used and its effect'.[209] The ICJ has also taken into account the specific intention of harming in the Oil Platforms case.[210]

Although the majority of the Tallinn Manual experts considered that the intention is irrelevant,[211] there are several pundits that do judge it a necessary element, probably building upon the assessment of the ICJ in the already referred Oil Platforms case. For Schmitt, a malicious cyber activity must be *intended* to directly cause physical damage to tangible objects or injury to human beings to be regarded as an 'armed attack'.[212] Likewise, Walter Sharp described an armed attack in the cyber field as 'any computer network attack conducted by a State that intentionally causes any destructive effect within the sovereignty territory of another State'.[213]

The jurisprudence of the ICJ provided an additional means of interpretation in the Nicaragua case resorting to the scale and effects test.[214] There, the ICJ expressly defined 'armed attacks' as the 'most grave' forms of use of force.[215] In another attempt to find a legal definition of 'armed attacks', legal experts generally point at the test proposed by Jean Pictet of 'scope, duration, and intensity' based on his 1958 commentary to common Article 2 of the Geneva Conventions.[216] In line with this approach, some authors like Joyner and

---

[208] DINSTEIN, Y., *Computer Network Attacks*, cit. note 55, p. 103.
[209] ZEMANEK, K., *Armed attack*, in Max Planck Encyclopedia of Public International Law, updated April 2010, available at available at https://opil.ouplaw.com/ (last accessed on 11 August 2021).
[210] *Oil Platforms (Islamic Republic of Iran v. United States of America),* Judgement, [2003] ICJ Reports 161, 6 November 2003, *('Oil Platforms'*), para. 64.
[211] *Tallinn Manual*, cit. note 13, Rule 13, commentary, para. 11.
[212] SCHMITT, M., *Computer Network Attack and the Use of Force*, cit. note 32, p. 929.
[213] SHARP, W., *Cyberspace and the Use of Force*, cit. note 197, p. 133.
[214] See *Nicaragua*, cit. note 154, para. 195.
[215] Ibid., para. 191; see also *Oil Platforms*, cit. note 210, para. 51.
[216] See SHARP, W., *Cyberspace and the Use of Force*, cit. note 197, p. 60; SKLEROV, M., *Solving the Dilemma of State Responses to Cyber-Attacks: A Justification for the Use of Active Defenses against States Who Neglect their Duty to Prevent*, in 'Military Law Review', Vol. 201, 2009, pp. 51-52; GRAHAM, D., *Cyber Threats and the Law of War*, in 'Journal of National Security Law and Policy', Vol. 4, 2010, p. 90.

Lotrionte emphasised the significance of the intensity, effects and duration of the malicious cyber activity.[217]

An additional source of interpretation of armed attacks arises from the already referred General Assembly Resolution 3314 (XXIX). The French version of the UN Charter employed the language 'armed aggression' instead of 'armed attack'. If a definition of aggression is sought, that resolution does not provide any assistance; however, it gave a hint of what is required for an armed attack to be considered aggression in Article 2, and the necessary element is 'sufficient gravity'.[218] It is of the utmost importance to recall that the prohibition of aggression is regarded as peremptory.[219] The International Law Commission defined a 'serious breach' as a 'gross or systematic failure by the responsible State to fulfil its obligation',[220] and 'systematic' as a violation committed in an organised and deliberate way.[221]

The scale and effects test gained traction within the group of experts of the Tallinn Manual, who reflected it in Rule 13. The experts agreed that any use of force that injures or kills persons or damages or destroys property would satisfy the scale and effects requirement.[222] However, they agreed that the law is unclear regarding the point in which such damage or injury failed to qualify as 'armed attack'.[223] Neither was there agreement in the group of experts on the qualification of severe non-destructive damage, like the economic one.[224] With regard to interference causing loss of functionality, some scholars considered that a cyberattack might be equated to a destructive act only in case that restoration of functionality requires replacement of *physical* components.[225]

---

[217] See JOYNER, C. AND LOTRIONTE, C., *Information Warfare as International Coercion*, cit. note 62, p. 863.
[218] A/RES/3314, cit. note 207, para. 2.
[219] See *Nicaragua*, cit. note 154, para. 190; Report of the International Law Commission 53rd Session (2001), Draft Articles on Responsibility of States for Internationally Wrongful Acts, UN Doc. A/56/10 ('*Draft Articles on State Responsibility*'), p. 112 (see commentary to Article 40, para. 4).
[220] Ibid., commentary to Article 40, para. 2.
[221] Ibid., para. 8.
[222] *Tallinn Manual*, cit. note 13, Rule 13, commentary, para. 6 (it is due to recall that although in Rule 11 the experts referred to a 'significant' damage, there is no such qualifying adjective in the description of para. 6 of the commentary to Rule 13. Also SCHMITT, M. AND VIHUL, L., *Proxy Wars in Cyberspace: the Evolving International Law of Attribution*, in 'Fletcher Security Review', Vol. 1, No 2, 2014, p. 67.
[223] *Tallinn Manual*, cit. note 13, Rule 13, commentary, para. 7.
[224] Ibid., para. 9.
[225] Ibid., Rule 30, commentary, para. 10. See also SCHMITT, M., *International Law in Cyberspace: The Koh Speech*, cit. note 35, p. 26, SCHMITT, M. AND WATTS, S., *Beyond State-Centrism*, cit. note 177, p. 5.

Admittedly, scholars do not share a uniform view on the feasibility of classifying malicious cyber activities as armed attacks, particularly due to the fact that they generally lack the physical characteristics traditionally associated with traditional military action. In this regard, Hollis argued that there is a gap between physical weaponry and cyber methods; thus, attempts to apply existing tenets to malicious cyber activities would result 'either in no clear rules emerging or a rule that contravenes other principles fundamental to the law of war'.[226]

In sharp contrast is the view that the qualification of malicious cyber activities as armed attacks is indeed feasible; therefore, resort to forceful responses under the existing body of international law would be admissible as well. In order to support that reasoning, scholars have applied three models like in the case of use of force: the instrument-based one (builds upon the concept of weapons), the consequence-based one (draws upon the kinetic equivalence model) and the target-based one (equates every attack against critical infrastructures as an armed attack).[227] The first model conceives a malicious cyber activity as an armed attack only if it employs military weapons.[228] The second model attempts to determine whether the damage caused by a new method of attack could have been achieved previously only with kinetic force. That model relies on the guidance and explanations regarding armed attacks in conventional terms to prove that malicious cyber activities can also become armed attacks due to their violent consequences.[229] The third analytical model –based on the target– is supported by authors like Sean Condron and Sharp, who justified self-defence measures in response to attacks causing damage to critical infrastructure.[230] For his part, Roscini clarified that attacks against critical infrastructures with *disruptive* effects (and non-destructive) will only meet the scale and effects threshold of an armed attack if they are *coordinated* and *seriously* disrupt *several* or *all* critical infrastructures of a *heavily* digitalised State for a *prolonged* time.[231]

There is no universal definition of critical national infrastructures (CNI) but in general terms they refer to the collection of systems and facilities that are essential to the

[226] HOLLIS, D., *Why States Need an International Law*, cit. note 28, p. 1040.
[227] See SKLEROV, M., *Solving the Dilemma*, cit. note 216, p. 55.
[228] See HATHAWAY, O., *The Law of Cyber-attack*, cit. note 101, pp. 845-846.
[229] See DINSTEIN, Y., *Computer Network Attacks*, cit. note 55, p. 103 ('A premeditated destructive computer network attack can qualify as an armed attack just as much as a kinetic attack bringing about the same-or similar-results').
[230] See CONDRON, S., *Getting It Right*, cit. note 97, p. 416; SHARP, W., *Cyberspace and the Use of Force*, cit. note 197, p. 129.
[231] See ROSCINI, M., *Cyber Operations and the Use of Force*, cit. note 178, p. 75.

well-being of a State (or even to its survival),[232] including communications, emergency services, transportation, security, food, water, banking and finance, health, energy and public services.[233] Each State determines its own CNI and, in fact, some States have already defined them domestically and have included some or most of the sectors previously mentioned (see chapter 3, section 3.7). Authors such as Condron suggested pre-selecting and disseminating information on CNI.[234] Likewise, Eric Jensen recommended publishing and continuing updating a list of CNI, for instance, with a mix of warning banners on the CNI websites and national statements or publications.[235] Although some academic commentators emphasised the need to create an international list of critical national infrastructures to confront the legal challenges that self-defence poses,[236] there is as yet no international attempt going in that direction.

In a nutshell, the diversity of opinions and the limited practice in the field helped increase the uncertainties and left many questions open, such as the one relating to the qualification of malicious cyber activities with devastating consequences in the finance of a State and the disruption or loss of functionality of critical infrastructures. According to the literature just reviewed, a group of experts support a cumulative requirement of gravity, duration and intent to differentiate a use of force from an armed attack in the cyber field. However, there are other views that deny the existence of a gap between uses of foce and armed attacks. These are some of the aspects that any international endeavour for security in the use of ICTs' governance will have to settle.

## 2.6.-STATE RESPONSIBILITY

According to well-established customary law, every international wrongful act of a State entails international responsibility. There is an internationally wrongful act when a conduct consisting of an action or omission is attributable to a State under international law

[232] See CONDRON, S., *Getting It Right*, cit. note 97, p. 407; SKLEROV, M., *Solving the Dilemma*, cit. note 216, p. 20; TSAGOURIAS, N., *Cyber Attacks, Self-Defence*, cit. note 85, p. 231.
[233] See TSAGOURIAS, N., *Cyber Attacks, Self-Defence*, cit. note 85, p. 231. See also United Nations General Assembly, Resolution 58/199, 23 December 2003, A/RES/58/199, 3rd paragraph of the preamble.
[234] See CONDRON, S., *Getting It Right*, cit. note 97, pp. 416 and 421.
[235] See JENSEN, E., *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense,* in 'Stanford Journal of International Law', Vol. 38, 2002, p. 236.
[236] See HOISINGTON, M., *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense,* in 'Boston College International and Comparative Law Review', Vol. 32, 2009, p. 453.

and constitutes a breach of an international obligation of that State.[237] Drawing from the aforementioned, there are two crucial issues to be explained here in order to determine State responsibility for a malicious cyber activity: first, it is required to examine and clarify what could be regarded as a wrongful act in the use of ICTs; and second, analyse the problem of attribution that characterises cyber activities.

**a) Wrongful acts in the cyber domain (objective element):**

Under international law, either an act or an omission of a State entails its responsibility.[238] Regarding the former, the previous section already provided a brief summary of possible violations of international law obligations: the prohibition of non-intervention and the prohibition on the use of force. In addition to those obligations, this section will introduce a third obligation for consideration: the exercise of due diligence. This thesis will limit the scope of study to these three obligations only, which does not mean that there might not be other obligations to be examined in future works.

As to the latter, it is nowadays generally accepted that the violation of the obligation to exercise due diligence entails State responsibility as well. This obligation was originally identidied in the jurisprudence of the ICJ in the Corfu Channel case where the Court concluded that 'every State shoulders an obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States'.[239]

In the aftermath of the 9/11, the Security Council passed Resolution 1373 (2001) which is a clear example that due diligence implies two types of obligations when the attacks are carried out by non-State actors: those that may be called 'forward-looking obligations' (to prevent)[240] and 'backward-looking obligations' (to investigate and prosecute).[241] The commentary of James Crawford to Article 14(3) of the Draft Articles on State Responsibility explains that the obligation to prevent requires 'that States take all reasonable or necessary measures without warranting that the event will not occur'.[242] There is no reference to the

[237] *Draft Articles on State Responsibility,* cit. note 219, Articles 1 and 2.
[238] Ibid., Article 2 and commentary to Article 1, para. 4.
[239] *Corfu Channel*, cit. note 156, p. 22.
[240] See United Nations Security Council, Resolution 1373, 28 September 2001 (preventive measures included in para. 2. b), d), g), for instance.
[241] See Ibid. (duty to prosecute and punish in para. 2.e), for instance.
[242] CRAWFORD, J., *The International Law Commission's Articles on State Responsibility: Introduction, Text, and Commentaries*, Cambridge, 2002 ('*Crawford Commentary*'). See commentary to Article 13, para. 14.

obligation to investigate and prosecute in the Draft Articles on State responsibility –it is an obligation that is fundamentally rooted in human rights law.

The forward-looking obligation to prevent was reflected in the Tallinn Manual in Rule 5, [243] which provided for an obligation to prevent the unlawful use of cyber infrastructure located in the territory of a State. Similar language was incorporated in the 2015 report of the GEE on ICTs in its paragraph 13(c).[244] Paragraph 13(a) incorporated another obligation of this type: 'to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security'.[245] The Tallinn Manual recognised that the obligation to prevent is complicated to comply with in the cyber realm by its very nature.[246] Furthermore, as pointed out by Matthew Hoisington, for a State to prevent a malicious cyber activity, it must firstly identify the intentions of the attacker as hostile, something that might be as difficult as deducing its identity.[247] This argument is one of the reasons behind the position of an 'emerging consensus' supporting that the due diligence obligation does not encompass preventive measures in the cyber realm,[248] which was encapsulated in the commentary to Rule 7 of Tallinn Manual 2.0.[249]

Tallinn Manual 2.0 incorporated a heading for due diligence, which includes Rules 6 and 7. According to Rule 6, a State should not allow 'its territory or the infrastructure under its governmental control to be used for operations that are contrary to the rights of the affected State under international law and have serious adverse consequences'.[250] Similar to the Crawford's commentary, the commentary to Rule 7 explains that due diligence is an obligation of conduct, not of results.[251] The obligation to prevent may be breached not only by inaction but also by insufficient or inefficient measures.[252] This time, the experts of Tallinn Manual 2.0 agreed that this obligation only applied to malicious cyber activities that amount

[243] *Tallinn Manual*, cit. note 13, Rule 5 reads: 'A State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States'.
[244] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174, 22 July 2015.
[245] Ibid.
[246] See *Tallinn Manual*, cit. note 13, Rule 5, para. 4.
[247] See HOISINGTON, M., *Cyberwarfare and the Use of Force,* cit. note 236, pp. 451- 452.
[248] See SCHMITT, M., *In Defense of Due Diligence in Cyberspace*, in 'The Yale Journal Forum', 2015, p. 75; *Tallinn Manual 2.0,* cit. note 40, Rule 6, commentary, para. 5.
[249] *Tallinn Manual 2.0,* cit. note 40, Rule 7, commentary, para. 7.
[250] *Tallinn Manual*, cit. note 13, Rule 6, commentary, paras 15 and 25.
[251] *Tallinn Manual 2.0,* cit. note 40, Rule 7, commentary, para. 24.
[252] Ibid., para. 2.

to an internationally wrongful act[253] and of which the territorial State knows or should have known.[254]

Regarding the backward-looking obligation to investigate and prosecute, the 2015 report of the GEE on ICTs introduced a reference to the obligation to prosecute terrorist and criminal use of ICTs in paragraph 13(d).[255] Tallinn Manual 2.0 included Rule 7, which deals with the obligation to halt malicious cyber activities affecting other States (which might also be considered a backward-looking obligation). The group of experts did not reach agreement on whether this rule applies only to ongoing activities or if it also covers those in an initial stage (for instance, when malware is installed but not yet activated).[256]

In sum, the objective element of State responsibility can be examined in light of, *inter alia*, the breach of the obligation of non-intervention, the prohibition on the use of force and the obligation to exercise due diligence. Hence, the first part of this analysis relating to State responsibility is accomplished.

**b) Attribution in the cyber realm (subjective element):**

Now it is the turn of the second part of the proposed analysis; namely, to address the so-called 'attribution problem'. As indicated at the beginning of this section, the second element required for a State to become internationally responsible is attribution of the act or omission to that State. International practice distinguished different cases of attribution, *inter alia*, the conduct of State organs,[257] the conduct of persons or entities exercising elements of governmental authority,[258] the conduct of organs placed at the disposal of a State by another State,[259] the conduct directed or controlled by a State[260] and the conduct acknowledged and adopted by a State as its own.[261]

[253] *Tallinn Manual 2.0,* cit. note 40 Rule 6, commentary, para. 17.
[254] Ibid., paras. 37 and 39. See also Rule 7, commentary, para. 9.
[255] UN Doc. A/70/174, cit. note 244.
[256] *Tallinn Manual 2.0,* cit. note 40, Rule 7, commentary, paras 3-4.
[257] *Draft Articles on State Responsibility*, cit. note 219, Article 4.
[258] Ibid., Article 5.
[259] Ibid., Article 6.
[260] Ibid., Article 8.
[261] Ibid., Article 11.

Regarding the scenario where non-State actors operate under the instructions or directions and control of a State, an on-going debate in international law circles exists about the level of control required for attribution. Under the 'effective control' test, non-State actors have to conduct the operations on behalf of the State.[262] In the Tadic case, the International Criminal Tribunal of Yugoslavia distinguished two standards and explained when each of them is applicable. The tribunal clarified that the 'effective control' test applied to individuals and unorganised groups. For such cases, specific instructions aimed at the commission of certain acts or public approval of those acts upon their commission is necessary.[263] To the contrary, it considered that the test applicable to organised groups is the 'overall control', whereby the State coordinates or helps in the general planning of its military activity'.[264]

Although the literature tends to address these two tests as a dichotomy between option A and B, it is appropriate to mention the different scope of both tests: while the 'effective control' is a test for attribution of State responsibility, the 'overall control' was a test used to define whether the war in Bosnia was an international or non-international conflict.[265] Moreover, the ICJ criticised the application of the 'overall control' test to the determination of State responsibility 'for it stretches too far, almost to a breaking point, the connection which must exist between the conduct of a State's organs and its international responsibility'.[266]

When addressing attribution matters, it is of the utmost importance to refer to the methods of proof. In the Nicaragua ruling, the ICJ acknowledged that the problem was not the legal process of imputing the act to a particular State but the prior process of tracing material proof of the identity of the perpetrator.[267] The ICJ applied different standards to assess evidence in its case law:[268] for instance, proof that provides 'clear evidence' of the

---

[262] See *Nicaragua*, cit. note 154, para. 109; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Hersegovina v. Serbia and Montenegro),* Judgement, [2007] ICJ Reports 43, 26 February 2007, paras 391-393 ('*Bosnia genocide*').
[263] See *Prosecutor v Tadic*, Case No IT-94-1, Appeals Chamber Judgment 15 July 1999, para. 120 ff.
[264] Ibid., para. 131.
[265] See TSAGOURIAS, N., *Cyber Attacks, Self-Defence*, cit. note 85, p. 239; *Bosnia Genocide*, cit. note 262, p. 404.
[266] *Bosnia Genocide*, cit. note 262, p. 406.
[267] See *Nicaragua*, cit. note 154, para. 57.
[268] See Speech by Judge Rosalyn Higgins, President of the International Court of Justice to the Sixth Committee of the General Assembly, 2 November 2007, available at https://www.icj-cij.org/ (last accessed on 11 August 2021).

effective control over the contras in the Nicaragua case,[269] 'fully conclusive' evidence of charges of exceptional gravity in the Bosnia Genocide case,[270] 'conclusive evidence' of the actual support for anti-Ugandan rebel groups in the Armed Activities in Congo case,[271] and proof that leaves 'no room for reasonable doubt' that Albania had knowledge of mine laying in her territorial waters in the Corfu Channel case.[272]

Turning the attention to malicious cyber activities, it is possible to affirm that attribution of such acts is difficult due to the particular characteristics already described earlier in this chapter: anonymity, the speed with which they can materialise and the possibility of launching a multi-stage cyberattack. The 2015 report of the GEE on ICTs reflected the attribution problem by affirming that the territory where a malicious cyber activity originates is not sufficient in itself to attribute the activity to that State.[273] Precisely these factors that make attribution difficult are the basis for some academic commentators like Shackelford considering that the 'overall control' test should apply to malicious cyber activities.[274] In effect, his explanation is that the 'effective control' test establishes a very high standard of proof.[275]

Tallinn Manual 2.0 introduced the matter of attribution of non-State actors in Rule 17 and provided two cases where attribution follows: a) instruction, direction or control of the State and b) when the State acknowledges and adopts a malicious cyber activity as its own. The former is built upon Article 8 of the Draft Articles on State Responsibility, and the test that the Tallinn Manual experts selected was the 'effective control'.[276] A State is in 'effective control' of a particular malicious cyber activity carried out by a non-State actor when it determines its execution and course.[277] The latter case (when the State acknowledges and adopts the operation as its own) is built upon Article 11 of the Draft Articles on State Responsibility and the ICJ's ruling in the Tehran Hostages case. There, the court established

---

[269] *Nicaragua*, cit. note 154, para. 109.
[270] See *Bosnia Genocide*, cit. note 262, para. 209.
[271] See also *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda),* Judgement, [2005] ICJ Reports 168, 19 December 2005, paras 303 and 336.
[272] *Corfu Channel*, cit. note 156, p. 18.
[273] UN Doc. A/70/174, cit. note 244, para. 28(f).
[274] See SHACKELFORD, S., *From Nuclear War to Net War*, cit. note 64, p. 235.
[275] See SHACKELFORD, S., *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, Conference on Cyber Conflict Proceedings 2010, CCD COE Publications, Tallinn (2010), pp. 203 and 206, available at https://ccdcoe.org/ (11 August 2021).
[276] *Tallinn Manual 2.0,* cit. note 40, Rule 17, commentary, para. 5.
[277] Ibid., para. 6.

that what entailed responsibility was not only the approval of the Iranian government but also the decision to perpetuate the occupation of the American Embassy.[278] Hence, Rule 17 of Tallinn Manual 2.0 established two cumulative requirements for attribution (acknowledgment and adoption as its own).[279]

There is a third position on the applicable test for non-State actors in the cyber domain: Nicholas Tsagourias criticised fixed and immutable attribution standards, such as the effective or overall control.[280] Making reference to the literal text of Article 8 of the Draft Articles on State Responsibility that simply refers to 'control' and to the commentary thereto, he proposed a flexible approach of 'control' that might adapt to the context in which it arises.[281]

If the legal framework provides clear rules on attribution, the incentives to carry out malicious cyber activities should probably decrease because States would be aware of the consequences of a possible response from the victim State. Precisely, the next section will deal with legal responses under international law.

## 2.7.- LEGAL RESPONSES:

An important consequence of State responsibility is that the victim State can lawfully and appropriately respond against the offender. Once it is determined against whom the response will be directed, it is necessary to define the appropriate measure. For such purposes, within the universe of malicious cyber activities, it is possible to distinguish among cyber incidents that do not reach the level of use of force, malicious cyber activities that reach the level of use of force short of an armed attack, and grave malicious cyber activities that reach the level of an armed attack.

For ease of reading, this section will be broken down into three sub-sections: the first one will start with the lowest level of response in terms of gravity; namely, responses that do not involve forceful measures (countermeasures). The second sub-section will deal with the

[278] See *United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)*, Judgement, [1980] ICJ Reports 3, 24 May 1980 (*'Tehran Hostages'*), para. 74.
[279] *Tallinn Manual 2.0,* cit. note 40, Rule 17, commentary, para. 16.
[280] See TSAGOURIAS, N., *Cyber Attacks, Self-Defence*, cit. note 85, p. 244.
[281] Ibid., p. 239.

most severe responses that involve the use of force. Finally, the third sub-section will provide an alternative solution in cases where neither countermeasures nor forceful measures are a lawful alternative.

### 2.7.1.-COUNTERMEASURES IN PEACETIME

This section will deal with malicious cyber activities that violate the non-intervention principle or those involving the use of force short of armed attacks. In such cases, a State may respond with non-forcible proportionate measures.[282]

Countermeasures consist of acts that otherwise would be unlawful. This fact is the main feature that differentiates them from retorsion, which consists of merely unfriendly acts that may be a response when there is no breach of an international obligation. On the other hand, the non-forcible nature of countermeasures [283] is the characteristic that distinguishes them from self-defence (forcible in nature). In line with this characteristic, countermeasures must be reversible as far as possible.[284] In other words, they should be non-destructive and should not employ the use of force.[285] In effect, it should be recalled that reprisals employing the use of force are forbidden by international law.[286]

Pursuant to the Draft Articles on State Responsibility, countermeasures are necessarily exceptional[287] and provisional.[288] Their purpose is to induce the responsible State to cease the internationally wrongful conduct if it is continuing and to provide reparation to the injured State. Thus, preventive countermeasures are unlawful since the on-going wrongful act is a requisite for them to be lawful. The aforementioned is tightly connected to their temporary character, which implies that countermeasures must cease when the responsible State has ceased its wrongful conduct or has made the appropriate reparation.

---

[282] See *Nicaragua*, cit. note 154, para. 249.
[283] *Draft Articles on State Responsibility,* cit. note 219, Article 50(1)(a).
[284] *Gabčíkovo-Nagymaros Project (Hungary/Slovakia),* Judgement, [1997] ICJ Reports 7, 25 September 1997 ('*Gabčíkovo-Nagymaros*'), para. 87.
[285] See *Crawford Commentary*, cit. note 242, commentary to Article 50.1, paras 3-5.
[286] A/RES/2625 (XXV), cit. note 161. It reads in the relevant part: 'States have a duty to refrain from acts of reprisal involving the use of force'.
[287] *Crawford Commentary*, commentary to Article 49, para. 1.
[288] Ibid., para. 7.

According to the jurisprudence of the ICJ in the Gabčíkovo-Nagymaros case [289] and the Draft Articles on State Responsibility,[290] countermeasures must meet certain conditions: firstly, they must be a response to an internationally wrongful act. Secondly, they need to be directed against a State. Thirdly, countermeasures must be proportionate to the injury suffered and should take into consideration the gravity of the internationally wrongful act and the rights involved. Fourthly, the injured State must first call upon the responsible State to discontinue the internationally wrongful act and/or provide reparation and notify about the decision to take countermeasures.

Countermeasures can prove to be a robust and flexible response in the field of ICTs but they face some shortcomings to comply with the conditions explained above. [291] Regarding the second condition, many malicious cyber activities are carried out by non-State actors against whom countermeasures cannot be a response unless their acts are attributable to a State. [292] However, Schmitt developed a minority argument that allows for countermeasures against non-State actors, considering that they are 'technically' against the State in which non-State actors are located.[293] He admitted that such countermeasures would violate the sovereignty of the target State. Yet, he countered criticism contending that the wrongfulness of such a response would be precluded by the lack of due diligence of the target State in putting an end to the attacks.[294]

A second shortcoming is to comply with the third condition (proportionality): a malicious code might have different stages of activation and damage is not usually predictable, as explained in section 2.3 above. Regarding the principle of proportionality, there is no need of equivalence of means, i.e. a response against a malicious cyber activity does not call for a cyber countermeasure. Instead, it requires that the degree of cyber force employed be limited in magnitude, intensity and duration.[295] An important clarification is made by Tallinn Manual 2.0 regarding the requisite of proportionality in the case of countermeasures as a response to the violation of the due diligence obligation. Rule 23

[289] See *Gabčíkovo-Nagymaros*, cit. note 284, paras 83, 85, 87.
[290] *Draft Articles on State Responsibility,* cit. note 219, Articles 51 and 52.
[291] See SCHMITT, M., *In Defense of Due Diligence*, cit. note 248, p. 77.
[292] See KESAN, J. AND HAYES, C., *Mitigative Counterstriking,* cit. note 31, p. 529; *Tallinn Manual 2.0,* cit. note 40, Rule 20, commentary, paras 5 and 7. Note that a different view was included in paras 8 and 9.
[293] See SCHMITT, M., *Peacetime Cyber Responses and Wartime Cyber Operations under International Law: An Analytical Vade Mecum'*, in 'Harvard National Security Journal', Vol. 8, 2017, p. 259.
[294] See SCHMITT, M., *In Defense of Due Diligence*, cit. note 248, p. 79.
[295] SEGURA-SERRANO, A., *Internet Regulation*, cit. note 76, p. 227.

provides that in such a case, the proportionality requisite is to be measured against the omission and not against the effects of the malicious cyber activity itself.[296]

A third shortcoming is to comply with the fourth condition: due to the particularly speedy nature of cyber activities, it might be necessary for an injured State to act immediately in order to preserve its rights without any notification.[297] Roscini even considered this requirement to be unrealistic in the case of countermeasures as a response to a malicious cyber activity.[298] However, the Tallinn Manual experts cautioned about an unnecessary escalation arising out of the combination of the speedy nature of malicious cyber activities and a precipitated response thereto.[299]

Countermeasures are by definition non-forcible measures; however, the experts of Tallinn Manual 2.0 did not have a uniform view regarding that requirement when applied to the security in the use of ICTs. While the majority of the experts were of the view that forcible countermeasures are not allowed,[300] a minority considered them lawful when they are taken in response to uses of force short of armed attack.[301] That view was built upon the separate opinion of Judge Simma in the Oil Platforms case. Simma interpreted the *dictum* of the ICJ in the Nicaragua case, and concluded that in case of force short of armed attack a State would not have a *full* right to self-defence but a right to defensive military action short of full scale self-defence.[302] Schmitt labelled such an approach 'self-defense lite'.[303]

From the above, it is safe to conclude that in case of malicious cyber activities that breach an international rule and that are below the threshold of armed attacks, countermeasures are *de jure* a viable response against responsible States. However, the response is *de facto* difficult to implement due to the particular characteristics of cyber activities. Furthermore, the available response directed to non-State actors is a big question mark. As pointed out by Katherine Hinkle: 'the law of countermeasures is far from ready to take on the challenges of the digital age'.[304] However, the international community is indeed

[296] *Tallinn Manual*, cit. note 13, Rule 23, commentary, paras 11 and 12.
[297] *Tallinn Manual 2.0,* cit. note 40, Rule 21, commentary, para. 11.
[298] See ROSCINI, M., *Cyber Operations and the Use of Force*, cit. note 178, p. 106.
[299] *Tallinn Manual 2.0,* cit. note 40, Rule 21, commentary, para. 2.
[300] *Tallinn Manual 2.0,* cit. note 40, Rule 22, commentary, para. 10.
[301] *Tallinn Manual 2.0,* cit. note 40, Rule 22, commentary, para. 12.
[302] See *Oil Platforms*, cit. note 210, Separate opinion of Judge Simma, pp. 332-333.
[303] SCHMITT, M., *Cyber Operations and the Jus Ad Bellum Revisited*, cit. note 184, p. 582.
[304] See HINKLE, K., *Countermeasures in the Cyber Context*, cit. note 123, p. 21.

moving towards a system of sanctions for malicious cyber activities, such as the already referred EU cyber toolbox. For a higher level of gravity of certain malicious cyber activities, there is also a higher level of possible responses: self-defence will be outlined in the next sub-section.

### 2.7.2.- SELF-DEFENCE

States have an inherent right of individual or collective self-defence if an armed attack occurs. Compared to countermeasures, self-defence is a forceful response to the gravest uses of force, namely to armed attacks. This is why this sub-section will attempt to examine self-defence as a response to malicious cyber activities amounting to armed attacks.

The right to self-defence is enshrined in Article 51 of the UN Charter and is considered customary international law by the ICJ jurisprudence[305] and the doctrine.[306] A completely different concept is 'pre-emptive' self-defence, an unlawful measure that operates in a preventive manner when the attack did not come into being.[307] Its origin is usually attributed to the 'Bush doctrine' envisaged in the 2002 National Security Strategy.[308] While 'pre-emptive' self-defence is based on a purely foreseeable or conceivable armed attack, 'anticipatory' self-defence is based on the imminence of the attack taking into consideration the parameters laid down in customary law; namely, a danger that is 'instant, overwhelming, leaving no choice of means, and no moment for deliberation' (requirements laid down in the Caroline case).[309] However, other authors prefer to stick to the conditions established in the text of Article 51.[310] Once the existence or imminence of an armed attack has been established, the armed attack needs to fulfill another requisite to allow self-defence as a response: the armed attack has to be intentional or deliberate.[311]

Likewise, there are certain criteria that self-defence has to fulfill to be a legal response. According to the ICJ jurisprudence, self-defence must be proportional to the armed attack

[305] Originally in *Nicaragua*, cit. note 154, para. 176.
[306] See *Draft Articles on State Responsibility,* cit. note 219, commentary to Article 21.
[307] See SEGURA-SERRANO, A., *Internet Regulation*, cit. note 76, p 229.
[308] DINSTEIN, Y., *War, Aggression and Self-Defence*, cit. note 42, p. 183.
[309] SHAW, M., *International Law,* cit. note 156, p. 820.
[310] JIMENEZ DE ARECHAGA, E., *International Law*, cit. note 153, p. 97: 'A State must comply with all the requirements established in Article 51 of the UN Charter, and not with some loose conditions mentioned in a diplomatic incident [...] some 140 years ago'.
[311] See *Oil Platforms*, cit. note 210, para. 64.

and necessary to respond to it –requirements that are also considered customary.[312] Proportionality allows assessing the force used to repel the attack but does not require identity or equivalence of means. Roscini explained that 'a disproportionate measure would not *per se* turn self-defence into an unlawful reprisal but would only render a State responsible for an excessive self-defence'.[313] Necessity requires that the forcible measure be the only way to repel the attack and that the Security Council is not already taking measures, as provided for in Article 51 of the UN Charter.

The exercise of self-defence against non-State actors can be traced back to the aftermath of 9/11 attacks, when Security Council Resolution 1368 (2001) made it clear that States may exercise their right to self-defence against non-State actors like terrorists.[314] However, it is worth recalling that the ICJ rejected the application of Article 51 in response to terrorist attacks from the occupied territory of Palestine in the Wall Advisory opinion (2004).[315]

Tallinn Manual 2.0 devoted Rules 71 to 75 to self-defence in the cyber field. Contrary to the ICJ case law already referred, the majority of the Tallinn Manual experts considered that the intention in the armed attack was irrelevant.[316] To the contrary, some academic commentators like Walter Sharp and Roscini attached importance to the intentional element.[317]

Turning the attention to the conditions that self-defence must meet, Rule 72 of Tallinn Manual 2.0 reflected the requirements of proportionality and necessity that any response in self-defence must comply with.[318] Segura-Serrano defined proportionality of cyber force as limited in magnitude, intensity and duration.[319] Kesan and Hayes took on board the danger of resorting to active defence because it may cause collateral damage as

---

[312] See *Nicaragua*, cit. note 154, para. 176; *Nuclear Weapons*, cit. note 188, para. 41.
[313] ROSCINI, M., *Cyber Operations and the Use of Force*, cit. note 178, p. 91.
[314] See BLANK, L., *International Law and Cyber Threats from Non-State Actors*, in 'International Law Studies', Vol. 89, 2013, p. 414. See also United Nations Security Council, Resolution 1368, 12 September 2001; Resolution 1373, cit. note 240.
[315] *The Wall*, cit. note 165, para. 139. For a critical view, see the separate declaration of Judge Buergenthal, para. 6.
[316] *Tallinn Manual 2.0,* cit. note 40, Rule 71, para. 14.
[317] See SHARP, W., *Cyberspace and the Use of Force*, cit. note 197, p. 134; ROSCINI, M., *Cyber Operations and the Use of Force*, cit. note 178, pp. 76-77.
[318] *Tallinn Manual 2.0,* cit. note 40, Rule 72.
[319] See SEGURA-SERRANO, A., *Internet Regulation*, cit. note 76, p. 227.

long as the technology is not sufficiently advanced to targeting a specific attacker.[320] Roscini argued that the requirement of necessity implies the identification of the author, verification of the intentional element and that the conflict cannot be solved by less intrusive means.[321]

According to Rule 73, self-defence arises if a cyber armed attack occurs or is inminent. As already explained before, imminence is not a condition of self-defence but of the armed attack to justify the legality of *anticipatory* self-defence. The experts of Tallinn Manual 2.0 distinguished between merely preparatory actions and the first stage of a malicious cyber activity[322] and thus agreed that *preventive* self-defence was unlawful.[323] David Graham considered that the imminence of an attack as required by the Caroline doctrine was a condition difficult to fulfill, if not impossible in malicious cyber activities.[324] Some experts supported the applicability of anticipatory self-defence to malicious cyber activities against sensitive systems that are critical to the national interests, i.e. CNI.[325] Schmitt considered that anticipatory self-defence might be lawful if carried out in the context of an overall armed attack; if the armed attack is imminent and if the reaction is in the last window of opportunity.[326] Finally, Dinstein supported *interceptive* but not anticipatory self-defence; i.e. a reaction to an event that is in the verge of occurring.[327] That author used a metaphor to reflect the difference between interceptive and preventive self-defence: 'There is nothing preventive about nipping an armed attack in the bud. But first there must be a bud'.[328]

Regarding immediacy, the Tallinn experts defined it as the condition that distinguishes self-defence from retaliation, although they acknowledged that it might be difficult to fulfill this requisite in certain circumstances.[329] The literature generally included

[320] See KESAN, J. AND HAYES, C., *Mitigative Counterstriking,* cit. note 31, p. 527.
[321] ROSCINI, M., *Cyber Operations and the Use of Force*, cit. note 178, p. 89.
[322] *Tallinn Manual 2.0,* cit. note 40, Rule 73, commentary, para. 7.
[323] Ibid., para. 10.
[324] GRAHAM, D., *Cyber Threats and the Law of War*, cit. note 216, p. 90.
[325] See SHARP, W., *Cyberspace and the Use of Force*, cit. note 197, p. 129; HOISINGTON, M., *Cyberwarfare and the Use of Force,* cit. note 236, p. 453; CONDRON, S., *Getting It Right*, cit. note 97, p. 416.
[326] See SCHMITT, M., *Computer Network Attack and the Use of Force*, cit. note 32, pp. 932-933; SCHMITT, M., *Peacetime Cyber Responses*, cit. note 293, p. 247.
[327] DINSTEIN, Y., *Computer Network Attacks*, cit. note 55, pp. 110-111.
[328] DINSTEIN, Y., *War, Aggression and Self-Defence*, cit. note 42, p. 191.
[329] *Tallinn Manual 2.0,* cit. note 40, Rule 73, commentary, para. 14.

the requirement of immediacy of self-defence against a grave malicious cyber activity precisely due to the instantaneous nature of cyber threats.[330]

The last point to be touched upon in this sub-section is self-defence as a response to malicious cyber activities conducted by non-State actors. Roscini distinguished two alternative approaches: one is to consider that every State has a right of self-defence against whoever the author is due to a primary rule contained in Article 51 of the UN Charter.[331] The other path is to consider that a State may exercise its right to self-defence against any other State to which malicious cyber activities by non-State actors may be attributable, including for its inability or unwillingness to stop the attacks (secondary rule).[332] Regarding the first approach, the experts of Tallinn Manual 2.0 did not hold a uniform opinion and described the issue as 'controversial'.[333] As to the second one, the experts further distinguished two situations: consensual and non-consensual self-defence against the State from which non-State actors launched the malicious cyber activity at stake. If the State consents to a response against non-State actors in its own territory, there will not be a violation of its territorial sovereignty. However, in non-consensual cases, legality of the attack directed against that State is a matter of disagreement.[334]

From the above, it is safe to conclude that an issue not resolved by the doctrine was the applicability of self-defence against non-State actors for malicious cyber activities that are not attributable to a State. For such cases, some scholars offered the resort to a plea of necessity, which will explained in the next sub-section.

### 2.7.3.-PLEA OF NECESSITY:

The plea of necessity is an exceptional legal tool foreseen in international law to safeguard an essential interest from a grave and imminent peril that has not yet occurred when there is no other means to repel it.[335] Compared to countermeasures and self-defence, the plea of necessity is not dependent on a conduct by a State (this means that it is not

[330] ROSCINI, M., *Cyber Operations and the Use of Force*, cit. note 178, p. 88; JENSEN, E., *Computer Attacks on Critical National Infrastructure*, cit. note 235, p. 209.
[331] ROSCINI, M., *Cyber Operations and the Use of Force*, cit. note 178, p. 80.
[332] Ibid., p. 81.
[333] *Tallinn Manual 2.0,* cit. note 40, Rule 71, commentary, paras 18-19.
[334] Ibid., para. 25.
[335] *Draft Articles on State Responsibility,* cit. note 219, commentary to Article 25, paras 14-16.

necessarily a response to a wrongful act).[336] In addition, Article 25(1)(b) of the Draft Articles on State Responsibility stipulates that a response based on necessity cannot impair an essential interest of another State or of the international community as a whole. Furthermore, Article 25(2) establishes limitations for two cases in which the plea of necessity cannot be invoked: (a) obligations that exclude reliance on the necessity and (b) in cases where the State invoking necessity contributed to the situation.

Tallinn Manual 2.0 included Rule 26 on necessity, where it particularly referred to malicious cyber activities against CNI. The Tallinn experts agreed that when such activities have a severe negative impact on the security, economy, public health, safety or environment of a State, they might fulfil the requirement of grave peril.[337] Due to the exclusion contained in Article 25(1)(b) of the Draft Articles on State Responsibility, a State may not attack CNI of another State relying on necessity.[338] Another interpretation that the experts of Tallinn Manual 2.0 made was the one regarding Article 25(2)(b) of the Draft Articles on State Responsibility. They agreed that the failure to prevent a malicious cyber activity in its own territory is not an obstacle to invoke necessity to react against the hacker.[339]

An important aspect that the experts of Tallinn Manual 2.0 underscored is the fact that the plea of necessity can be invoked against malicious cyber activities conducted by non-State actors that are not attributable to any State because necessity does not require a conduct of a State to react against.[340] Moreover, they considered that a reaction against malicious cyber activities whose origin is not clear might be justified on the basis of necessity.[341] Although the main difference between self-defence and the plea of necessity is that the latter is a non-forceful response, they were split as to whether that limitation applied to the cyber domain.[342]

In a nutshell, the majority of the experts of Tallinn Manual 2.0 interpreted the plea of necessity as the fallback solution that might fill many gaps in the general legal framework of responses (retorsion, countermeasures and self-defence). In effect, under that approach

[336] Ibid., commentary to Article 25, para. 2.
[337] See *Tallinn Manual 2.0,* cit. note 40, Rule 26, commentary, para. 5.
[338] Ibid., commentary, para. 8.
[339] Ibid., para. 19.
[340] Ibid., para. 10.
[341] Ibid., para. 11.
[342] Ibid., para. 18.

victim States of malicious cyber activities carried out by non-State actors not attributable to States, and victim States of malicious cyber activities that may not be attributed to any subject due to the attribution problem might find a solution in the plea of necessity.

## 2.8.- REGULATORY PROSPECTS:

The previous sections have provided elements for considering future regulatory prospects. The debate on the security in the use of ICTs dates back to the end of the nineties; however, the topic has only recently reached its best *momentum*. This section is divided into two further sub-sections: one will address intergovernmental discussions and will provide an overview of national positions regarding the crucial aspects of this topic, the appropriate forum for debates and future work. The second sub-section will briefly review the arguments of some academic commentators regarding the necessity and feasibility of a particular legal framework for malicious cyber activities.

### 2.8.1.- SECURITY IN THE USE OF ICTs AT THE UNITED NATIONS:

Security in the use of ICTs is on the agenda of UNGA First Committee for more than two decades now. This sub-section will address the debates in a twofold manner: firstly, it will review the evolution of the mechanisms established to address the matter at the United Nations; and secondly, it will review the evolution of State positions.

#### a) Evolution of the mechanisms at the United Nations:

For ease of reading, the evolution will be broken down into three moments:

1. The first moment: 1998-2000

This period began in 1998 when the Russian Federation for the first time tabled a resolution on 'information security' at UNGA First Committee, which was adopted without a vote as the already referred Resolution 53/70. One of its preambular paragraphs already introduced the concern that technologies could potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security, and that they might adversely affect the security of States.

In the operative paragraphs, three significant features were identifiable: firstly, the resolution called on addressing the issue in a multilateral forum, something that is critical to preserve the inclusiveness and transparency of the discussion. Secondly, it invited States to consider the advisability of developing international principles that would enhance international security; and finally, it decided to include an agenda item on the topic in the following year.

Notably, this resolution made reference to neither information weapons nor information war, concepts included in the annex to the letter that the Permanent Representative of the Russian Federation sent to the Secretary-General in September 1998.[343] Moreover, the Russian Federation submitted a document in response to the request made by UNGA Resolution 53/70, in which definitions of 'information war' and 'information weapons' were proposed.[344]

2. The second moment: 2001-2017

A second period can be distinguished from the end of 2001 onwards, when UNGA Resolution 56/19 requested the Secretary-General to set up a GEE on ICTs to consider existing and potential threats in the sphere of 'information security' and possible cooperative measures to address them.[345] The Secretary-General established a GGE that held its first session from 12 to 16 July 2004 and met for the second time in 2005 without reaching any consensus.

A second GEE on ICTs was set up in 2009[346] and resumed the work on this topic upon a request made by the General Assembly in 2005.[347] The outcome document of this group was a report released in July 2010, which concluded with recommendations for further

[343] Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General, reproduced in UN Doc. A/C.1/53/3, 30 September 1998, Annex, para. 3(b).
[344] UN. Doc. A/54/213, cit. note 63, para. 15: 'information war' was defined as the 'Confrontation between States in the information field, with a view to damaging information systems, processes and resources and vital structures, and undermining another State's political and social systems, as well as the mass psychological manipulation of a State's population and the destabilisation of society'. The definition of 'information weapon' is reproduced in note 63 *supra*.
[345] United Nations General Assembly, Resolution 56/19, 29 November 2001, A/RES/56/19.
[346] The GGE was composed by: Belarus, Brazil, China, Estonia, France, Germany, India, Israel, Italy, Qatar, the Republic of Korea, the Russian Federation, South Africa, the United Kingdom, and the United States.
[347] United Nations General Assembly, Resolution 60/45, 8 December 2005, A/RES/60/45.

development of confidence-building measures to reduce the risk of misperception resulting from ICT disruptions, identification of capacity-building measures and elaboration of common terms and definitions.[348]

The third GEE on ICTs was set up in 2012[349] upon a request made by the General Assembly in 2011.[350] Its consensus report of 2013 concluded arguing that existing international law applies to ICT environment; that common understandings on how norms derived from existing international law shall apply to State behavior and that the use of ICTs by States requires further study and opens up the door to the possibility of developing additional norms in the future.[351] With such formulation in the report, States struck a balance between positions claiming for a new set of rules and those pleading for the application of existing international law.

It should be noted that this report adopted a mixed language, sometimes prescriptive[352] and sometimes softer[353] in the form of what the GGE called 'Recommendations on norms, rules and principles of responsible State behaviour' (the heading of chapter III of the report) which included, *inter alia,* State sovereignty, the applicability of the UN Charter, the respect for human rights and State responsibility. In the same part of the report, under paragraph 18, the GGE simply 'noted' (did neither endorse nor commend) the proposal for a code of conduct for information security, submitted by the Russian Federation, China, Tajikistan, and Uzbekistan.[354]

In chapter IV of the report, the GEE on ICTs suggested developing 'voluntary confidence-building measures', mainly relating to information exchange and cooperation. It

[348] UN Doc. A/65/201, cit. note 21, para. 18.
[349] The GGE was composed by: Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, the Russian Federation, the United Kingdom, and the United States.
[350] United Nations General Assembly, Resolution 65/41, 8 December 2010, A/RES/65/41.
[351] UN Doc. A/68/98, cit. note 74, paras 16 and 21.
[352] Ibid., para. 21: 'State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms'; 'States must meet their international obligations regarding internationally wrongful acts attributable to them. States must not use proxies…' (para 23).
[353] Ibid., para. 22: 'States should intensify cooperation against criminal or terrorist use of ICTs…'; 'States should encourage the private sector and civil society to play an appropriate role to improve security…' (para. 24); 'Member States should consider how best to cooperate in implementing the above norms and principles of responsible behaviour…' (para. 25).
[354] The draft code is attached to the letter contained in UN Doc. A/66/359, cit. note 20.

is important to take into consideration this clear-cut distinction between 'norms, rules and principles' in one chapter and 'voluntary confidence-building measures' in another one.

Another GGE[355] was established upon a new request made by the General Assembly in 2013.[356] The consensus report of 2015[357] did not shed light on what 'norms, rules and principles' meant,[358] yet this time the GGE attempted to clarify the concept of 'voluntary, non- binding *norms* of responsible State behaviour' and did so in the following terms:

> [voluntary non-binding] norms do not seek to limit or prohibit action that is otherwise consistent with international law. Norms reflect the expectations of the international community, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States. Norms can help to prevent conflict in the ICT environment and contribute to its peaceful use to enable the full realization of ICTs to increase global social and economic development.[359]

This definition was the prelude to a series of recommendations in the report (and unlike the 2013 report, this one employed only the 'should' form), *inter alia*: cooperation to enhance ICT security, not to knowingly allow State territory to be used for internationally wrongful acts in the field of ICT, cooperation to investigate and prosecute, protection of human rights, protection of national critical infrastructure and assistance to other States and the protection of emergency response teams.[360]

As to how international law applies to the use of ICTs, the GEE on ICTs included a non-exhaustive list of views, in particular, that States have jurisdiction over ICT

---

[355] Belarus, Brazil, China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, the Republic of Korea, the Russian Federation, Spain, the United Kingdom, and the United States.
[356] United Nations General Assembly, Resolution 68/243, 27 December 2013, A/RES/68/243.
[357] UN Doc. A/70/174, cit. note 244.
[358] The ILC has referred to these concepts in the following terms: 'The word "norm" is sometimes understood to have a broader meaning than other related words such as "rules" and "principles" and to encompass both. It is, however, to be noted that in some cases, the words "rules", "principles" and "norms" can be used interchangeably', see Report of the International Law Commission 71st Session (2019), Peremptory Norms of General International Law (*jus cogens*), UN Doc. A/74/10, p. 148 (see conclusion 1, para. 8). In another report, the ILC concluded the following: 'The International Court of Justice and the Commission do not seem to make a clear distinction between "rules" and "principles", but they agree that the latter may be regarded as norms with a more general and more fundamental character', see First Report on General Principles of Law by Marcelo Vázquez-Bermúdez, Special Rapporteur, UN Doc. A/CN.4/732, 5 April 2019, para. 151.
[359] Un Doc. A/70/174, cit. note 244, para. 10.
[360] Ibid., chapter III, para. 13.

infrastructure located in the territory of a State; that the UN Charter is applicable in its entirety to ICTs; that States 'must' not use proxies to commit internationally wrongful acts; that humanitarian principles as well as other principles apply, such as the peaceful settlement of disputes, non-intervention and State sovereignty.[361] The GGE further recommended in its 2015 report that a new GGE should further study how international law applies to the use of ICTs by States, including norms, rules and principles of responsible behaviour, confidence-building measures and capacity-building.[362]

In addition, another set of recommendations was included in chapter IV of the 2015 report (concerning confidence-building measures) and in chapter V (international cooperation and assistance). Like the previous report, this one also 'noted'[363] a *revised* draft for a code of conduct on information security.[364]

Upon the recommendations of the GEE on ICTs in its 2015 report, the General Assembly requested the Secretary-General to establish in 2016 a new GGE with the mandate to continue studying the issue and examine how international law applies to the use of ICTs.[365] Unfortunately, this GGE could not reach consensus on a report in 2017, showing 'how fragile and carefully crafted any previous agreements were'.[366] However, it is important to note that the General Assembly called upon States to be guided in their use of ICTs by the 2015 report of the GGE on ICTs.[367]

3. The third moment: 2018 till the present

After the 'no-report' situation in 2017, a third period commenced in the history of negotiations on security in the use of ICTs. In 2018 the General Assembly passed two resolutions with two separate mechanisms to continue considering the issue:

---

[361] Ibid., para 28. An express reference to 'international humanitarian law' was avoided to reach consensus on the report.
[362] Ibid., para. 34.
[363] Ibid., para. 12.
[364] This draft code is annexed to Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, UN Doc. A/69/723, 13 January 2015.
[365] United Nations General Assembly, Resolution 70/237, 23 December 2015, A/RES/70/237. Adopted without a vote.
[366] TIKK, E. AND KERTTUNEN, M., *The Alleged Demise of the UN GGE: An Autopsy and Eulog,* Cyber Policy Institute (2017), p. 15, available at https://cpi.ee/ (last accessed on 11 August 2021).
[367] UN Doc. A/RES/70/237, cit. note 365, op. 2(a).

• An open-ended working group (OEWG) entitled 'Developments in the field of information and telecommunications in the context of international security',[368] proposed by the Russian Federation and co-sponsored by several G77 States and China.[369] This group met in June 2019 for organisational matters, and engaged in a more substantive discussion later in September of the same year. The OEWG issued a consensus report in May 2021 which for the first time focuses on sustainable development, in addition to international peace and security, and human rights.[370]

A part of the report concludes that ICT activities contrary to obligations under international law that intentionally damage critical infrastructures could pose a threat to State sovereignty, economic development and the safety and well-being of persons.[371] It does not make any assessment regarding a potential right to use of force.

The report refers to the the eleven rules, norms and principles contained in the 2015 report of the GGE on ICTs and underscores that pursuant to UNGA Resolution 70/237 States are called upon to be guided by them. Importantly, it clarified that norms of responsible State behaviour do not replace existing binding international law, but simply provide guidance on what is responsible behaviour.[372] States concluded that the dialogue in the OEWG was a confidence-building measure in itself.[373]

UNGA Resolution 75/240 established another OEWG 2021-2025 to continue the work concluded by the previous group.[374]

• Another GEE[375] on ICTs, entitled 'Advancing responsible behaviour in cyberspace in the context of international security',[376] proposed by the United States and co-sponsored

[368] United Nations General Assembly, Resolution 73/27, 5 December 2018, A/RES/73/27.
[369] Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/C.1/73/L.27/Rev.1, 29 October 2018.
[370] Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Final Substantive Report, UN Doc. A/AC.290/2021/CRP.2, 10 March 2021, paras 2-3.
[371] Ibid., para. 19.
[372] Ibid., para. 25.
[373] Ibid., para. 43.
[374] United Nations General Assembly, Resolution 75/240, 31 December 2020, A/RES/75/240.
[375] Australia, Brazil, China, Estonia, France, Germany, India, Indonesia, Japan, Jordan, Kazakhstan, Kenya, Mauritania, Mexico, Morocco, the Netherlands, Norway, Romania, the Russian Federation, Singapore, South Africa, Switzerland, the United Kingdom, the United States, and Uruguay.
[376] United Nations General Assembly, Resolution 73/266, 22 December 2018, A/RES/73/266.

by Australia, Canada, Japan, Israel and several European countries.[377] This GGE concluded its mandate in 2021 with a consensus report that also reaffirmed the importance of sustainable development.[378] Likewise, this report also addressed in particular the respect for human rights in the digital era, in particular the reight to privacy and the freedom of expression.[379] It elaborated on the norms of responsible State behavour contained in the 2015 report and on how international law applies to ICTs activities, and recommended further study.

Although initial differences, both mechanisms concluded with reports that acknowledge the need to be guided by the cumulative work of the GGEs and OEWGs. Moreover, the work of both mechanisms was commended by UNGA Resolution 75/32, which calls upon States to be guided by the 2010, 2013 and 2015 reports.[380] In addition, it decides that the General Assembly will consider the outcomes of both groups and decide thereafter on any future work.

**b) Evolution of State positions:**

States have engaged for several years in discussions about malicious cyber activities and how the international community should address them. They agreed and disagreed on three main points: the scope of the topic, the regulatory instrument and the right venue for negotiations.

1. <u>The scope of the topic:</u>

Regarding the first aspect, at the initial stage of the exchange of views, the United Kingdom and the United States focused on criminal and terrorist activities.[381] Initially, China

[377] Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, UN Doc. A/C.1/73/L.37, 18 October 2018.
[378] Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 28 May 2021, para. 5 (advanced copy of the report).
[379] Ibid., para. 39.
[380] United Nations General Assembly, Resolution 75/32, 7 December 2020, A/RES/75/32. Voting record : 163 -10-7.
[381] UN. Doc. A/54/213, cit. note 63, pp. 11-12. See also UN Doc. A/59/116, cit. note 381, United Kingdom, p. 11.

also only referred to criminal and terrorist activities.[382] One of the first States that referred to cyber threats stemming from States was Cuba.[383]

The Russian Federation referred to threats from criminal, terrorist and military purposes.[384] Concerning the military use of information, the Russian Federation raised concerns from an early stage about 'information warfare' and 'information weapons' with similar destructive capacity to a weapon of mass destruction.[385] Moreover, the Russian Federation expected that the GEE on ICTs would remediate the absence of a legal definition of, *inter alia*, information weapons.[386] Cuba was also of the view that ICTs could become a weapon designed or used to cause harm to the infrastructure of a State.[387] In 2005 Brazil – following the same line of reasoning– echoed the concerns regarding 'cyber warfare' and recommended addressing its impact and the potential need for disarmament and non-proliferation regimes.[388]

Mexico was the only State that expressed that developments in space technology and satellites were unquestionably linked to international security issues and thus requested expanding the mandate of the GEE on ICTs to this subject.[389]

In 2013, the United Kingdom further elaborated its views and referred to threats originating from nation-States, State proxies, non-State actors and organised criminal gangs.[390] One year later, Switzerland also focused on individual perpetrators, political activists, criminal organisations and terrorists or State spies who want to disrupt and

[382] UN Doc. A/59/116, cit. note 381, China, para. 2.
[383] UN. Doc. A/54/213, cit. note 63, Cuba, para. 15.
[384] Ibid., Russian Federation, paras 9 and 12.
[385] Ibid., Russian Federation, para. 5.
[386] Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/58/373, 17 September 2003, Russian Federation, para. 13.
[387] Ibid., Cuba, para. 11; UN Doc. A/59/116, cit. note 381, Cuba, para. 4; Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/65/154, 20 July 2010, Cuba, para. 3.
[388] Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/60/95/Add.1, 21 September 2005, Brazil, p. 3.
[389] Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/62/98, 2 July 2007, Mexico, paras 2 and 4.
[390] UN Doc. A/68/156, cit. note 15, United Kingdom, p. 16.

destabilise the State and society.[391] Germany addressed the feasibility of a 'cyberwar' in its submission of 2015[392] and India, in 2016.[393]

2. The regulatory instrument:

Beyond the discussion on the substance, States also devoted an important amount of time to examine the feasibility of developing a new instrument to address security in the use of ICTs.

Since its inception, the Russian Federation had a preventive approach[394] rather than a reactive one, where malicious cyber activities were a viable method of war that might eventually activate the right to self-defence and the applicability of humanitarian law. In this line, the Russian Federation consistently advocated for and focused on possible work towards the elaboration of a *lex specialis* for information security. That is the reason behind several initiatives, such as the already referred 1998 draft resolution on this topic,[395] the two drafts code of conduct for information security and the proposal for a 'Convention on International Information Security by United Nations Member States'.[396]

From the very beginning, Cuba also called on to ensure the progressive development of international law in this area, including the elaboration of an adequate legal framework that would enhance the security of information systems.[397] The Cuban approach was progressive, starting by non-binding guidelines and then working on a binding instrument.[398] This progressive approach was also adopted by the Russian Federation delegate, who had proposed a first draft with principles in 2000, a couple of years after introducing the topic in

[391] Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/69/112, 30 June 2014, Switzerland, p. 15.
[392] UN Doc. A/70/172, cit. note 15, Germany, p. 7.
[393] UN Doc. A/71/172, cit. note 15, India, p. 11.
[394] UN Doc. A/C.1/53/3, cit. note 343: 'In our opinion, such a threat requires that preventive measures be taken today. We cannot permit the emergence of a fundamentally new area of international confrontation, which may lead to an escalation of the arms race based on the latest developments of the scientific and technological revolution and, as a result, divert an enormous amount of resources that are so necessary for peaceful creativity and development'.
[395] Ibid., para. 3(c).
[396] Convention on International Information Security (Russian Federation), available at http://www.mid.ru/ (last accessed on 11 August 2021).
[397] UN. Doc. A/54/213, cit. note 63, Cuba, para. 22.
[398]UN Doc. A/58/373, cit. note 386, Cuba, para. 27: 'It is imperative to work towards the formulation of non-binding guidelines and also towards the adoption of norms which can take the form of multilateral and legally binding international agreements or protocols'.

the General Assembly.[399] That State expected that such principles might take the form of a multilateral declaration that would subsequently (in the longer term)[400] be incorporated into a multilateral international legal instrument.[401] When the first GEE on ICTs was established, the Russian Federation was enthused with the possibility of moving the multilateral discussion of this matter to a qualitatively new phase.[402]

On the opposite side, there is a group of States that assessed that the existing legal framework, in particular Article 51 of the UN Charter and international humanitarian law, applies to the cyber realm and that consequently there is no need for a multilateral instrument. Within this group, the United States argued that it would be premature to formulate overarching principles of information security in all its aspects.[403] At the initial stage of negotiations, the United Kingdom was ready to study the need for the development of specific principles to enhance the security of global systems and help combat information terrorism and criminality.[404]

In 2004, the United States dismissed the need for an international convention outright [405] and called upon States to implement the eleven principles drafted by the Group of Eight.[406] The United Kingdom aligned itself with the United States and recalled that the law of armed conflicts, in particular the principles of necessity and proportionality, governed the use of technologies.[407] Moreover, the United Kingdom drew attention to the document entitled 'Guidelines for the Security of Information Systems and Networks — towards a culture of security' of the Organization for Economic Cooperation and Development (OECD).[408] In 2010, the United Kingdom reaffirmed that the existing principles of

[399] Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/55/140, 10 July 2000, Russian Federation, p. 3.
[400] UN Doc. A/58/373, cit. note 386, Russian Federation, para. 19.
[401] UN. Doc. A/54/213, cit. note 63, Russian Federation, para. 11.
[402] UN Doc. A/58/373, cit. note 386, Russian Federation, para. 8.
[403] UN. Doc. A/54/213, cit. note 63, United States, para. 12.
[404] Ibid., United Kingdom, para. 4.
[405] Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/59/116/Add.1, 28 December 2004, United States, para. 5.
[406] Ibid., United States, para. 12. The Group of Eight (G8) refers to the group of eight highly industrialised nations (France, Germany, Italy, the United Kingdom, Japan, the United States, Canada, and the Russian Federation). The Russian Federation was part of the G8 from 1994 until 2014 when it became suspended by the other members.
[407] UN Doc. A/59/116, cit. note 381, United Kingdom, para. 3.
[408] Ibid., para. 5.

international law on the use of force and the law of armed conflict provided an appropriate framework.[409]

With the 2013 report of the GEE on ICTs as a backdrop, shortly thereafter several States expressed views that were already similar to those in the report. The United Kingdom reiterated that attempts to conclude comprehensive multilateral treaties, codes of conduct or similar instruments would not contribute positively to enhancing cybersecurity for the near future.[410] The preferred approach of that State was to develop a normative framework of acceptable State behaviour based on existing principles of international law and customary international norms.[411] A similar position was held by Japan, in favour of non-binding general norms of behaviour.[412] In the same year, Canada further expressed the view that existing treaty and customary international law was applicable –in particular the UN Charter– the international human rights law and the international humanitarian law.[413]

Germany also submitted its opinion in 2013 in a document, where it considered that ambiguity about what norms apply in cyberspace created additional unpredictability to the problems of attribution.[414] That State strongly supported work on norms, rules or principles of responsible State behaviour and confidence-building measures in cyberspace.[415] Finally, the Netherlands was of the opinion that the development of norms for State conduct would not require a reinvention of international law but instead they would need to ensure consistency in the application of existing international legal frameworks.[416]

The position of China deserves a separate observation: that State argued from 2004 onwards that information technology should abide by the UN Charter and other internationally accepted principles.[417]

---

409 UN Doc. A/65/154, cit. note 387, United Kingdom, para. 7.
410 UN Doc. A/68/156, cit. note 15, United Kingdom, p. 19.
411 Ibid.
412 Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/156/Add.1, 9 September 2013, Japan, p. 15.
413 Ibid., Canada, p. 4.
414 Ibid., Germany, p. 5.
415 Ibid., Germany, p. 8.
416 Ibid., Netherlands, p. 17.
417 UN Doc. A/59/116, cit. note 381, China, para. 2; UN Doc. A/61/161, 18 July 2006, China, p. 4; UN Doc A/62/98, cit. note 389, China, para. 3.

3. The venue for discussions:

The third and final point of note that this part will address is the discussion on the right venue to conduct negotiations. For the Russian Federation, work in this area had to be conducted within the framework of the UN,[418] including the Conference on Disarmament in Geneva.[419] The United States considered that the topic did not only fall within the remit of UNGA First Committee but also under UNGA Second or Sixth Committee.[420] Concurring with the preceding States, China held that the UN was the appropriate setting in which to explore the issue of information security,[421] and Cuba also supported expressly the efforts in UNGA First Committee.[422] Germany expressed in 2017 that it was time to broaden the debate and involve the wider UN membership to make the work on ICTs in the context of international security universal.[423] Australia recalled that other fora were working on the matter and that this endeavour within the UN would duplicate work in the field.[424] Mexico acknowledged work in other bodies but considered that the undergoing study on this issue could be helpful.[425] Furthermore, that State expressed that presentations by experts or discussions on the topic might take place in conjunction with the work of UNGA First Committee or other disarmament fora.[426]

As a concluding remark, it is possible to expect that this debate will continue in the next years. The OEWGs will provide a renewed opportunity for a more extensive number of States to engage in the discussions and exchange national views on the security in the use of ICTs and how international law applies to cyber threats. It is also expected that the new GGE will continue working on responsible State behaviour.

### 2.8.2.-DOCTRINE:

According to the description above, it s virtually undeniable that some norms on State behaviour and confidence-building measures are necessary –that is the minimum that

[418] UN Doc. A/58/373, cit. note 386, Russian Federation, para. 4.
[419] UN. Doc. A/54/213, cit. note 63, Russian Federation, para. 11.
[420] Ibid., United States, para. 1.
[421] UN Doc A/62/98, cit. note 389, China, para. 6.
[422] UN Doc. A/65/154, cit. note 387, Cuba, para. 17.
[423] UN Doc. A/72/315, cit. note 15, Germany, p. 13.
[424] UN. Doc. A/54/213, cit. note 63, Australia, para. 4.
[425] UN Doc. A/59/116/Add.1, cit. note 405, Mexico, para. 6.
[426] UN Doc A/62/98, cit. note 389, Mexico, para. 1.

States agree to engage in. The need for a specific instrument governing the security in the use of ICTs is more contentious. Although this debate at the intergovernmental level does not appear to move forward beyond the statements made by several delegations, the examination of the topic continues within the doctrine, which is also well divided between those in favour and those against a binding solution. The purpose of this section is to systematise divergent opinions in the legal literature in one direction or another.

**a) Arguments in favour of the applicability of existing international law:**

Several experts are of the view that a rigid instrument regulating the security in the use of ICTs would restrict the freedom of State action to conduct malicious cyber activities. Within this line of thought, Duncan Blake and Joseph Imburgia explained that a binding solution would mean giving away too much about State cyber capabilities.[427] Glennon reflected on the fact that policy-makers seek out rules that permit what they are willing to do but at the same time wish to limit what their adversaries can do.[428] A similar position is laid out by Lawrence Muir, who pointed at the asymmetrical national positions in terms of technology and warfare capacities.[429] Phillip Johnson assessed a multilateral convention extremely unlikely in the short term because few States understand capabilities and vulnerabilities sufficiently to determine what principles of international law would best serve national interests.[430] He also considered it unlikely that the General Assembly would pass a 'law declarative' resolution in a foreseeable future.[431]

Schmitt and Liis Vihul also acknowledged the reluctance of States to binding rules until they completely understand how they may play out and thus can assess the costs and benefits of such prohibitions and limitations.[432] They posited that ambiguity in the existing legal framework might be useful and that normative clarity is not necessarily helpful.[433] Although Schmitt considered a 'normative evolution' more likely, namely the emergence of

[427] See BLAKE, D. AND IMBURGIA, J., *'Bloodless Weapons'?*, cit. note 57, p. 194.
[428] See GLENNON, M., *The Dark Future of International Cybersecurity Regulation*, in 'Journal Of National Security Law & Policy', Vol. 6, 2013, p. 568.
[429] MUIR, L., *The Case Against an International Cyber Warfare Convention,* in 'Wake Forest Law Review Online', Vol. 5, 2011, pp. 3-4.
[430] See JOHNSON, P., *Is It Time for a Treaty*, cit. note 96, pp. 451.
[431] Ibid., p. 447.
[432] SCHMITT, M. AND VIHUL, L., *The Nature of International Cyber Norms*, cit. note 34, pp. 19 and 20.
[433] Ibid., p. 26.

a new understanding of treaty law,[434] he highlighted that leaving malicious cyber activities unregulated would necessarily leave cyber systems at risk.[435]

Interestingly, Johann-Chritoph Woltag pointed at the divergence between global networks and national values as a factor that may make a uniform regulation complicated, which would be the reason for its non-existence.[436] Dinstein considered that there is no point in seeking a new treaty promulgating a code of conduct in the field of ICTs because States would not be willing; hence, a treaty would only state existing norms relating to armed conflicts.[437]

As to the possibility of a new customary rule, scholars are likewise sceptic. Schmitt and Vihul contended that States tend to be cautious in supporting or condemning malicious cyber activities in their international rhetoric until they become fully aware of the costs and benefits of the position of the others.[438] According to those authors, the reluctance of States in having a clearer position on the legality of a malicious cyber activity would render unlikely the prompt crystallisation of a new customary rule governing cyberspace.[439]

Finally, it is necessary a comment regarding those authors that focused their argumentation on the virtues of the existing international law and not on the lack of State will. One of them is Roscini, who argued that although there is a lack of specific *jus ad bellum* for malicious cyber activities, the UN Charter and customary law are flexible enough to regulate them as well.[440] Another one is Morth, who assessed that Article 2(4) and Article 51 of the UN Charter are the best tools to address the issues of security in the use of ICTs due to their flexibility and legitimacy.[441]

**b) Arguments in favour of a specific instrument of international law:**

---

[434] SCHMITT, M., *Cyber Operations and the Jus ad Bellum Revisited*, cit. note 184, p. 604.
[435] SCHMITT, M., *In Defense of Due Diligence*, cit. note 248, p. 69.
[436] See WOLTAG, J., *Computer Network Operations*, cit. note 71, p. 15.
[437] DINSTEIN, Y., *Cyber War and International Law*, cit. note 201, p. 286.
[438] See SCHMITT, M. AND VIHUL, L., *The Nature of International Cyber Norms*, cit. note 34, p. 28.
[439] Ibid.
[440] See ROSCINI, M., *World Wide Warfare: Jus ad Bellum and the Use of Cyber Force*, in '*Max Planck Yearbook of United Nations Law',* Vol. 14, 2010, p. 130.
[441] See MORTH, T., *Considering Our Position*, cit. note 49, p. 599.

Despite the voices against, a part of the literature still favours the adoption of a specific instrument governing malicious cyber activities and responses thereto. As mentioned previously, Schmitt is aware of the risk of unregulated malicious cyber activities; therefore, he is also of the view that a 'new and unique normative framework' to address malicious cyber activities is necessary and foreseeable since they represent a new instrument of coercion.[442] Raboin explained that the existing legal framework is inadequate for malicious cyber activities on three counts: the difficulty of tracking the hacker, the exercise of jurisdiction in the cyber domain and the different approaches in the characterisation of the use of force.[443]

Hollis argued that there is a need for what he called an 'international law of information operations or ILIO'. He gave four reasons for his proposal: there are serious translation problems when transposing the existing regime to malicious cyber activities, the existence of asymmetrical malicious cyber activities conducted by non-State actors, the existence of overlapping legal regimes that might be applicable is confusing, and the fact that the current regime limits the benefits of malicious cyber activities.[444]

Some academic commentators looked more in-depth into specific aspects that should be addressed by a new instrument. For instance, Michael Robbat proposed a convention sanctioning negligent use of 'information warfare' and addressing extradition for these cases.[445] Hathaway suggested negotiating an international treaty with two central features: 1) a shared definition of cybercrime, cyberattack and cyber warfare and 2) a call for more international cooperation in information sharing, evidence collection and criminal prosecution.[446] Michael Berkham proposed certain areas to be addressed by a treaty, *inter alia*, the identification of the victim and the problem of non-State actors.[447] Silver proposed a new instrument ensuring legal cooperation to prosecute guilty persons.[448]

---

[442] SCHMITT, M., *Computer Network Attack and the Use of Force*, cit. note 32, p. 934.
[443] See RABOIN, B., *Corresponding Evolution: International Law and the Emergence of Cyber Warfare,* in 'Journal of the National Association of Administrative Law Judiciary', Vol. 31, No 2, 2011, p. 640 ff.
[444] See HOLLIS, D., *Why States Need an International Law*, cit. note 28, p. 1039.
[445] See ROBBAT, M., *Resolving the Legal Issues,* cit. note 83.
[446] See HATHAWAY, O., *The Law of Cyber-Attack*, cit. note 101, p. 880.
[447]See BARKHAM, J., *Information Warfare*, cit. note 94, p. 102.
[448]See SILVER, D., *Computer Network Attack*, cit. note 50, p. 94.

Unlike the previous authors, Johnson considered that the most straightforward approach would be to negotiate a multilateral treaty declaring broad relevant principles of international law, like the 1967 Outer Space Treaty.[449] He mentioned some of the proposed principles, such as the obligation not to damage, to disrupt or interfere with information systems; that malicious cyber activities violate sovereignty and threaten international peace and security; and that interference causing death, injury or serious or widespread damage will be considered to be equivalent to an armed attack.[450] Delibasis proposed a '*jus novum*': he contended that there is a need for the modernisation of existing legal norms but recommended taking advantage of the already existing regulatory framework on 'information warfare' and building upon precedents in the field of the sea and space law (similar to the view of Johnson).[451]

Regardless of the discussion on whether a new instrument is desirable –which seems to be more a political than a technical issue– this sub-section attempted to enable the reader to identify the challenges that the international community would face with a specific instrument. This review does not intend to be exhaustive but aims to show how diverse views at the present stage are. It appears to be difficult that a homogenous position on the desirability of a new instrument could emerge in the short term; however, that reality is no indication that the debate is closed or exhausted or that States could not reach a compromise solution in the mid- or longer-term.

## 2.9.- CONCLUSIONS:

This chapter has described the state of the art in the analysis of whether existing international law is applicable to the security in the use of ICTs, and whether the existing legal framework is sufficient or adequate to address malicious cyber activities depending on their features, scale and effects. However, the research revealed that there are more questions than answers. In effect, a reinterpretation or adaptation of existing international law is offered by some as the most immediate solution to face the new threats arising out of technological breakthroughs. However, extending existing law to threats that were inexistent

[449] See JOHNSON, P., *Is It Time for a Treaty*, cit. note 96, p. 446.
[450] Ibid.
[451] See DELIBASIS, D., *State Use of Force in Cyberspace for Self-Defence*, cit. note 1, pp. 21 and 22.

at the time of the adoption of relevant instruments raises concerns due to the consensualist characteristic of international law.

While the Tallinn Manual (in both versions) was the first and most comprehensive study in the field of 'cyber operations', it reveals many weaknesses. It is important to bear in mind that the very essence of that work is merely an analysis carried out at the core of an international military organisation (the NATO Cooperative Cyber Defence Centre of Excellence); hence, it conveys an inherently military approach. Furthermore, the group of experts was not geographically representative. In effect, all of them come from North America and Western Europe; there was no expert from the Russian Federation, China[452] or from the developing countries. Such a group can only provide a biased view or at least an incomplete description of positions; and accordingly, the value of the proposed rules cannot be other than limited. Moreover, the experts consistently relied on military manuals of four countries: Canada, Germany, the United Kingdom and the United States and did not explain why 'the international legal community generally considers these four manuals to be especially useful', as pointed out in the Manual's background information. The experts did not reach consensus on all the issues at stake and observers were left aside of the consensus-building process. The experts acknowledged in the background note that State practice is not well developed and 'that publicly available expressions of *opinio juris* are sparse' in the cyber field.[453] However, they scarcely addressed two decades of State submissions to the Secretary-General in the context of 'Developments in the field of information and telecommunications in the context of international security'.

Key issues were not settled in either of the two versions of the Tallinn Manual, *inter alia*: which is the threshold for uses of force and armed attacks, whether countermeasures against non-State actors are lawful or not, if the due diligence obligation encompasses the obligation to take preventive measures or whether significant economic loss may trigger a forcible response. A review of the footnotes of Tallinn Manual 2.0 reveals that no reference has been made to any of the consensus reports of the GEE on ICTs although they are enlisted in the bibliography. Important conclusions of the reports, such as the obligation of States not to use proxies to commit internationally wrongful acts (2013 Report of the GEE

[452] Only in Tallinn Manual 2.0.
[453] *Tallinn Manual 2.0,* cit. note 40, Rules and Commentary, p. 3.

on ICTs) and the obligation to cooperate to prevent harmful practices are absent when dealing with due diligence in Rules 6 and 7.

An intergovernmental discussion in the field of security in the use of ICTs is of the utmost importance and is already taking place. The introduction of the topic into the agenda of the General Assembly was the beginning of a long path that is still in continuous movement. National positions are clear and different stances need to be worked out to reach consensus. Essential progress on thorny issues was achieved in 2013 and 2015 when the GGEs on ICTs released the first set of recommendations, acknowledging the application of international law. At that opportunity, the GEEs on ICTs concluded that it was necessary to reach common understandings on how such norms shall apply to State behaviour and that additional norms could be developed over time. The recent reports of the GGE and the OEWG confirm that further work should be carried out. Particular attention should be paid to the application of international law to malicious cyber activities against critical infrastructures and provide more definitions regarding loss of functionality, disruptive effects and non-State actors conducting such activities.

The UN has to play a leading role in promoting dialogue among member States in a multilateral, governmental, transparent and an all-inclusive format. That forum has the virtues that an academic exercise lacks: views are not individual opinions but State positions, and as such they are a significant element in the assessment of State practice, in the interpretation of current international law and a means to channel and convey political will. The UN is opening the game to a broader array of players including those that, due to their underdeveloped technological or digital capacities, would have not had a voice in a different mechanism. It is providing the opportunity for member States to approach the issue holistically, not only dealing with the military aspects or addressing cyber threats from a warfare standpoint alone.

Although the Tallinn Manual is a commendable piece of work that serves as food for thought, it has to be underscored that its value in terms of progressive development of law is null. At the end of the day, States have to contribute to an evolutionary response of the law to the changing reality and the new threats that technological developments pose. States need to lead the process; a consensual solution has to be found to avoid unilateral (re)actions that might add more instability and insecurity to the peaceful use of cyberspace. The

establishment of two concurring mechanisms under the auspices of the UN gives hopes that work in that direction will be duly undertaken. It is for States to determine how pressing the need for a compromise solution is and start pursuing that objective.

This chapter provided several elements –which together with the progress to be made in chapters 3 and 5– will contribute to answering **research question 1** (whether there is a regulatory framework applicable to the convergence of the cyber and space domains). This chapter has also given a necessary background for the future assessment that is necessary to answer **research question 4** (which is the competent body to deal with these issues) and **research question 5** (which is the best way to address cyber threats in the space domain), which will be answered in chapter 5.

# CHAPTER 3
# SPACE CYBERSECURITY AND INTERNATIONAL SPACE LAW

## 3.1.-INTRODUCTION

The previous chapter provided a general overview on two issues: first, it reviewed the state of the art regarding the potential application of certain rules of international law regarding three specific matters: the prohibition of non-intervention and the use of force; State responsibility (international wrongful acts and attribution) and responses (countermeasures, self-defence and plea of necessity). Second, it described the negotiations on security in the use of ICTs at the UN and provided a picture of State positions regarding three issues: the scope of the topic dealing with ICTs, the preferred regulatory instrument and the right venue for negotiations.

This chapter is crucial to understand the meaning of 'space cybersecurity' in the present research. Following the same scheme of the previous chapter, section 2 clarifies terminological issues, in particular the concept of several covert malicious activities. It then draws a distinction between malicious electromagnetic and cyber activities and thus differentiates space cybersecurity from space security. Section 3 focuses strictly on space cybersecurity: it explains how space and ground segments of space systems can be affected by malicious cyber activities. Building upon the contents previously reviewed, section 4 proposes a classification of malicious space cyber activities. Similar to the outlined characteristics of cyberspace and cyber activities in chapter 2, section 5 addresses the characteristics of outer space and space activities. Whereas the previous chapter reviewed some iconic cases in the framework of cybersecurity, this chapter describes emblematic cases concerning space cybersecurity in section 6. Section 7 examines the connection between space systems and critical infrastructures and argues that not only do space systems serve as a fundamental support of CNI but that they also are critical infrastructures themselves. This argument is substantiated under a two-pronged analysis: first, the examination of aspects that support the argument of space systems being CNI; and second, the analysis of relevant State practice that is in line with this submission.

The other part of this chapter is devoted to the law, policy and governance of space activities –the difference between those concepts is explained in section 8. That part is divided into three sub-sections: first, an outline of COPUOS as the venue for international space law-making; second, a brief description of treaty law, customary and *jus cogens* norms governing outer space and space activities; and third, a review of the concept of soft law in international space law. Section 9 focuses on the core provision of the Outer Space Treaty that lays the foundation for the integration of international law into space law: Article III. That section is broken down into two sub-sections: one dealing with the interaction between international space law and the UN Charter, and the other one examines relevant interactions with telecommunications law.

Private international and domestic space law are excluded from the scope of this research; hence, they are not included in the analysis made in this chapter.

Elements of the research made for this chapter were employed in the publication: JAMSCHON MAC GARRY, L.,*The Footprint of Latin America in International Space Law,* in FROEHLICH, A. (ed.), *Space Fostering Latin American Societies* (Part II), 2021.

## 3.2.-TERMINOLOGY

This section will clarify the difference between malicious electromagnetic and cyber activities in order to understand what is encompassed by 'space cybersecurity' in this thesis. It will contend that the former do not strictly fall under 'space cybersecurity' but under the broader concept of 'space security'. For that purpose, the present section will proceed on the basis of a two-level analysis: the distinction of the space segments and the identification and definition of certain covert malicious activities.

**a) Distinction of space segments:**

This chapter will only focus on three segments of space systems:[454] the space segment, the communications segment (up/downlink and crosslink) and the ground segment.

[454] As described in the Allied Joint Doctrine for Air and Space Operations, there might be more segments: 'In a wider context, space systems can be expanded to include the following: ground stations; launch facilities;

1. The ground segment:

The ground segment includes satellite communication (SATCOM) transmitters and receptors, which are critical to the normal operation of satellites.[455] This segment encompasses the facilities, equipment and infrastructure that support the command and control (C2) of the space segment; it is the segment that receives telemetry data from satellites. Ground stations, which are equipped with software defined radio (SDR) responsible for receiving the signals from space objects and turning them into communications via demodulation, belong to this segment.[456] The SDR also sends orders of two types to the space object: orders for the operation of the satellite (for instance, for orbiting or positioning) and orders to command the payload (for example, for a camera to take photographs). This segment –compared to the other two ones– is more vulnerable because it might be targeted by both physical (i.e. kinetic attacks against the building itself) and non-physical force (malicious cyber activities).

2. The communications segment (up/downlink and crosslink):

This segment is an information conduit that connects the space segment with the ground station and *vice versa* using the electromagnetic spectrum. The link includes telemetry, tracking and commanding (TT&C).[457] There are also links that connect satellites with each other (crosslinks).

The uplink communications may be of two types: for instance, for TV and communications retransmission or for command of the satellite.[458] The latter are critical for the management and proper operation of the space object. Signals sent from space to ground stations belong to the downlink segment and are essential for the proper reception of data.

3. The space segment:

---

satellite production, checkout, and storage facilities; communications links; user terminals; and Spacecraft (both manned and unmanned)'. See Allied Joint Doctrine for Air and Space Operations, NATO Standard AJP-3.3, Edition B Version 1, April 2016, p. 5-2, available at https://www.japcc.org/ (last accessed on 11 August 2021).

[455] GARINO, B. AND GIBSON, J., *Space System Threats*, Air University Press, 2009, p. 273, available at https://aerospace.csis.org/ (last accessed on 11 August 2021).

[456] OAKLEY, J., *Cybersecurity for Space: Protecting the Final Frontier*, Alabama, 2020 (see chapter 1).

[457] US Joint Chiefs of Staff, Joint Publication 3-14, Space Operations, 10 April 2018, available at https://fas.org/ (last accessed on 11 August 2021).

[458] GARINO, B. AND GIBSON, J., *Space System Threats*, cit. note 455, p. 275.

This one includes satellites, space stations and reusable space transportation systems. These assets are transmitters of signals sent to the ground stations that receive them, decode space data and transform it into useful information for society.

Now, the two segments that operate digitally are the space and ground segments. In very simple terms, the ground station and satellites host computer systems, programmes and data that command space objects and that enable communications with them. The communications between the space and ground segments take place via signals in the electromagnetic field. However, these communications are programmed and enabled via computer systems, programmes and data hosted in the space and ground segments. This means that the communications (up/downlink or crosslink) segment is targetable either *directly* and *physically* with electromagnetic threats or *indirectly* and *cybernetically* via the computer, programmes and data that command those communications. In the former case, electromagnetic threats operate directly against the target and cause their effects in the same segment, whereas in the latter case, malicious cyber activities operate directly against computer systems, programmes and data, and cause effects in any of the three space segments. The distinction between what is direct and what is indirect is important to determine if there is identity between target and effects; or contrarily, disassociation of them (see figure 1).

In sum, targeting communications *directly* is only feasible via electromagnetic threats because the electromagnetic spectrum is physical; therefore, is only targetable via physical forces, i.e. by electromagnetic signals. To the contrary, computer operating systems, programmes and data are non-physical; hence, their vulnerabilities can only be exploited directly by non-physical threats, i.e. with cyber malicious codes. In this line, some authors have considered that while electromagnetic threats should be characterised as 'external' to the systems under attack because they exploit physical vulnerabilities; cyber ones should be characterised as 'internal' to the systems because they exploit non-physical vulnerabilities.[459]

[459] LIVINGSTONE, D. AND LEWIS, P., *Space, the Final Frontier for Cybersecurity*?, Chatham House, 2016, p. 21, available at https://www.chathamhouse.org/ (last accessed on 11 August 2021).

| MALICIOUS ACTIVITY | TARGET | EFFECTS | | RESULTS |
|---|---|---|---|---|
| | | DIRECT | INDIRECT | |
| electromagnetic | communications | communications | satellite | association |
| cyber | ground | | communications<br>satellite | disassociation |
| cyber | satellite | satellite | | association |

**Table 1: Association and disassociation of targets and effects**

**b) Identification and definition of certain covert malicious activities:**

In order to better understand the difference between malicious electromagnetic and cyber activities, this part will shed some light on the concepts of spoofing, jamming, laser and hacking. All these threats will be labelled as 'covert malicious activities' (they comprise malicious electromagnetic and cyber activities). The expression 'covert malicious activities' serves two purposes: on the one hand, it avoids controversial warfare language (such as 'electronic warfare', 'electronic weapons' or 'cyber/information warfare', 'cyber/electronic weapons'); and on the other, it refers to a common feature of these activities: the attribution problem.

It should be clarified that the specialised literature tends to include all these threats under the more encompassing concept of 'counterspace capabilities' (a concept that applies to kinetic threats as well), which is indeed an expression connected with warfare language. 'Counterspace capabilities' (offensive or defensive) are defined by the United Nations Institute for Disarmament and Research (UNIDIR) as 'military capabilities that seek to prevent an adversary from exploiting space to their advantage'. Chapter 4, section 4.6 will refer to the American 'space control' policy, which concretely reflects this concept. The Joint Operating Environment 2035, a document produced in 2016 by the Joint Chiefs of State,

described six contexts for future conflict, where the fourth consists of 'disrupted global commons'. That scenario –the report explains– encompasses competition in orbit (even during peacetime), co-orbital jamming and the use of ground-based lasers to dazzle or destroy imaging sensors.[460] All these threats are counterspace capabilities.

Before starting with the definition of each covert malicious activity, it is important to point at two common characteristics they share: one is the already referred attribution problem and the other is the role that they play in the furtherance of 'information dominance'. Regarding the former, as already explained in chapter 2, one of the most challenging hurdles of malicious cyber activities is the attribution problem and this also applies to electromagnetic threats: in the case of jamming, it might be difficult to distinguish interference caused by human action, solar activity or orbit congestion; and therefore, attribution and awareness become difficult.[461] The second feature mentioned above is that malicious electromagnetic and cyber activities are means for the furtherance of 'information dominance'. This concept dates back to the 70s, when it was coined in military jargon[462] and defined as 'a condition in which a nation possesses a greater understanding of the strengths, weaknesses, interdependencies, and centers of gravity of an adversary's military, political, social, and economic infrastructure than the enemy has on friendly sources of national power'.[463] This means that malicious covert activities are a significant tool to access others' information, impede access to certain information the other is seeking to obstain or destroy valuable information that the other has obtained.

The next step in this section will be to describe the already referred covert malicious activities and determine whether they belong to the electromagnetic or cyber realm.

1. Spoofing:

Spoofing is a malicious activity whose main purpose is to send misleading commands as if the attacker were an authorised user. In effect, spoofing manipulates the *communication*

[460] Joint Chiefs of State, *The Joint Force in a Contested and Disordered World,* 2016, p. 32, available at https://www.jcs.mil/ (last accessed on 11 August 2021).
[461] See HARRISON, T., JOHNSON, K. AND ROBERTS, T., *Space Threats Assessment 2018*, CSIS, 2018, p. 4, available at https://www.csis.org/ (last accessed on 11 August 2021).
[462] LEE, J., *Counterspace Operations for Information* (Thesis presented to the Faculty of the School of Advanced Airpower Studies, Maxwell Airforce Base), Alabama, 1994, p. 3.
[463] Ibid.

between the transmitter (satellite) and the receiver (ground station). It distorts or replaces the information with false data, although it continues to appear to be true. In particular, this threat can modify the signal on the position, location and condition of a satellite.[464] Spoofing could affect banks and stock exchanges by manipulating automated time-stamps on transactions.[465] It can also affect early warning systems for nuclear attacks detection, leading to a nuclear launching based on a wrong warning.[466]

In short, spoofing affects integrity of information,[467] which is one of the three main characteristics of information security. It should be recalled that integrity, along with confidentiality and availability, comprise the so-called 'CIA triad' (an acronym made up of the first letter of each of the characteristics). As Mark Stamp explained, integrity deals with preventing or at least detecting unauthorised changes to data; confidentiality deals with preventing unauthorised reading of information and availability of information began to be affected since denial of service (DoS) emerged as a new threat to the security of ICTs.[468]

Spoofing global positioning systems (GPS) is relatively easy and accessible since the technological barriers to do it are relatively low; therefore, it is accessible to any individual with sufficient know-how and some funds.[469] Spoofed signals can induce a wrong position or time and prevent successful localisation, navigation and time synchronisation.[470]

2. Jamming:

Jason Fritz defined jamming as the practice of 'flooding or overpowering a signal, transmitter, or receiver, so that the legitimate transmission cannot reach its destination'.[471] This type of interference of the *communications* segment can be carried out through deliberate

---

[464] MOON, M., *The Space Domain and Allied Defence*, NATO Parliamentary Assembly, 2017, p. 8, available at https://www.nato-pa.int/ (last accessed on 11 August 2021).
[465] LEWIS, P. AND LIVINGSTONE, D., *The Cyber Threat in Outer Space*, in 'Bulletin of Atomic Scientists', 21 November 2016, p. 19, available at www.thebulletin.org (last accessed on 11 August 2021).
[466] STOUTLAND, P. AND PITTS-KIEFER, S., *Nuclear Weapons in the New Cyber Age*, Report of the Cyber-Nuclear Weapons Study Group, 2018, p. 17, available at www.nti.org (last accessed on 11 August 2021).
[467] LIVINGSTONE, D. AND LEWIS, P., *Space, the Final Frontier for Cybersecurity*?, cit. note 459, p.18; VARMA, T. AND UPADHYAY, A., *Meaconing and Spoofing Attacks Evaluation with Enhancement in Security for Satellite Communication*, in 'International Open Access Journal', Vol. 2, No. 3, 2018, p. 521.
[468] STAMP, M., *Information Security: Principles and Practice*, New Jersey, 2011, pp. 2-3.
[469] HUTCHINS, R., *Cyber Defense of Space Assets*, Tufts University, 2016, available at www.cs.tufts.edu (last accessed on 11 August 2021).
[470] VARMA, T. AND UPADHYAY, A., *Meaconing and Spoofing Attacks*, cit. note 467, p. 521.
[471] FRITZ, J., *Satellite Hacking: a Guide for the Perplexed*, in 'Bulletin of the Centre for East-West Cultural and Economic Studies', Vol. 10, No. 1, December 2012- May 2013, p. 34.

use of radio noise or electromagnetic signals.[472] The jamming link is a radio frequency (RF) signal of approximately the same frequency of the target link (in the case where the uplink is jammed) or more powerful (in the case where the downlink is jammed) which is transmitted via the same transponder or antenna. Kanika Grover added to the definition of jamming the element of intentionality to differentiate jamming (deliberate use of signals to disrupt communications) from interference (unintentional disruption).[473]

When the uplink is jammed, the effects are seen in the downlink (and not in the uplink): the result is loss of or a corrupted downlink.[474] When the downlink is jammed, there is an immediate impact in the information flow.[475]

Jamming can be considered less harmful in relation to other covert malicious activities, since it neither harms the system permanently, nor affects the integrity of the information; it only affects the transmission temporarily. That is the reason why jamming is considered a 'completely reversible' practice: once the jammer is off, communications revert to normal.[476]

Signals of civil GPS satellites are considerably more vulnerable to jamming than signals of military satellites, because the latter are more robust.[477] Jamming military signals is called 'meaconing' and is carried out when encrypted signals are recorded and rebroadcasted with a slight delay of a few seconds.[478]

3. Laser:

Lasers are devices that deliver high frequency energy which can be directed with nefarious purposes to the target, even if it is located far away. Depending on their power, lasers can disrupt or blind the sensors of the satellite (low power), damage a part or completely destroy

[472] See MOON, M., *The Space Domain and Allied Defense*, cit. note 464, p. 8.
[473] GROVER, K., *Jamming and Anti-Jamming Techniques in Wireless Networks: A Survey,* in 'International Journal of Ad Hoc and Ubiquitous Computing', Vol. 17, No. 4, 2014, p. 1.
[474] GARINO, B. AND GIBSON, J., *Space System Threats*, cit. note 455, p. 275.
[475] Ibid., p. 276.
[476] HARRISON, T., JOHNSON, K. AND ROBERTS, T., *Space Threats Assessment 2018*, cit. note 461, p. 4; HARRISON, T., JOHNSON, K. AND ROBERTS, T., *Space Threats Assessment 2019,* CSIS, 2019, p. 4, available at https://www.csis.org/ (last accessed on 11 August 2021).
[477] See RAJESWARI PILLAI RAJAGOPALAN, *Electronic and Cyber Warfare in Outer Space*, UNIDIR, May 2019, p. 6, available at https://www.unidir.org/ (last accessed on 11 August 2021).
[478] See HARRISON, T., JOHNSON, K. AND ROBERTS, T., *Space Threats Assessment 2018*, cit. note 461, p. 4; HARRISON, T., JOHNSON, K., AND ROBERTS, T, *Space Threats Assessment 2019*, cit. note 476, p. 5.

them (high power).[479] Blinding a satellite is usually called 'dazzling'.[480] Many of these malicious practices can be conducted through rendezvous proximity operations (RPO) via 'stalker' anti-satellites[481] designed to interfere or threaten other satellites nearby either with laser or electromagnetic force.[482]

On 23 March 1983, the President of the United States Ronald Reagan announced his intention to embark upon the so-called 'Strategic Defense Initiative'.[483] Its purpose was to develop a programme that would enable the United States to identify and automatically destroy a large number of incoming ballistic missiles. At that time he envisaged a scenario with space-based laser systems that were not yet developed. Those plans were then considered science fiction as depicted in the film 'Star Wars' (1977). Unfortunately, lasers are no longer science fiction. They may be activated from Earth or from another space object in space and –like previously described malicious activities– *directly* affect the target. However, it is important to note that lasers usually target the space segment and not the communications segment, as spoofing and jamming do. This means that here there is association between target and effects. However, if lasers are commanded digitally, a malicious cyber activity might *directly* target the computer system that commands the laser and *indirectly* affect the satellite (space segment). In that case, there would be a disassociation of target and effects.

4. Hacking:

Jeffrey Bardin defined this concept as 'the reconfiguring or reprogramming of the system to function in ways not facilitated by the owner, administrator, or designer'.[484] This means that an unauthorised external agent (a hacker) penetrates the programmes, data or systems for different purposes, such as to spy, steal, leak data or interfere with or modify the

[479] WILSON, T., *Threats to United States Space Capabilities*, available at http://www.fas.org/ (last accessed on 11 August 2021); GARINO, B. AND GIBSON, J., *Space System Threats*, cit. note 455, p. 277.
[480] RAJESWARI PILLAI RAJAGOPALAN, *Electronic and Cyber Warfare in Outer Space*, cit. note 477, p. 7.
[481] CHOW, B., *Space Arms Control: A Hybrid Approach,* in 'Strategic Studies Quarterly', Vol. 12, No. 2, 2018, p. 108.
[482] See CHOW, B., *Stalkers in Space: Defeating the Threat*, in 'Strategic Studies Quarterly', Vol. 11, No. 2, 2017, p. 84.
[483] See US Strategic Defense Initiative, 1983, available at the US online archives https://2001-2009.state.gov/ (last accessed on 11 August 2021).
[484] BARDIN, J., *Satellite Cyberattack Search and Destroy*, in VACCA, J. (ed.), *Computer and Information Security,* Cambridge, 2017, p. 1175.

normal operation of space systems.[485] The modification of the normal operation of the space system implies that any of the three segments can be affected by malicious cyber activities but –as already explained– they cannot target communications *directly,* as electromagnetic threats do. Malicious cyber activities can affect communications only *indirectly* by targeting computer systems, programmes and data that operate them (disassociation of target and effects).

In conclusion, covert malicious activities are tactically flexible (they may inflict a diverse degree of damage), untraceable (it is difficult to both detect the attacker and differentiate them from non-intentional failure or malfunction) and accessible to both State and non-State actors; they may cause temporary and reversible damage or not, and are less expensive than kinetic options. They can be directed to any of the three segments of space systems but the communications (up/downlink) and the ground segments are the easiest targets. The ground segment is perhaps the Achilles heel of space systems because it is most vulnerable for two reasons: on the one hand, it is easily targetable by either kinetic or non-kinetic malicious activities; and on the other hand, it is comparatively less expensive to target than the other segments due to its accessibility. Conversely, the space segment is the most difficult to target and requires more sophisticated means: while it is possible to hit it with kinetic means, such as ground-based anti-satellites, this option might be politically and monetarily costly.

Jamming is relatively inexpensive. While jamming the uplink can lead to the failure of the mission if conducted during critical commanding stage, targeting the downlink is easier and more reliable, particularly due to the increased satellite autonomy. One advantage of directed energy (lasers) is that its effect is instantaneous; thus, the opportunities to avoid it are reduced. Malicious cyber activities require a higher degree of know-how if compared with jamming but like the latter, they are relatively inexpensive. Whereas space hacking requires a high degree of understanding of the systems being targeted, it does not necessarily involve significant financial resources. Jamming is a preferred option over kinetic attacks against satellites on the geostationary orbit due to the costs arising from distance.

[485] See KALLENDER, P., *Waking up to a New Threat: Cyber Threats and Space*, in 'Trans. JSASS Aerospace Tech. Japan', Vol. 12, 2014, p. 9.

The Center for Strategic and International Studies (CSIS) in its Space Threat Assessment reports of 2018 and 2019 clearly differentiated between electromagnetic threats and 'cyberattacks': while the former affect the signals (e.g. spoofing and jamming), the latter affect data itself and the systems that use this data.[486] In the same line, Ryan Hutchins divided attacks into two categories: physical (e.g. spoofing and jamming) and computer systems attacks (hacking).[487]

However, the specialised literature is not uniform regarding this clear-cut distinction. As pointed out by Bardin, radio frequency interference and jamming have been confused with hacking, which might change as satellites increase the use of on-board computers (OBC) with remote updating needs and patching requirements.[488] Pierluigi Paganini included jamming, eavesdropping and spoofing (electromagnetic threats) under the broader umbrella of hacking.[489] Likewise, Fritz broke down hacking into jam, eavesdrop, hijack and control.[490] The fact that some authors do not draw a clear difference between malicious electromagnetic and cyber activities[491] has led to imprecise definitions, expressions and qualifications of malicious cyber activities:

- Imprecise definitions:

A clear example of this is the definition of 'jamming' provided by Paganini as a 'hacking method often used to interfere with communication for distribution of media for censorship purposes'.[492] In the same vein, Maitha Alshaer considered that 'jamming' is 'the easiest way of hacking', where the attacker mixes the signal with a rogue one, leading to interferences and limited interruption of services.[493] Despite this initial confusion, that author clearly referred to the communications segment; however, the confusion then grew again

[486] HARRISON, T., JOHNSON, K. AND ROBERTS, T., *Space Threats Assessment 2018*, cit. note 461, p. 4; HARRISON, T., JOHNSON, K. AND ROBERTS, T, *Space Threats Assessment 2019*, cit. note 476, p. 4.
[487] HUTCHINS, R., *Cyber Defense of Space Assets*, cit. note 469.
[488] BARDIN, J., *Satellite Cyberattack Search and Destroy*, cit. note 484, p. 1180.
[489] PAGANINI, P., *Satellite infrastructures - Principal cyber threats*, Rome, 3 December 2013, slide 15, available at www.aofs.org (last accessed on 11 August 2021).
[490] FRITZ, J., *Satellite Hacking,* cit. note 471, p. 34.
[491] The possibility of merging both fields is examined in: WEEDEN, B. AND SAMSON, V. (eds), *Global Counterspace Capabilities: an Open Source Assessment*, Colorado-Washington, 2019, p. 7-1, available at https://swfound.org/ (21 July 2021).
[492] PAGANINI, P., *Satellite Infrastructures - Principal Cyber Threats*, cit. note 489, slide 8.
[493] ALSHAER, M., *Cyberattacks on Satellites Review & Solutions,* available at www.academia.edu (last accessed on 11 August 2021).

when she expressed that 'jamming' can be both orbital and terrestrial[494] (rather than against up/downlinks). Another example is the definition of 'jamming' proposed by Grover as 'a subset of denial of service (DoS) attacks in which malicious nodes block legitimate communication by causing intentional interference in networks'.[495]

- Imprecise expressions:

An example of this is the expression used by Gregory Falco 'spoof a satellite',[496] instead of 'spoof a signal'. Likewise, the summary of a workshop held by the Chatham House Royal Institute on 24 January 2013 indicates that malicious cyber activities can target the communication links to and from satellites.[497]

- Imprecise qualifications:

Rajeswari Pillai Rajagopalan considered that 'jamming' is one of the most common types of cyberattacks on space systems.[498] Gregory Falco observed that 'GPS jamming' is a cyberattack because of the manipulation of the signal.[499] Although Fritz examined 'jamming' under the title of 'hacking', he admitted that 'jamming' would fall more appropriately under the category of 'electromagnetic warfare'.[500] He also recognised that there is a discussion as to what pertains to 'computer network operations' and what belongs to 'electromagnetic warfare'.[501] The table with threats proposed by Michael Sheehan[502] and its modified version in a joint publication by Massimo Pellegrino and Stang is also an example of this confusion.[503]

In light of the description made above, this section can conclude arguing that spoofing, jamming and lasers should be classified as malicious electromagnetic activities and hacking would fall under the malicious cyber activities' umbrella. Both are covert malicious

---

494 Ibid.
495 GROVER, K., *Jamming and Anti-jamming Techniques in Wireless Networks,* cit. note 473, p. 1.
496 FALCO, G., *Cybersecurity Principles for Space Systems*, in 'Journal or Aerospace Information Systems', 2018, p. 5.
497 *Making the Connection: The Future of Cyber and Space*, cit. note 68.
498 RAJESWARI PILLAI RAJAGOPALAN, *Beyond Outer Space Treaty – Time for New Mechanisms?*, in LELE, A. (ed.), *50 years of the Outer Space Treaty. Tracing the Journey*, New Delhi, 2017, p. 176.
499 FALCO, G., *Cybersecurity Principles for Space Systems*, cit. note 496, p. 8.
500 FRITZ, J., *Satellite Hacking,* cit. note 471, p. 35.
501 Ibid., p. 34.
502 SHEEHAN, M., *Defining Space Security*, in SCHROGL, K-U., HAYS, P., ROBINSON, J., MOURA, D. AND GIANNOPAPA, C. (eds), *Handbook of Space Security. Policies, Applications and Programs*, New York, 2015, p. 11.
503 PELLEGRINO, M. AND STANG, G., *Space Security for Europe*, ISSUE Report No. 29, Paris, 2016, p. 23, available at https://espas.secure.europarl.europa.eu/

activities and affect space security; only hacking as described above falls strictly under space cybersecurity (see figure 2).

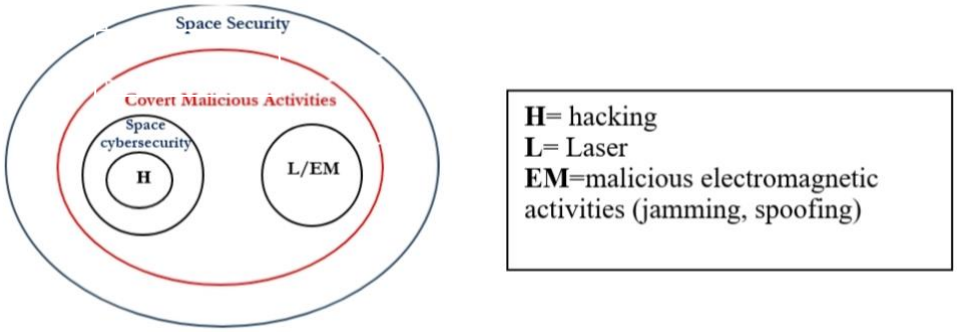


**Figure 2: Space Security and Space Cybersecurity**

## 3.3.- SPACE CYBERSECURITY:

Vulnerabilities in space assets may present along the whole supply chain,[504] which includes the design, development, launch and operation of space objects. In addition to that, there are three important factors in the production and operation of space assets that expand the vulnerability window: firstly, encryption of space assets –in particular of satellites– exponentially increases the costs and reduces efficiency of the asset.[505] Secondly, vulnerabilities remain unpatched during their long lifespan (satellites can have a lifespan of between five and thirty years).[506] Thirdly, several space assets use commercial off-the-shelf technology (COTS) with low barriers to access, which means low cybersecurity standards.[507] For that reason, commercial satellites (and more specifically CubeSats) tend to be more vulnerable than military ones.[508]

A 2014 report produced by IOActive revealed that cyber vulnerabilities (such as backdoors, hardcoded credentials, undocumented insecure protocols and weak encryption

[504] FALCO, G., *Cybersecurity Principles for Space Systems*, cit. note 496, p. 3.
[505] FRITZ, J., *Satellite Hacking,* cit. note 471, p. 28; PAGANINI, P., *Satellite Infrastructures - Principal Cyber Threats*, cit. note 489, slide 15.
[506] KALLBERG, J., *Designer Satellite Collisions from Covert Cyber War*, in 'Strategic Studies Quarterly', Vol. 6, No. 1, 2012, pp. 130.
[507] See FALCO, G., *Cybersecurity Principles for Space Systems*, cit. note 496, pp. 4-5. See also FRITZ, J., *Satellite Hacking,* cit. note 471, p. 28.
[508] See WEEDEN, B., *Space Security Index 2019. Featuring a Global Assessment of Space Security*, Ontario, 2019, p. 113, available at https://spacesecurityindex.org/ (last accessed on 11 August 2021).

algorithms) were present in most of the Inmarsat and Iridium SATCOM terminals.[509] When Iridium was created as a satellite constellation to provide GPS services to the Pentagon, cybersecurity was not a concern.[510] Yet things changed drastically and space cybersecurity became a concerning issue. For instance, NASA has increasingly become a target of a sophisticated form of malicious cyber activity designated 'advanced persistent threats' (APTs).[511] This term is used to refer to State or non-State actors, with both the capacity and intent to persistently and effectively target a specific organisation,[512] to steal or modify information from computer systems and networks over a long time period without being detected.[513] The NASA 2019 report acknowledged being a regular target of malicious cyber activities.[514]

The previous section clarified that the communication between the space and ground segments (up/downlink) or between satellites (crosslink) can be targeted *directly* through electromagnetic threats or affected *indirectly* via malicious cyber activities. This part will explain how malicious cyber activities can *directly* target either the ground or space segments and directly or indirectly affect the satellite. In other words, space assets in orbit can be affected *indirectly* by hacking the ground station or affected *directly* by accessing the OBC. This will be further explained in two separate parts:

**a) Hacking a space object *indirectly* through a ground station:**

It is possible to distinguish three points of cyber access to ground stations: internal vulnerabilities of the computer systems, external and internal threats. The terminals in a ground station are frequently off-the-shelf computers, generally known and replicated.[515] Unpatched software, hardcoded passwords and exploitable bugs are some of the possible *internal* vulnerabilities to the systems. This is not the only point of exploitation for a hacker

[509] See generally SANTAMARTA, R., *A Wake-up Call for SATCOM Security*, IOActive Research, 2014, available at https://ioactive.com/ (last accessed on 11 August 2021). Inmarsat is a British company and Iridium is an American company, both operating communications satellites constellations.
[510] See FALCO, G., *Cybersecurity Principles for Space Systems*, cit. note 496, p. 1; FALCO, G., *The Vacuum of Space Cybersecurity*, AIAA Space Forum, Orlando, 18 September 2018, p. 2, available at https://arc.aiaa.org/ (last accessed on 11 August 2021).
[511] NASA Financial Report 2012, p. 116, available at www.nasa.gov (last accessed on 11 August 2021).
[512] KALLENDER, P., *Waking up to a New Threat*, cit. note 485, p. 3.
[513] HUTCHINS, R., *Cyber Defense of Space Assets*, cit. note 469.
[514] NASA Report, *Cybersecurity Management and Oversight at the Jet Propulsion Laboratory*, June 2019, p. 2, available at https://oig.nasa.gov/ (last accessed on 11 August 2021).
[515] PELLEGRINO, M. AND STANG, G., *Space Security for Europe*, cit. note 503, p. 27.

willing to gain access into a ground station: *external* threats are feasible via the Internet if there is no proper 'logical separation' of the network, for which firewalls are a useful and necessary tool to isolate the perimeters of the ground station compound (to avoid external intruders). However, there might be also *internal* intruders; namely, irresponsible or ill-intentioned employees that may endanger the security of the systems either accessing restricted networks or altering them.

Hacking a ground station could lead to gaining the command and control of a satellite, shut down all communications and permanently damage the space object.[516] It could also deny, degrade or manipulate the satellite transmission; or even access to information captured by the satellite through its sensors.[517] The hacker might delete or replace the encryption keys of the space object and establish communications with nefarious purposes. The malicious cyber activity can also affect the manoeuvring of a satellite, making it collide against another one, decay or lower its orbit until it re-enters the Earth, burns up and ends the mission. This is possible when targeting the satellite positioning to erroneously conduct it in a certain direction to collide with another space object or with space debris (the latter case is called 'hypervelocity of the eight ball' i.e. the 'hitting of targeted satellites, directly or indirectly, with the intent to destroy the target with collision by hypervelocity objects').[518] These cases are specially concerning because not only does space debris potentially replicate the destructive effects, but also because the consequence of such malicious cyber activity will likely increase the population of space debris in outer space.

**b) *Direct* hacking of space assets in orbit:**

The OBC of a satellite can allow reconfiguration and software updates, which increases its vulnerability.[519] These vulnerabilities enable an attacker to target and *directly* affect the space object in orbit. There are two windows of opportunity: one temporal and one geographical. The former is the timeframe during which the attacker can successfully carry out a malicious cyber activity. The *temporal* window of opportunity depends on the orbit

[516] RAJESWARI PILLAI RAJAGOPALAN, *Electronic and Cyber Warfare in Outer Space*, cit. note 477, p. 10.
[517] U.S.-China Economic and Security Review Commission, 2011 Report to Congress of the U.S.-China Economic and Security Review Commission, Washington, 2011, p. 216, available at https://www.uscc.gov/ (last accessed on 11 August 2021).
[518] KALLBERG, J., *Designer Satellite Collisions,* cit. note 506, p. 132.
[519] Ibid., p. 130.

where the satellite is located. Preliminarily, it should be recalled that there are different orbits, the most common include the low Earth orbit (LEO) located between 100 and 1500 km above the Earth, medium Earth orbit (MEO) located between LEO and GEO, geosynchronous or geostationary orbit (GSO or GEO) located at around 36.000 km, high Earth orbit (HEO) and polar orbits.[520]

For instance, an Earth observation satellite located in an orbit around 600 km away takes around 90 minutes to complete one orbit (16 times a day). In a scenario where the satellite opens the communication channel (the channel used to command and control the satellite) only while in visibility of the ground station, a hacker located at mid latitudes might have around 10 minutes, once or twice a day, to conduct the malicious cyber activity (since this is the maximum time where the satellite might be visible from the location of the hacker). Differently, a geostationary satellite located at around 36.000 km (GEO) completes its orbit in 24 hours, which is the time needed for the Earth to complete a full turn around its axis. This means that the satellite remains at the same point above the hacker during the whole day (this is the timeframe the attacker has to conduct the malicious cyber activity, on the assumption that the communication channel is open the whole day) but from a farther distance. Finally, GPS satellites located at around 19.000 km (MEO) complete their orbit in around 12 hours but GPS needs at least three satellites for positioning (called 'trilateration'). This means that the hacker would have several hours during the day to command the cyber threat. In other words: the closer the satellite, the shorter the timeframe within which to target it. Conversely, the farther the satellite, the longer the timeframe.

In addition to the temporal factor, there is also a simultaneous *geographical* window of opportunity to successfully hack directly a space asset in orbit. As mentioned before, the hacker needs to access the satellite communications channel to hack the satellite itself. If the communications beam is focused or pointed at the ground station, this channel would be accessed only within a certain distance of the ground station. Communications via electromagnetic signals would be reachable only within a radius of a few kilometres from the ground station –the so-called 'coverage area' or 'footprint'.[521] In the case of a laser beam, this

[520] FRITZ, J., *Satellite Hacking,* cit. note 471, p. 23. There are other orbits such as molniya, tundra, sun-synchronous, and Lagrange points (See GEORGESCU, A., GHEORGHE, A., PISO, M. AND KATINA, P., *Critical Space Infrastructures. Risk, Resiliency and Complexity*, Cham, 2019, p. 26).
[521] MOUNTIN, S., *The Legality and Implications of Intentional Interference with Commercial Communication Satellite Signals*, in 'International Law Studies', Vol. 90, 2014, p. 128.

radius will be much smaller. This is the geographical window of opportunity that the hacker has to comply with to successfully conduct a malicious space cyber activity. If a geostationary satellite covers one third of the globe surface, the hacker might have a much larger geographical frame to carry out the malicious cyber activity depending on the spread of the communication channel. In conclusion, geostationary satellites might be easier cyber targets since the hacker has a larger time- and geographical frame to operate. In addition, geostationary satellites might be operative for 10 to 15 years and old generations currently in service may lack appropriate protection against malicious cyber activities, which makes them particularly vulnerable.

An advantage in choosing to hack a satellite *directly* is that space-borne systems do not allow physical access; thus, lack of access to the computer system nullifies several options for evidence gathering.

In 2016, China was the first country to launch a hack-proof satellite. It was nicknamed Micius, after a Chinese scientist from the 5th century B.C.E.[522] The 'Quantum Experiments at Space Scale' (QUESS) beams quantum-encrypted information between an orbiting satellite and ground stations and thus makes encryption unbreakable.[523] There are other States that experimented with quantum technology, such as Japan, Singapore and the United States.[524] Canada and the European Space Agency (ESA) are working on the development of quantum technology applied to the space industry as well.[525]

In terms of protective measures against malicious cyber activities, Julio Vivero and Luca del Monte proposed sharing a homogeneous methodological approach for introducing space cybersecurity measures in the space industry.[526] For his part, Edward Amoroso proposed a scheme of ten protective measures for malicious cyber activities against critical

[522] WALL, M., *China Launches Pioneering 'Hack-Proof' Quantum-Communications Satellite,* 16 August 2016, available at www.space.com (last accessed on 11 August 2021).
[523] DILLOW, D., LIN, J. AND SINGER, S., *China's Race to Space Domination*, 20 September 2016, available at www.popsci.com (last accessed on 11 August 2021).
[524] VILLORESI, P., *Quantum Communications in Space*, 19 February 2019. Presentation available at www.unoosa.org (last accessed on 11 August 2021); YATSU, M., *Not Only China: Quantum Satellite Communication on the Rise in the Indo-Pacific*, 26 September 2018, available at www.thediplomat.com (last accessed on 11 August 2021).
[525] WEEDEN, B., *Space Security Index 2019*, cit. note 508, p. 117.
[526] VIVERO, J. AND DEL MONTE, L., *Space Missions Cybersecurity*, SpaceOps 2014 Conference, Pasadena, 2014, pp. 1-2, available at https://arc.aiaa.org/ (last accessed on 11 August 2021).

infrastructures (deception, separation, diversity, consistency, depth, discretion, collection, correlation, awareness and response).[527]

In sum, this section explained the concept of space cybersecurity in this thesis, and clarified two possible ways of hacking space assets. The next section will propose a classification of malicious space cyber activities, based on the level and characteristics of the damage caused.

## 3.4.-PROPOSED CLASSIFICATION OF MALICIOUS SPACE CYBER ACTIVITIES:

In chapter 2, reference was made to the wide variety of malicious cyber activities ranging from mere interference to destruction. This premise was again collected in the previous sections, which laid the ground for the classification to be proposed in the present section. The rationale behind this exercise is to pave the way to the elucidation of the applicable legal framework and possibly to the identification of lacunae, which will be made in chapter 5.

**a) Space Cyber Interference**:

Interference is what Bin Cheng designated as a 'soft-kill technique'; i.e. an activity with temporary *disruptive* effects.[528] Applied to space systems, interference can cause the temporary unavailability of data or the delay in its transmission. It should be pointed out that even if space interference is not destructive *per se*, it may also have destructive consequences if –due to the temporary interference– an avoidance manoeuvre is hindered and damage is caused in flight. It might also cause destruction on Earth if, for instance, a GPS satellite is interfered and delayed information is delivered to a military operation.[529] However, it could be argued that in this case destruction is only remotely foreseeable by the hacker and probably not even intended.

[527] See generally AMOROSO, S., *Cyberattacks: Protecting National Infrastructure*, Burlington, 2011.
[528] CHENG, D., *China's Military Role in Space*, in 'Strategic Studies Quarterly', Vol. 6, No. 1, 2012, p. 67.
[529] MOUNTIN, S., *The Legality and Implications of Intentional Interference with Commercial Communication Satellite Signals*, cit. note 521, p. 120.

**b) Space Cyberattacks:**

Space cyberattacks can be placed in a different level of threats since they produce *destructive* consequences (Cheng calls these 'hard-kill techniques').[530] The Space Security Index 2019 (a report produced annually by prestigious institutions in the field of space security) defined space cyberattacks as the 'use of software and network techniques to compromise, control, interfere or destroy computer systems linked to satellite operations'.[531] As explained by Jan Kallberg, cyberattacks are traditionally one shot because hackers exploit a vulnerability that can be eliminated afterwards or corrected by updated technology.[532] According to the conclusions reached in chapter 2, destruction seems to be a necessary element of the definition of space cyberattacks. However, it should be borne in mind that certain commands of a space asset invariably lead to the end of the space mission even if they do not cause immediate destruction. For this reason, this thesis will divide space cyberattacks into different categories:

**b.1.-Destructive space cyberattacks:**

b.1.1-Full destruction of the satellite: A concrete example is a cyberattack that takes over the command and control of the satellite with the aim of completely destroying it. In this case, destruction can ensue directly by hijacking the satellite, directing it towards another space object, space debris or towards an asteroid until it collides, or towards the sun until it completely burns up. The destruction of a satellite in space produces debris as a side effect.

b.1.2.- Destruction of essential elements for the life of the satellite: A space cyberattack may be directed to seize control of critical elements for the life and operation of the satellite. If they are partially destroyed, only the lifespan of the satellite will be affected. This could be caused, for instance, by damaging the batteries and the thrusters through an overload of commands. If the destruction is complete, this will mean the end of the satellite.

b.1.3.- Destruction of critical instruments for the mission: Another scenario of destructive space cyberattacks might arise in case of overload of commands that destroy the payload of the satellite, such as the camera or the storage space for data, for instance. If

[530] CHENG, D., *China's Military Role in Space*, cit. note 528, p. 67.
[531] WEEDEN, B., *Space Security Index 2019*, cit. note 508, p. 112.
[532] KALLBERG, J., *Designer Satellite Collisions,* cit. note 506, p. 134.

destruction is total, the consequence will be the end of the mission. If destruction is partial, the mission will become permanently inefficient. In this case, command might still be feasible (including disposal manoeuvres) but the instruments will either operate deficiently or not operate at all.

b.1.4.- Data destruction: The destruction or loss of data collected by the space mission might be accomplished through a cyber intrusion and deletion. The destruction of data affects neither the life of the satellite nor the continuity of the mission; in general, it would only affect temporarily the efficacy of the mission.

**b.2.- Permanent Disruptive space cyberattacks:** The difference between this case and space interference studied in point (a) is that the latter is temporary. Here, two scenarios are distinguishable:

b.2.1.-Permanent disruption of essential elements for the life of the satellite: This could happen when the hacker disables the thrusters or the transponders; thus, command of the satellite is completely hindered and hence the satellite becomes *de facto* defunct; namely, space debris orbiting around the Earth. In effect, debris is an object that is no longer functional and cannot be controlled anymore.[533] However, if the essential elements affected are the thermal control of the satellite or the control of the solar panels, command might still be possible if enough energy is available and thus the satellite operator may conduct manoeuvres to instruct the re-entry into Earth (and final destruction) of the satellite or to re-direct it into the graveyard. If such command is no longer possible, it will end orbiting in space as debris.

b.2.2.-Permanent disruption of critical instruments for the mission: This is the case, for instance, where the hacker targets the camera that takes photographs or the atom clock of a GPS satellite without physically destroying it but affecting its functions. Here, command of the satellite might still be possible but the instruments will not operate properly or not at all. In this case, the mission becomes almost –if not totally– impossible. In this scenario, commanded disposal is still an option.

[533] DIEDERIKS-VERSCHOOR, I. AND KOPAL, V., *An Introduction to Space Law*, Alphen aan den Rijn, 2008, p. 128.

**b.3. Complete exhaustion of energy:** Another scenario is when the satellite is commanded to carry out unnecessary manoeuvres exhausting the energy it stores to operate. The complete consumption of fuel will cause the end of the mission and the end of life of the satellite, transforming it into space debris, which is impossible to dispose of via commands. Partial exhaustion is not destructive since it would only reduce the lifespan of the satellite.

**c) Space Cyber Espionage**:

Unlike previous categories, this one is neither disruptive nor destructive. Cyber espionage has been defined as the 'act or practice of obtaining secrets from individuals, competitors, rivals, groups, governments and enemies also for military, political, or economic advantage using illegal exploitation methods on internet, networks, software and/or computers'.[534] This practice belongs to the group of malicious cyber activities that aim to information 'exploitation', as explained in chapter 2. However, it should be borne in mind that cyber espionage can be carried out for exploratory purposes, i.e. to conduct preparatory intelligence actions for a potential and future malicious cyber activity that might have either *destructive* or *disruptive* effects. In such cases, cyber espionage might be considered the first stage of space interference or of a cyberattack.

| TARGET | MALICIOUS CYBER ACTIVITY | COMMAND | LEVEL OF DAMAGE | DIRECT CONSEQUENCES | INDIRECT CONSEQUENCES |
|---|---|---|---|---|---|
| | | | | | |

[534] KALLENDER, P., *Waking up to a New Threat*, cit. note 485, p. 2.

| | | | | | | |
|---|---|---|---|---|---|---|
| **D** | **SATELLITE** | **Space cyberattacks**<br><br>**(b)** | Control over the satellite | Total Destruction (b.1.1.) | End of life | Impossible command for disposal: Space debris |
| | **ESSENTIAL ELEMENTS FOR SATELLITE's LIFE** | | Commands over certain elements of the satellite | Total Destruction (b.1.2.)<br><br>or<br><br>Permanent disruption (b.2.1) | End of life | Impossible command for disposal: Space debris |
| | | | | Partial destruction (b.1.2) | Reduction of lifespan | Disposal might still be possible |
| | **ENERGY POWER** | | Wrong manoeuvres | Total exhaustion (b.3) | End of life | Impossible command for disposal: Space debris |
| | **CRITICAL INSTRUMENTS FOR THE SPACE MISSION** | | Command over the payload of the satellite | Total destruction (b.1.3.)<br><br>or<br><br>Permanent disruption (b.2.2) | End of mission | Disposal might still be possible |
| | | | | Partial | Partial end of mission | |
| | | | Deletion | Total or Partial (b.1.4) | Information loss | |

| | | | | | | |
|---|---|---|---|---|---|---|
| N D | DATA | Space cyber espionage (c) | Intrusion | | Information theft or exploratory for a future cyberattack | |
| | COMMUNICATION SYSTEMS | Space cyber interference (a) | Temporary Disruption | | Reduction of efficiency | |

**D=Destructive**
**ND=Non-destructive**

**Table 2: Malicious space cyber activities**

The severity of damage can also be measured according to the purpose of the targeted space object: satellites that provide early warning, meteorological and communications information are clearly critical. So are the satellites used for military purposes, such as reconnaissance, nuclear explosion detection, missile early warning and surveillance. Such targets can be differentiated from small satellites for educational aims (not related to essential State functions). It is worth mentioning that small satellites are an easy target since they usually present several vulnerabilities due to COTS technology and low security measures.

Another factor in the measurement of damage is the cost of the mission. Satellites in LEO are less expensive and easier to manufacture; hence, space hackers willing to cause more severe damage would have a second reason to target a satellite in GEO rather than in LEO (the first reason would be the critical services that they provide). Likewise multinational scientific undertakings to conduct experiments are quite expensive, such as space telescopes (for instance, Hubble, Spitzer or Kepler) or space probes (for instance, Rosetta, Philae, Spirit or Opportunity Rovers). As reported by ESA, the cost of the International Space Station

(ISS), including development, assembly and operation costs for a 10-year period is around €100 billion.[535]

Last but not least, it is important to note that injury or death of persons on board (astronauts or tourists) is another factor in the measurement of damage. In effect, a completely different paradigm for space cybersecurity arose with human spaceflight. Examples of human spaceflight include the Vostok capsule taking the first man into outer space, Yuri Gagarin; Apollo 11, commanded by the first man to step on to the lunar surface, Neil Armstrong; the Soyuz capsule that takes humans to the International Space Station (ISS) in the LEO to conduct experiments. In such cases, the consequences of a space cyberattack might cause human injury, death or psychological harm.

In sum, this section proposed a classification of malicious space cyber activities taking into consideration several factors: target, command, level of damage and direct/indirect consequences. All these elements impact on the qualification of malicious cyber activities from a legal standpoint.

## 3.5.-CHARACTERISTICS OF OUTER SPACE AND SPACE ACTIVITIES:

One of the first studies related to space cybersecurity examined the commonalities of the cyber and space domains, i.e. the intersection between outer space and cyberspace.[536] This section will go a step further and will set out not only commonalities, but also the differences. For that purpose, it will establish parallels with the characteristics of cyberspace and cyber activities explained in chapter 2.

### a) Outer space as a global commons:

Much has been written about the qualification of outer space. Most commentators agree that outer space is a *res communis omnium*, i.e. an area open to all States and not subject to appropriation by anyone. Other legal experts labelled outer space as *res extra commercium*[537]

[535] Information available at the website of ESA: https://www.esa.int/
[536] BAYLON, C., *Challenges at the Intersection Cyber Security and Space Security*, Chatham House, December 2014, available at https://www.chathamhouse.org/ (last accessed on 11 August 2021).
[537] Cepelka and Gilmour considered outer space a *res extra commercium*, see CEPELKA, C. AND GILMOUR, J., *The Application of General International Law in Outer Space*, in 'Journal of Air Law and Commerce', Vol. 36, No. 1, 1970,

and rejected the qualification as *res communis* since there is neither a joint sovereignty over outer space nor a right of veto.[538]

There is also an academic discussion as to whether outer space is the 'province of all mankind' or the 'common heritage of mankind'. As Vladimir Kopal clarified, the phrase 'and shall be the province of all mankind' in Article I of the Outer Space Treaty[539] does not refer to outer space itself but to its exploration and use.[540] It should be recalled that 'the province of all mankind' was a formulation originally proposed by the Soviet delegation.[541] The rationale behind this wording was that the interest of all mankind should be taken into account; not the interests of specific States.[542] To the contrary, the Moon Agreement does provide that the Moon and its natural resources are the 'common heritage of mankind' (Article 11).[543] Whereas some authors have merged these concepts,[544] others draw a clear distinction between them.[545] Rüdiger Wolfrum explained that the principle of common

p. 32; Cheng considered outer space a *res extra commercium* (territory no subject to national appropriation), see CHENG, B., *The Extraterrestrial Application of International Law,* in CHENG, B., *Studies in International Space Law*, Oxford, 1997. Oxford Scholarship Online Version: March 2012, p. 81.

[538] CHENG, B., *The Extraterrestrial Application of International Law,* cit. note 537, p. 88.

[539] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, adopted on 16 December 1966, and entered into force on 10 October 1967, 610 UNTS 205.

[540] See KOPAL, V., *International Legal Regime on Outer Space: Outer Space Treaty, Rescue Agreement and the Moon Agreement,* in Proceedings of United Nations/Nigeria Workshop on Space Law, Vienna, 2006, p. 9

[541] HOBE, S., *Article I* (Outer Space Treaty), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. I), Cologne, 2009, p. 31 (para. 17).

[542] Ibid., p. 39 (para. 52).

[543] Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, adopted on 5 December 1979, entered into force on 11 July 1984, 1363 UNTS 3.

[544] Cocca highlighted that the expression 'common heritage of mankind' was used for the first time at the UN in 1967 by himself, and while he accepted that this principle was not incorporated expressly in a treaty until the draft Moon Agreement in 1970, he suggested that the contents of Articles I and II encapsulated the concept of common heritage of mankind (COCCA, A., *The Advances in International Law through the Law of Outer Space*, in 'Journal of Space Law', Vol. 9, 1981, pp. 14-15). He even suggested replacing the 'vague expression of "province of all mankind" by the more meaningful expression "common heritage of mankind"' (COCCA, A., p. 16). Cfr. JAKHU, R., *Evolution of the Outer Space Treaty*, in LELE, A. (ed.), *50 years of the Outer Space Treaty. Tracing the Journey, Institute for Defense Studies & Analyses*, New Delhi, 2017, p. 14 (he referred to the use of the common heritage expression by Oscar Schachter in 1952). Wolter considered that Article I of the Outer Space Treaty reflected the core of the common heritage of mankind principle and that this principle was already introduced in UNGA Resolution 1472 (XIV). See WOLTER, D., *The Peaceful Purpose Standard of the Common Heritage of Mankind Principle in Outer Space Law*, in 'ASILS Journal of International Law', Vol. 9, 1985, pp. 125-126. Wolter also considered that the use and exploration for the benefit of all is the element that distinguishes the common heritage of mankind from a *res communis* as applied to the high seas (WOLTER, D., p. 130). See also SCHMIDT, Y., *International Space Law and Developing Countries*, in BRÜNNER, C. AND SOUCEK, A. (eds), *Outer Space in Society, Politics and Law*, Vienna-New York, 2011, pp. 696-697: 'Although the phrase common heritage of mankind is not explicitly found in the Outer Space Treaty, textual support can be found in it for each of the five principles'.

[545] RATHORE, E. AND GUPTA, B., *Emergence of Jus Cogens Principles in Outer Space Law*, in 'Astropolitics', Vol. 18, No. 1, 2020, p. 4; TRONCHETTI, F., *Fundamentals of Space Law and Policy*, Harbin, 2013, pp. 13-14, VON DER DUNK, F., *International Space Law*, in VON DER DUNK, F. (ed.), *Handbook of Space Law*, Cheltenham-Northampton, 2015, pp. 57-58; SOUCEK, A., *International Law*, in BRÜNNER, C. AND SOUCEK, A. (eds), *Outer Space in Society,*

heritage of mankind reflected the spirit of a given historic period (*Zeitgeist*),[546] characterised by the convergence of early developments in the law of the sea, space law, and –to a lesser degree– the regime protecting the environment of the Antarctica.[547] Although there is no definition of 'common heritage of mankind',[548] several authors considered that for a domain to be considered as such, it needs a mechanism with an authority for equal distribution of the exploited resources regardless of the degree of participation.

Despite these divergences in the literature, there is wide (but not unanimous)[549] agreement that outer space (including the Moon and other celestial bodies) is a 'global commons',[550] i.e. a space not owned by anyone but crucial to the future of all humankind.[551] This characteristic is the legal extension of the combination of two core provisions of the Outer Space Treaty: Articles I and II. The former foresees that the exploration and use of outer space shall be the province of all mankind and Article II provides that it cannot be subject to national appropriation by claim of sovereignty, by means of use or occupation or by any other means. The combination of both provisions created a balance of interests between spacefaring and non-spacefaring nations, and any attempt to appropriate outer

*Politics and Law*, Vienna-New York, 2011, p. 327; VON DER DUNK, F., *Contradictio in Terminis or Realpolitik? A Qualified Plea for a Role of 'Soft Law' in the Context of Space Activities*, University of Nebraska Faculty Publications, 2012, p. 40, available at https://digitalcommons.unl.edu/ (last accessed on 11 August 2021); HOBE, S., *Article I* (Outer Space Treaty), cit. note 541, p. 37 (para. 46); HOBE, S., *Space Law- an Analysis of its Development and its Future*, in BRÜNNER, C. AND SOUCEK, A. (eds), *Outer Space in Society, Politics and Law*, Vienna-New York, 2011, p. 479; CHRISTOL, C., *The Common Heritage of Mankind Provision in the 1979 Agreement Governing the Activities of States on the Moon and Other Celestial Bodies*, in 'The International Lawyer', Vol. 14, No. 3, 1980, pp. 451-452.

[546] See WOLFRUM, R., *The Principle of the Common Heritage of Mankind*, in 'Zeitschrift für Ausländisches Öffentliches Recht und Völkerrecht', 1983, pp. 312-313, available at https://www.zaoerv.de/ (last accessed on 11 August 2021).

[547] Wolfrum made express reference to Recommendation XI-I of the Antarctic Consultative Parties, which refers to the interests of mankind in the Antarctica.

[548] See PORRAS, D., *The "Common Heritage" of Outer Space: Equal Benefits For Most of Mankind,* in 'California Western International Law Journal', Vol. 37, No. 1, 2006, p. 145.

[549] See generally HERTZFELD, H., WEEDEN, B. AND JOHNSON, C., *How Simple Terms Mislead Us: the Pitfalls of Thinking about Outer Space as a Commons,* 2015, available at https://swfound.org/ (last accessed on 11 August 2021).

[550] MEYER, P., *Outer Space and Cyberspace: a Tale of Two Security Realms*, in OSULA, A. AND RÕIGAS, H. (eds), *International Cyber Norms*, Tallinn, 2016, p. 157; *Assured Access to the Global Commons*, NATO Allied Command Transformation, April 2011, p. 4, available at https://www.act.nato.int/ (last accessed on 11 July 2021); DELPECH, T., *Nuclear Deterrence in the 21st Century: Lessons from the Cold War for a New Era of Strategic Piracy, Santa Monica*, 2012, p. 141-142, available at https://www.rand.org/ (last accessed on 11 August 2021); KOPAL, V., *International Legal Regime on Outer Space*, cit. note 540, p. 9; SADEH, E., *Evolution of Policy and Law for International Space Governance*, in LELE, A. (ed.), *50 Years of the Outer Space Treaty. Tracing the Journey*, New Delhi, 2017, p. 154; Our Common Agenda, Report of the Secretary-General, United Nations, New York, 2021, available at https://www.un.org/ (last accessed on 9 October 2021).

[551] FISK, L., *Space as a Global Commons*. Presentation available at https://www.unoosa.org/ (last accessed on 11 August 2021).

space or parts thereof would be detrimental to that balance.[552] A recent paper written by John Goehring suggests that the notion of 'global commons' might be conceived as an enabling concept or as a constraining one. Viewed from the enabling perspective, the commons enables prosperity, security and global order (i.e. in a military or geopolitical context).[553] As a constraining concept, the commons is associated with the notion of 'common heritage of mankind' (i.e. in an economic context).[554]

Although space as a global commons was almost a settled issue –even for the United States–,[555] it should be recalled that the debate has recently been ignited by a executive order signed on 6 April 2020 by former President Trump titled 'Encouraging International Support for the Recovery and Use of Space Resources'.[556] The backdrop of this order is the policy of recovery and use of resources in outer space established by the US Commercial Space Launch Competitiveness Act.[557] What is more striking is that Section 1 of the executive order reads: 'Outer space is a legally and physically unique domain of human activity, and the United States does not view it as a global commons'. Goehring has argued that the meaning of 'global commons' referred to in this provision is the one described in his paper as the constraining or economic notion (see above).[558]

**b) Dual-use of outer space:**

In the wake of space activities there was a military interest at stake based on the geopolitical context at the time: the Cold War. Even if most of the national space programmes were initiated by military forces, nowadays military, civil and commercial sectors are increasingly dependent on and involved in space activities.

---

[552] See FREELAND, S. AND JAKHU, R., *Article II* (Outer Space Treaty), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. I), Cologne, 2009, p. 58 (para. 60).
[553] GOEHRING, J., *Why isn't Outer Space a Global Commons*?, in 'Journal of National Security Law and Policy', Vol. 11 __ (forthcoming 2021), p. 2, available at https://jnslp.com/ (last accessed on 17 August 2021).
[554] Ibid., p. 5.
[555] See JOHNSON-FREESE, J., *A Space Mission Force for the Global Commons of Space*, in 'SAIS Review of International Affairs', Vol. 36, No. 2, Summer-Fall 2016, pp. 6-7, 12; HYTEN, H., *Space Mission Force: Developing Space Warfighters for Tomorrow,* Air Force Space Command, White Paper, 29 June 2016, p. 2, available at https://www.afspc.af.mil/ (last accessed on 11 August 2021).
[556] Executive Order on Encouraging International Support for the Recovery and Use of Space Resources, 6 April 2020, available at https://www.whitehouse.gov/ (last accessed on 11 August 2021).
[557] Public Law 114 - 90 - U.S. Commercial Space Launch Competitiveness Act of 2015.
[558] GOEHRING, J., *Why isn't Outer Space a Global Commons*?, cit. note 553, p. 10.

Military missions rely on space products and services for intelligence, reconnaissance and surveillance, for shared early warning, for terrestrial and environmental monitoring, for satellite communications (SATCOM) and for position, timing and navigation.[559] Space has become what many academic commentators call a 'force multiplier' when integrated into joint operations.[560] This means that space is integrated into fundamental State security capabilities and is regrettably considered a warfare domain. In effect, it should be recalled that NATO included space into the list of operational domains in the London Summit (2019).[561] NATO does not possess satellites of its own but relies on the space assets provided by its allies (it does own and operate a number of terrestrial elements though, such as SATCOM anchor stations and terminals).[562]

In addition to the above referred military uses, space has also many vital civil applications (including telecommunications, meteorology and disaster prevention). Furthermore, after the end of the confrontation between the East and the West in the 90s more aspects were integrated into the strategic value of space for national policies (linked to the betterment and progress of the society) and not only those aimed at increasing power and prestige at the international level.[563]

Traces of the dual-use characteristic can be found in the international legal order governing outer space. More precisely, Article IV of the Outer Space Treaty has cooperated abundantly to the discussion on the dual-use nature of outer space. That provision has its source of inspiration in the Partial Test Ban Treaty of 1963[564] and in UNGA Resolution 1884 (XVIII).[565] For some authors, Article IV in fact filled the lacunae left by the Partial Test Ban

---

[559] Allied Joint Doctrine for Air and Space Operations, cit. note 454, p. 5-3.
[560] Ibid, p. 5-1; DELPECH, T., *Nuclear Deterrence in the 21st Century*, cit. note 550, p. 146; BATSANOV, S., *The Outer Space Treaty: Then and Now*, in POWERS, J. (ed.), *Celebrating the Space Age*, UNIDIR Conference Report, Geneva, 2-7 April 2007, p. 53; WOLFF, J., *'Peaceful Uses' of Outer Space has permitted its Militarization—Does it also mean its Weaponization?*, in VIGNARD, K. (ed.), *Making Space for Security*, UNIDIR Disarmament Forum, 2003, p. 10.
[561] London Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in London 3-4 December 2019, available at https://www.nato.int/ (last accessed on 11 August 2021).
[562] Allied Joint Doctrine for Air and Space Operations, cit. note 454, p. 5-1.
[563] VENET, C., *The Political Dimension*, in BRÜNNER, C. AND SOUCEK, A. (eds), *Outer Space in Society, Politics and Law*, Vienna-New York, 2011, p. 76.
[564] Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water, concluded on 5 August 1963, and entered into force on 10 October 1963, 43 UNTS 480 (Partial Test Ban Treaty).
[565] United Nations General Assembly, Resolution 1884 (XVIII), 17 October 1963, A/RES/1884 (XVIII). See op. 2(a) which is reproduced almost verbatim in Article IV of the Outer Space Treaty.

Treaty since the former prohibits the *placement* of nuclear weapons in outer space.[566] In effect, Article I of the latter instrument only bans nuclear tests and nuclear explosions of any kind in the atmosphere and beyond, including outer space. The discussion on what 'peaceful purposes' means has stimulated numerous debates (next chapter will return to the dichotomy between military and non-aggressive purposes).

Article IV paragraph 2 of the Outer Space Treaty provides that the Moon and other celestial bodies shall be used 'exclusively for peaceful purposes' but it does not say anything about outer space. This intentional omission was envisaged to allow the use of reconnaissance satellites.[567] The Cologne Commentary of the Outer Space Treaty considered that the inclusion of the word 'exclusively' in the second paragraph of Article IV left no room for any military use whatsoever of the Moon and other celestial bodies.[568] However, the same paragraph allows certain military uses (military personnel for scientific research or for any other peaceful purposes). In light of this, legal experts make a clear distinction between 'militarisation' and 'weaponisation' of outer space.[569] While the former comprises space activities that support military operations, the latter is 'the deployment of weapons that can project force to, from, in, and through space'.[570]

Dual-use of outer space leads to an important consequence: it is difficult to determine in advance if space assets are of an aggressive nature or not. Examples of dual-use space assets are satellites themselves: they may be used for Earth observation or climate forecasting, but they can also be used against another space object. GPS satellites, for instance, may be used to determine military tactics and detect missile systems or may be used to find locations in a family car. A third example is the rocket technology: it may be used to launch satellites or to launch missiles and ground-based ASATs.

---

[566] See GRIMAL, F. AND SUNDARAM, J., *The Incremental Militarization of Outer Space: A Threshold Analysis*, in 'Chinese Journal of International Law', Vol. 17, 2018, p. 58.
[567] SCHROGL, K-U. AND NEUMANN, J., *Article IV* (Outer Space Treaty), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. I), Cologne, 2009, pp. 81-82 (para. 42); TRONCHETTI, F., *Legal Aspects of the Military Uses of Outer Space*, in VON DER DUNK, F. (ed.), *Handbook of Space Law*, Cheltenham-Northampton, 2015, p. 338.
[568] SCHROGL, K-U. AND NEUMANN, J., *Article IV* (Outer Space Treaty), cit. note 567, p. 82 (para. 45).
[569] TRONCHETTI, F., *Legal Aspects of the Military Uses of Outer Space*, cit. note 567, p. 333.
[570] Ibid., p. 334. See also TRONCHETTI, F., *Fundamentals of Space Law and Policy*, cit. note 545, p. 72, MASSON-ZWAAN, T., *Legal Principles Governing the Exploration and Use of Outer Space in Times of Peace and War*, in 'ELSA magazine', Vol. 8, No. 2, 2008, p. 8, available at https://openaccess.leidenuniv.nl/ (last accessed on 11 August 2021).

For some authors, this characteristic makes difficult crafting a definition of 'space weapon';[571] and arms control mechanisms become far from an easy endeavour.[572] A restriction of dual-use assets on the basis of their military threat would lead to a restriction of their usage for civil purposes.

**c) High cost and wide accessibility:**

Access to space –i.e. the capacity to launch and operate own satellites– is very restrictive in terms of costs, which can range from 10 to 400 million US Dollars.[573] Costs of satellite production are also high: for instance, building a weather satellite is around 290 million US Dollars, and a spy satellite might cost 100 million US Dollars.[574] Morgan Stanley estimated that the global space industry generates currently revenue of 350 billion US Dollars.[575] A more cost-effective option is to place in orbit a small satellite, which would cost around 550.000 US Dollars.[576]

Nowadays, the States that have launching capabilities are very few: these are the Russian Federation, the United States, France, Japan, China, India, Israel, Iran and North Korea. Only 52 States[577] and two international organisations have registered satellites in orbit with the UN registry by 2021.[578]

Due to this reality, international cooperation is the bedrock of the extension of access to space and its benefits to non-spacefaring nations. Wolfrum defined the concept of 'international cooperation' on the basis of the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the

---

[571] BAYLON, C., *Challenges at the Intersection Cyber Security and Space Security*, cit. note 536, p. 11.
[572] See MEYER, P., *Outer Space and Cyberspace*, cit. note 550, p. 159.
[573] BROWN, G. AND HARRIS, W., *How Much do Satellites Cost*, available at https://science.howstuffworks.com/ (last accessed on 11 August 2021).
[574] Ibid.
[575] STANLEY, M., *Space: Investing in the Final Frontier*, 2 July 2019, available at www.morganstanley.com (last accessed on 11 August 2021).
[576] A Basic Guide to Nanosatellites, available at https://alen.space/ (last accessed on 11 August 2021).
[577] Algeria, Argentina, Australia, Austria, Azerbaijan, Belarus, Belgium, Bhutan, Brazil, Canada, Chile, China, Colombia, Denmark, Egypt, Finland, France, Germany, Guatemala, Hungary, India, Indonesia, Israel, Italy, Japan, Kenya*, Lao PDR, Lithuania, Luxembourg, Malaysia, Mexico, Monaco, Mongolia, New Zealand, Norway, Pakistan, Papua New Guinea, Paraguay, Peru, Philippines, Poland, Republic of Korea, the Russian Federation, Slovakia, South Africa, Spain, Sweden, Turkey, the United Arab Emirates, the United Kingdom, Uruguay, the United States (up to October 2021). *Kenya's launch was the first satellite launched with the cooperation of OOSA under the initiative 'Access to Space'.
[578] ESA and EUMETSAT.

Charter of the United Nations[579] as 'the voluntary co-ordinated action of two or more States which takes place under a legal regime and serves a specific objective'.[580]

International cooperation is a principle embedded in several space resolutions starting by UNGA Resolutions 1721 (XVI)[581] and 1962 (XVIII),[582] and is contained in the preamble and the operative text of the Outer Space Treaty. COPUOS and its two Subcommittees –assisted by the Office of Outer Space Affairs (OOSA)– is the unique platform at the global level for international cooperation in space activities.[583] In 1996, the General Assembly passed the renowned resolution containing the Declaration on International Cooperation in the Exploration and Use of Outer Space for the Benefit and in the Interest of All States, Taking into Particular Account the Needs of Developing Countries[584] (see section 3.8.3).

Furthermore, international cooperation was also the subject matter of a particular working group established under the Legal Subcommittee of COPUOS in 2014, chaired by the Japanese Setsuko Aoki. It produced a report in 2017 that was an important contribution to the UNISPACE+50 process by describing different alternatives for international cooperation (regional, bilateral and multilateral mechanisms). [585] Also furthered by UNISPACE+50, OOSA is carrying out the initiative 'Access to Space', an example of triangular cooperation (UN, spacefaring and non-spacefaring nations or emerging space States) to use and benefit from space technologies and applications.

The costs of space access set the stage for the privatisation and commercialisation of outer space, both acknowledged in the report of the Third UN Conference on Space Exploration and Peaceful Uses of Outer Space (also known as UNISPACE III).[586] One

[579] A/RES/2625 (XXV), cit. note 161.
[580] WOLFRUM, R., *Cooperation*, in Max Planck Encyclopedia of Public International Law, updated April 2010, available at available at https://opil.ouplaw.com/ (last accessed on 11 August 2021).
[581] United Nations General Assembly, Resolution 1721 (XVI), 20 December 1961, A/RES/1721 (XVI).
[582] United Nations General Assembly, Resolution 1962 (XVIII), 13 December 1963, A/RES/1962(XVIII).
[583] See annually adopted resolution on International cooperation in the peaceful uses of outer space.
[584] United Nations General Assembly, Resolution 51/122, 13 December 1996, A/RES/51/122 ('Space Benefits Declaration').
[585] Report of the Working Group on the Review of International Mechanisms for Cooperation in the Peaceful Exploration and Use of Outer Space on the work conducted under its multi-year workplan, UN Doc. A/AC.105/C.2/112, 13 April 2017.
[586] Report of the Third UN Conference on Space Exploration and Peaceful Uses of Outers Space, UN Doc. A/CONF. 184/6, 18 October 1999, paras 39 and 47.

positive aspect of these phenomena –usually referred to with the term 'New Space'–[587] is that it makes space access more innovative and cheaper for private and governmental actors;[588] but on the other hand, it raises space cybersecurity issues.[589] Even if there is a tendency to use the terms 'privatisation' and 'commercialisation' of space interchangeably, it is necessary to recall that they are two different concepts, although interrelated ones. Whereas the former is described as the participation of the private sector in the space industry, the latter might be considered a consequence of the former; namely, the financial gain in exchange of a space product or service. Fabio Tronchetti differentiated between a broad meaning of commercialisation (private capital allocated to the provision of space services regardless of the public or private nature of the consumer) and a narrow one (where the consumer is only private).[590]

It is incontestable that space is no longer an exclusively State-centred activity. At the dawn of the space era, space activities carried a lot of weight in terms of power, prestige and dominance. They played an important role in the struggle for security, military and ideological superiority between the United States and the Soviet Union (some authors called that period the 'Space Age 1.0').[591] The involvement of the space sector is a fact that started bashfully in the 80s[592] and consolidated a decade later, notably due to the need for lower costs and for access to new financial sources. As early as 1988, a Directive on National Space Policy of President Reagan gave a sign of this trend: 'the United States shall encourage and not preclude the commercial use and exploitation of space'.[593]

The privatisation of space activities consolidated around a characteristic phenomenon that marked the 90s: globalisation and the Washington Consensus. In addition, an important political and historical watershed shaped the future of space activities: the end of the Cold War, which ushered space actors into the so-called 'Space Age 2.0'. This brought

[587] MANULIS, M., BRIDGES, C.P., HARRISON, R. et al., *Cyber Security in New Space*, in 'International Journal of Information Security', 2020.
[588] RAJESWARI PILLAI RAJAGOPALAN, *Electronic and Cyber Warfare in Outer Space*, cit. note 477, p. 3.
[589] FIDLER, D., *Cybersecurity and the New Era of Space Activities,* Articles by Maurer Faculty, 2018, available at https://www.repository.law.indiana.edu/ (last accessed on 11 August 2021).
[590] TRONCHETTI, F., *Fundamentals of Space Law and Policy*, cit. note 545, pp. 72-73
[591] VENET, C., *The Political Dimension*, cit. note 563, p. 73. Also JASENTULIYANA, J., *Ensuring Equal Access to the Benefits of Space Technologies for All Countries*, in 'Space Policy', Vol. 10, No. 1, 1994, p. 8.
[592] TRONCHETTI, F., *Fundamentals of Space Law and Policy*, cit. note 545, p. 62.
[593] Presidential Directive on National Space Policy, 11 February 1988, available at https://www.hq.nasa.gov/(last accessed on 11 August 2021).

about a change in geopolitics; and with that, the incorporation of States with emerging space capabilities into the space concert. As early as 1999, the Space Millennium Declaration recognised the 'growing contribution of the private sector to the promotion and implementation of space activities'.[594]

A first step in the privatisation of space activities began with the involvement of public-private partnerships (PPPs) and then moved towards completely privately financed projects. Some examples of this process are the privatisation of the following intergovernmental consortia: the International Maritime Satellite Organization (INMARSAT) was established in 1979, privatised in 1999 and transformed into Inmarsat Plc.; the International Telecommunications Satellite Consortium (INTELSAT) was established in 1962, privatised in 2001 and transformed into Intelsat Ltd., the European Telecommunication Satellite Organisation (EUTELSAT) was established in 1977, privatised in 2001 and transformed into Eutelsat Ltd. and the Intersputnik International Organisation (INTERSPUTNIK) was established in 1971, privatised in 2003 and transformed into Intersputnik Holding Ltd. It should be borne in mind that these intergovernmental organisations were an important platform to pool resources and financial means for projects that could not be carried out by single States in those early days.

Nowadays, the international community witnesses a scenario where private actors have gained a foothold in areas of space activities that were traditionally reserved to States. The most recent example was the launch of the Crew Dragon capsule produced by SpaceX on 30 May 2020, which sent American astronauts Bob Behnken and Doug Hurley to the ISS. This event marked a breakthrough in the space industry since it was the first time a private company produced and launched a successful manned-spaceflight. In addition, the launch attracted international attention because it was the first time since 2011 that the United States sent American astronauts on an American vehicle from American soil after the cancellation of the Space Shuttle programme.[595]

---

[594] The Space Millennium: Vienna Declaration on Space and Human Development, Third United Nations Conference on the Exploration and Peaceful Uses of Outer Space (UNISPACE III), held in Vienna from 19 to 30 July 1999, see the preamble.

[595] This was so due to a change in the Fiscal Year 2010 during the Obama Administration in order to rely on the private sector for launch vehicles to send astronauts to the ISS instead of relying on NASA. On this issue, see TRONCHETTI, F., *Fundamentals of Space Law and Policy*, cit. note 545, pp. 75-76.

A final point of note is that the privatisation of outer space also urged an adaptation in the mechanisms for dispute settlement, originally envisaged for inter-State controversies, anchored in the freedom of choice among the possibilities provided in Article 33 of the UN Charter (negotiation, enquiry, mediation, conciliation, arbitration or judicial settlement). There are very few provisions in the UN space treaties on dispute settlement. In effect, Article IX of the Outer Space Treaty refers to consultations and Article XIV of the Liability Convention provides for dispute settlement through negotiations; or in case of failure, via a Claims Commission. In light of the new reality of the privatisation of outer space, on 6 December 2011 the Permanent Court of Arbitration (PCA) adopted the Optional Rules for Outer Space Disputes Relating to Outer Space Activities.

Building on the characteristics already outlined and on further elements from this research, it is possible to identify the following commonalities between cyberspace and outer space:

- Both are key enablers of essential State activities and of socioeconomic development (on the contribution of space to development, see section 3.7).

- Both shall be used for peaceful purposes but there is an increasing militarisation and a more considerable threat of their weaponisation favoured by the difficulties of control and verification mechanisms, lack of clear definitions and a blurred line between military and civil uses.

- Both are considered warfare domains by some States and military alliances (fourth and fifth domains, respectively).

- Both are cross-cutting sectors (this issue will be further developed in section 3.7).

All these commonalities support the argument that there is in fact an intersection of the cyber and space domains as explained in the seminal paper by the Chatham House Royal Institute referred at the beginning of this section. However, this is not the end of the story. There are a handful of differences that reveal that a tailor-made legal approach to space cybersecurity is still desirable:

- Whereas outer space is a natural environment, cyberspace is a man-made one.

- Whereas cyberspace is easily accessible, outer space is completely the opposite. However, it is important to highlight that the threshold of entry has been reduced in the last two decades; this is a trend that was enabled by active international cooperation and the increasing involvement of the private sector.

- Whereas outer space has been accompanied from an early stage by a binding regime, this is not the case of the cyber domain.

- Whereas the origin of outer space activities was strongly military, the origin of cyber activities was civil.

## 3.6.-OVERVIEW OF EMBLEMATIC CASES OF MALICIOUS SPACE CYBER ACTIVITIES:

Space cybersecurity incidents have become commonplace and thousands of them are constantly reported. This section will account only for a selection of the most outstanding cases of space cybersecurity.

### a) 1998: US-German ROSAT X-Ray satellite

On 20 September 1998, hackers took control of the US-German ROSAT X-Ray satellite by penetrating into computers at the Goddard Space Flight Center in Maryland.[596] The hackers then instructed the satellite to spread its solar panels directly towards the sun.[597] This command effectively fried its batteries and rendered the satellite useless. The defunct satellite crashed back to Earth in 2011.[598]

### b) 2007: US Intelsat communications satellite

[596] SCHNEIER, B., *Cyberattacks against NASA*, 4 December 2008, available at https://www.schneier.com (last accessed on 11 August 2021).
[597] See article entitled *Hackers Could Shut Down Satellites – or Turn Them into Weapons*, 12 February 2020, available at https://theconversation.com/ (last accessed on 11 August 2021).
[598] DEKEL, T. AND LEVI, R., *Space Security Capabilities and Trends,* in Space Security Conference 2011: Building on the Past, Stepping Towards the Future, UNIDIR, 2011. Presentation available at https://swfound.org (last accessed on 11 August 2021).

This is an incident that differs from other cases because it allegedly involved a non-State actor, a group of Sri Lankan separatists called the Liberation Tigers of Tamil Eelam.[599] The purpose of this malicious cyber activity was to send broadcasts to other countries from a satellite positioned over the Indian Ocean for communicating propaganda.[600] The Executive Vice President of Intelsat and General Counsel Phillip Spector held that the separatists had stolen an empty transponder frequency for the broadcasts and qualified the operations as piracy.[601]

**c) 2007-2008: US Earth observation Landsat 7 and Terra EOS AM–1**

The Landsat 7 is managed jointly by NASA and the US Geological Survey. It underwent twelve or more minutes of interference on 20 October 2007 and once again on 23 July 2008. The Terra EOS AM-1, managed by NASA, experienced some minutes of interference on 20 June 2008 and again on 22 October 2008. In the three incidents of 2008 the perpetrator achieved all steps required to command the satellite but did not issue commands.[602]

Although the 2011 report of the US-China Commission to the Congress did not attribute the incidents to China, it concluded that space and counterspace activities conducted by China were part of a larger strategy of 'space supremacy'.[603]

**d) 2013: International Space Station laptops**

The ISS was not directly connected to the Internet until 2010;[604] however, before and after then, the ISS was infected by malware several times through the laptops and memory sticks used by astronauts on board.[605] The ISS was expected to have faster Internet thanks

[599] FRITZ, J., *Satellite Hacking,* cit. note 490, p. 24; MILLER, G., *Space Pirates, Geosynchronous Guerrillas, and Nonterrestrial Terrorists. Nonstate Threats in Space*, in 'Air & Space Power Journal', Fall 2019, p. 39.
[600] BARDIN, J., *Satellite Cyberattack Search and Destroy*, cit. note 484, p. 1173.
[601] See article entitled *Sri Lankan Terrorist Attacks*, 13 April 2017, available at http://www.impactlab.net (last accessed on 11 August 2021).
[602] U.S.-China Economic and Security Review Commission (2011), cit. note 517, p. 216.
[603] Ibid., p. 220.
[604] MALIK, T., *NASA Launches Astronaut Internet in Space*, 22 January 2010, available at https://www.space.com/ (last accessed on 11 August 2021).
[605] WALDRON, K., *Space: the Last Frontier for Cybersecurity*, 28 July 2018, available at https://thehill.com/(last accessed on 11 August 2021).

to the Columbus Ka-band Terminal, a British contribution that brought speeds of up to 50 Megabits per second in 2020.[606]

In November 2013, the cosmonauts Oleg Kotov and Sergei Ryazansky performed a hand-off of the Sochi 2014 Winter Olympic Games Torch during a space walk outside the ISS.[607] Allegedly, personal removable storage devices being carried by them infected the space station with viruses.[608] Although no details were given regarding the damage done by the malware to the computer systems of the ISS, it was said that the virus took hold of the space-based computers.[609]

**e) 2014: US National Oceanic and Atmospheric Administration weather satellite**

In 2014, hackers targeted the information systems of a satellite from the National Oceanic and Atmospheric Administration (NOAA). Part of the mission of this satellite was to understand and predict changes in weather, oceans, climate and coasts, and share that knowledge and information with other agencies and the public for protecting life, property and economy.[610] The attack forced NOAA to take down the system and stop transmitting satellite images to the National Weather Service for two days to seal off the vital data.[611]

**f) 2014: Ukrainian telecommunications satellite**

Chapter 2 (section 2.4) already referred to the conflict between Ukraine and the Russian Federation. Glib Phakarenko made a detailed account of the malicious cyber

---

[606] MORRISON, R., *Broadband in Space*!, 13 February 2020, available at https://www.dailymail.co.uk/ (last accessed on 11 August 2021).
[607] See article entitled *Sochi 2014 Olympic Torch Makes Historic Space Walk*, 9 November 2013, available at https://www.olympic.org/ (last accessed on 11 August 2021).
[608] See article entitled *The International Space Station Struggles with Computer Virus Infections Contracted by Astronauts*, 13 November 2013, available at https://www.news.com.au/ (last accessed on 11 August 2021).
[609] See article entitled *International Space Station attacked by 'virus epidemics'*, 12 November 2013, available at https://www.theguardian.com/ (last accessed on 11 August 2021).
[610] National Oceanic and Atmospheric Administration Final Report, *Significant Security Deficiencies in NOAA's Information Systems create Risks in its National Critical Mission*, 15 July 2014, available at https://www.oig.doc.gov/ (last accessed on 11 August 2021).
[611] U.S.-China Economic and Security Review Commission, 2015 Report to Congress of the U.S.-China Economic and Security Review Commission, Washington, 2015, p. 296, available at https://www.uscc.gov/ (last accessed on 11 August 2021).

activities conducted during the conflict that started earlier in 2013. The operations illustrated in his report also included those that took control of the national satellite platform Lybid.[612]

There are also reports from attacks that exploited commercial satellites which were unencrypted.[613] Kaspersky Lab, a Russian company specialised in antivirus and cybersecurity, made public a research revealing that Turla –a Russian-speaking group (also called Snake or Uroburos)– was carrying out malicious cyber activities exploiting satellite-based internet links.[614] This type of malicious cyber activities has been labelled as an APT.[615] However, it is not possible to verify if this group is linked to the Russian government as some sources contend.[616]

The cases just described reveal that vulnerabilities in space assets are commonplace, that malicious space cyber activities may affect any kind of space asset and that they can be conducted either by States or by non-State actors. The next section will explain why targeting a satellite can affect essential State services.

## 3.7.-CRITICAL NATIONAL INFRASTRUCTURES AND SPACE ASSETS

Since space assets rely mostly on cyber networks, the linkages between cyberspace and outer space become a critical vulnerability.[617] Chapter 2 (section 2.5) already made reference to the concept of critical national infrastructures, which broadly speaking can be conceived as the collection of assets and systems that are essential to the socioeconomic well-being of the population and the survival of a State. In that opportunity, reference was made to some academic commentators arguing that non-destructive malicious cyber activities against CNI may be qualified as uses of force if they are disruptive enough; they might even be considered as armed attacks if the disruption meets the scale and effects threshold. Furthermore, targeting a critical infrastructure might justify a plea of necessity for

[612] See generally PAKHARENKO, G., *Cyber Operations at Maidan: a First-Hand Account*, in GEERS, K. (ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, Tallinn, 2015, p. 62.
[613] JONES, S., *Russian Group accused of Hacking Satellites*, 9 September 2015, available at https://www.ft.com/ (last accessed on 11 August 2021).
[614] TANASE, S., *Satellite Turla: APT Command and Control in the Sky*, 9 September 2015, available at https://securelist.com/ (last accessed on 11 August 2021).
[615] Ibid.
[616] See HARRISON, T., JOHNSON, K. AND ROBERTS, T., *Space Threats Assessment 2019*, cit. note 476, p. 24.
[617] WEEDEN, B., *Space Security Index 2019*, cit. note 508, p. 113.

a response. In sum, the qualification of a structure as critical is of the utmost importance in the context of security in the use of ICTs.

It is general knowledge that transportation networks, water grids or electric networks belong to CNI; however, little attention is still being paid to the underlying systems that make these important assets work; namely, space systems. In effect, space assets provide the technological backbone for *other* critical infrastructures, such as the synchronisation of power grids and telecommunication networks.[618] Falco, for instance, recognised that space systems are fundamental underlying components of most critical infrastructures, yet when he tried to learn lessons from cybersecurity in other sectors he spoke about 'other' critical infrastructures, [619] giving the impression that space systems themselves are critical infrastructures.

This section will argue that space systems are both CNI themselves and also enablers of other CNI. To back this premise, a two-pronged approach is proposed: firstly, explain the reasons that allow space systems to be considered CNI; and secondly, examine the practice of a group of States.

**a) Reasons to consider space systems as CNI:**

The Space Threat Assessment report of 2019 categorised satellites as 'the infrastructure of the infrastructure'.[620] Several academic commentators agreed expressly that space assets are CNI.[621] In this regard, Pellegrino and Stang considered that the reliance of both civilian and military users on space systems allows placing them in the area of critical infrastructure.[622] Furthermore, due to the importance of space for the commerce, key governmental responsibilities and security, Markus Hesse and Marcus Hornung similarly argued that space systems should be seen and treated as critical infrastructures.[623]

---

[618] PELLEGRINO, M. AND STANG, G., *Space Security for Europe*, cit. note 503, p. 21.
[619] FALCO, G., *The Vacuum of Space Cybersecurity*, cit. note 510, p. 1.
[620] HARRISON, T., JOHNSON, K. AND ROBERTS, T., *Space Threats Assessment 2019*, cit. note 476.
[621] See for instance: PAGANINI, P., *Satellite Infrastructures - Principal Cyber Threats*, cit. note 489, slide 4; FRITZ, J., *Satellite Hacking,* cit. note 471, p. 21; DEL MONTE, L. *Towards a Cybersecurity Policy for a Sustainable, Secure and Safe Space Environment*, Proceedings of the 64th International Astronautical Congress (IAC), 2013, p. 1.
[622] PELLEGRINO, M. AND STANG, G., *Space Security for Europe*, cit. note 503, p. 21.
[623] HESSE, M. AND HORNUNG, M., *Space as a Critical Infrastructure*, in SCHROGL, K-U., HAYS, P., ROBINSON, J., MOURA, D. AND GIANNOPAPA, C. (eds), *Handbook of Space Security. Policies, Applications and Programs*, New York, 2015, pp. 188 and 198.

A group of researchers working under the project 'Space Systems as Critical Infrastructure' –led by the Romanian Space Agency– concluded in a recent study (2019) that space systems are themselves becoming what they called a 'critical space infrastructure' (CSI).[624] They defined CSI as follows:

> (…) a set of interdependent system-of-systems encompassing workforce, environment, facilities and multidirectional interactions essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, whose destruction or disruption would have a significant impact in a given state.[625]

The concept of 'system-of-systems' (similar to the previously referred 'infrastructure of infrastructures') incorporated in the study of Liviu Muresan and Alexandru Georgescu[626] is interesting in the context of the argument of the present research since it reflects the notion that space infrastructures supplement or complement critical terrestrial infrastructures. It enhances the interdependent and cross-cutting nature of space systems. But from another angle, that very description poses a problem that a well-developed society faces: the more dependent on the system-of-systems, the more vulnerable it becomes. This will be defined as the 'techno dependence dilemma'.

On the understanding that space systems are CNI, not only does space cybersecurity need to address malicious space cyber activities *vehicled* through space systems, but also malicious space cyber activities that *target* directly space assets. This is a fine distinction that del Monte brought to the forefront in the International Astronautical Congress in 2013.[627]

The qualification of space systems as critical infrastructures may be substantiated in two main reasons; namely, the contribution of space to socioeconomic development and the contribution of space to national security:

1. <u>Contribution of space to socioeconomic development:</u>

[624] GEORGESCU, A. et al., *Critical Space Infrastructures. Risk, Resiliency and Complexity*, cit. note 520, p. 21.
[625] Ibid.
[626] MUREŞAN, L. AND GEORGESCU, A., *The Road to Resilience in 2050,* in 'The RUSI Journal', 2015, p. 59.
[627] DEL MONTE, L., *Towards a Cybersecurity Policy for a Sustainable, Secure and Safe Space Environment*, cit. note 621, p. 2.

In the context of this research, the focus on critical infrastructures is of the utmost importance due to the role that they play in the socioeconomic development of society. Likewise, space and its spin-offs contribute substantially to the furtherance of the betterment on Earth. The link between space and socioeconomic benefits is one of the core issues addressed with particular interest by COPUOS under the agenda item 'Space technology for sustainable socioeconomic development' (within the Scientific and Technical Subcommittee). Moreover, the General Assembly usually refers to this aspect in its annual resolution on international cooperation.[628]

How do space assets contribute to the daily well-being of humankind? Space systems are critical for energy grids, air traffic and telecommunication networks, as already described. They are essential to obtain information on weather phenomena and forecast, and to extend education to the most remote areas. They allow policy-makers to track epidemics, monitor natural disasters, reveal climate change effects and create maps for agricultural purposes. Moreover, satellites provide the microsecond-level timing required for stock market transactions. Should the availability of such timing become unavailable, the economy could be crippled, leading to shortages of food, water, medicine and commodities.[629]

2. Contribution of space to national security:

Another aspect that makes space systems fall into the category of CNI is the role that they play in the military domain.[630] Certain space capabilities are a building block in the security and defence of the State (essential aspects of national infrastructures), such as space situational awareness, missile warning, nuclear detonation detection, surveillance, intelligence and reconnaissance. State functions such as crisis management and humanitarian operations, verification of international treaties and arms control agreements, as well as the fight against organised crime and terrorism are also a component of the security chapter of space as CNI.

[628] See for example: United Nations General Assembly, Resolution 71/90, 6 December 2016, A/RES/71/90, preamble; Resolution 70/82, 9 December 2015, A/RES/70/82, para. 24; Resolution 69/85, 5 December 2014, A/RES/69/85, preamble; Resolution 68/75, 11 December 2013, A/RES/68/75, para. 23.
[629] HUTCHINS, R., *Cyber Defense of Space Assets*, cit. note 469.
[630] COMAN, M. AND BADEA, D., *The Critical Space Infrastructure and its Importance to Military Operations*, International Conference Knowledge-Based Organization, Vol. XXV, No. 1, 2019, p. 51, available at https://sciendo.com/ (last accessed on 11 August 2021).

To reinforce the argument made in this section, the next sub-section will account for a selection of State practice. As will be outlined, some governments have already expressly declared space systems as pertaining to CNI[631] and some are setting up space forces to defend them.

**b) State practice:**

This sub-section includes information on a group of space actors selected on two grounds: the importance of their space programmes and the development of their cyber capabilities. It should be borne in mind that since space infrastructures need to be understood as cross-cutting, it is not surprising that for some States space as such does not constitute a separate or individual sector of critical infrastructure.

- **The United States:** It should be recalled that in 1978, a directive on the National Space Policy during the Carter Administration established some principles, among which purposeful interference with operational space systems had to be viewed as an infringement upon sovereign rights, allowing for the right to self-defence.[632] The same principles were reproduced in a directive of 1982 during the Reagan Administration[633] and also in the Space Policy of 1996 (Clinton Administration).[634]

In the Rumsfeld Commission Report (2001), the Commissioners asserted that 'the U.S. is an attractive candidate for a "Space Pearl Harbor"'.[635] Eleven years later, former US Secretary of Defense Leon Panetta warned against a 'Cyber Pearl Harbor' in the following terms:

> The collective result of these kinds of attacks [attacks on critical infrastructures] could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss

631 VIVERO, J. AND DEL MONTE, L., *Space Missions Cybersecurity*, cit. note 526, p. 1.
632 See Presidential Directive NSC-37, "National Space Policy", May 11, 1978, available at https://www.hq.nasa.gov/ (last accessed on 11 August 2021). See also PETRAS, C., *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 'Journal of Air Law and Commerce', Vol. 67, No. 4, 2002, p. 1226.
633 See National Security Decision Directive No. 42, "National Space Policy", July 4, 1982, available at https://www.hq.nasa.gov/ (last accessed on 11 August 2021).
634 Presidential Decision Directive/NSC-49/NSTC-8, National Space Policy, September 14, 1996, available at https://irp.fas.org/ (last accessed on 11 August 2021).
635 Report to the Commission to Assess United States National Security Space Management and Organization, 11 January 2001, p. viii, available at https://spp.fas.org/ (last accessed on 11 August 2021).

> of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability.[636]

Traces of satellites considered as CNI can already be found in the Homeland Security Act of 2002, passed in the aftermath of the 9/11 terrorist attacks in 2001. One of its provisions foresees developing a comprehensive national plan for securing the key resources and critical infrastructures of the United States, including telecommunications systems (satellites are expressly mentioned).[637] In the same direction, the National Security Strategy (2010) in the Obama Administration promoted the use of the inherent right to self-defence in the following terms: 'To promote security and stability in space, we will pursue activities consistent with the inherent right of self-defense, deepen cooperation with allies and friends, and work with all nations toward the responsible and peaceful use of space'.[638]

The US Patriot Act 2011 defined critical infrastructures as follows:

> (...)systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[639]

In addition, the Presidential Policy Directive - Critical Infrastructure Security and Resilience of 2013 identified sixteen critical sectors. One of them is the communications sector.[640] Some media sources have echoed the lobby made by the space industry to be designated as a critical sector as well.[641] Communications is an 'enabling sector' across all the other critical sectors for the United States, and includes communications via satellites.[642] In

---

[636] Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York, 11 October 2012, available at https://archive.defense.gov/ (last accessed on 11 August 2021).
[637] Public Law 107–296 US Homeland Security Act of 2002.
[638] US National Security Strategy, May 2010, available at https://obamawhitehouse.archives.gov/(last accessed on 11 August 2021).
[639] Public Law 107- 56-Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.
[640] Presidential Policy Directive -- Critical Infrastructure Security and Resilience, The White House, Office of the Press Secretary, 12 February 2013, available at https://obamawhitehouse.archives.gov/(last accessed on 11 August 2021).
[641] WATERMAN, S., *Space Industry seeks Designation as Critical Infrastructure*, 14 October 2019, available at https://www.airforcemag.com/ (last accessed on 11 August 2021). See also HITCHENS, T., *NSC Makes Cyber Security For Space Industry 'Top Priority'*, 23 October 2019, available at https://breakingdefense.com/ (last accessed on 11 August 2021).
[642] See the website of the Cybersecurity and Infrastructure Security Agency of the United States: https://www.cisa.gov/communications-sector (last accessed on 11 August 2021).

addition, some authors observed that since the defence industry and the transportation systems are included in these critical sectors, so should the aerospace sector.[643]

Last but not least, it should be recalled that during the Trump Administration the United States created the US Space Force, which was established in December 2019 with the enactment of the National Defense Authorization Act for Fiscal Year 2020.

- **The Russian Federation:** The first observation to be made is of a terminological character: the Russian Federation tends to use the expression 'critically important objects' instead of 'critical infrastructures'.[644] A report by the Finnish Institute of International Relations on the Russian CNI, explained that the Russian policy passed from a 'hazards approach' in the early 90s (focused on natural catastrophes and technology-generated situations) to an approach focused on *objects* critical to national security since 2003.[645] It is important to recall that 2001 meant a change in the security paradigm also for this country due to the rise of terrorism as an international threat. The report further explained that the Russian policy in 2005 was tied to 'critically important objects', among which information and telecommunications were included.[646] In 2008, the Information Security Doctrine of the Russian Federation established several methods for ensuring the information security of that country, which included the legislative entrenchment in the domestic production of communications satellites.[647] The Doctrine of Information Security of the Russian Federation (2016) defined 'information infrastructure' as a combination of information objects, information systems, Internet websites and communication networks located in the territory or under the Russian jurisdiction.[648]

[643] See SHACKELFORD, S. AND RUSSELL, S., *Above the Cloud: Enhancing Cybersecurity in the Aerospace Sector*, in 'FIU Law Review', Vol. 10, No. 2, 2015, p. 640.
[644] PURSIAINEN, C., *Russia's Critical Infrastructure Policy: What do we Know about it?,* in 'European Journal for Security Research', Vol. 6, 2020, p. 24.
[645] PYNNÖNIEMI, K., *The Evolution of Russian Policy on Critical Infrastructure Protection,* in PYNNÖNIEM, K., (ed.), *Russian Critical Infrastructures. Vulnerabilities and Policies*, Helsinki, 2012, pp. 39-40.
[646] Ibid., p. 43.
[647] Information Security Doctrine of the Russian Federation (2008), cit. note 18.
[648] Doctrine of Information Security of the Russian Federation, 5 December 2016, available at https://www.mid.ru/ (last accessed on 11 August 2021).

The Aerospace Forces is the new branch of the Armed Forces of the Russian Federation, which is committed since August 2015 to repelling aerospace threats and protecting infrastructures from aerospace strikes of the enemy.[649]

- **China:** The US-China Economic and Security Review Commission concluded that China views space as a critical military and economic vulnerability for the Americans. This could explain the active deployment of direct-ascent, cyber, electromagnetic and co-orbital 'counterspace weapons' capable of targeting nearly every class of space asset.[650] In 2017 a draft Regulation on Security Protection for Critical Information Infrastructure included an array of sectors for critical information infrastructure, among which telecommunications, radio, TV networks and the Internet were included.[651] China has recently released its Security Protection Regulations for Critical Information Infrastructure (2021), which include, *inter alia*, telecommunications and technology industries as critical information infrastructures, and also 'other important network facilities and information systems that, if damaged, lost or data are disclosed, may seriously endanger national security, national economy and people's livelihood, and the public interest'.[652]

As part of a reform of the Peoples' Liberation Army carried out in December 2015, China established the Strategic Support Force, an organisation designed to better integrate space, cyber, and electronic capabilities into the army's operations.[653]

- **The European Union:** Similarly to the reaction in the United States after the 9/11 attacks, the terrorist attacks in Madrid in 2004 led to the Communication issued by the European Commission on the protection of critical infrastructures in the fight against terrorism. The document explains that 'critical infrastructures' (CI) consist of those 'physical

---

[649] See Ministry of Defence of the Russian Federation, Aerospace Forces, see https://eng.mil.ru/ (last accessed on 11 August 2021).
[650] U.S.-China Economic and Security Review Commission, 2019 Report to Congress of the U.S.-China Economic and Security Review Commission, Washington, 2019, p. 360, available at https://www.uscc.gov/ (last accessed on 11 August 2021).
[651] JONG-CHEN, J. AND O'BRIEN, B., *A Comparative Study: The Approach to Critical Infrastructure Protection in the U.S., E.U., and China*, Digital Future Project, November 2017, available at https://www.wilsoncenter.org/ (last accessed on 11 August 2021).
[652] Order of the State Council of the People's Republic of China no. 745, published on 16 August 2021 and entered into force on 1 September 2021, available at http://www.gov.cn/ (last accessed on 10 October 2021).
[653] POLLPETER, K., CHASE, M. AND HEGINBOTHAM, E., *The Creation of the PLA Strategic Support Force and its Implications for Chinese Military Space Operations*, Santa Monica, 2017, p. 31, available at www.rand.org (last accessed on 11 August 2021).

and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States'.[654]

The Green Paper on a European Programme for Critical Infrastructure Protection (2005) defined 'critical information infrastructure' (CII) as the ICT systems that are critical for themselves or that are essential for the operation of critical infrastructures and expressly mentioned telecommunications and satellites as examples.[655] Annexed to the Green Paper is an indicative list of eleven CI sectors: the eleventh is space and research.[656]

The Communication from the Commission on a European Programme for Critical Infrastructure Protection (2006) defined 'European critical infrastructures' (ECI) as those which are of the highest importance for the Community and which if disrupted or destroyed would affect Member States.[657] The Council Directive 2008/114/EC defined CI as follows:

> (…) an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.[658]

Another important milestone for the EU took place in 2011 when the European Commission catalogued space infrastructures as CI and qualified them as both an instrument and an asset.[659] As early as 2012 a space asset was identified as ECI. In effect, the Commission Staff Working Document considered Galileo –the European Global Navigation Satellite Systems (GNSS)– the first EU owned critical infrastructure.[660] As of

---

654 Commission Communication (EC), Critical Infrastructure Protection in the fight against terrorism, COM (2004) 702 final, 20 October 2004.
655 Commission Communication (EC), Green Paper on a European Programme for Critical Infrastructure Protection, COM (2005) 576, 17 November 2005.
656 Ibid. Annex II.
657 See Commission Communication (EC), European Programme for Critical Infrastructure Protection, COM (2006) 786 final, 12 December 2006.
658 Council Directive (EU) 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, OJ L 345/75.
659 Commission Communication (EU), Towards a Space Strategy for the European Union that Benefits its Citizens, COM (2011) 152 final, 4 April 2011.
660 Commission Staff Working Document (EU), New approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure, SWD (2013) 318 final, 28 August 2013.

August 2018, EU Member States designated 93 ECIs, the identities of which are not public information.[661]

- **France:** Official information provided online by the General Secretariat for Defence and National Security defined critical infrastructures as 'institutions, structures or facilities that provide the essential goods and services forming the backbone of French society and its way of life'.[662] France identified twelve critical sectors, among which space and research is one of them, in line with the European policy.

On 13 July 2019, President Macron announced the approval of the military space doctrine, which would allow France to ensure defence from and through space. He also advanced the creation of the Space Command within the Air Force in September that year and advanced the creation of a future Army of the Air and Space.[663] The Space Defence Strategy of France (2019) foresees the exercise of the right to use self-defence to defend space capabilities.[664] The presentation speech of the French Minister of the Armed Forces clearly stated that when a hostile act has been detected, characterised and attributed, France would be able to respond to it in an appropriate and proportionate manner, in accordance with the principles of international law.[665]

- **India:** In a research paper entitled 'Identifying Critical Infrastructure Sectors and their Dependencies: An Indian Scenario', the authors identified thirteen critical infrastructures on the basis of exploring important literature on the subject, brainstorming sessions with experts and one-on-one interviews with experts. One of the sectors that they

[661] Commission Staff Working Document (EU), Executive Summary of the Evaluation of Council Directive 2008/114 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection, SWD (2019) 308 final, 23 July 2019.
[662] The Critical Infrastructure Protection in France, January 2017, available at http://www.sgdsn.gouv.fr/ (last accessed on 11 August 2021).
[663] Emmanuel Macron's Speech at the Hotel de Brienne, 13 July 2019, available at https://www.elysee.fr/ (last accessed on 11 August 2021).
[664] The French Ministry for the Armed Forces, Space Defence Strategy, Report of the 'Space' working group, 2019, p. 38, available at https://www.defense.gouv.fr (last accessed on 11 August 2021).
[665] President Macron announced the creation of a Space Unit on 14 July 2019. On 25 July 2019 the French Minister of Defence Florence Parly delivered a speech on the Space Strategic Defence to the Command of Air Defence and Air Operations, available at https://www.defense.gouv.fr/ (last accessed on 11 August 2021).

identified as critical in India is telecommunications, and they included satellite communications under the category of 'vital products and services'.[666]

In June 2019, India set up the Defence Space Research Agency (DSRO) which has been entrusted with the task of creating space warfare weapon systems and technologies.[667]

- **Israel**: Israel joined the space club in 1988, when it launched Ofeq-1 from the locally built Shavit launch vehicle.[668] Although an Israeli analyst has contended that the lack of satellite information during the Yom Kippur war and the dependence on imagery from the United States was a kind of catalyser of an indigenous space programme,[669] a paper published by the Israeli Ministry of Foreign Affairs mentioned other reasons. The article written by the Chairman of the Israeli Space Agency Isaac Ben-Israel explained that the Israeli space programme was a by-product of the 1979 peace treaty with Egypt because they needed own spy satellites to verify that Egypt was not moving missiles into the demilitarised peninsula.[670] Finally, in 1995 Israel gained independence in the reconnaissance field with the launch of Ofeq-3. Thanks to its space programme, the country develops, produces and launches its own satellites as a premise of its State security.

In a joint publication, Deganit Paikowsky, Isaac Ben-Israel and Tal Azoulay explained that Israel has no official publication that presents its security policy.[671] However, they gave an important insight into it. Based on a report submitted by Ben Gurion in 1953 and the work of a committee appointed in 2004-2005 by former Premier Ariel Sharon and his Defence Minister Shaul Mofaz, they concluded that a strong space programme was highly important to the national security of Israel and for the existence of the State. They also quoted the Commander of the Israeli Air Force, Eliezer Shkedi, at the 2007 Ilan Ramon

---

[666] SINGH, A., GUPTA, M. AND OJHA, A., *Identifying Critical Infrastructure Sectors and their Dependencies: An Indian Scenario*, in 'International Journal of Critical Infrastructure Protection', 2014, p. 5.
[667] See article entitled *Defence Space Research Agency: Modi govt approves new Body to develop Space Warfare Weapon Systems*, in 'India Today', 11 June 2019, available: https://www.indiatoday.in/ (last accessed on 11 August 2021).
[668] ELLIMAN, W., *Israel in Space*, January 2003, available at https://mfa.gov.il/ (last accessed on 11 August 2021).
[669] ZORN, E., *Israel's Quest for Satellite Intelligence*, 8 May 2007, available at https://www.cia.gov/ (last accessed on 11 August 2021).
[670] BEN-ISRAEL, I. AND KAPLAN, Z., *Out of this World: Israel's Space Program*, available at https://mfa.gov.il/ (last accessed on 11 August 2021).
[671] PAIKOWSKY, D., BEN-ISRAEL, I. AND AZOULAY, T., *Israeli Perspective on Space Security*, in SCHROGL, K-U., HAYS, P., ROBINSON, J., MOURA, D. AND GIANNOPAPA, C. (eds), *Handbook of Space Security. Policies, Applications and Programs*, New York, 2015, p. 496.

Annual Space Conference saying that the 'the operational importance of space is increasing constantly'.[672]

- **Japan:** The Action Plan on Information Security Measures for Critical Infrastructures that was issued by the Information Security Policy Council in 2005 defined CI as 'business entities providing highly irreplaceable services [...] essential for people's social lives and economic activities'. [673] It identified ten critical sectors, among which, telecommunications was included.[674] The fourth edition of the Cybersecurity Policy for Critical Infrastructure Protection (2017) also included information and communication within critical infrastructures.[675]

In May 2020, Japan created the Space Operations Squadron as the first space domain mission unit of the Japan Self-Defense Forces.[676]

- **The United Kingdom**: The Public Summary of Sector Security and Resilience Plans (2017) defined critical infrastructures as follows:

> (...) those critical elements of Infrastructure (facilities, systems, sites, property, information, people, networks and processes), the loss or compromise of which would result in major detrimental impact on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or to loss of life.[677]

The United Kingdom identified thirteen critical sectors: among which, space is one of them.[678] That country established in April 2021 the UK Space Command as a Joint

---

[672] *Ibid.*, p. 501.
[673] Decision by the Information Security Council of Japan, Action Plan on Information Security Measures for Critical Infrastructure, 13 December 2005, available at https://www.nisc.go.jp/ (last accessed on 11 August 2021).
[674] Ibid.
[675] Government of Japan, The Cybersecurity Policy for Critical Infrastructure Protection, April 18, 2017, available at https://www.nisc.go.jp/ (last accessed on 11 August 2021).
[676] Ministry of Defense and Self-Defense Forces of Japan, Launch of the Space Operations Squadron, Japan Defense Focus No. 125, July 2020, available at https://www.mod.go.jp/ (last accessed on 11 August 2021).
[677] Cabinet Office of the United Kingdom, Public Summary of Sector Security and Resilience Plans, December 2017, p. 5, available at www.gov.uk/ (last accessed on 11 August 2021).
[678] Ibid.

Command staffed from the Royal Navy, British Army, Royal Air Force and the Civil Service.[679]

In sum, this section laid out both theoretical and practical arguments to conclude that space assets are not only enablers of CNI but they are CNI themselves. At the theoretical level, they fulfill the conditions to be considered critical to the State survival. At the practical level, it is possible to outline the following conclusions: 1) terrorist attacks triggered important advancements in national legislation regarding critical infrastructure in general, 2) the European policy regarding critical infrastructure has possibly influenced European national legislation to the effect that space be incorporated as a critical sector, 3) the telecommunications sector including satellites[680] is a kind of fallback option to include space as critical infrastructure, and is in fact the option chosen by many States, and 4) space systems and their applications are a fundamental necessity to safeguard the very existence of the State.

In addition, the selected practice reveals that a handful of States consider it appropriate to protect space assets with armed force. In that context, the assessment made by some experts that attacks against CNI would allow for a forceful response in self-defence (chapter 2, section 2.7.2) appears to be backed by the emerging practice of the main space powers setting up space forces or space commands and enacting military doctrines delineating such a possible response. Whether that is desirable or in accordance with international law –including space law– is far from settled (see section 3.9.1).

## 3.8.-SPACE POLICY, SPACE LAW AND SPACE GOVERNANCE: INTERCONNECTIONS AND DIFFERENCES

At the outset, it may be useful to clarify three concepts that should not be considered interchangeable: space law, space policy and space governance. However, this does not mean that they are not interlinked; to the contrary, they influence each other.

[679] See UK Space Command, published on 1 April 2021, available at https://www.gov.uk/ (last accessed on 11 August 2021).
[680] ITU adopts a broad definition of telecommunications that encompasses also satellite communications: 'Any transmission, emission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems'. Constitution of the International Telecommunication Union, concluded on 22 December 1992 and entered into force on 1 July 1994, 1825 UNTS 143. See Constitution, 1012.

**a) Space policy:** Fabio Tronchetti defined it as 'a nation's strategy regarding its civilian space program and the military and commercial utilization of outer space'.[681] This definition, however, omits to consider that the European Union,[682] the African Union[683] and NATO[684] also have a space policy; thus, the description of 'nation's strategy' falls short of covering those cases.

**b) Space law:** Sergio Marchisio explained in the framework of the 10th United Nations Workshop on Space Law (a traditional event that takes place on the first session day of the annual Legal Subcommittee of COPUOS) that this concept refers to all the rules aiming at regulating the activities in outer space of States and other subjects, including private operators.[685] It should be clarified that activities *in* outer space include those *directed towards* outer space[686] or *relating* to outer space.[687] Soviet authors like Gedanny Zhukov and Yuri Kolosov have defined 'international space law' as the specific rules of international law regulating the relations among States and with international intergovernmental organisations, and the relations of the latter among themselves regarding their space activities.[688] There is wide consensus that the wording 'activities *in* outer space' in the Outer Space Treaty includes activities linked to the launching, the operation, or the return of space objects.[689]

In *lato sensu*, space law is a system that comprises rules, norms and principles[690] of different types: international, domestic; private and public; political and legal; binding and

---

[681] TRONCHETTI, F., *Fundamentals of Space Law and Policy*, cit. note 545, see the overview section.
[682] Council (EC), Resolution on the European Space Policy, 10037/07, 25 May 2007.
[683] African Space Policy towards Social, Political and Economic Integration, available at https://au.int/ (last accessed on 11 August 2021).
[684] PAULAUSKAS, K., *Space: NATO's Latest Frontier*, 13 March 2020, available at https://www.nato.int/ (last accessed on 11 August 2021).
[685] MARCHISIO, S., *Space Law and Governance*, 10th United Nations Workshop on Space Law 'Contribution of Space Law and Policy to Space Governance and Space Security in the 21th Century', 5-8 September 2016, Vienna, p. 2, available at https://unoosa.org/ (last accessed on 11 August 2021).
[686] See GERHARD, M., *Article VI* (Outer Space Treaty), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. I), Cologne, 2009, p. 107 (para 21).
[687] LYALL, F. AND LARSEN, P., *Space Law. A Treatise*, Farnham-Furlington, 2009, p. 2.
[688] ZHUKOV, G AND KOLOSOV, Y., *International Space Law*, Moscow, 2014 (translated by Boris Belitzky), p. 17.
[689] RIBBELINK, O., *Article III* (Outer Space Treaty), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. I), Cologne, 2009, p. 66 (para. 9).
[690] The present author concurs with von der Dunk that the space law system not only comprises rules, but also norms and principles. See VON DER DUNK, F., *International Space Law*, cit. note 545, pp. 121- 122. Vladimir Kopal made reference to a 'wider concept of space law' that comprises the UN space treaties and the sets of UN principles; other international space agreements; and national laws implementing and completing international norms. See KOPAL, V., *Origins of Space Law and the Role of the United Nations*, in BRÜNNER, C. AND SOUCEK, A. (eds), *Outer Space in Society, Politics and Law*, Vienna-New York, 2011, pp. 232.

non-binding. More restricted opinions doubt about the inclusion of soft law and political commitments.

**c) Global Space governance**: The concept of 'global governance' was defined in the report of the Commission on Global Governance titled 'Our Global Neighbourhood'.[691] Building upon that notion, in 2014 the Second Manfred Lachs International Conference on Global Space Governance (an initiative of the McGill University of Canada) concluded with the so-called Montreal Declaration on the matter. The preamble reads: 'that the concept of global governance is comprehensive and includes a wide range of codes of conduct, confidence-building measures, safety concepts, international institutions, international treaties and other agreements, regulations, procedures and standards'.[692] It has also been defined as a 'movement' to negotiate responses to space-related problems.[693] At this juncture, it is possible to conclude that this is the most encompassing of the three concepts since it includes not only domestic and international instruments, but also institutions.

In a nutshell, this section builds on the assumption that the global space governance is influenced by the interaction of different space policies which shape space law. In effect, State representatives (plus EU representatives) participate in international law-making fora and convey their positions according to instructions based on policy grounds. Additionally, space law contributes to the global space governance in that it is one of its constituent elements. In turn, the global space governance permeates the whole system inwards to influence space policy and domestic law. How is this influence set in motion? In a twofold manner: a) where States (or other intergovernmental stakeholders, like the EU) already have a space policy and own space law, space governance determines if the relevant legislative instruments need to be amended or adapted and b) where States and other regional stakeholders do not have a space policy yet, space governance sets the parameters and the guidance for its development and for law-making, including capacity building and outreach activities. This is illustrated in the following figure:

---

[691] Commission on Global Governance, *Our Global Neighbourhood*, 1995, available at https://www.gdrc.org/ (last accessed on 11 August 2021).
[692] Second Manfred Lachs International Conference on Global Space Governance, held at McGill University, Montreal, 29-31 May 2014, available at https://www.mcgill.ca/ (last accessed on 11 August 2021).
[693] STELMAKH, O., *Global Space Governance for Sustainable Development*, Presentation during the UNISPACE+50 HLF, Dubai, 2016, available at www.oosa.org (last accessed on 11 August 2021).

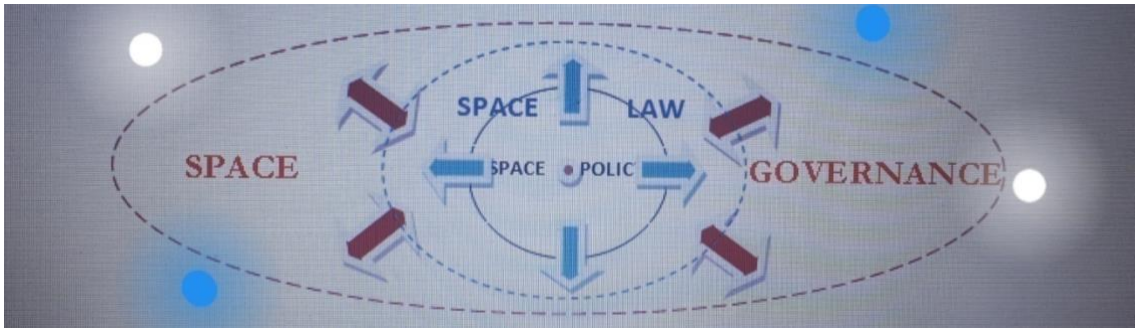


**Figure 3: Interaction between space policy, space law and space governance**

### 3.8.1.-COPUOS IN THE GLOBAL SPACE GOVERNANCE: THE LAW-MAKING STAR

COPUOS was originally established as an *ad hoc* committee by UNGA Resolution 1348 (XIII),[694] with a mandate to report to the General Assembly on how to facilitate international cooperation in the space field and on legal problems that might emerge in the exploration of outer space. At that time, the membership of COPUOS was limited to 18 members.[695] One year later, UNGA Resolution 1472A (XIV)[696] transformed it into a permanent subsidiary body of the General Assembly and increased its membership to 24 States;[697] and in 1961, it reached 28 Member States.[698] The ambition is to pursue the universalisation of COPUOS, and on the way to achieving that goal, the Committee has currently increased its membership to 95 Members (as to January 2019).[699]

On the basis of the same resolution, the expanded COPUOS met on 19 March 1962 for the first time in New York.[700] A representative from a neutral State was appointed as the Chair: the Ambassador from Austria, Franz Matsch.[701] Although the Soviet bloc stood up

[694] United Nations General Assembly, Resolution 1348 (XIII), 13 December 1958, A/RES/1348 (XIII).
[695] Argentina, Australia, Belgium, Brazil, Canada, Czechoslovakia, France, India, Iran, Italy, Japan, Mexico, Poland, Sweden, USSR, Egypt, the United Kingdom, and the United States.
[696] United Nations General Assembly, Resolution 1472A (XIV), 12 December 1959, A/RES/1472(XIV).
[697] New members: Albania, Austria, Bulgaria, Hungary, Romania and Lebanon.
[698] United Nations General Assembly, Resolution 1721E (XVI), 20 December 1961, A/RES/1721E (XVI). This resolution mentions the new members: Chad, Mongolia, Morocco and Sierra Leone.
[699] For the membership evolution, see: https://www.unoosa.org/
[700] Report of the Committee on the Peaceful Uses of Outer Space (1962), UN Doc. A/5181, 27 September 1962, para. 2.
[701] Ibid., para. 3.

for the unanimity rule for making decisions and the West for the majority rule,[702] the Chair considered that the Committee had reached an agreement to make decisions without a vote –something that was reflected in the final report.[703] Basically, this is how the rule of consensus was born (consensus means that decisions on an issue are made as long as there is no objection).[704] Decisions by consensus usually lead to vague and flexible wordings. Furthermore, a text adopted by consensus does not guarantee ratification at a later stage, as demonstrated by the Moon Agreement.[705] In the same year, COPUOS established its two Subcommittees: the Legal Subcommittee (LSC) and the Scientific and Technical Subcommittee (STSC). Paraphrasing Manfred Lachs, the cooperation between jurists and scientists in COPUOS is significant and symbolic for the progress of either field.[706]

The development of international space law under the auspices of COPUOS –and in particular of its LSC– is usually examined by the literature in a scheme of stages, periods or phases.[707] Thus, the history of space law is usually divided into three stages: 1) the UN treaties (1960-1980), 2) UNGA Resolutions with principles (mid 90s) and 3) other non-binding documents. A few law experts added a fourth stage at the very beginning: a preparatory stage from the late 50s to the mid-60s,[708] or even earlier (Second War World II and before).[709]

---

[702] See CHENG, B., *United Nations Resolutions on Outer Space: 'Instant' International Customary Law?*, in CHENG, B., *Studies in International Space Law*, Oxford, 1997. Oxford Scholarship Online Version: March 2012, p. 127; CHENG, B., *The United Nations and the Development of International Law Relating to Outer Space,* in CHENG, B., *Studies in International Space Law*, Oxford, 1997. Oxford Scholarship Online Version: March 2012, p. 163.
[703] UN Doc. A/5181, cit. note 700, para. 4.
[704] See GALLOWAY, E., *Consensus Decisionmaking by the United Nations Committee on the Peaceful Uses of Outer Space,* in 'Journal of Space Law', Vol. 7, No 1, 1979, p. 4.
[705] DANILENKO, G., *International Law-Making for Outer Space*, in 'Space Policy', Vol. 37, 2016, p. 180.
[706] LACHS, M., *Some Reflections on the State of the Law of Outer Space*, in 'Journal of Space Law', Vol. 9, No. 1&2, 1981, pp. 10-11.
[707] JANKOWITSCH, P., *The Background and History of Space Law*, in VON DER DUNK, F. (ed.), *Handbook of Space Law*, Cheltenham-Northampton, 2015, p. 26; KOPAL, V., *Origins of Space Law and the Role of the United Nations*, cit. note 690, p. 229; SOUCEK, A., *International Law*, cit. note 545, p. 359; VON DER DUNK, F., *Contradictio in Terminis or Realpolitik*?, cit. note 545, p. 32 ff.; HOBE, S., *Space Law- an Analysis of its Development and its Future*, cit. note 545, pp. 479 ff; MARCHISIO, S., *The Evolutionary Stages of the Legal Subcommittee of the United Nations Committee on the Peaceful Uses of Outer Space (COPUOS)*, in 'Journal of Space Law', Vol. 31, 2005, pp. 224 ff; HOBE, S. AND TRONCHETTI, F., *Historical Background and Context* (SB Declaration), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. III), Cologne, 2015, pp. 313-314 (paras 24-25).
[708] TRONCHETTI, F., *Fundamentals of Space Law and Policy*, cit. note 545, p. 6. See also RATHORE, E. AND GUPTA, B., *Emergence of Jus Cogens Principles*, cit. note 545, p. 1, VON DER DUNK, F., *International Space Law*, cit. note 545, p. 38, TRONCHETTI, F., *Soft Law*, in BRÜNNER, C. AND SOUCEK, A. (eds), *Outer Space in Society, Politics and Law*, Vienna-New York, 2011, p. 628.
[709] LYALL, F. AND LARSEN, P., *Space Law. A Treatise*, cit. note 687, p. 3 ff.

This chapter will deviate from that traditional way of dealing with international space law in stages. The reason behind the new methodology is to avoid linking binding and non-binding rules to a specific period of time, which does not appear to reflect the more complex reality. Indeed, transparency and confidence-building measures are present throughout the Outer Space Treaty; UNGA Resolutions (non-binding *per se*) permeate the whole formation process of international space law; and expectations for a binding treaty on PAROS in the present are still not given up, at least by some States. Moreover, the debate on binding and non-binding instruments is not a novel issue. Already when UNGA Resolution 1962 (XVIII) was negotiated, the Soviet Union stood up for a treaty while the United States preferred a resolution.[710] The result was an agreement on the form[711] and the substance:[712] the text was firstly adopted as a resolution but years later the Outer Space Treaty reproduced the principles contained in the resolution. A similar discussion 'binding v. non-binding instrument' arose during the negotiations of the Rescue Agreement.[713]

For all these reasons, this research will resort to an outline based on more substantial elements rather than temporal periods. The proposed scheme is to address international space law focusing on space treaties, customary law and *jus cogens* in the next section. Separately, section 3.8.3 will focus on the discussion of soft law.

### 3.8.2. OVERVIEW OF INTERNATIONAL SPACE LAW: TREATIES, CUSTOMARY LAW AND *JUS COGENS*

At the backdrop of the formation of international space law there are three easily identifiable sources that will be labelled here as 'the geopolitical, legal and technological triad' (see figure 4). The geopolitical source consisted in the competition between the United States and the Soviet Union for the supremacy of power, security and dominance through the development of technology to use nuclear power, missiles and to reach outer space. The legal

[710] CHENG, B., *United Nations Resolutions on Outer Space*, cit. note 702, p. 130; ZHUKOV, G. AND KOLOSOV, Y., *International Space Law*, cit. note 688, pp. 19-20.
[711] CHENG, B., *United Nations Resolutions on Outer Space*, cit. note 702, p. 133.
[712] CHENG, B., *The 1967 Space Treaty*, Oxford, 1997, in CHENG, B., *Studies in International Space Law*, Oxford Scholarship Online Version: March 2012, p. 219.
[713] Agreement on the Rescue of Astronauts, the Return of Astronauts and Return of Objects Launched into Outer Space, adopted on 19 December 1967, and entered into force on 3 December 1968, 672 UNTS 119. MARBOE, I., NEUMANN, J. AND SCHROGL, K-U, *Historical Background and Context* (Rescue Agreement), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. II), Cologne, 2013, p.13 (para. 13).

source relates to the development of legal regimes in three other areas: air (with the 1919 Paris Convention and the 1944 Chicago Convention), the Antarctic (with the 1959 Antarctic Treaty) and the nuclear (with the Partial Test Ban Treaty of 1963, unanimously welcomed by UNGA Resolution 1884 (XVIII)). Last but not least, the technological source of this triad refers to the first leaps in space technology initially inspired by the Geophysical Year: the first artificial satellite (1957), the first living creature in outer space (1957), the first man in space (1961), the first woman in space (1963), the first picture of the Moon (1966) and the first human being to set foot on the Moon (1969).

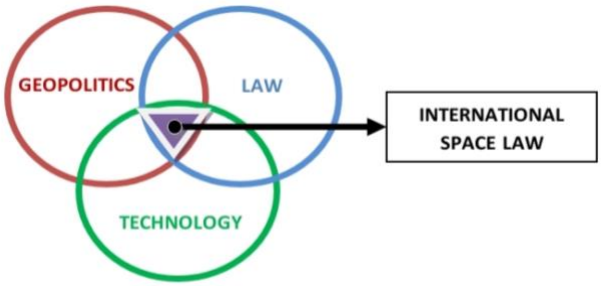


**Figure 4: International space law as a triad**

Public international space law has a few features that make it a particular branch of international law:[714] it is a fragmented system with elements agreed upon in different fora by delegations that are sometimes integrated by different experts.[715] It is a young area of international law,[716] although the first traces can be tracked to the beginning of the last century with the writings of Konstantin Tsiolkovsky and Vladimir Mandl.[717] In addition, public international space law is not yet a complete system;[718] rather, it is a developing one.[719] Intentional lacunae have given a particular flexibility to it and the vague language allows for

[714] See ZHUKOV, G. AND KOLOSOV, Y., *International Space Law*, cit. note 688, p. 13.
[715] DANILENKO, G., *International Law-Making for Outer Space*, cit. note 705, p. 182. See also METCALF, K., *A Legal View on Outer Space and Cyberspace: Similarities and Differences*, Tallinn, 2018, p. 6, available at https://ccdcoe.org/ (last accessed on 11 August 2021).
[716] KERREST, A., *Space Law and the Law of the Sea*, in BRÜNNER, C. AND SOUCEK, A. (eds), *Outer Space in Society, Politics and Law*, Vienna-New York, 2011, p. 254.
[717] TRONCHETTI, F., *Fundamentals of Space Law and Policy*, cit. note 545, p. 4; KOPAL, V. AND HOFMANN, M., *Vladimir Mandl,* in HOBE, S. (ed.), *Pioneers of Space Law*, Leiden-Boston, 2013, p. 62; KOPAL, V., *Origins of Space Law and the Role of the United Nations*, cit. note 690, p. 221. Lyall also mentioned earlier harbingers, such as Emile Laude (1910), V.A. Zarzar (1926), Herman Potočnik (1928).
[718] TRONCHETTI, F., *Fundamentals of Space Law and Policy*, cit. note 545, p. 3
[719] KOPAL, V., *International Legal Regime on Outer Space*, cit. note 540, p. 17. See also TRONCHETTI, F., *Fundamentals of Space Law and Policy*, cit. note 545, p. 3.

its adaptability.[720] As a consequence of its incompleteness, it can be considered that it is a system in evolution.[721] Moreover, international space law is State-centred[722] because at the time of its original formation space activities were conducted by States (next chapter will explain how this characteristic influenced the regime of responsibility and liability of the Outer Space Treaty).

Some pundits have posited that space law is anticipatory and that it governs issues that might become a reality in the future.[723] Although this might prove true for some issues (such as Article 11 of the Moon Agreement), for others, space law has been more reactive (for instance, in the Rescue Agreement, as will be explained below).

There is another characteristic to be outlined here and this is the low level of enforceability of international space law. In effect, none of the space treaties provide for a compulsory dispute settlement before the ICJ, nor do they establish a Space Court. In any case, space powers such as the United States, the Russian Federation and China have not accepted the compulsory jurisdiction of the ICJ (Article 36 (2) of the ICJ Statute).[724] Furthermore, the Claims Commission foreseen in the Liability Convention only has a recommendatory character unless the parties otherwise decide (Article XIX(2) of the Liability Convention).

### a) The UN Space Treaties:

The Space treaties are the result of the agreement between the two space powers at the time of negotiation. As explained before, several concepts are vague or imprecise possibly due to the need for an agreement in the overall text. This poses a problem since only a meeting of the parties might fill the absence of legal definitions of concepts such as 'national activities', 'peaceful purposes', 'damage' or 'fault' in the treaties,[725] yet they do not provide any 'built-in system' for such consultations.[726] Nowadays, the gaps and lacunae in treaty law

[720] BLOUNT, P., *Renovating Space: The Future of International Space Law*, in 'Denver Journal of International Law and Policy', Vol. 40, 2011, pp. 524-525 and 527.
[721] METCALF, K., *A Legal View on Outer Space and Cyberspace*, cit. note 715, p. 2.
[722] See SACHDEVA, G., *Outer Space Treaty: an Appraisal*, in LELE, A., *50 years of the Outer Space Treaty. Tracing the Journey,* Institute for Defense Studies & Analyses, New Delhi, 2017, p. 25.
[723] DANILENKO, G., *International Law-Making for Outer Space*, cit. note 705, p. 181.
[724] The whole list of States that accepted the compulsory jurisdiction can be consulted at: https://www.icj-cij.org/en/declarations (last accessed on 11 August 2021).
[725] MARCHISIO, S., *Space Law and Governance*, cit. note 685, p. 9.
[726] BATSANOV, S., *The Outer Space Treaty: Then and Now*, cit. note 560 , p. 54.

tend to be filled by national legislation that reinterprets fundamental principles for national interest, disregarding the special balance achieved at the time of negotiation.[727] An example of the aforementioned trend is notably depicted by the already referred case of the US Act on Recovery and Use of Space Resources (see section 3.5). Likewise, in the field of space cybersecurity, in September 2020 the United States adopted the 'Cybersecurity Principles for Space Systems'.[728]

1. The Outer Space Treaty:

The Outer Space Treaty was adopted by UNGA Resolution 2222 (XXI)[729] following an agreement between the two space powers on the draft text sponsored by 43 States.[730] It was affirmed that the treaty has created a new branch of public international law.[731] Furthermore, the Argentinian Ambassador Aldo Cocca considered that the provisions of the Outer Space Treaty meant an advance in the legal sciences because of the precursory nature of the treaty.[732] The principles enshrined in this treaty are the pillars of the current system of international space law.[733]

The Outer Space Treaty has been labelled by legal experts as 'the cardinal instrument',[734] the 'Charter of outer space',[735] the 'Bible of space law,'[736] the 'constitution for space',[737] the '*Grundnorm* of space law',[738] or 'the hallmark of global space governance',[739] just to mention a few. It was also described as 'one of the outstanding law-making treaties of

[727] DE MAN, P., *State Practice, Domestic Legislation and the Interpretation of Fundamental Principles of International Space Law*, in 'Space Policy', 2017, p. 2.
[728] Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems, 4 September 2020, available at https://www.whitehouse.gov/ (last accessed on 11 August 2021).
[729] United Nations General Assembly, Resolution 2222 (XXI), 19 December 1966, A/RES/2222 (XXI).
[730] CHENG, B., *The United Nations and the Development,* cit. note 702, p. 157.
[731] See LSC Summary Records 10th Session, UN Doc. A/AC.105/C.2/SR.154, p. 19; JANKOWITSCH, P., *The Background and History of Space Law*, cit. note 707, p. 2; see also VON DER DUNK, F., *International Space Law*, cit. note 545, p. 29; NEGER, T. AND WALTER, E., *Space Law- an Independent Branch of the Legal System*, in BRÜNNER, C. AND SOUCEK, A. (eds), *Outer Space in Society, Politics and Law*, Vienna-New York, 2011, pp. 234-235.
[732] COCCA, A., *The Advances in International Law through the Law of Outer Space*, cit. note 544, p. 20.
[733] KOPAL, V., *Origins of Space Law and the Role of the United Nations*, cit. note 690, p. 231.
[734] TRONCHETTI, F., *Fundamentals of Space Law and Policy*, cit. note 545, p. 8.
[735] WOLTER, D., *The Peaceful Purpose Standard,* cit. note 544, p. 133.
[736] SOUCEK, A., *International Law*, cit. note 545, p. 298.
[737] BLOUNT, P., *Renovating Space: The Future of International Space Law,* cit. note 720, p. 517; SCHMIDT, Y., *International Space Law and Developing Countries,* cit. note 544, p. 693.
[738] SACHDEVA, G., *Outer Space Treaty: an Appraisal*, cit. note 722, p. 25.
[739] JAKHU, R., *The future of the Outer Space Treaty*, in LELE, A. (ed.), *50 years of the Outer Space Treaty. Tracing the Journey,* Institute for Defense Studies & Analyses, New Delhi, 2017, p. 185.

contemporary international law as a whole',[740] as 'fundamental and reflective of *jus naturale*',[741] as an 'outstanding and very progressive treaty',[742] as 'the foundation of all space law',[743] as 'the most important and comprehensive international convention governing outer space',[744] as 'an arms control treaty'[745] or even as 'the most important arms control development since the Partial Nuclear Test Ban Treaty of 1963'.[746] These expressions reveal how much respect this instrument inspires within the specialised literature.

Although the treaty is open to all States, it entered into force only with a qualified and quantified ratification (upon the deposit of ratification instruments of five States, including the United States, the United Kingdom and the Soviet Union).

Despite the obscure provisions, lack of definitions and the limitations emanated from the changes in technology and the involvement of new space actors, the treaty should not be opened for review but clarified or supplemented by further instruments.[747] Until the present, 110 States have ratified this treaty.

2. The Rescue Agreement:

Only one year after the Outer Space Treaty, the General Assembly unanimously commended the Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space (the Rescue Agreement).[748] The reasons behind the expeditious negotiation of this instrument may be found in two tragic incidents at the time: firstly, the fire in the Apollo I capsule that would take the first three American astronauts to the Moon on 27 January 1967, which ended with the mission and their lives.

---

[740] MARCHISIO, S., *International Legal Regime on Outer Space: Liability Convention and Registration Convention*, in Proceedings of United Nations/Nigeria Workshop on Space Law, Vienna, 2006, p. 18.
[741] RATHORE, E. AND GUPTA, B., *Emergence of Jus Cogens Principles*, cit. note 545, p. 17.
[742] BATSANOV S., *The Outer Space Treaty: Then and Now*, cit. note 726, p. 51.
[743] VON DER DUNK, F., *International Space Law*, cit. note 545, p. 49.
[744] JAKHU, R., *Evolution of the Outer Space Treaty*, cit. note 544, p. 13.
[745] SCHROGL, K-U. AND NEUMANN, J., *Article IV* (Outer Space Treaty), cit. note 567, p. 72 (para. 6).
[746] Statement of President Johnson, reproduced in LYALL, F. AND LARSEN, P., *Space Law. A Treatise*, cit. note 687, p. 514; SCHROGL, K-U. AND NEUMANN, J., *Article IV* (Outer Space Treaty), cit. note 567, p. 74 (para 11).
[747] See KOPAL, V., *International Legal Regime on Outer Space*, cit. note 540, p. 17.
[748] United Nations General Assembly, Resolution 2345 (XXII), 19 December 1967, A/RES/2345 (XXII).

Secondly, the accident of the capsule Soyuz I with a similar fate for its Soviet commander on 24 April 1967.[749]

The Rescue Agreement builds upon Article V and VIII of the Outer Space Treaty and its underlying spirit is marked by humanitarian considerations.[750] The scope of the Convention is limited to astronauts in distress on Earth (after landing), not in space.[751]

Although the treaty is open to all States, it only entered into force with a qualified and quantified ratification (upon the deposit of ratification instruments of five States, including the United States, the United Kingdom and the Soviet Union, which are besides the depository pursuant to Article 7). Until the present, 98 States have ratified this treaty. In addition, three intergovernmental organisations have made a declaration of acceptance of rights and duties under this Convention: EUMETSAT, ESA and INTERSPUTNIK.[752]

3. The Liability Convention:

After nine years of negotiations, the Liability Convention[753] was finally adopted by UNGA Resolution 2777 (XXVI).[754] This instrument is also a further elaboration of a provision of the Outer Space Treaty; namely, Article VII.

The regime of liability will be addressed in detail in chapter 5, section 5.2. Only one aspect will be noted here: unlike previous treaties, this one entered into force with only a quantified ratification (upon the deposit of ratification instruments with the United States, the United Kingdom and the Soviet Union of five States, pursuant to its Article XXIV). Until the present, 98 States have ratified this treaty. In addition, four intergovernmental organisations have made a declaration of acceptance of rights and duties under this Convention: EUMETSAT, EUTELSAT, ESA and INTERSPUTNIK.[755]

---

[749] See KOPAL, V., *International Legal Regime on Outer Space*, cit. note 540, p. 12, CHENG, B., *The United Nations and the Development,* cit. note 702, p. 158.
[750] KOPAL, V., *International Legal Regime on Outer Space*, cit. note 540, p. 12; see also SOUCEK, A., *International Law*, cit. note 545, p. 333; HOBE, S., *Space Law- an Analysis of its Development and its Future*, cit. note 545, p. 477.
[751] TRONCHETTI, F., *Fundamentals of Space Law and Policy*, cit. note 545, p. 10.
[752] As to 1 January 2020. See https://www.unoosa.org/
[753] Convention on International Liability for Damage Caused by Space Objects, adopted on 29 November 1971, and entered into force on 1 September 1972, 961 UNTS 187.
[754] United Nations General Assembly, Resolution 2777 (XXVI), 29 November 1971, A/RES/2777 (XXVI).
[755] As to 1 January 2020. See https://www.unoosa.org/

4. The Registration Convention:

The Registration Convention[756] was adopted by UNGA Resolution 3235 (XXIX)[757] and entered into force on 15 September 1976. Its registration regime co-exists with the one implemented by UNGA Resolution 1721B (XVI)[758] although the latter is not binding but voluntary.[759] For those States that are not parties to the Registration Convention and also for the registry of launches carried out before the entry into force of this convention, registration is governed by this UNGA Resolution. Resolution 1721B calls upon States to furnish information promptly to COPUOS via the Secretary-General, who maintains a public registry of this information.[760]

While national registration is implicit in Article VIII of the Outer Space Treaty,[761] that provision is further complemented by the *lex specialis* contained in the Registration Convention, which introduced the binding obligation to register space objects launched into space.[762]

Regardless of whether a space object is launched by a private entity or by a State, it shall be registered domestically according to Article II of the Registration Convention. The State of registry has to regulate by national law the licensing mechanism for private entities because the Registration Convention binds only upon States. Thus, the State of registry has to maintain a national registry (this formality is constitutive of the right to exercise jurisdiction and control)[763] and furnish the information to the UN Secretary-General (this is a means of publicity).[764] The Convention does not provide any time limit to comply with this obligation; it only provides that it should be 'as soon as practicable'.

---

[756] Convention on Registration of Objects Launched into Outer Space, concluded on 14 January 1975 in New York, and entered into force on 15 September 1976, 1023 UNTS 15.
[757] United Nations General Assembly, Resolution 3235 (XXIX), 12 November 1974, A/RES/3235(XXIX).
[758] A/RES/1721B (XVI), cit. note 698.
[759] See MARCHISIO, S., *International Legal Regime on Outer Space*, cit. note 740, p. 24.
[760] A/RES/1721B (XVI), cit. note 698, ops 1 and 2.
[761] SCHMIDT-TEDD, B. AND MICK, S., *Article VIII* (Outer Space Treaty), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U.(eds), *Cologne Commentary on Space Law* (Vol. I), Cologne, 2009, p. 148 (para. 6).
[762] Ibid. p. 148 (paras 3, 7 and 8); SCHMIDT-TEDD, B., MALYSHEVA, N., STELMAKH, O. et al., *Article II* (Registration Convention), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. II), Cologne, 2013, pp. 259-260 (para. 66).
[763] SCHMIDT-TEDD, B. AND MICK, S., *Article VIII* (Outer Space Treaty), cit. note 761, p. 157 (para. 47).
[764] SCHMIDT-TEDD, B., MALYSHEVA, N., STELMAKH, O. et al., *Article II* (Registration Convention), cit. note 762, p. 252 (para. 46).

The registration of a space object launched into orbit or beyond allows the identification of the State of registry but if there is more than one launching State, they should determine which the State of registry is, in line with the second paragraph of Article II of the Registration Convention. The launching State is defined in Article I (a) of the Registration Convention and in Article I (c) of the Liability Convention as the State which launches or procures the launching of a space object or a State from whose territory or facility a space object is launched. Once the space object has been registered domestically, the State of registry has to provide the information required under Article IV of the Registration Convention to the Secretary-General, who maintains a register for full and open access to information as required in Article III of the same treaty.

In order to improve the practices on registration, the Legal Subcommittee of COPUOS established a working group that ultimately led to the adoption of UNGA Resolution 62/101 entitled 'Recommendations on enhancing the practice of States and international intergovernmental organizations in registering space objects'. [765] The recommendations refer to information to be furnished for registrations, agreements in case of joint launches, registration in case of more than one launching State, change of ownership of space objects, designation of contact points and registration by intergovernmental entities.

Under the joint regime established by Article VIII of the Outer Space Treaty, the Registration Convention and UNGA Resolution 1721B, the State of registry retains jurisdiction and control. This concerns the applicability of national criminal and civil law (including intellectual property).[766] There is no territorial jurisdiction in outer space because there is no title to outer space and there is no title because none can appropriate it.[767] However, this should not be understood as the inexistence of jurisdiction at all. Cheng elaborated on this concept and argued that the regime of international space law establishes the quasi-jurisdiction of a State over space objects registered with it and personnel thereof[768] unless such persons are not subject to the quasi-territorial 'jurisaction' of any State (in that case they would become under personal jurisdiction of the State of nationality).[769] This does

[765] United Nations General Assembly, Resolution 62/101, 17 December 2007, A/RES/62/101.
[766] SCHMIDT-TEDD, B. AND MICK, S., *Article VIII* (Outer Space Treaty), cit. note 761, p. 159 (para. 59).
[767] See SOUCEK, A., *International Law*, cit. note 545, pp. 313 and 316 (this is why space cannot be considered a *res nullius*).
[768] CHENG, B., *The Extraterrestrial Application of International Law*, cit. note 537, pp. 73-74. See also CEPELKA, C. AND GILMOUR, J.,*The Application of General International Law in Outer Space*, cit. note 537, pp. 34-35
[769] CHENG, B., *The Extraterrestrial Application of International Law*, cit. note 537, p. 79.

not mean that space objects adopt the 'nationality' of the State of registry but simply that space activities become 'national space activities' of the State of registry.[770]

Although the treaty is open to all States, it entered into force with only a quantified ratification (upon the deposit of ratification instruments of five States). Unlike the previous three treaties, this one provides that it will be open for signature in the UN headquarters in New York and that the General Assembly will be the depositary (Article VIII). It has been argued that this change might have been due to the admission to the UN of China in 1971 and of the two Germanies in 1973.[771]

Until the present, 69 States have ratified this treaty. In addition, four intergovernmental organisations have made a declaration of acceptance of rights and duties: EUMETSAT, EUTELSAT, ESA and INTERSPUTNIK.[772]

5. The Moon Agreement:

The Moon Agreement was adopted by consensus by UNGA Resolution 34/68.[773] A draft including the concept of the common heritage of mankind was presented by Argentina to the Legal Subcommittee,[774] which was later superseded by a Soviet draft that eliminated such reference.[775] Article 11 of the Agreement incorporates the common heritage concept, considered controversial and the reason for the poor international adherence.[776]

The treaty has been dubbed as a 'second generation space treaty'[777] or also the 'wallflower' of the treaties (a name often used by the Mexican Delegate to COPUOS to make reference to this instrument). There are mainly economic reasons linked to the disincentive to the private exploitation of resources that keep States adamant to adhere to it: the duty to share the technology and the extracted resources with other States not participating in the activities, and the prohibition of appropriation of resources in place contained in Article 11).

---

[770] See MARCHISIO, S., *International Legal Regime on Outer Space*, cit. note 740, p. 26.
[771] CHENG, B., *The United Nations and the Development*, cit. note 702, p. 169.
[772] As to 1 January 2020. See https://www.unoosa.org/
[773] United Nations General Assembly, Resolution 34/68, 5 December 1979, A/RES/34/68.
[774] Draft Agreement on the Moon and other Celestial Bodies (Argentina), UN Doc. A/AC.105/C.2/L.54, 13 June 1969. Cfr. CHRISTOL, C., *The Common Heritage of Mankind*, cit. note 545, pp. 432-433.
[775] CHENG, B., *The United Nations and the Development,* cit. note 702, pp. 161-162. See the proposal by the USSR made available to the LSC as UN Doc. A/8391, 4 June 1971.
[776] KOPAL, V., *International Legal Regime on Outer Space*, cit. note 540, p. 16.
[777] SOUCEK, A., *International Law*, cit. note 545, p. 358.

More political reasons can be found in the end of the bilateral *détente* between the United States and the Soviet Union as consequence of the invasion by the latter of Afghanistan in 1979, and the hostages taken in the American Embassy in Teheran.[778]

The provisions of this instrument are modest compared to Part XI of the Convention on the Law of the Sea, which provides for the establishment of the Seabed Authority (an international organisation) and a system for disputes settlement through the International Tribunal for the Law of the Sea. Unlike the sea regime (including its 1994 complementary agreement), the Moon Agreement does not establish any international mechanism for the exploitation of resources; it only postpones its establishment. In effect, the fifth paragraph of Article 11 provides for a *pactum de contrahendo*[779] to establish an international regime for the exploitation of resources sometime in the future –when this becomes feasible– and in accordance with Article 18 of the Moon Agreement.[780]

Although the treaty is open to all States, it entered into force with a quantified ratification (upon the deposit of ratification instruments of five States) coupled with a temporal requirement: at the thirtieth day upon the fulfilment of the former requisite. Until the present, 18 States have ratified this treaty.

**b) <u>Customary Space Law:</u>**

One of the benefits of customary law is its flexibility and capacity to adapt to circumstances.[781] While custom has traditionally been considered the sum of State practice and *opinio juri sive necessitatis,* as provided for in Article 38 of the ICJ Statute, Cheng developed the concept of 'instant custom' in an article written in 1965.[782] That concept implies the emergence of a customary rule without the need to verify a long-standing practice or a practice at all; in other terms, with the mere existence of only one constitutive element: the *opinio juris*.[783] He also considered it necessary for important space players to be behind the

[778] JASENTULIYANA, N., *The UN Space Treaties and the Common Heritage Principle*, in 'Space Policy', 1986, p. 297.
[779] CHENG, B., *The United Nations and the Development,* cit. note 702, p. 162.
[780] Article 11 (5) of the Moon Agreement.
[781] See RATHORE, E. AND GUPTA, B., *Emergence of Jus Cogens Principles*, cit. note 545, p. 5.
[782] CHENG, B., *United Nations Resolutions on Outer Space: "Instant" International Customary Law ?',* in 'Indian Journal of International Law', Vol. 5, 1965.
[783] CHENG, B., *United Nations Resolutions on Outer Space,* cit. note 702, pp. 139 and 147.

formation of the custom.[784] This is why he advocated for the denomination of 'general international law' instead of 'international customary law'.[785]

The ICJ in the North Sea Continental Shelf case collected the idea that a custom may also emerge in a short period of time. The dispute concerned the delimitation of the continental shelf between the Federal Republic of Germany and Denmark on the one hand; and between the Federal Republic of Germany and the Netherlands, on the other. The Parties asked the Court to state the principles and rules of international law applicable. In that framework, the Court rejected the contention that the rule of equidistance was already a customary rule before the Geneva Convention on Continental Shelf entered into force. Furthermore, it rejected the emergence of a customary rule upon the Convention. In its ruling, the Court observed that although the time element was not decisive, State practice should have been both extensive and virtually uniform, including the practice of the States particularly affected.[786]

The dissenting opinions of Judges Lachs and Sorensen provided significant elements of analyisis. The former explicitly made reference to customary law in the formation of space law:

> [...] the first instruments that man sent into outer space traversed the airspace of States and circled above them in outer space, yet the launching States sought no permission, nor did the other States protest. This is how the freedom of movement into outer space, and in it, came to be established and recognized as law within are markably short period of time. Similar developments are affecting, or may affect, other branches of international law.[787]

The reference made by Sorensen to the absence of State protest is what is sometimes called 'negative practice'.[788] He reflected further on the concept of 'custom' in a context of short practice –an argument that had already been brought up by Cheng in his article of

---

[784] CHENG, B., *The United Nations and the Development,* cit. note 702, pp. 191 and 211.
[785] CHENG, B., *United Nations Resolutions on Outer Space*, cit. note 702, pp. 139 and 178.
[786] *North Sea Continental Shelf (Federal Republic of Germany v. Denmark; Federal Republic of Germany v. Netherlands)*, [1969] ICJ Reports 3, 20 February 1969, para. 74 ('*Continental Shelf*').
[787] Ibid., Dissenting opinion of Judge Lachs, pp. 230-231.
[788] See Report of the International Law Commission 70th Session (2018), Draft Conclusions on Identification of Customary International Law with commentaries, UN Doc. A/73/10, p. 133 (see commentary to conclusion 6, para. 3).

1965. Sorensen appears to agree with him: 'The word "custom", with its traditional time connotation, may not even be an adequate expression for the purpose of describing this particular source of law'.[789]

Later on, some academic commentators have argued that the exercise of self-defence against terrorists after the 9/11 could constitute another example of instant customary international law.[790] Despite the above, the ILC adheres to the 'two-element approach' for the identification of international customary law and has concluded that both practice and *opinio juris* are necessary to determine the existence and content of a rule of customary international law.[791]

Other authors considered that custom was the very first source of international space law.[792] The Outer Space Treaty contains several provisions that are now considered custom (either because they pre-existed treaty law or because they crystallised as such).[793] In effect, the principle of free use and exploration of outer space that is enshrined in Article I is considered to be customary law.[794] This chapter made already reference to Article II as general international law[795] and the next section will address its *jus cogens* nature. Article III is also a provision that is considered to embody customary law.[796]

Regarding Article IV, there are scarsely traces in the specialised literature regarding the qualification of its content as customary law. The only reference that could be found in this line was a statement made by the representative of Sri Lanka to the UNGA First Committee contending that the annual presentation of the PAROS resolution and the almost universal endorsement of its principles had transformed this provision into

---

[789] *Continental Shelf,* cit. note 786. Dissenting opinion Judge Sorensen, pp. 244-245.
[790] See GRAY, C., *The Use of Force and the International Legal Order*, cit. note 166, p. 604.
[791] See UN Doc. A/73/10, cit. note 788, commentary to conclusion 2, paras 4-5.
[792] VERESHCHETIN, V. AND DANILENKO, G., *Custom as a Source of International Law of Outer Space*, in 'Journal of Space Law', Vol. 13, No. 1, 1985, p. 25.
[793] See STEER, C., *Sources and Law-Making Processes Relating to Space Activities*, in JAKHU, R. AND DEMPSEY, P. (eds), *Routledge Handbook of Space Law*, London-New York, 2017, p. 8; JAKHU, R. AND FREELAND, S., *The Relationship between the Outer Space Treaty and Customary International Law*, 67th International Astronautical Congress 2016, available at https://ssrn.com/ (last accessed on 11 August 2021).
[794] See HOBE, S., *Article I* (Outer Space Treaty), cit. note 541, p. 29 (para. 13); HERTZFELD, H., WEEDEN, B. AND JOHNSON, C., *How Simple Terms Mislead Us,* cit. note 549, pp. 3-4.
[795] CHENG, B., *The United Nations and the Development,* cit. note 702, p. 189; FREELAND, S. AND JAKHU, R., *Article II* (Outer Space Treaty), cit note 552, pp. 45-46 (para. 4); BLOUNT, P., *Renovating Space: The Future of International Space Law,* cit. note 720, p. 517.
[796] LYALL, F. AND LARSEN, P., *Space Law. A Treatise*, cit. note 687, p. 510.

customary law.[797] To the contrary, Article VI (responsibility for national activities), VII (liability for damage caused by a space object) and Article VIII (registration of space objects) were considered by several authors as general international law.[798] While Marchisio suggested that the obligations contained in Article IX of the Outer Space Treaty are in the process of becoming customary law,[799] Nicolas Matte had already categorised this provision as customary in the late 80s.[800]

Beyond the rules of customary nature contained in the Outer Space Treaty, different academic commentators are of the view that there are also other rules relating to outer space that can be considered part of the general international space law. For instance, Frans von der Dunk suggested that the 100 km delimitation line of outer space might be considered a rule of customary law.[801] In concert with that assessment, some Soviet experts have argued that this rule was expressly or tacitly recognised by almost all States.[802] They have also considered that the practice of allowing innocent passage when launching space objects could have given place to the emergence of local or particular –not yet general– custom.[803] Some principles contained in UNGA Resolution 41/65 on remote sensing (see the section 3.8.3 devoted to soft law) are also considered customary law, such as the access to data of the sensed State relating to its territory.[804] Other authors argued that UNGA Resolutions adopted by unanimity offer prospects for their contents to become customary.[805]

### c) Space *Jus cogens*:

[797] Quoted in JAKHU, R., *United Nations Principles on Outer Space,* in Proceedings of United Nations/Nigeria Workshop on Space Law, Vienna, 2006, p. 37, available at https://unoosa.org/ (last accessed on 11 August 2021).
[798] SOUCEK, A., *International Law*, cit. note 545, p. 340; CHENG, B., *The United Nations and the Development,* cit. note 702, p. 176. See KERREST, A. AND SMITH, J., *Article VII* (Outer Space Treaty), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. I), Cologne, 2009, p. 129 (para. 6).
[799] MARCHISIO, S., *Article IX* (Outer Space Treaty), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. I), Cologne, 2009, p. 181 (para. 47).
[800] MATTE, N., *Environmental Implications and Responsibilities in the Use of Outer Space*, in 'Annals Air & Space L.', Vol. 14, 1989, p. 439.
[801] VON DER DUNK, F., *International Space Law*, cit. note 545, p. 73.
[802] See VERESHCHETIN, V. AND DANILENKO, G., *Custom as a Source of International Law of Outer Space*, cit. note 792, p. 27.
[803] Ibid., p. 29.
[804] VON DER DUNK, F., *Contradictio in Terminis or Realpolitik*?, cit. note 545, pp. 42 and 52; VERESHCHETIN, V. AND DANILENKO, G., *Custom as a Source of International Law of Outer Space*, cit. note 792, p. 29. See also JAKHU, R., *United Nations Principles on Outer Space,* cit. note 797, pp. 32 and 33.
[805] See for instance VON DER DUNK, F., *International Space Law*, cit. note 545, p. 104.

The Vienna Convention on the Law of the Treaties (1969)[806] determines that a peremptory norm of general international law (*jus cogens*) is a norm accepted and recognised by the international community of States as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character. Furthermore, Article 64 of the same instrument provides that any norm conflicting with it is void. An additional consequence of *jus cogens* norms is that they create obligations *erga omnes*. It should be borne in mind that certain obligations relating to the global commons are obligations *erga omnes*, although they are not necessarily established by peremptory norms.[807]

The topic of this particular category of norms has been on the agenda of the ILC since 2015.[808] The Special Rapporteur Mr. Dire Tladi (South Africa) produced four reports dedicated to the study of the nature of these norms, the requirements for their identification, their consequences and effects. The fourth report (2019) produced a non-exhaustive list of peremptory norms that the ILC had considered as such in its previous work[809] (that work includes the commentary to draft Article 50 of the Vienna Convention on the Law of the Treaties on treaties conflicting with peremptory norms, the report on fragmentation of international law and the Draft Articles on State Responsibility).[810]

Neither that illustrative list nor the list of other possible *jus cogens* norms[811] includes any norm of international space law. However, there is consensus among scholars that the non-appropriation rule enshrined in Article II of the Outer Space Treaty has gained a *jus cogens* status.[812] The reason behind this assessment is that already at the time of the Outer

---

806 Vienna Convention on the Law of Treaties, concluded on 23 May 1969, and entered into force on 27 January 1980, 1155 UNTS 331.
807 Report of the International Law Commission 58th Session (2006), Fragmentation of International Law: Difficulties arising from the Diversification and Expansion of International Law, UN Doc. A/61/10, para. 251 (38).
808 Report of the International Law Commission 67th Session (2015), Other Decisions and Conclusions of the Commission, UN Doc. A/70/10, para. 286.
809 Fourth Report on Peremptory Norms of General International Law (*jus cogens*) by Dire Tladi, Special Rapporteur, Official Records of the General Assembly, Seventy First Session, UN Doc. A/CN.4/727, paras 60 and 137 (prohibition of aggression, genocide, slavery, apartheid and racial discrimination, crimes against humanity, torture, the right to self-determination and basic rules of humanitarian law).
810 Ibid., para. 56 ff.
811 Ibid., paras 122-123 (the right to life, the principle of non-refoulement, the prohibition of human trafficking, the right to due process (the right to a fair trial), the prohibition of discrimination, environmental rights, and the prohibition of terrorism).
812 FREELAND, S. AND JAKHU, R., *Article II* (Outer Space Treaty), cit. note 552, p. 55 (paras. 45) and p. 57 (para. 56); CEPELKA, C. AND GILMOUR, J.,*The Application of General International Law*, cit. note 537, p. 46.

Space Treaty negotiations, it was already well-established and accepted that claims of sovereignty over outer space or parts thereto were incompatible with its *res communis omnium* nature.[813]

Some authors have even gone further and argued that sovereign equality of States in outer space, freedom of use of outer space, prohibition of installation and use of nuclear weapons and weapons of mass destruction in outer space and space as the province of mankind are also *jus cogens*.[814] Ram Jakhu considered that the principle of common public interest is a norm of *jus cogens* that imposes obligations *erga omnes*.[815] Ricky Lee contended that there is some support for considering Articles III and IV in this category.[816] Others have considered humanitarian rules regarding astronauts as part of the peremptory norms of space law.[817] G.S. Sachdeva promoted what he named the '*jus cogens* Panchsheel' (five principles, in Sanskrit language) of space law: outer space a province of mankind, freedom of access to outer space, state responsibility for space activities, prohibition of placement of nuclear weapons and weapons of mass destruction in orbit around the Earth and the rescue and return of astronauts and space objects.[818]

### 3.8.3.- SOFT LAW: THE REINVENTION OF INTERNATIONAL SPACE LAW?

The expression 'soft law' is as an oxymoron because –as some experts have correctly pointed out– it inherently conveys a contradiction due to the fact that the law is always hard (i.e. binding).[819] There is no universal definition of soft law; however, Daniel Thürer described it in the Max Planck Encyclopedia of Public International Law as 'a specific form of social rules in the penumbra of international law'.[820]

---

[813] FREELAND, S. AND JAKHU, R., *Article II* (Outer Space Treaty), cit. note cit note 552, p. 49 (para. 21).
[814] RATHORE, E. AND GUPTA, B., *Emergence of Jus Cogens Principles*, cit. note 545, p. 17.
[815] JAKHU, R., *Legal Issues relating to the Global Public Interest in Outer Space*, in 'Journal of Space Law', Vol. 32, 2006, p. 48.
[816] LEE, R., *The Jus ad Bellum in Outer Space: The Interrelation between Article 103 of the Charter of the United Nations and Article IV of the Outer Space Treaty*, in 'Proc. on L. Outer Space', Vol. 45, 2002, p. 141.
[817] CEPELKA, C. AND GILMOUR, J.,*The Application of General International Law in Outer Space*, cit. note 537, p. 48.
[818] SACHDEVA, G., *Select Tenets of Space Law as Jus Cogens*, in VENCATA RAO, R., GOPALKRISHAN, V. AND ABHIJEET, K. (eds), *Recent Developments in Space Law. Opportunities & Challenges*, Bengaluru, 2017, pp. 17 and 25-26.
[819] VON DER DUNK, F., *Contradictio in Terminis or Realpolitik*?, cit. note 545, p. 48.
[820] THÜRER, D., *Soft Law*, in Max Planck Encyclopedia of Public International Law, March 2009, available at https://opil.ouplaw.com/ (last accessed on 11 August 2021).

Space experts like Steven Freeland defined 'soft law' as 'written instruments that might purport to specify standard of conduct, but do not emanate from the traditional "sources" of public international law'.[821] Christian Brünner and Georg Königsberger defined 'soft law' as rules of conduct or behaviour that are complied with 'by other means that are not sanctions in a formal way'.[822] They clarified that they understand the concept in a broad sense, i.e. including rules created by public authorities and those emanated from societal institutions.[823]

However, a part of the literature has referred to 'soft law' in a pejorative manner. For instance, Cheng expressed that 'pseudo-law can be the worst enemy of the Rule of Law'.[824] In the same line, Stephan Hobe argued that space law does not comport with the rule of law.[825] Although Brian Wessel agreed that soft law provides a lower level of rule of law, he argued that such a conclusion should not lead to avoid non-binding instruments.[826]

Hobe also rejected the idea of interpreting binding instruments through non-binding instruments which have no legal force.[827] This criticism by Hobe was contested by Wessel, who asserted that a non-binding instrument might be an authoritative interpretation of a treaty if it is drafted and adopted by the same body that negotiated the treaty.[828] In support of the interpretative role of non-binding instruments, Marchisio argued that soft law plays an important role in the interpretation of treaties since it provides evidence of subsequent practice (in the terms of Article 31(3)(b) of the Vienna Convention on the Law of the Treaties).[829]

---

821 FREELAND, S., *The Role of 'Soft Law' in Public International Law and its Relevance to the International Legal Regulation of Outer Space, in* MARBOE, I. (ed.), *Soft Law in Outer Space: The Function of non-binding Norms in International Space Law,* Vienna, 2012, p. 19.
822 BRÜNNER, C. AND KÖNIGSBERGER, G., *'Regulatory Impact Assessment' — A Tool to Strengthen Soft Law Regulations*, in MARBOE, I. (ed.), S*oft Law in Outer Space: The Function of Non-Binding Norms in International Space Law*, Vienna, 2012, p. 89.
823 Ibid.
824 CHENG, B., *United Nations Resolutions on Outer Space*, cit. note 702, p. 150.
825 HOBE, S., *The Importance of the Rule of Law for Space Activities,* in 52 Proc. of the Colloquium on the Law of Outer Space, 2009, quoted in WESSEL, B., *The Rule of Law in Outer Space: The Effects of Treaties and Nonbinding Agreements on International Space Law*, in 'Hastings Int'l & Comp. L. Rev.', Vol. 35, No. 2, 2012, pp. 300-301.
826 WESSEL, B., *The Rule of Law in Outer Space,* cit note 825, p. 314.
827 Ibid., p. 301.
828 Ibid., p. 320.
829 MARCHISIO, S., *Space Law and Governance*, cit. note 685, p. 10.

The nature of UNGA resolutions has stimulated numerous debates that have not led to uniform conclusions but to a wide variety of opinions: there are academic commentators that considered them to be simply soft law, yet others described them as a reflection of State practice or of *opinio juris*, or even of customary law if repeated in time. Others focused on the voting pattern to determine their legal value, increased in case of unanimous adoption.[830] Some authors are of the view that the principles contained in UNGA Resolution 1962 (XVIII) were soft but *de facto* international law. Those authors added that once they became reflected in the Outer Space Treaty, they turned into hard and *de jure* law.[831] Other scholars have underscored the political and moral value of UNGA Resolution 51/122 containing the Space Benefits Declaration.[832]

It is not the purpose of this section to dwell on this discussion or to review all the opinions. One conclusion is clear: the General Assembly was not empowered by the UN Charter with legislative powers.[833] This function is vested upon States and this is what makes international law a horizontal system. Hence, the binding force that UNGA resolutions may possibly gain does not emanate from themselves but from the will of States to transform the force and nature of its content into hard law.[834] Nonetheless, the ICJ held in the Nuclear Weapons Advisory Opinion that General Assembly resolutions may sometimes have a 'normative character'.[835]

The record of international space law reflects an intensive reliance of the international community on UNGA resolutions, such as the following:

**a) Resolution 37/92 on Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting:**

[830] See CHENG, B., *United Nations Resolutions on Outer Space*, cit. note 702, pp. 136-137.
[831] RATHORE, E. AND GUPTA, B., *Emergence of Jus Cogens Principles*, cit. note 545, p. 2.
[832] HOBE, S. AND TRONCHETTI, F., *Future Perspectives* (SB Declaration), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Laws* (Vol. III), Cologne, 2015, p. 356 (para. 126).
[833] PETERSON, M., *The UN General Assembly* (Global Institutions Series), London-New York, 2006, pp. 4-5.
[834] See *Lotus,* cit. note 155, p. 18: 'The rules of law binding upon States therefore emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law…'.
[835] *Nuclear Weapons*, cit. note 188, para. 70.

These principles were adopted with a vote by UNGA Resolution 37/92,[836] which established a balance between the interests of sensing and sensed States.[837] This was the first and the last time that a resolution in the field of space law was not adopted by consensus.[838] From the group of UNGA resolutions to which this section will refer, this is the only one that employs a recommendatory language with the should-form. The other ones employ the imperative 'shall-language'.

**b) Resolution 41/65 on Principles Relating to Remote Sensing of the Earth from Outer Space:**

The linchpin under discussion with the negotiation of UNGA Resolution 41/65[839] was whether there was an obligation of consent for sensing on the territory of another country –a divergent view between mainly the developed and developing countries. Nowadays, there is no discussion on the existence of a rule of customary law that allows for freedom of remote sensing without consent.[840]

**c) Resolution 47/68 on Principles Important to the Use of Nuclear Power Sources in Outer Space:**

Earlier in this chapter, it was argued that space law was reactive in several aspects. An example of such an assertion is UNGA Resolution 47/68[841] containing principles addressing the concerns around the use of nuclear power sources, essential for intergalactic spaceflights. The event that motivated the negotiation of these principles in COPUOS was the accident of Cosmos 954 on 24 January 1978, an ocean-surveillance satellite, whose radioactive fragments fell on Canadian territory.[842] In that opportunity, Canada claimed

[836] United Nations General Assembly, Resolution 37/92, 10 December 1982, A/RES/37/92, adopted by 107 votes to 13, with 13 abstentions.
[837] JAKHU, R., *United Nations Principles on Outer Space,* cit. note 797, p. 32.
[838] STUBBE, P., *Historical Background and Context* (DBS Principles), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. III), Cologne, 2015, p. 6 (para. 1).
[839] United Nations General Assembly, Resolution 41/65, 3 December 1986, A/RES/41/65.
[840] JAKHU, R., *United Nations Principles on Outer Space,* cit. note 797, pp. 32 and 33.
[841] United Nations General Assembly, Resolution 47/68, 14 December 1992, A/RES/47/68 (adopted without a vote).
[842] ESCOLAR, G. AND REYNDERS, M., *Historical Background and Context* (NPS Principles), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. III), Cologne, 2015, p. 197 (para. 3). See also GOROVE, S., *Cosmos 954: Issues of Law and Policy*, in 'Journal of Space Law', Vol. 6, 1978, p. 138.

through diplomatic channels compensation for expenses incurred in locating, recovering, removing and testing radioactive debris and cleaning up affected areas.[843]

At the request of Canada, a working group within the Scientific and Technical Subcommittee was established in 1979 to study the possibility of a technical regime of standards to regulate the use of nuclear power sources. In addition, in 1985 and again upon the request of Canada, the Legal Subcommittee was given the mandate to produce a set of principles on the matter.[844] Of the utmost importance is Principle 3, which establishes guidelines and restrictive criteria for the use of nuclear power sources.

**d) Resolution 51/122 on Declaration on International Cooperation in the Exploration and Use of Outer Space for the Benefit and in the Interest of All States, Taking into Particular Account the Needs of Developing Countries:**

The background of UNGA Resolution 51/122[845] is marked also by a *Zeitgeist*, notably the adoption of the New International Economic Order (NIEO) by the General Assembly without a vote in 1974. UNGA Resolution 3201 (S-VI) defined 'international cooperation' as a shared goal and a common *duty* of all countries.[846] Already in 1978, Colombia made reference to the NIEO during the negotiations of the Moon Agreement.[847]

The negotiations at the Legal Subcommittee of COPUOS started upon a proposal originally tabled by Venezuela in 1986 and co-sponsored by the Group of 77, with the intention of introducing the ideas of the NIEO into space matters.[848] Developing countries were of the view that Article I of the Outer Space Treaty was not only an appeal to international cooperation but an obligation.[849] The discussions reflected once again the polarisation of positions between the developing and the developed world. The final result was of paramount importance since this declaration has been considered an authoritative

[843] *Draft Articles on State Responsibility,* cit. note 219, see commentary to Article 36, para. 13, as an example of compensation for the costs in responding to damage created by pollution.
[844] United Nations General Assembly, Resolution 40/162, 16 December 1985, A/RES/40/162. See op. 4(b).
[845] A/RES/51/122, cit. note 584.
[846] United Nations General Assembly, Resolution 3201 (S-VI), 1 May 1974, A/RES/3201 (S-VI). See op. 3.
[847] LSC Summary Records-17th Session, UN Doc. A/AC.105/C.2/SR. 291, 22 March 1978, p. 6.
[848] HOBE, S. AND TRONCHETTI, F., *Historical Background and Context* (SB Declaration), cit. note 707, pp. 306-307.
[849] JASENTULIYANA, J., *Ensuring Equal Access to the Benefits,* cit. note 591, p. 9.

instrument of interpretation of Article I of the Outer Space Treaty, and it also provided the legal and political background for UNISPACE III.[850]

Some principles deserve special mention here: Principle 2 establishes that States are free to determine all aspects of their participation in international cooperation in the exploration and use of outer space on an equitable and mutually acceptable basis (the idea of international cooperation as a duty was removed) and Principle 7 seeks to strengthen the role of COPUOS, *inter alia*, as a forum for the exchange of information on national and international activities in the field of international cooperation in the exploration and use of outer space.

In a nutshell, regardless of the opposing views relating to the value and role of soft law in international law, it is uncontestable that UNGA resolutions containing principles are an integral part of the global space governance.

## 3.9.-INTERNATIONAL LAW AND INTERNATIONAL SPACE LAW: ARTICLE III OF THE OUTER SPACE TREATY

Pursuant to Article III of the Outer Space Treaty, space activities shall be carried out in accordance with international law. This provision gives a clear signal that space law is part of the more encompassing system of international law, and that it is not a complete autonomous subsystem –something that on the other hand is inconceivable.[851] The Vienna Convention on the Law of the Treaties (Article 31(3)(c)) is the legal foundation for the systemic integration,[852] according to which 'treaties are a creation of the international legal system'.[853]

At the outset, it should be emphasised that Article III of the Outer Space Treaty is neither the first nor the only reference to international law in space law. UNGA Resolution

[850] HOBE, S. AND TRONCHETTI, F., *Historical Background and Context* (SB Declaration), cit. note 707, pp. 315-316 (paras 31 and 33). UNISPACE III is the Third United Nations Conference on the Exploration and Peaceful Uses of Outer Space, Vienna, 19-30 July 1999. One of the actions sought by that conference was to increase the access to space benefits by developing countries.
[851] See SIMMA, B. AND PULKOWSKI, D., *Of Planets and the Universe: Self-contained Regimes in International Law,* in 'European Journal of International Law, Vol. 17, No. 3, 2006, p. 492.
[852] DÖRR, O. AND SCHMALENBACH, K. (eds), *Vienna Convention on the Law of the Treaties. A Commentary*, Berlin-Heidelberg, 2012, pp. 560-561 (para. 89).
[853] UN Doc. A/61/10, cit. note 807, p. 413 (para. 17).

1721A (XVI) had already confirmed the application of international law to outer space and the celestial bodies as a 'principle'.[854] One year later, the respect of international law in carrying out space activities was included in the preamble of UNGA Resolution 1802 (XVII) with a 'should-formulation'.[855] Then, UNGA Resolution 1962 (XVIII) increased the force in the language using the 'shall-formulation' and placed it within the operative paragraphs.[856] Finally, the Outer Space Treaty transformed it into a legal obligation under Article III, with the 'shall-formulation'.

However, a remarkable point is that none of the legal sources mentioned before refers to *relevant* international law, which would have been a more precise formulation since international law *in toto* is not applicable.[857] As some authors have underscored, Article III is not a blanket extension of the entire realm of international law to outer space and the celestial bodies.[858]

During the negotiations of Article III, the delegate of France pointed at the vagueness of the reference to international law and the UN Charter, and proposed determining which principles of international law were meant by that reference.[859] In another opportunity, France –and later Brazil as well–[860] expressed reservations regarding the reference to the applicability of international law and the UN Charter to outer space.[861] The Cologne Commentary on pace Law has considered that non-intervention, non-aggression, non-use of force and self-defence are included in that reference.[862] Likewise, principles of other fields of international law –like the precautionary principle of environmental law– are imported into space law.[863]

---

[854] A/RES/1721B (XVI), cit. note 698, op. 1 (a).
[855] United Nations General Assembly, Resolution 1802 (XVII), 14 December 1962, A/RES/1802 (XVII).
[856] A/RES/1962 (XVIII), cit. note 582, see op. 4.
[857] RIBBELINK, O., *Article III* (Outer Space Treaty), cit. note 689, p. 67 (para. 12).
[858] MAOGOTO, J. AND FREELAND, S., *Space Weaponization and the United Nations Charter Regime on Force: A Thick Legal Fog or a Receding Mist?*, in 'The International Lawyer', Vol. 41, No. 4, 2007, p. 1098.
[859] LSC Summary records 5th Session (1966), UN Doc. A/AC.105/C.2/SR.64, p. 6; LSC Summary records 5th Session (1966), UN Doc. A/AC. 105/C.2/SR. 69, p. 5.
[860] LSC Summary records 5th Session (1966), UN Doc. A/AC.105/C.2/SR.71, p. 17.
[861] LSC Summary records 5th Session (1966), UN Doc. A/AC.105/C.2/SR.70, p. 14.
[862] RIBBELINK, O., *Article III* (Outer Space Treaty), cit. note 689, p. 67 (para. 13).
[863] Ibid., (para. 14).

### 3.9.1.-INTERACTION BETWEEN THE UN CHARTER AND INTERNATIONAL SPACE LAW

The Outer Space Treaty makes reference *expressis verbis* to the UN Charter in Article III. There is a clear common denominator between the Outer Space Treaty and the UN Charter: both strive for peace and security as the main purpose. When several norms regulate the same issue, the principle of harmonisation should be applied ensuring compatibility among the obligations, as the ILC Study Group on the Fragmentation of International Law has adviced.[864] International space law is considered the *lex specialis* in the universe of public international law; thus, the general principle *lex specialis derogat legi generali* applies in case of contradictory provisions. However, Article 103 of the UN Charter provides that in case of conflict between the obligations under the Charter and the obligations under any other international agreement, the provisions of the Charter prevail (*lex superior*).[865]

When it comes to international peace and security in the field of space law, particular attention deserves Article IV of the Outer Space. It is well-established that the Outer Space Treaty has only a partial demilitarisation clause in Article IV first parapraph,[866] which does not prohibit conventional weapons in outer space.[867] In contrast, Article IV second paragraph provides that the Moon and the celestial bodies shall be used *exclusively* for peaceful purposes. By the same token, the Moon Agreement outlaws the threat or use of force on the Moon and celestial bodies. The *argumentum ex silentio* would be that the use of force is completely forbidden on the Moon and the celestial bodies but not in outer space (which is a fallacy). Different views can be exposed here regarding this issue.

Schmitt –one of the Directors of the Woomera Manual on the International Law of Military Space Operations–[868] argued that pursuant to Article III of the Outer Space Treaty, States may use weapons from or against space assets as long as such use is within the exceptions permitted by the UN Charter (i.e. in self-defence or upon a decision of the

[864] UN Doc. A/61/10, cit. note 807, p. 408.
[865] Security Council decisions are also *lex superior*. See UN Doc. A/61/10, cit. note 807, p. 420.
[866] SCHROGL, K-U. AND NEUMANN, J., *Article IV* (Outer Space Treaty), cit. note 567, p. 80 (para 39).
[867] Ibid., p. 71 (para. 3) and p. 80 (para. 39).
[868] The Woomera Manual aims to address and comment extant law applicable to military activities associated with the space domain, see https://law.adelaide.edu.au/. Other similar manuals are: the San Remo Manual (sea), the Harvard Manual (air) and Tallinn Manual (cyberspace).

Security Council).[869] By the same token, von der Dunk postulated that the prohibition on the use of force and its two exceptions are 'imported' to space law via Article III of the Outer Space Treaty.[870] However, when he fleshed out Article 2(4) of the UN Charter, he further scrutinised the wording 'use of force against the territorial integrity or political independence of any state' and its application to the space domain. Since the principle of non-appropriation governs pursuant to Article II of the Outer Space Treaty,[871] he concluded that only State practice, *opinio juris* or the the action of the Security Council will determine if a satellite might be equated with a State's territory for the purposes of the application of the prohibition of Article 2(4).[872] In any case, it should be recalled that Article 2(4) has also the residual formulation 'or in any other manner inconsistent with the Purposes of the United Nations'.

Although a literal reading of Article 42 of the UN Charter does not foresee the possibility of the Security Council making a decision on the use of force in outer space, Lee argued that in such a case States would be bound to comply with that decision due to Articles 25 and 48 of the UN Charter.[873] Moreover, he contended that on the grounds of Article 103 of the UN Charter, States would have to comply with such decision as an obligation that prevails over the space treaties.[874] That commentator explained that the only way to completely include or exclude the use of space force is by amending Articles 42 and 51 of the UN Charter.[875]

On the opposite side, Marko Markov argued that the prohibition on the use of force in outer space emanates from the preamble and Article I of the Outer Space Treaty, which would neutralise the application of Article 51 of the UN Charter.[876] This conclusion –he explained– is supported by the text of Article 103 of the UN Charter, which only provides for obligations and not for rights to prevail over other treaties.[877] Gérardine Goh argued that the annual resolution on international cooperation since the origins of COPUOS is a clear

---

[869] See SCHMITT, M., *International Law and Military Operations in Space*, in BONGDANDY, A. AND WOLFRUM, R. (eds), *Max Planck Yearbook of United Nations Law*, Vol. 10, 2006, pp. 102-103.
[870] VON DER DUNK, F., *Armed Conflicts in Outer Space: Which Law Applies*?, in 'International Law Studies', Vol. 97, 2021, pp. 199 and 208.
[871] Ibid., p. 209.
[872] Ibid., 230.
[873] LEE, R., *The Jus ad Bellum in Outer Space,* cit. note 816, p. 147.
[874] Ibid.
[875] Ibid.
[876] MARKOV, M., *Against the So-Called 'Broader' Interpretation of the Term 'Peaceful' in International Space Law*, Proceedings of the Eleventh Colloquium on the Law of Outer Space, 1968, p.79.
[877] Ibid.

evidence of a customary rule prohibiting the use of force in outer space.[878] Nonetheless, she proposed a protocol to the Outer Space Treaty where the parties would both agree to a prohibition on the use of force in outer space and would acknowledge that nothing in the protocol would impair the inherent right to self-defence.[879]

Despite the absence of a discussion on the topic in COPUOS (although reiterated requests were made by the Russian Federation), some academic commentators agreed that the right to self-defence of Article 51 of the UN Charter applies *in*[880] and *to* outer space[881] but this is far from being universally accepted.[882] The topic came to the forefront during the negotiation of the set of guidelines on long-term sustainability of outer space activities (see chapter 4), in particular in the context of the discussion on the removal of space debris by a State which is not the State of registry. Against this backdrop, some authors linked the prohibition on the use of force with the suzerainty of the State of registry over space objects registered with it.[883]

The most recent development regarding the right to self-defence in outer space at intergovernmental level was the Brussels Summit NATO communiqué, which stated that attacks *to, from*, or *within* outer space could lead to the invocation of Article 5, a decision that would be taken on a case-by-case basis.[884]

Last but not least, the application of the principle of non-intervention to the outer space context has never been properly discussed. Clearly, there is no exercise of State sovereignty in outer space; however, the State of registry exercises jurisdiction and control over the relevant space objects.

---

[878] GOH, G., *Keeping the Peace in Outer Space: a Legal Framework for the Prohibition of the Use of Force*, in 'Space Policy', Vol. 20, 2004, pp. 264-265.
[879] Ibid., see Appendix A.
[880] MAOGOTO, J. AND FREELAND, S., *Space Weaponization and the United Nations*, cit. note 858, p. 1099; RIBBELINK, O., *Article III* (Outer Space Treaty), cit. note 689, p. 65 (para. 2); WOLFF, J., *'Peaceful Uses' of Outer Space has Permitted its Militarization,* cit. note 560, p. 8. See also VON DER DUNK, F., *Armed Conflicts in Outer Space*, cit. note 870, p. 225.
[881] LYALL, F. AND LARSEN, P., *Space Law. A Treatise*, cit. note 687, pp. 511 and 526.
[882] See PETRAS, C., *The Use of Force in Response to Cyber-Attack,* cit. note 632, p. 1249.
[883] See FROEHLICH, A., *The Right to (Anticipatory) Self-Defence in Outer Space to Reduce Space Debris*, in FROEHLICH, A. (ed.) *Space Security and Legal Aspects of Active Debris Removal*, Cham, 2019, pp. 82-83.
[884] Brussels Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021, para. 33, available at https://www.nato.int/ (last accessed on 11 August 2021).

### 3.9.2.-INTERACTION BETWEEN TELECOMMUNICATIONS LAW AND INTERNATIONAL SPACE LAW

This section will deal with a particular branch of international law which is closely related to space law since it governs a specific constituent element of the already explained space systems: the communications segment (up- or downlink). As already explained, this segment comprises the electromagnetic signals between the space asset and the ground station; and in specific cases, the signals between satellites (crosslinks). In order to better understand the legal regime, this section will start by clarifying some necessary concepts in layman language.

This chapter already referred to the up-, down- and crosslink as part of space systems. These types of communications belong to the electromagnetic spectrum; namely, a group of signals of different types. In particular, satellite communications exist in the radio spectrum, which is a part of the electromagnetic spectrum (See figure 5).

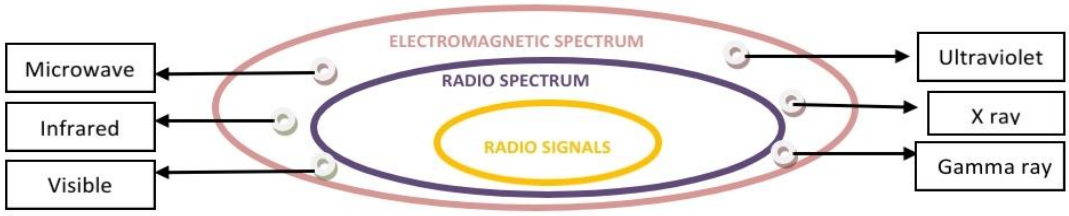


**Figure 5: Electromagnetic spectrum and radio signals**

The International Telecommunication Union (ITU) is an international organisation and a UN specialised agency; and as such, one of the institutions that are part of the global space governance. Its legal framework includes the Constitution, the Convention and the Radio Regulations. While COPUOS was tasked with promoting international cooperation in the peaceful uses of outer space, one of the purposes of the ITU is to promote international cooperation for the improvement and rational use of all kinds of telecommunications. The ITU is divided into three sectors but the Radiocommunication Sector (ITU-R) and the Telecommunication Development Sector (ITU-D) are the most significant for the purposes of this research.

### a) ITU Radiocommunication Sector (ITU-R):

ITU-R is relevant in this research because radiocommunications (up-, down- and crosslinks) are fundamental to space missions. Article 12(1) of the ITU Constitution provides that the role of this sector is to ensure the rational, equitable, efficient and economical use of the radio-frequency spectrum by all radiocommunication services, including those using the geostationary orbit. For its part, Article 44(2) of the same instrument establishes that radio frequencies and associated orbits including the geostationary orbit are limited natural resources and that they must be used rationally, efficiently and economically. Another provision that deserves attention is Article 45(1) of the ITU Constitution, which establishes that all stations –whichever their purpose is– must be established and operated avoiding *harmful interference* to the radio services or communications of other States or of operating agencies. Finally, Article 15(1) of the ITU Radio Regulations forbids unnecessary superfluous, false, misleading or non-identifiable signals.

'Harmful interference' is defined by the annex to the ITU Constitution as 'interference which endangers the functioning of a radionavigation service or of other safety services or seriously degrades, obstructs or repeatedly interrupts a radiocommunication service operating in accordance with the Radio Regulations'.[885] In case of harmful interference, the ITU Constitution provides for bilateral negotiations in Article 56 and in case of failure, recourse to arbitration is possible pursuant to the procedure established in Article 41 of the ITU Convention.

Some technical terms need to be clarified before further explanation: the *wavelength* is the distance between a point in a wave to the identical point in the next. The *frequency* is the number of times the wave goes up and down within a specified time interval; it is measured in Hertz (put simply, if twelve waves are completed in a second, that implies a frequency of 12 Hertz, if four waves are completed in a second, the frequency is 4 Hertz). The higher the frequency, the shorter the wavelength, and *vice versa*: the lower the frequency, the longer the wavelength (See figure 6 below). A group of frequencies is called a *frequency band*. The difference between the maximum and the minimum of a band is the *bandwidth* (for instance, in a band of 600 Mhz, 700Mhz and 800 Mhz; the bandwidth is 800-600=200Mhz).

[885] Constitution of the International Telecommunication Union, cit. note 680. See Annex, 1003.

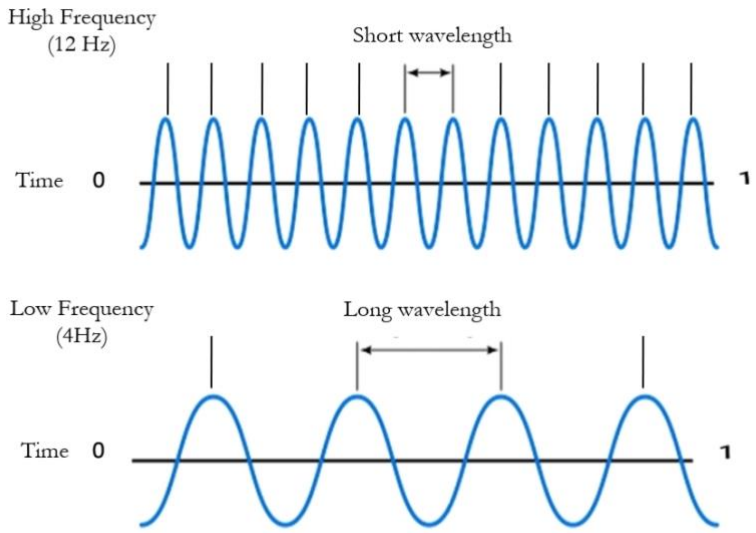


**Figure 6: Signals, frequencies and wavelengths**

One of the functions of the ITU according to Article 1 of its Constitution is to *allocate* bands of the radio-frequency spectrum. This implies their reservation at the international level for their *use* by one or more terrestrial or space radiocommunication services or the radio astronomy service under specified conditions.[886] States reach agreements on this during world or regional radio conferences[887] and then are included in the Table of Allocations provided for in Article 5 of the Radio Regulations.

Once the band is allocated, radio frequencies are *allotted* for use by one or more *administrations* for a terrestrial or space *radiocommunication service*. Designated frequency channels are entered into a plan adopted by the competent conference.[888]

Finally, States have the sovereign prerogative to *assign* a frequency to a particular operator to be used[889] or retain it for State use.[890] In this case, the ITU is responsible for ensuring that such an assignment is in conformity with the Table of Allocations. According

[886] ITU Radio Regulations, Article 1(16).
[887] Constitution of the International Telecommunication Union, cit. note 680, Article 13(1), (2).
[888] ITU Radio Regulations, Article 1(17).
[889] Ibid., Article 1(18).
[890] VON DER DUNK, F., *Legal Aspects of Satellite Communications*, in VON DER DUNK, F. (ed.), *Handbook of Space Law*, Cheltenham-Northampton, 2015, p. 474.

to the information received on assignments, the ITU examines whether there could be interferences. If the assignment is to be found favourable, it is registered in the Master International Frequency Register and future assignments will have to take due account of it to avoid interferences.[891] This registration of radio frequency and orbital locations with the ITU is a mechanism of international coordination to avoid interference and optimise the use of orbits.[892]

In the Minneapolis Plenipotentiary Conference of 1998, the ITU was given competence over orbits for placing satellites. Important is the allocation of slots in the geostationary orbit, an integral part of the outer space (the allocation does not give property rights because this orbit also falls under the provision of non-appropriation of Article II).[893] Satellites placed there constantly remain over the same geographic location and therefore are able to broadcast continuously to a specific region on Earth.

The last point that deserves attention in the context of this research is Recommendation ITU-R S.1003.2, which deals with the environmental protection of the geostationary orbit from space debris.[894]

**b) <u>ITU Telecommunication Development Sector (ITU-D):</u>**

ITU-D was established in 1992 by the Additional Plenipotentiary Conference held in Geneva. There are two contributions from ITU-D to highlight here: one related to cybersecurity and the other one regarding the close link between ICTs and the achievement of the Sustainable Development Goals (SDGs).

As to the former, it is useful to point out that even if the ITU was not originally mandated to deal with security issues (as already explained, one of its purposes was to promote international cooperation), this field was added later on as a result of the the World Summit on Information Society (WSIS), which was an event promoted and managed by the

[891] ITU Radio Regulations, Article 8.
[892] See CHENG, B., *The United Nations and Outer Spac*e, in CHENG, B., Studies in International Space Law, Oxford, 1997. Oxford Scholarship Online Version: March 2012, p. 99.
[893] SCHROGL, K-U. AND NEUMANN, J., *Article IV* (Outer Space Treaty), cit. note 567, p. 61 (paras 70-71). Cfr. Bogota Declaration, which declared that the geostationary orbit is not part of outer space.
[894] Environmental Protection of the Geostationary-Satellite Orbit, Recommendation ITU-R S.1003-2 (12/2010).

ITU.[895] The Declaration of Principles and the Plan of Action (2003) devoted a section to 'building confidence and security in the use of ICTs', and affirmed that information and network security is a prerequisite and a pillar of an 'information society',[896] a concept already addressed in chapter 2. It also considers that cybersecurity should be dealt with at appropriate national and international levels.[897]

Moreover, the ITU crafted a definition of 'cybersecurity', which reads in the following terms: 'Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets'.[898] On that basis, the ITU launched the Global Cybersecurity Agenda in 2007, a framework for international cooperation to enhance confidence and security in the information society. It is important to underscore that the mandate of the ITU in the field of cybersecurity is only limited to the technical and development spheres of cybersecurity.[899]

With regard to the latter; namely, the contribution of ICTs to the SDGs, it is important to mention that UN Secretary-General Guterres recalled the contribution of ICTs in the furtherance of the SDG Goals and emphasised the need to do more to bridge the digital divide and to protect the society from cyberattacks at the World Telecommunication Development Conference 2017 hosted in Buenos Aires (entitled 'ICT for Sustainable Development Goals').[900] The Buenos Aires Declaration (the outcome document of the summit) affirmed that ICTs are a 'key enabler for social, environmental, cultural and economic development'[901] and that they can contribute to attaining the SDGs. This is clearly a point of contact with space assets, since they also play a critical role in the furtherance of socioeconomic development, as already explained in section 3.7.

---

[895] United Nations General Assembly, Resolution 56/183, 21 December 2001, A/RES/56/183, see ops 3 and 1.
[896] Declaration of Principles of the World Summit on Information Society, 12 December 2003, WSIS-03/GENEVA/DOC/4-E, see B.5 (para. 35); Plan of Action of the World Summit on Information Society, 12 December 2003, WSIS-03/GENEVA/DOC/5-E, see section C.5.
[897] Declaration of Principles of the WSIS, cit. note 896, section B.5 (para. 37).
[898] Recommendation ITU–T X.1205, approved on 18 August 2008.
[899] ITU Resolution 130 (Rev. Dubai, 2018).
[900] Final Report of the World Telecommunication Development Conference (WTDC-17), Buenos Aires, Argentina, 9-20 October 2017, available at https://www.itu.int/ (last accessed on 11 August 2021).
[901] Ibid. 27.

In sum, the ITU provides a regime that is applicable to the topic at stake on three counts: First, Article 45 of the ITU Constitution establishes an obligation not to cause harmful interference with radio communications, which is one of the space segments studied above. Second, Recommendation ITU-R S.1003.2 makes clear that when a satellite is at the end of its life in GEO (this may be as a consequence of a malicious cyber activity as explained in section 3.4), it should be removed to the graveyard orbit. Third, the ITU provides relevant elements to promote international cooperation to enhance confidence in the use of ICTs. Most importantly, it provides a working definition of 'cybersecurity' that fits the mandate of a UN organisation that is not tasked with security matters but with international cooperation.

## 3.10.-CONCLUSIONS

In the wake of the space age, space assets were built in ways that presumed their safety, something that led some academic commentators to call space a 'sanctuary from attack'.[902] However, nowadays the reality is completely different and, as the Munich Security Conference 2020 reported, outer space is no longer a sanctuary.[903]

One of the purposes of this chapter was to delimit the concept of 'space cybersecurity' and its scope in order to understand that not every covert malicious activity is a malicious space cyber activity. The previously referred issue is necessary to have a clear understanding that space security –which will be defined in chapter 4, section 4.2– includes several threats, also those falling under space cybersecurity.

This chapter also proposed a classification of malicious space cyber activities, which will be a necessary tool for the research to be carried out in chapter 5. Another step given in this chapter was to substantiate the premise that space systems are *per se* critical infrastructures. This contributes to the assessment of damage to space systems in the broader context of security in the use of ICTs in general. In effect, Chapter 2 put forward the argument by some authors that malicious cyber activities against critical infrastructures might activate the application of Article 51 of the UN Charter under certain conditions. For such

[902] See COLBY, E., *From Sanctuary to Battlefield: a Framework for a U.S. Defense and Deterrence Strategy for Space*, in 'Center for a New American Security', January 2016, p. 7, available at https://www.cnas.org/ (last accessed on 11 August 2021).
[903] Munich Security Conference 2020 (Westlessness), available at https://securityconference.org/ (last accessed on 11 August 2021). See also RAJESWARI PILLAI RAJAGOPALAN, *Electronic and Cyber Warfare in Outer Space*, cit. note 477, p. 12.

conclusion to possibly be transposable to the space domain, it was required to first determine if space systems qualify as critical infrastructures. Although the premise could be verified both in theory and practice, the exercise of self-defence remains as controversial in outer space as in the cyber domain.

The second part of this chapter dealt exclusively with legal matters. Space law, telecommunications law and international law joined in an introduction to the regime applicable to space cybersecurity that will be developed in chapter 5. The sources of international space law were reviewed in this chapter, i.e. the UN space treaties, customary law and *jus cogens* norms. The concept of 'soft law' was discussed in light of the literature, and particular emphasis was made on UNGA resolutions, their normative character and their interpretative value.

The analysis of Article III of the Outer Space Treaty paved the way to the examination of the relations between space law and international law in general. Finally, reference was made to the ITU regime that applies to the intersection of the two realms under examination in this thesis: outer space and cyberspace.

In sum, this chapter has contributed to partially answering **research question 1** (whether there is a regulatory framework applicable to the convergence of the cyber and space domain) and **research question 2** (to what extent space and telecommunications law can be applied to cyber threats against space assets) by explaining the role of the ITU and the telecommunications regime. The former will be complemented by chapter 5, which will ultimately complete the answer. In addition, it has provided the background information on space debris resulting from malicious space cyber activities, which will be useful to continue the analysis on its connection with the long-term sustainability of space activities in the next chapter. Ultimately, this chapter and the next one will answer **research question 6** (how the regulation of space cybersecurity can contribute to the long-term sustainability of outer space activities and the global governance of outer space).

# CHAPTER 4:
# SPACE SECURITY, SAFETY AND SUSTAINABILITY OF OUTER SPACE ACTIVITIES

## 4.1.-INTRODUCTION

The previous chapter has explained the concept of space cybersecurity and proposed a classification of malicious space cyber activities. Such exercise made clear that an important consequence of certain space cyberattacks is the creation of space debris. It also defined the scope of what falls under the more reduced remit of space cybersecurity and distinguished it from the broader field of space security. This chapter will focus on space debris and the link between such threat and the concept of space security, space safety and long-term sustainability of outer space activities.

The proper operation and provision of data and services by space systems may be endangered by both natural phenomena (such as space weather and the impact of asteroids) and human action (kinetic, electromagnetic threats or malicious cyber activities). An additional threat to space assets is space debris, which is even more concerning today when megaconstellations comprised of hundreds of satellites proliferate.

Therefore, the interlinked examination of security, safety and long-term sustainability of outer space activities is a crucial issue that should be addressed with a holistic approach and a comprehensive strategy. This approach touches on issues that somehow or other are considered to fall under the mandate of different multilateral bodies; namely, COPUOS, UNGA First and Fourth Committees; and the Conference of Disarmament. Thus, the international community faces the challenge of dealing with the subject in different venues of negotiation, avoiding duplication of work and maintaining full consistency. On the other hand, the international community needs to strike a balance between working in silos and addressing matters with an integrated approach.

This chapter aims to make a review of the work on security, safety and long-term sustainability of outer space activities taking into consideration the national positions of key space players. To this end, it will review the discussions for negotiating a set of guidelines on the long-term sustainability of outer space activities in COPUOS. It will then outline the draft Code of Conduct of Outer Space Activities proposed by the European Union outside the remits of the UN. The last section of this chapter will address other initiatives related to space security tabled at the Conference on Disarmament and UNGA First Committee, in particular the work on transparency and confidence-building measures in outer space activities, the draft Treaty on the Prohibition of Placement of Weapons in Outer Space and the policy of no first placement of weapons in outer space. The last sub-section of this chapter outlines the practice of joint meetings of UNGA First and Fourth Committees, and makes an assessment of their potentiality in future endeavours on space safety, security and long-term sustainability of outer space activities.

Contents of this chapter were employed as inputs in the publication: JAMSCHON MAC GARRY, L., *Long-term sustainability of outer space activities: achievements and prospects,* in FROEHLICH, A. (ed.), *Space Fostering Latin American Societies* (Part I), 2020.

## 4.2.-TERMINOLOGY

At the outset, this section will make some preliminary clarifications of the terminology that will be used in this research:

**a) Sustainable development, long-term sustainability of space activities, sustainability in outer space and sustainability from outer space:**

It should be recalled that the concept of 'sustainability' dates back to the ancient writers of China, Greece and Rome. It referred to the philosophy of living in harmony with nature and neighbours. In the 17th century, the renowned philosopher Baruch von Spinoza developed the ethical principle *Suum esse conservare*, i.e. the preservation of one's own being in harmony with nature. Closer to our age, in the 70s a report by the Club of Rome[904] entitled 'The Limits to Growth' reached the conclusion that if the growth trends in world population,

[904] The Club of Rome is an international think tank based in Switzerland, with an extra office in Brussels. See https://www.clubofrome.org/about-us/

industrialisation, pollution, food production, and resource depletion continue unchanged, the limits to growth in this planet would be reached in the following century.[905] In order to alter such a result, the report considered it necessary to establish ecological and economic stability that is sustainable far into the future.[906]

But the policy-oriented meaning of 'sustainable development' arose implicitly during the 1972 UN Conference on the Human Environment in Stockholm, which strongly connected the notions of environment and development. The Declaration on the Human Development established in Principle 1 that there is a responsibility to protect and improve the environment for present and future generations.[907] Two years later, the Cocoyoc Declaration expressed the ideal of a world living 'in partnership with nature and in solidarity with future generations'.[908] The 1982 World Charter took up this idea of 'living in harmony with nature' as the basis for development and peace, and also made reference to the preservation of natural resources and ecosystems for present and future generations.[909]

The World Commission on Environment and Development (WCED)[910] contributed in a significant way to the definition of 'sustainable development'. The 1987 report of the WCED entitled 'Our Common Future' defined this concept as the 'development that meets the needs of the present without compromising future generations to meet their own needs'.[911] The reference to the 'future generations' became a rooted notion in the field of environmental law and sustainable development, as acknowledged by the ILC Special Rapparteur on the protection of the atmosphere, Shinya Murase.[912] Judge Cançado Trindade

[905] MEADOWS, D.&D., RANDERS, J. AND BEHRENS, W., *Limits to Growth*, New York, 1972.
[906] Ibid., p. 24.
[907] Report of the United Nations Conference on the Human Environment, Stockholm, 5-16 June 1972, UN Doc. A/CONF.48/14/Rev.1, p. 4.
[908] United Nations Environment Programme: the Cocoyoc Declaration adopted by the participants in the UNEP/UNCTAD Symposium on 'Patterns of Resource Use, Environment and Development Strategies' held at Cocoyoc, Mexico, from 8 to 12 October 1974, p. 6. It is appropriate to point out that this declaration also referred back to the NIEO.
[909] United Nations General Assembly, Resolution 37/7, 28 October 1982, A/RES/37/7 (preamble).
[910] It is also known as the Brundtland Commission (after the name of the Norwegian Prime Minister Ms. Gro Harlem Brundtland, who was the Chair of the Commission). It was established by United Nations General Assembly, Resolution 38/161, 19 December 1983, A/RES/38/161.
[911] Report of the World Commission on Environment and Development (Brundtland Commission), UN Doc. A/42/427, 4 August 1987. Annex 'Our Common Future'.
[912] See International Law Commission, Sixty-ninth Session, Fourth Report on the Protection of the Atmosphere by Shinya Murase, UN Doc. A/CN.4/705, 31 January 2017, para. 87.

referred to the 'future generations' as the 'inter-temporal element' of the precautionary principle[913] in the following terms:

> This temporal dimension is articulated through the formulation of the theory of 'intergenerational equity'; all members of each generation of human beings, as a species, inherit a natural and cultural patrimony from past generations, both as beneficiaries and as custodians under the duty to pass on this heritage to future generations.[914]

After the 1987 report, several instruments contributed to shaping and giving content to the concept of 'sustainable development' which became and remained until nowadays the 'leading concept of international environmental policy'.[915] These instruments are the Rio Declaration (1992), the Convention on Biological Biodiversity (in force since 1993) and the United Nations Framework Convention on Climate Change (in force since 1994),[916] which together with the creation of the Commission on Sustainable Development,[917] were some of the achievements of the Earth Summit.[918] While the Stockholm Declaration of 1972 was the first document on principles of environmental law (Principle 21 became particularly important),[919] the Rio Declaration (particularly Principle 2)[920] became a milestone since this

[913] It should be recalled that the precautionary 'approach' is one of the 'principles' of the Rio Declaration that requires a preventive action from States. See Principle 15 of the Rio Declaration: 'in order to protect the environment, the precautionary approach shall be widely applied by States according to their capabilities'.
[914] *Pulp Mills on the River Uruguay (Argentina v. Uruguay),* Judgement [2010] ICJ Reports 14, 20 April 2010 *('Pulp Mills')*, Separate Opinion of Judge Cançado Trindade, para. 120.
[915] BIRNIE, P., BOYLE, A. AND REDGWELL, C., *International Law & the Environment*, Oxford, 2009, p. 53.
[916] PRASAD, D., *Relevance of the Sustainable Development Concept for International Space Law: An Analysis*, in 'Space Policy', Vol. 47, 2019, p. 167.
[917] The Commission for Sustainable Development was replaced by the High-level Forum on Sustainable Development in 2013, established by United Nations General Assembly, Resolution 66/288, 27 July 2012, A/RES/66/288 ('The Future We Want').
[918] The United Nations Conference on Environment and Development (UNCED) or 'Earth Summit', was held in Rio de Janeiro, Brazil, from 3-14 June 1992.
[919] Principle 21 reads as follows: 'States have the sovereign right to exploit their own resources pursuant to their own environmental policies, and the responsibility to ensure that activities within their jurisdiction or control do not cause damage to the environment of other States or of areas beyond the limits of national jurisdiction'.
[920] Principle 2 reads as follows: 'States have, in accordance with the Charter of the United Nations and the principles of international law, the sovereign right to exploit their own resources pursuant to their own environmental *and developmental* policies, and the responsibility to ensure that activities within their jurisdiction or control do not cause damage to the environment of other States or of areas beyond the limits of national jurisdiction' (emphasis added).

document is said to have contributed to the progressive development of environmental law.[921]

The jurisprudence of the ICJ has also played an important role in the development of this notion. In effect, the Court returned to the definition of sustainable development of 1987 in the Gabčíkovo Nagymaros case (1997). Hungary and Slovakia (then Czechoslovakia) had signed a Treaty in 1977 for the construction of a dam on the River Danube but Hungary –based on environmental arguments regarding the expected volumes of water into the old bed of the Danube and its tributaries– decided to suspend and abandon the works on the Nagymaros project. In reaction to that, Czechoslovakia activated the 'provisional solution' enshrined in the Special Agreement, which led Hungary to request the ICJ to declare that the former was internationally responsible for ensuing loss and damage. There, the Court articulated the *concept* of 'sustainable development' as 'the need to reconcile the economic development with the protection of the environment' and concluded that sustainable development had become a new norm.[922] Interestingly, the ICJ also considered that these 'new' norms and standards should be observed not only in future activities but also in those begun in the past.[923]

In the case of the Pulp Mills (2010) also before the ICJ, Argentina claimed that Uruguay had breached the 1975 Statute with the authorisation, construction and commissioning of two pulp mills on the River Uruguay due to the effects of such activities on the quality of the waters. The ICJ concluded that Article 27 of the 1975 Statute embodied the interconnectedness between the equitable and reasonable use of a shared resource and 'the balance between economic development and environmental protection that is the essence of sustainable development'.[924]

The fact that the ICJ concluded in both cases that the parties concerned should *cooperate* to manage the risks of damage to the environment created by their action is of paramount importance. That conclusion has a particular relevance in space matters, where international cooperation is in effect one of the main pillars of outer space activities, as

[921] VIIKARI, L., *The Environmental Element in Space Law. Assessing the Present and Charting the Future*, Leiden-Boston, 2008, p. 128.
[922] *Gabčíkovo-Nagymaros*, cit. note 284, para. 140.
[923] Ibid.
[924] *Pulp Mills,* cit. note 914, para. 177.

already explained in chapter 3 (see section 3.5). In particular, Article IX of the Outer Space Treaty provides that the principle of cooperation and mutual assistance shall guide space activities and that States shall avoid harmful contamination. This provision should be read in light of the ruling in the Pulp Mills case. There, the ICJ considered that there is an obligation under general international law to conduct impact assessments where there is a risk on a shared resource.[925]

Based on these rulings, a part of the doctrine has considered that sustainable development has a normative character but not a customary one.[926] However, it should be recalled that in the Nuclear Weapons Advisory Opinion (1996), the ICJ acknowledged that the general obligation of States to respect the environment including areas beyond national control (the already referred Principle 21 of the Stockholm Declaration) is 'now part of the corpus of international law relating to the environment'.[927]

Beyond the referred international jurisprudence, additional content has been provided to the concept of 'sustainable development' by the ILA with the New Delhi Declaration of Principles of International Law Relating to Sustainable Development (2002). Particular attention should be given to the principle of equity (second principle), which includes the intra- and inter-generational equity, embedded in the 1987 definition of 'sustainable development'. 'Inter-generational' equity is defined as 'that principle of ordering of the community of mankind which will make it possible for every generation, by virtue of its own effort and responsibility, to secure a proportionate share in the common good of the human species'.[928] 'Intra-generational' equity is formulated as 'the obligation to ensure a just allocation of the utilization of resources among human members of the present generation, both at the domestic and global levels'.[929]

The only space treaty that can be said to encapsulate the notion of sustainable development is the Moon Agreement, presumably influenced by the Stockholm postulates.

---

[925] *Pulp Mills*, cit. note 914, para. 204.
[926] PRASAD, D., *Relevance of the Sustainable Development Concept*, cit. note 916, p. 167; BRECCIA, P., *Article III of Outer Space Treaty and its Relevance in the International Space Legal Framework*, 67th International Astronautical Congress (IAC), Guadalajara, 26-30 September 2016, p. 10.
[927] *Nuclear Weapons*, cit. note 188, para. 29.
[928] ILA Resolution 3/2002: New Delhi Declaration of Principles of International Law Relating to Sustainable Development, in ILA Report of the Seventieth Conference in New Delhi, 2-6 April 2002.
[929] Ibid.

That treaty foresees the obligation of 'due regard to the interests of present and future generations as well as to the need to promote higher standards of living and conditions of economic and social progress and development' (Article 4).

Unlike the Earth's environment, the environment in outer space is less resilient to recovery from damage and more difficult to preserve. The previous chapter has already mentioned that international environmental law also applies to outer space by virtue of Article III of the Outer Space Treaty. Moreover, some authors have interpreted that the principles of inter- and intra-generational equity are implicitly enshrined in Article I of that treaty.[930] Although it is safe to assert that the Outer Space Treaty laid the ground for the application and integration of international environmental law into space law, it should be recalled that it was not until 1999 that the concept of sustainable development became a central topic on the agenda of COPUOS.

Indeed, in that year the environmental and development aspects of space activities came under the spotlight of UNISPACE III. The operative paragraph 3 of the Space Millennium Declaration (the outcome document of the conference) refers to the 'shared objective' of sustainable development. This focus on the *objective* is then collected by the ICJ in the Pulp Mills case in the following terms: 'the need to strike a balance between the use of the waters and the protection of the river consistent with the objective of sustainable development'.[931]

In the 67th International Astronautical Congress, Pierfrancesco Breccia explained that the ICJ had superseded its previous consideration of sustainable development as a *concept* qualifying it as an *objective* in the Pulp Mills case.[932] However, it should be underscored that the ICJ reaffirmed the content of 'sustainable development' outlined in the Gabčíkovo Nagymaros case as a balance between the use and protection of a natural resource (regardless of the qualification either as a concept or as an objective).[933]

---

[930] BRECCIA, P., *Article III of Outer Space Treaty*, cit. note 926, p. 8; Prasad also considered the principle of intra-generational equity to be reflected in Article 1 of the Outer Space Treaty. See PRASAD, D., *Relevance of the Sustainable Development Concept*, cit. note 916, p. 168.
[931] *Pulp Mills*, cit. note 914, para. 177.
[932] BRECCIA, P., *Article III of Outer Space Treaty*, cit. note 926, p. 10.
[933] *Pulp Mills*, cit. note 914, para. 177.

After UNISPACE III, the World Summit of Sustainable Development in 2002 was another important milestone connecting space and sustainable development. This was an event that focused on several challenges, including the conservation of natural resources. The Johannesburg Plan of Implementation explicitly linked space technology and sustainable development.[934]

Thus far, this section has addressed the broad notion of 'sustainable development'. However, this chapter will focus on a narrower one; namely, the 'long-term sustainability of outer space activities'. This terminology has only recently been introduced in COPUOS (see section 4.4) due to an increased awareness of the limited nature of space resources and the multiplication of diverse space actors.[935] In effect, although the STSC has been addressing space debris since 1994,[936] the Space Debris Mitigation Guidelines did not incorporate references to either 'sustainable development' nor 'long-term sustainability of space activities'. However, it might be affirmed that the underlying concept was implicitely incorporated in the background part of the document, which states that mitigation measures are necessary 'towards preserving the outer space environment for future generations'.

When Mark Williamson explained that space ethics consisted of 'what we should and shouldn't do in outer space',[937] he referred to the impact of actions in space on Earth and on the space environment itself. The former encompasses the environmental problems caused on Earth by space activities. These include damage caused on populations and lands located in the surrounding of a launching base due to the propellant rests that are expelled during the launching stage, and harm caused by the chemicals contained in the launching fuel, such as oxides of nitrogen, aluminum and chloride that damage the ozone layer that protects life on Earth from ultraviolet rays.[938]

Regarding the impact of space activities in outer space, Ray Williamson defined a 'sustainable outer space' as 'one in which all humanity can continue to use […] for peaceful

[934] Report of the World Summit on Sustainable Development, including the Plan of Implementation of the World Summit on Sustainable Development, UN Doc. A/CONF.199/20, 4 September 2002, para. 132.
[935] MARTINEZ, P., *Development of an International Compendium of Guidelines for the Long-Term Sustainability of Outer Space Activities*, in 'Space Policy', Vol. 43, 2018, p. 13.
[936] For earlier developments in the field of space debris, see SOUCEK, A., *Negotiation and Drafting History* (SDM Guidelines), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. III), 2015, p. 612 (paras 4-5).
[937] WILLIAMSON, M., *Space Ethics and Protection of the Space Environment*, in 'Space Policy', Vol. 19, 2003, p. 48.
[938] See for instance, VIIKARI, L., *The Environmental Element in Space Law,* cit. note 921, pp. 30 and 31.

purposes and socioeconomic benefit over the long term'.[939] In sum, sustainability *in* outer space should be understood as a synonym with long term-sustainability of space activities as employed in COPUOS; i.e. the preservation of outer space for future generations.

A completely different expression is 'sustainability *on* Earth', developed by ESPI at its 2007 conference. This concept refers to how space tools can help prevent natural disasters on Earth and prepare the world for its new geographical features.[940] For instance, the Charter on Space and Major Disasters contributes to sustainable development *on* Earth since it is a mechanism that makes satellite data and products available to support disaster management.[941]

The previous chapter already described outer space as a global commons (see section 3.5). Now, this chapter will connect that concept with the one of 'sustainable development'. In a famous article, the American biologist Garrett Hardin referred to the 'tragedy of the commons' to demonstrate that 'freedom in a commons brings ruins to all'.[942] In other words 'a commons without governance, […] results in a "tragedy of the commons"'.[943] He explained his theory starting by implicitly making an analogy with the well-known 'security dilemma', a term coined by John Herz in the 50s (the security dilemma is addressed again in section 4.5). Building upon that dilemma, Hardin applied the 'tragedy of the commons' to pollution problems. Broadly speaking, the idea of the tragedy is explained by using the picture of a herdsman in a pasture: the herdsman will try to keep as many cattle as possible on the commons but although every additional animal will benefit him because it will be a source of additional gains, this will overgraze the pasture used by all the other herdsmen and thus spreads the costs. The damage caused is borne by every herdsman, not only by himself. Hardin then concluded that 'each man is locked into a system that compels him to increase his herd without limit in a world that is limited'.[944]

---

[939] WILLIAMSON, R., *Assuring the Sustainability of Space Activities*, in 'Space Policy', Vol. 28, 2012, p. 155.
[940] See ABOU YEHIA, J., *Threats, Risks, and Sustainability—Answers from Space: Results of the ESPI Conference*, in 'Space Policy', Vol. 24, 2008, p. 114.
[941] See FERRETTI, S., FEUSTEL BÜECHL, J., GIBSON, R. et al., *Space for Sustainable Development,* ESPI Report No. 59, Vienna, June 2016, p. 14, available at https://espi.or.at/ (last accessed on 11 August 2021).
[942] See HARDIN, G., *The Tragedy of the Commons*, in 'Science', Vol. 162, No. 3859, 1968, p. 1244.
[943] SADEH, E., *Evolution of Policy and Law for International Space Governance*, cit. note 550, p. 154.
[944] HARDIN, G., *The Tragedy of the Commons*, cit. note 942.

A step further in this theorisation is made by Erin Clancy, who applied the 'tragedy of the commons' developed by Hardin to the *global* commons. Her 'tragedy of the global commons' integrates the concept of sustainable development with the common heritage of mankind. Remarkably, Clancy contended that making an area a common property does not promote its conservation *per se*.[945] On the contrary, she argued that sustainable development and the common heritage principle focus on how States can divide the profits of exploitation instead of on protecting the relevant areas.[946] This situation consequently –she continued– leads to overexploitation and overuse and thus to the tragedy of the global commons.[947]

A more encouraging view was developed by Elinor Ostrom, the first woman awarded with the Nobel Prize in economics. She identified ten variables for the effective use of commons in the absence of a central authority, as a way to counter-argue the idea that they are destined to a tragedy.[948] Roger Hurwitz examined her model and applied it to cyberspace. His essay concluded that if individuals using a commons know that overuse will deteriorate it, they can agree to limit their behaviour, 'providing the costs of coming to agreement and enforcing it are affordable'.[949] This idea is connected with the optimistic assessment made by Katrin Metcalf that 'self-regulation' by relevant private and public stakeholders might be a possible approach to regulate cyber and outer space.[950]

**b) Space security and space safety:**

Sustainability in outer space is closely linked to space security and safety. It should be pointed out that not all languages distinguish semantically between the terms security and safety. The term 'security' is usually understood as the freedom from risk or danger (external aspect) and 'safety' as the condition of being protected from risk or danger or having the control over them (internal aspect).

---

[945] See CLANCY, E., *The Tragedy of the Global Commons*, in 'Indiana Journal of Global Legal Studies', Vol. 5, No 2, 1998, p. 603.
[946] Ibid., pp. 606 and 607.
[947] Ibid., p. 614.
[948] For a deeper analysis of her model, see OSTROM, E., *Governing the Commons: The Evolution of Institutions for Collective Action (Political Economy of Institutions and Decisions),* Cambridge, 1990.
[949] HURWITZ, R., *Depleted Trust in the Cyber Commons*, in 'Strategic Studies Quarterly', Vol. 6, No. 3, 2012, p. 41.
[950] METCALF, K., *A Legal View on Outer Space and Cyberspace*, cit. note 715, pp. 9-10.

The literature defines these terms with certain nuances. Some experts have considered that 'space security' refers to threats caused voluntarily and of aggressive nature.[951] Others have described that notion as being concerned with the absence of unjustifiable man-made or natural threats to space assets.[952] Peter Martinez explained that space actors tend to use that term to refer to the maintenance of order, predictability and safety in space and the avoidance of actions that would ultimately undermine the success of a mission, the operational safety, and the freedom to carry out activities in outer space.[953] The Space Security Index 2019 defined 'space security' in the following terms: 'The secure and sustainable access to, and use of, space and freedom from space-based threats'.[954]

A part of the literature distinguishes three meanings of 'space security': the use of space objects for security and military objectives (outer space for security), security of space objects against risks and natural or man-made hazards (security in outer space) and safety of people and the environment on Earth against natural disasters and risks from outer space (security from outer space).[955] When this research uses the term 'space security', it refers to the second meaning.

The concept of 'space safety' has been given a different meaning. Tronchetti defined the notion as the 'absence or mitigation of risks associated with civilian uses of outer space'.[956] For his part, Marchisio clarified that the term 'safety' mainly means management of risks.[957]

---

[951] See ROBINSON, J., *The Status and Future Evolution of Transparency and Confidence-Building Measures,* in ROBINSON, J., SCHAEFER, M., SCHROGL, K-U., VON DER DUNK, F. (eds), *Prospects for Transparency and Confidence-Building Measures in Space*, ESPI Report No. 27, Vienna, 2010, p. 10.

[952] RATHGEBER, W., REMUSS, N. AND SCHROGL, K-U., *Space Security and the European Code of Conduct for Outer Space Activities*, in 'Disarmament Forum', Vol. 4, 2009, p. 1; REMUS, N., *Space and Security*, in BRÜNNER, C. AND SOUCEK, A. (eds), *Outer Space in Society, Politics and Law*, Vienna, 2011, p. 519; TRONCHETTI, F., *Fundamentals of Space Law and Policy*, cit. note 545, p. 70.

[953] MARTINEZ, P., *Space Sustainability*, in SCHROGL, K-U., HAYS, P., ROBINSON, J., MOURA, D. AND GIANNOPAPA, C. (eds), *Handbook of Space Security. Policies, Applications and Programs*, New York, 2020, p. 2, available at www.swfound.org (last accessed on 11 August 2021).

[954] WEEDEN, B., *Space Security Index 2019*, cit. note 508, see section entitled 'Introduction'.

[955] MAYENCE, J., *Space Security: Transatlantic Approach to Space Governance*, in ROBINSON, J., SCHAEFER, M., SCHROGL, K-U., VON DER DUNK, F. (eds), *Prospects for Transparency and Confidence-Building Measures in Space*, ESPI Report No. 27, Vienna, 2010, p. 35, available at https://espi.or.at/ (last accessed on 11 August 2021). See also: SHEEHAN, M., *Defining Space Security*, cit. note 502, pp. 8 and 10; PELLEGRINO, M. AND STANG, G., *Space Security for Europe*, ISSUE Report No. 29, Paris, 2016, p. 2, available at https://espas.secure.europarl.europa.eu/ (last accessed on 11 August 2021).

[956] TRONCHETTI, F., *Fundamentals of Space Law and Policy*, cit. note 545, p. 44.

[957] See MARCHISIO, S., *Security in Space: Issues at Stake*, in 'Space Policy', 2015, p. 1. See also MARCHISIO, S., *The Final Frontier: Prospects for Arms Control in Outer Space (Global Security Policy Brief)*, European Leadership Network, July 2019, p. 3, available at https://www.europeanleadershipnetwork.org/ (last accessed on 11 August 2021).

From a practical standpoint, safety, sustainability and security are interconnected terms; this is why Martinez uses the abbreviation '3S',[958] which this thesis will borrow and employ to refer to all these concepts in a unified and interrelated manner. However, it is to be borne in mind that this integrated three-pronged conception is a recent development. This is correctly pointed out by Christopher Newman and Mark Williamson, who expressed that 'the Outer Space Treaty remains a creature of its time'.[959] The underlying idea of this phrase is that the Outer Space Treaty only focused on space security; this is why there is no mention of space debris or other threats related to space safety in its text.[960]

**c) Space debris, space debris mitigation, space debris remediation and space traffic management:**

Space debris is one of the most serious threats to the long-term sustainability of outer space activities. The outcome document of UNISPACE II (1982) had already warned about the problem of space debris in the future and thus called for measures.[961] The General Assembly includes a paragraph referring to the problem of space debris in its annual resolution on international cooperation in the peaceful uses of outer space since 1989.[962] Yet, there is neither an international instrument that prohibits its creation nor one that punishes the omission of mitigation or remediation measures.

Likewise, there is no legally binding treaty that defines what space debris is; however, soft law instruments give hints on this concept. For instance, the Guidelines on Space Debris Mitigation of COPUOS (2007) define space debris in the background part as 'all man-made objects, including fragments and elements thereof, *in Earth orbit or re-entering the atmosphere*,

[958] MARTINEZ, M., *Challenges for Ensuring the Security, Safety and Sustainability of Outer Space Activities,* in 'Journal of Space Safety Engineering', 2019.
[959] NEWMAN, C. AND WILLIAMSON, M., *Space Sustainability: Reframing the Debate*, in 'Space Policy', Vol. 46, 2018, pp. 31 and 32.
[960] Ibid.
[961] Report of the Second United Nations Conference on the Exploration and Peaceful Uses of Outer Space, UNISPACE II, UN Doc. A/CONF.101/10, 9-21 August 1982, para. 289.
[962] United Nations General Assembly, Resolution 44/46, 8 December 1989, A/RES/44/46, op. 23; Resolution 45/72, 11 December 1990, A/RES/45/72, op. 23; Resolution 46/45, 9 December 1991, A/RES/46/45, op. 24; Resolution 47/67, 14 December 1992, A/RES/47/67, op. 24 (this resolution also considers that the topic could be an appropriate subject for an in-depth study, see op. 26).

that are non-functional' (emphasis added).[963] This is exactly the same definition that can be found in a position paper of the International Academy of Astronautics (IAA).[964]

These definitions certainly take inspiration from the definition of the Report on Space Debris of the Technical and Scientific Subcommittee of COPUOS (1999), where 'space debris' was defined as follows:

> all man-made objects, including their fragments and parts, whether their owners can be identified or not, *in Earth orbit or re-entering the dense layers of the atmosphere* that are non-functional with no reasonable expectation of their being able to assume or resume their intended functions or any other functions for which they are or can be authorized (emphasis added).[965]

A broader definition had been crafted by the ILA Draft International Instrument on the Protection of the Environment from Damage Caused by Space Debris (1994). In that document, space debris had been defined as 'man-made objects *in outer space*, other than active or otherwise useful satellites, when no change can reasonably be expected in these conditions in the foreseeable future' (emphasis added).[966] Unlike the previous ones, this definition encompasses man-made objects in outer space and not only those in Earth orbit or re-entering the atmosphere. Additionally, it avoided using the 'functionality' criterion to consider a space object as space debris; this is the reason for the additional language 'or otherwise useful'.[967]

In practical terms, space debris includes leaking fuel, paint flakes, tools used during space walks and other waste ejected during space missions, defunct satellites and pieces

[963] United Nations General Assembly, Resolution 62/217, 22 December 2007, A/RES/62/217, para. 26. See 'Background' of the Space Debris Mitigation Guidelines.
[964] Position Paper on Space Debris Mitigation, Implementing Zero Debris Creation Zones, International Academy of Astronautics, ESA, Noordwijk, 15 October 2005, available at http://www.esa.int/ (last accessed on 11 August 2021).
[965] Technical Report on Space Debris, UN Doc. A/AC.105/720, New York, 1999, para. 6.
[966] BOCKSTIEGEL, K-H., *ILA Draft Convention on Space Debris / ILA Konventions-Entwurf zu Weltraumtrummern / Un Projet de Convention de l'ILA sur les Debris Spatiaux*, in 'German Journal of Air and Space Law', Vol. 43, No. 4, 1994, pp. 396-400, Annex 2.
[967] VIIKARI, L., *The Environmental Element in Space Law,* cit. note 921, p. 33.

resulting from collisions, explosions or degradation of space objects.[968] Launchers are the source of the largest population of heavy debris in orbit.[969]

The already referred 2007 Guidelines address space debris 'mitigation'; namely, they foresee measures to avoid the creation of new space debris in *future* space activities. This concept is completely different from space debris 'remediation', which aims to reduce and eliminate *existing* space debris. Remediation mainly aims to remove existing pieces of orbital debris through active debris removal tools (ADR).[970] Taking into consideration Article VIII of the Outer Space Treaty, which provides that space objects are under the jurisdiction and control of the State of registry, any ADR would require the consent of such a State.

ADR is still in its infancy or, in other terms, under development. An example of such active measures is the Clear Space project of the ESA, a start-up led consortium to develop a satellite with four arms to capture and remove space debris from orbit.[971] This project is planned to be launched in 2025. China launched Aolong-1 with robotic arms for grappling other satellites to inspect or service them in 2016. Although these capabilities are peaceful, there are still concerns as to the possibility of transforming ADR into a threat for space security.[972]

The last notion that this section will address is 'space traffic management' –a concept very much connected to space safety and long-term sustainability of space activities. Similarly to the case of 'space debris', there is no legally binding instrument providing a definition for this term. The IAA crafted a definition in 2006 for the first time in the following terms: 'a set of technical and regulatory provisions for guaranteeing safe access to outer space, operations in outer space and return from outer space to Earth free from physical or radio frequency interference'.[973]

---

[968] Ibid., p. 32.
[969] Position Paper on Space Debris Mitigation, cit. note 964, p 31.
[970] POPOVA, R. and SCHAUS, V., *The Legal Framework for Space Debris Remediation as a Tool for Sustainability in Outer Space*, in 'Aerospace', Vol. 5, 2018, pp. 7-8.
[971] For more information, see https://clearspace.today/
[972] U.S.-China Economic and Security Review Commission (2019), cit. note 650, p. 383.
[973] CONTANT-JORGENSEN, C., LÁLA, P. AND SCHROGL, K-U., (eds), *Cosmic Study on Space Traffic Management*, Paris, 2006, p. 17, available at www.iaaweb.org/ (last accessed on 11 August 2021). See also LALÁ, P., *Study on Space Traffic Management by the International Academy of Astronautics,* in POWERS, J. (ed.), *Celebrating the Space Age*, UNIDIR Conference Report, Geneva, 2-7 April 2007, p. 180.

NASA drafted a definition of 'space traffic safety' (*safety* instead of management) as follows:

> [f]reedom from those conditions in orbital space that may lead to incidents resulting in harm (death or injury to astronauts and spaceflight participants, damage to public welfare, damage or loss of spacecraft, interference to spacecraft). Incidents of specific concern are collisions or orbital breakups.[974]

For its part, the German space agency (Deutsches Zentrum für Luft- und Raumfahrt) defined 'space traffic management' in a white paper entitled 'Implementation of a European Space Traffic Management System' as follows:

> Execution of all necessary Managing and Monitoring & Control Operations (including routine and contingency scenarios) to ensure safe ballistic travel of manned and unmanned Suborbital Space Vehicles (SSVs) and spaceplanes through Near-Earth space and airspace under consideration of the existing European Air Traffic Management System and Infrastructure.[975]

The topic was incorporated for discussion as a single issue on the agenda of the Legal Subcommittee of COPUOS in 2015.[976] That year, a workshop on the matter was organised by the IISL and the European Centre for Space Law (ECSL), where the Chief of Space Services of the ITU, Yvon Henri, explained in his presentation that: 'Space Traffic Management provides an approach to enter into, operate in and return from space, safe from any interference'.[977]

As correctly pointed out in a paper of the IISL entitled 'Space Traffic Management: Top Priority for Safety Operations', despite the variety of definitions, they all focus on safety,

---

[974] BROWN, O. et al., *Orbital Traffic Management Study – Final Report*, National Aeronautics and Space Administration (NASA) and Science applications International Corporation (SAIC), 21 November 2016, available at https://www.spacepolicyonline.com/ (last accessed on 11 August 2021).
[975] TÜLLMANN, T. et. al., *On the Implementation of a European Space Traffic Management System*, DLR GfR, June 2017, p 1, available at https://elib.dlr.de/ (last accessed on 11 August 2021).
[976] Report of the 57th Session of COPUOS (2014), UN Doc. A/69/20, para. 283.
[977] HENRI, Y., *Frequency Management and Space Traffic Management*, presentation available at https://www.unoosa.org/ (last accessed on 11 August 2021).

space debris and the space environment.[978] This is the reason why this concept is as important in this research as the 3S.

Last but not least, very much connected to the 3S is the characterisation of the space environment with the abbreviation '3C' (congested, contested and competitive).[979] The American Ambassador Gregory Schulte –then Deputy Assistant Secretary of Defense for Space Policy– clarified these concepts in a presentation he gave in Singapore. There, he explained that space is becoming congested due to increasing space debris, contested because an expanding number of States is creating counterspace capabilities and competitive due to increasing space actors.[980]

## 4.3.- SPACE DEBRIS MITIGATION GUIDELINES: THE BOTTOM-UP APPROACH

Section 4.2 has just differentiated between the impact of space activities on Earth and in outer space. This is an important distinction to start addressing space debris since their effects can endanger the environment on Earth or in outer space. The incident of Cosmos 954 is a clear example of the potential that space debris has to bring about environmental damage on Earth. In effect, the Soviet satellite disintegrated and scattered radioactive debris over a large area in Northern Canada.[981]

However, more significant for this research is the impact of space debris *in* outer space. There are two critical incidents that are usually mentioned when it comes to space debris:

**a) The Chinese Anti-satellite:**

[978] See TAIATU, C., *Space Traffic Management: Top Priority for Safety Operations*, 60th IISL Colloquium on the Law of Outer Space, Adelaide, 26 September 2017, p. 3, available at https://iislweb.org/ (last accessed on 11 August 2021).
[979] See, for instance, Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities, UN Doc. A/68/189, 29 July 2013, para. 6.
[980] SCHULTE, G., *Protecting Global Security in Space*, Presentation at the S. Rajaratnam School of International Studies Nanyang Technological University, Singapore May 9, 2012, available at https://archive.defense.gov/ (last accessed on 11 August 2021).
[981] For a thorough analysis of the liability issues involved, see JAKHU, R., *Iridium-Cosmos Collision and its Implications for Space Operations*, in SCHROGL, K-U., RATHGEBER, W., BARANES, B. AND VENET, C. (eds), *Yearbook on Space Policy 2008/2009*, Vienna-New York, 2010, pp. 255 ff.

The Chinese anti-satellite test (ASAT) deliberately targeted and destructed a non-functional weather satellite Fengyun 1, also from China. As a result of this activity carried out in 2007, the number of space debris increased in an amount comparable to the previous 14 years of space activity.[982] Although the literature tends to reiterate this test as a kind of landmark in the space debris records, it should be noted that this anti-satellite test was actually not the first one in history. To the contrary, the United States tested the first anti-satellite in 1959[983] but demonstrated self-restraint in developing ASATs during the first twenty years of the space age[984] due to the signing of the Anti-Ballistic Missile Treaty (ABM) and the first Strategic Arms Limitation Talks (SALT I).[985] This scenario changed under the Ford Administration, when the first legislation enabling the American ASAT programme was enacted.[986] During the 80s, the Cold War tensions made ASATs grow in importance.[987] In those years, UNGA Resolution 36/97C (1981) already expressed in its preamble concerns about the threat posed by anti-satellite systems and put the prohibition of them as a topic on the agenda of the UNGA 37th session.[988]

This description clearly reveals that the Chinese ASAT test in 2007 was not the first one in history, let alone the last one. In effect, in 2008 the United States conducted Operation Burnt Frost to destroy a satellite with modified missile defence technology that was falling out of orbit.[989] On 27 March 2019, India –prompted by the 2007 ASAT conducted by its perennial adversary–[990] conducted Mission Shakti and thus became the fourth State to test an ASAT. As an explanation for this mission, India submitted that the aim was to verify its capability to safeguard its space assets. In a speech delivered on the very same day, the Prime Minister of India Bharat Mata ki Jai announced that the country had accomplished the

---

[982] PARDINI, V. AND ANSELMO, L., *Evolution of the Debris Cloud Generated by the Fengyun-1c Fragmentation Event,* 2007, p. 1, available at https://ntrs.nasa.gov/ (last accessed on 11 August 2021).
[983] HARRISON, T., JOHNSON, K. AND ROBERTS, T., *Space Threats Assessment 2019*, cit. note 476, p. 25.
[984] See PETRAS, C., *The Use of Force in Response to Cyber-Attack,* cit. note 632, p. 1223.
[985] Ibid., pp. 1222-1223.
[986] Ibid., p. 1224.
[987] See JAKHU, R., *Iridium-Cosmos Collision*, cit. note 981, p. 264. See article entitled *Bold Orion Weapons System 199 (WS-199B*), available at https://www.globalsecurity.org/ (last accessed on 11 August 2021).
[988] United Nations General Assembly, Resolution 36/97C, 9 December 1981, A/RES/36/97C.
[989] JOHNSON-FREESE, J., *A Space Force Mission for the Global Commons of Space*, in 'SAIS Review of International Affairs', Vol. 36, No. 2, Summer-Fall 2016, p. 9. That author considered that missile defensive tests are more acceptable than ASATs (see p. 12).
[990] SET, S., *India's Space Power: Revisiting the Anti-Satellite Test*, Carnegie Endowment for International Peace, September 2019, available at https://carnegieendowment.org/ (last accessed on 11 August 2021).

mission with indigenous technology, which was a matter of pride for every Indian.[991] Nonetheless, he assured the international community that India had no intention of threatening anyone. He underscored that the test was 'an effort to secure a fast growing India', emphasised that his country rejected the weaponisation of outer space and an arms race in it, and concluded that the test would not in any way change that position.[992] This is an important message since it conveyed that India had reached the technological level of a select team of space powers.

The most recent ASAT test was allegedly carried out on 15 July 2020. The United States Space Command accused the Russian Federation of having conducted a non-destructive test of a space-based anti-satellite device.[993] Compared to the one previously mentioned, this one was entirely conducted in space; i.e. another space object was injected into orbit from Cosmos 2543 instead of being launched from the ground (these threats are usually described as 'space-to-space capabilities'). In response to these accusations, the Kremlin Spokesman Dmitry Peskov affirmed that the Russian Federation had been and continued to be focused on the complete demilitarisation of outer space.[994]

**b) The Collision of Iridium 33 and Cosmos-2251:**

The second incident that this section will point at is the accidental collision on 10 February 2009 between Iridium 33 (a satellite built by an American company and launched into space by a Russian Proton from Kazakhstan) and Cosmos-2251 (a Russian State-owned communications satellite),[995] which brought about 1875 catalogued break-up pieces larger than 10 cm.[996]

Although these incidents are relatively recent, as early as 1978 the famous American Astrophysicist Donald Kessler created a model to prove that the increase in satellites would

[991] Speech by Prime Minister on 'Mission Shakti', India's Anti-Satellite Missile test conducted on 27 March, 2019, available at https://mea.gov.in/ (last accessed on 11 August 2021).
[992] Ibid.
[993] Space Command Public Affairs Office, *Russia Conducts Space-Based Anti-Satellite Weapons Test*, 23 July 2020, available at https://www.spacecom.mil/ (last accessed on 11 August 2021).
[994] See article entitled *Russia Committed to Full Demilitarization of Outer Space*, 24 July 2020, available at https://tass.com/ (last accessed on 11 August 2021).
[995] See WEEDEN, B., *Iridium-Cosmos Collision*, Fact Sheet, updated November 10, 2010, available at https://swfound.org/ (last accessed on 11 August 2021). See also JAKHU, R., *Iridium-Cosmos Collision*, cit. note 981, p. 254.
[996] Ibid.

lead to an increase in space debris caused by intentional and unintentional malfunctions that would cause further collisions increasing the emerging space debris.[997] This model is widely known as the Kessler Syndrome or the Kessler Effect.

In 1999 the Scientific and Technical Subcommittee of COPUOS delivered the already referred technical report on space debris, which assessed that 'man-made space debris today poses little risk to the successful operations'.[998] Twenty years later, the scenario has changed completely, which is confirmed by the amount of work devoted to the issue currently at COPUOS.[999]

The work on a set of guidelines for space debris mitigation started at a technical level and was carried out by a group of space agencies, gathered in the Inter-Agency Space Debris Coordination Committee (IADC).[1000] Some authors considered this precedent as an example to follow in the field of space security –this would mean starting the work with a like-minded group before engaging in a wider debate.[1001]

The technical discussions concluded in 2002 with a short but concise non-legally binding document. It contains several definitions followed by guidelines that encompass launch, mission and disposal phases of spacecrafts for the reduction of space debris in normal operations and break-ups in orbit. They also pursue measures for passivation of stored energy.[1002] Guideline 5.2.3 deserves particular attention since it recommends avoiding intentional destruction of a spacecraft and other harmful activities.

---

[997] KESSLER, D. AND COUR-PALAIS, B., *Collision Frequency of Artificial Satellites: The Creation of a Debris Belt*, in 'Journal of Geophysical Research', Vol. 83, No. A6, 1978, p. 2637.
[998] UN Doc. A/AC.105/720, cit. note 965, para. 136.
[999]Space debris is addressed in both the STSC and LSC. It is also included in the yearly UNGA resolution on international cooperation and was also included in the UNISPACE+50 UNGA resolution.
[1000] Italian Space Agency (ASI), British National Space Centre (BNSC), Centre National d'Etudes Spatiales (CNES), China National Space Administration (CNSA), Deutsches Zentrum für Luft-und Raumfahrt (DLR), European Space Agency (ESA), Indian Space Research Organisation (ISRO), Japan, National Aeronautics and Space Administration (NASA), National Space Agency of Ukraine (NSAU) and Russian Aviation and Space Agency (Rosaviakosmos).
[1001] PELLEGRINO, M. , PRUNARIU, D. AND STANG, G., *Security In Space: Challenges to International Cooperation and Options for Moving Forward*, 67th International Astronautical Congress (IAC), Guadalajara, 26-30 September 2016, p. 13, available at https://swfound.org/ (last accessed on 11 August 2021).
[1002] Inter-Agency Space Debris Coordination Committee Space Debris Mitigation Guidelines, UN Doc. A/AC.105/C.1/L.260, 29 November 2002.

The guidelines were revised and adopted by COPUOS in 2007.[1003] If both versions (IADC and COPUOS) are compared, the one annexed to the 62nd session report of COPUOS does not include the terms and definitions of the IADC version (except for the already mentioned definition of space debris placed in the background part). IADC guidelines 5.1 (on the limitation of debris release during normal operations) and 5.2 (on the prevention of on-orbit break-ups) are similar to COPUOS guidelines 1 and 2; and IADC guideline 5.2.3 (on avoidance of intentional destruction and other harmful activities) is similar to COPUOS guideline 4. IADC guidelines 5.3.2 (on objects passing through the LEO region) and 5.3.1 (post-mission disposal from GEO) are encapsulated in COPUOS guidelines 6 and 7. IADC guideline 5.2.1 (on the post mission break-ups resulting from stored energy) and 5.4 (on the prevention of on-orbit collisions) are contained in COPUOS guidelines 5 and 3. None of the instruments includes active space debris removal.

Space debris has become very topical in the discussions on the long-term sustainability of outer space activities because of the cumulative effect that will inevitably affect future generations: space debris at an altitude of 1.000 km can remain in orbit for a thousand years until re-entry in Earth, and space debris in the geostationary orbit (36.000 km) can take millions of years to come down.[1004] The higher the altitude where space debris is located the longer its lifespan in orbit.[1005]

The examination of the legal aspects of space debris at the LSC was an issue for which the ILA had been advocating during its 46th and 47th sessions in 2007 and 2008, respectively.[1006] In 2008, the agenda of the LSC included a single item entitled 'General Exchange of Information on National Mechanisms relating to Space Debris Mitigation Measures'.[1007] In 2010 and 2011, the Czech Republic proposed an agenda item to transform the guidelines into a set of principles on space debris to be elaborated by the LSC,[1008] but the proposal did not meet consensus. The item on general exchange of information, however,

---

[1003] Report of the 50th Session of COPUOS (2007), UN Doc. A/62/20, Annex.
[1004] See JAKHU, R., *Iridium-Cosmos Collision*, cit. note 981, p. 261.
[1005] WRIGHT, D., *Orbital Debris Produced by Kinetic-Energy Anti-Satellite Weapons*, in POWERS, J. (ed.), *Celebrating the Space Age*, UNIDIR Conference Report, Geneva, 2-7 April 2007, p. 161.
[1006] Information on the Activities of International Intergovernmental and Non-Governmental Organizations Relating to Space Law, UN Doc. A/AC.105/C.2/L.265, 16 January 2007 and A/AC.105/C.2/L.270, 25 January 2008.
[1007] Report of the 47th Session of the LSC (2008), UN Doc. A/AC.105/917, para. 150.
[1008] Report of the 49th Session of the LSC (2010), UN Doc. A/AC.105/942, paras 169 and 170(h); Report of 50th Session of the LSC (2011), UN Doc. A/AC.105/990, para. 163.

remained on the agenda until the present days. Upon a joint initiative of Germany, the Czech Republic and Canada in 2013, a compendium of space debris mitigation standards adopted by States and international organisations is published on a dedicated page of the website of the OOSA since 2014 and is periodically updated.[1009]

Now, why is space debris important in a research focused on space cybersecurity? This section has just outlined that space debris may be caused by collisions and these collisions may be intentional (for instance, the Chinese ASAT) or unintentional (for instance, the Iridium-Cosmos collision). As explained in the previous chapter, there are several malicious space cyber activities that might lead directly or indirectly to the creation of space debris. Consequently, space cybersecurity should be considered a necessary premise in space debris mitigation policies.

## 4.4.-SUSTAINABILITY ON THE AGENDA OF COPUOS: A DECADE OF WORK ON THE LONG-TERM SUSTAINABILITY (LTS)

The most remote precedent of the intention to address topics related to LTS in a more integrated manner within COPUOS can be traced back to 2001-2003, during the STSC chairmanship of Karl Doetsch (Canada).[1010]

Some years later, the French delegation proposed including an agenda item on long-term sustainability at the STSC of COPUOS in 2009.[1011] This new agenda item entitled 'Long-term sustainability of space activities' was mainly focused on space debris and its impact on space traffic.[1012] Noteworthily, the French delegate Gerard Brachet had already proposed the topic when he was Chair of COPUOS during the period 2006-2007.[1013] However, the issue was not ready for discussion at that time.

[1009] See Compendium of Space Debris Mitigation Standards adopted by States and International Organizations, UN Doc. A/AC.105/C.2/2019/CRP.14, 5 April 2019. The last updated compendium is dated 17 June 2021.
[1010] See MARTINEZ, P., *Development of an International Compendium*, cit. note 935, p. 14.
[1011] Report of the 52nd Session of COPUOS (2009), UN Doc. A/64/20, para. 161.
[1012] Report of the 46th Session of the STSC (2009), UN Doc. A/AC.105/933, 2009, para. 80.
[1013] Future Role and Activities of COPUOS (submitted by the Chair), UN Doc. A/AC.105/L.268, 10 May 2007; Future Role and Activities of the Committee on the Peaceful Uses of Outer Space (submitted by the Chair), UN Doc. A/AC.105/L.268 Corr. 1, 1 June 2007.

The original proponents of the topic had suggested a bottom-up approach. This method implied discussions initiated at a technical level so that when a draft was submitted to the decision-making level, it would be easier to achieve agreements instead of reopening the negotiated text.[1014] A clear example of such an approach is the already referred Space Debris Mitigation Guidelines of COPUOS, one of the instruments of soft law that made a significant contribution to the 3S in 2007, fifty years after the launch of Sputnik 1.

From the beginning, the idea of negotiating a set of guidelines on the long-term sustainability of space activities was to complement the existing regime with a non-binding instrument rather than amending the treaties. In such an endeavour, it was important to take into account the new reality and challenges in the space field. The guidelines had to promote monitoring, communication and international cooperation in order to avoid future collisions, interference and disruption of satellite information, and safeguard the regular operation of space missions.

At that time, an informal group of countries interested in the subject began to meet with OOSA and ESA. The group focused on threats and natural causes of disturbances affecting space systems (space weather, solar eruptions and micrometeorites, for instance).[1015] In those days, it was not foreseen to include issues such as jamming, spoofing or malicious space cyber activities. The STSC was dealing with space debris as a separate topic on the agenda since 1994,[1016] an effort that reached its highest point with the adoption of the referred Space Debris Mitigation Guidelines of COPUOS.

These precedents paved the way to putting the topic of LTS on the agenda of the STSC, which was delayed until 2010. The topic gained momentum after the already referred collision of Iridium 33 with Cosmos-2251 (this is another example of reactive regulation of space law, as referred to in chapter 3, section 3.8.2). Once the issue was added on the agenda of the STSC, a specific working group was established under the chairmanship of Peter Martinez (from South Africa),[1017] which held sessions until 2018.

---

[1014] BRACHET, G., *The Origins of the Long-term Sustainability of Outer Space Activities*, in 'Space Policy', Vol. 28, 2012, p. 162.
[1015] Long-term Sustainability of Activities in Outer Space (France), UN Doc. A/AC.105/C.1/L.303, 9 February 2010.
[1016] Report of the 31st Session of the STSC (1994), UN Doc. A/AC.105/571, paras 63-74.
[1017] Report of the 47th Session of the STSC (2010), Doc. A/AC.105/958, paras 181, 182.

The United States provided a complement to the French proposal by suggesting to divide the topics into four clusters,[1018] which led to the establishment of four expert groups within the Working Group on LTS:[1019] Expert Group A (on sustainable space utilisation supporting sustainable development on Earth), Expert Group B (on space debris, space operations and tools to support collaborative space situational awareness), Expert Group C (space weather) and Expert Group D (on regulatory regimes and guidance for actors in the space arena). While these expert groups were a kind of deliberative body, the Working Group was instead the negotiating body.[1020]

In those years, the eight Millennium Development Goals were an excellent catalyst for the work on sustainable development viewed from the broader scope of the agenda of the United Nations. In particular, Goal 7 (aimed at maintaining environmental sustainability) was much connected to the goals of LTS proposed in COPUOS.

After 2015, a new UN global agenda with its 17 Sustainable Development Goals (SDGs) replaced the driving force of long-term sustainability at COPUOS. This agenda was not particularly focused on developing countries as the previous one but on the entire international community. LTS was reinforced by the UNISPACE+50 process, which enhanced the idea of space as a driver for socioeconomic development. UNISPACE+50 can be considered the most important event in COPUOS since UNISPACE III in 1999. Its *leitmotiv* was the commemoration of the 50th anniversary of the First Conference on Exploration and Peaceful Uses of Outer Space (UNISPACE I, in 1968).

As a result of the UNISPACE+50 high-level segment held on 18 and 19 June 2018, COPUOS adopted a resolution which was approved by the General Assembly without a vote. Its paragraph four encourages States to:

> […] continue to promote and actively contribute to strengthening international cooperation in the peaceful uses of outer space and the global governance of outer

[1018] Long-term Sustainability of Outer Space Activities (United States), UN Doc. A/AC.105/C.1/2011/CRP.17, 7 February 2011.
[1019] Terms of Reference and Methods of Work of the Working Group on the Long-term Sustainability of Outer Space Activities of the Scientific and Technical Subcommittee, UN Doc. A/AC.105/C.1/L.307, 24 January 2011, para. 24; Nominations of Members of Expert Groups and List of Points of Contact Communicated to the Secretariat as of 9 June 2011, UN Doc. A/AC.105/2011/CRP.15 and Add. 1, 9 June 2011.
[1020] MARTINEZ, P., *Space Sustainability*, in SCHROGL, K-U., HAYS, P., ROBINSON, J., MOURA, D. AND GIANNOPAPA, C. (eds), *Handbook of Space Security. Policies, Applications and Programs*, New York, 2015, p. 265.

> space activities, addressing challenges to humanity and sustainable development, ensuring *the long-term sustainability of outer space activities* and facilitating the realization of the 2030 Agenda for Sustainable Development, taking into account the particular needs of developing countries;[1021] (emphasis added)

While the most ambitious goal for COPUOS would have been to achieve consensus on the guidelines on long-term sustainability before UNISPACE+50, adopt them in that session and then refer them to the General Assembly later that year, unfortunately that could not be achieved even in a long negotiation at the 55th session of the STSC. Despite that heated meeting in 2018, States achieved more flexible positions in 2019, which enabled the adoption of the first set of guidelines by COPUOS and the endorsement by the General Assembly, concomitantly with the celebration of the fiftieth anniversary of the first man on the Moon.

As the following sections will depict, the guidelines have both strong and weak points. Although the adoption of this first set of guidelines should be regarded as an important achievement, the truth is that it is an incomplete one. Disagreement on the mandate and irreconcilable positions on core issues are a clear signal that both procedural and substantial issues are still to be settled.

### 4.4.1.- THE GRULAC PROPOSAL: THE RATIONALE BEHIND THE WORDING 'ONLY'

During the 52nd session of the STSC in 2015, the Group of Latin American and the Caribbean (GRULAC) endorsed and made own a proposal originally submitted by Brazil with the following elements: first, it proposed to include a definition of 'long-term sustainability of outer space activities' in the preamble built upon the outcome document of the Conference on Sustainable Development Rio+20, entitled 'The Future We Want'.[1022]

The definition that the GRULAC had originally proposed articulated the idea that sustainability was a need to adjust the objectives of access, exploration and use of outer space *only* for peaceful purposes with the need to preserve and protect the environment taking into

[1021] United Nations General Assembly, Resolution 73/6, 26 October 2018, A/RES/73/6.
[1022] A/RES/66/288, cit. note 917.

account the needs of future generations.[1023] However, this wording did not reach consensus and LTS was finally defined as follows:

> the ability to maintain the conduct of space activities indefinitely into the future in a manner that realizes the objectives of equitable access to the benefits of the exploration and use of outer space for peaceful purposes, in order to meet the needs of the present generations while preserving the outer space environment for future generations.[1024]

Secondly, the GRULAC proposal suggested including in those guidelines that provided that national legislation should be consistent with international space law, that States review and amend legislation contradicting such standards. It also suggested adding language to the effect that States could not invoke national interest or national legislation to carry out actions contrary to space governance.

Finally, the GRULAC proposed including a new guideline that could be labelled as a 'non-proliferation clause', whereby States should commit to developing space activities *solely* for peaceful purposes through their national legislation. That guideline had to be complemented with an amendment in another guideline including explicit language to reaffirm the importance of preventing an arms race in outer space.

The first and third proposals had a common denominator, which was that outer space activities had to be preserved *only/solely* for peaceful purposes. Unfortunately, that raised old discussions on how States interpret 'peaceful uses of outer space'.[1025]

---

[1023] Comments and Proposed Amendments to the Updated set of Draft Guidelines for the Long-term Sustainability of Outer Space Activities (submitted by the GRULAC), UN Doc. A/AC.105/C.1/2015/CRP.19/Rev.1, 9 February, 2015.
[1024] Report of the 62nd Session of COPUOS (2019), UN Doc. A/74/20, Annex II, para. 5.
[1025] GASPARINI ALVES, P., *Prevention of an Arms Race in Outer Space. A Guide to the Discussions in the Conference of Disarmament*, UNIDIR/91/79, New York, 1991, Part I, p. 12, available at https://www.unidir.org/ (last accessed on 11 August 2021); FREELAND, S., *The Laws of War in Outer Space*, in SCHROGL, K-U., HAYS, P., ROBINSON, J., MOURA, D. AND GIANNOPAPA, C. (eds), *Handbook of Space Security. Policies, Applications and Programs*, New York, 2015, p. 95; GRIMAL, F. AND SUNDARAM, J., *The Incremental Militarization of Outer Space,* cit. note 566, p. 51; WOLTER, D., *The Peaceful Purpose Standard,* cit. note 544, p. 123.

The second part of the GRULAC proposal prospered; thus, review and amendment of national regulatory frameworks as needed was included in section II.A of the guidelines (dedicated to policy and regulatory framework for space activities).[1026]

The third of the proposals was the most difficult to agree on. In fact, up to the time of concluding this research States have been unable to reach consensus on a non-proliferation clause (which for much of the negotiations until the adoption of the first set of guidelines was guideline 7). As already advanced, the proposal brought about some issues around the term 'solely'. Firstly, delegations discussed whether to employ the word 'only',[1027] 'exclusively'[1028] or 'solely', and exchanged views on whether any difference in the meaning existed among these formulations. In that regard, reference was made to the text of UNGA Resolution 1348 (XIII), which employed the word 'only'. However, other delegations argued that such language had been overcome in successive documents and that the Outer Space Treaty did not include that terminology. It is important to point out that the reference to outer space for 'exclusively' peaceful purposes has also been employed several times in PAROS resolutions.[1029]

An intersessional meeting was convened between 5 and 9 September 2015 where guideline 7 was again discussed along with the inclusion of the non-weaponisation of outer space. The arguments against its inclusion were basically three: the absence of a definition of 'weapons', the lack of agreement on the issue at the Conference on Disarmament and the mandate of COPUOS.

---

[1026] UN Doc. A/74/20, cit. note 1024, guidelines A.1 and A.2.
[1027] A/RES/1348 (XIII), cit. note 694. See first preambular paragraph.
[1028] This term was included originally in UNGA Resolution 1148 (XII): United Nations General Assembly, Resolution 1148 (XII), 14 November 1957, A/RES/1148 (XII), op. 1(f). The wording 'exclusively for peaceful purposes' is also used in Article IV second paragraph of the Outer Space Treaty (1967), which originated in a similar wording contained in Article 1 of the Antarctic Treaty (1959): 'Antarctica shall be used for peaceful purposes only'. Note, however, that Article IV of the Outer Space Treaty only provides for the complete demilitarisation of the Moon and other celestial bodies, but not of outer space. This was then confirmed in Article 3 of the Moon Agreement (1979). Years later, this wording was taken up in the UN Convention on the Law of the Sea (1982), which provides in Article 141 that '(t)he Area shall be open to use exclusively for peaceful purposes'.
[1029] See for instance: United Nations General Assembly, Resolution 38/70, 15 December 1983, A/RES/38/70, op. 1; Resolution 40/87, 12 December 1985, A/RES/40/87, op. 2; Resolution 42/33, 30 November 1987, op. 2; Resolution 44/112, 15 December 1989, A/RES/44/112, para. 1. From 1990 onwards this reference was eliminated.

The best result for the GRULAC would have been to include in this guideline the non-weaponisation, a commitment to avoid an arms race and a reference to the report of the GGE on TCBMs in outer space activities (see section 4.5).[1030] It is important to recall that according to its terms of reference, the Working Group on LTS had to consider appropriate linkages with the work of the GGE on TCBMs in outer space activities –this again provides evidence that the work of UNGA First and Fourth Committees is tightly linked. However, the aspirations from the GRULAC were not welcomed and various alternatives were evaluated, including reproducing the text of Article IV of the Outer Space Treaty.[1031]

In June 2016, the mandate of the Working Group on LTS was about to expire and no consensus on several guidelines (including guideline 7) and the preamble had been achieved. Based on the mandate granted by COPUOS in 2015, the Chair of the Working Group prepared a working paper for the 2016 session. That was the last one before the submission of the document to the plenary meeting later that year, as the original mandate foresaw. In that document, he broke down the guidelines into three categories: guidelines on which the Working Group on LTS was very close to achieving consensus, guidelines for which the Working Group might reasonably expect to achieve consensus within the existing work plan (guideline 7 was in this group) and guidelines for which the Working Group might find it difficult to achieve consensus on all their constituent elements within the existing work plan.[1032]

The final disussions of the Working Group on LTS concluded within the framework of the 53rd session of the STSC in 2016 with a deadlock caused by the differences between the States that wanted to submit the first set of guidelines to the consideration of COPUOS and extend the mandate to address the remaining ones, and those who preferred to extend the mandate without adopting a first set. In that scenario, the future of the guidelines became uncertain.

---

[1030] UN Doc. A/68/189, cit. note 979.

[1031] On Article IV, see FREELAND, S., *The Laws of War in Outer Space*, cit. note 1025, p. 95. See also WILLIAMS, M., *Safeguarding Outer Space: on the Road to Debris Mitigation,* in *Security in Space: The Next Generation—Conference Report*, 31 March–1 April 2008, UNIDIR, 2008, p. 84, available at https://unidir.org/ (last accessed on 11 August 2021). Professor Williams considered that Article IV of the Outer Space Treaty contains 'obscure provisions concerning the demilitarization and denuclearization'.

[1032] Ideas for the Way Forward on the Draft Set of Guidelines for the Long-Term Sustainability of Outer Space Activities (submitted by the Chair), UN Doc. A/AC.105/C.1/2016/CRP.3, 28 January 2016.

Having held the second intersessional meeting on 6 and 7 June, States agreed on twelve guidelines at the 59th session of COPUOS in 2016.[1033] This 'first set' of guidelines would be ready for implementation by States and international organisations. In the same meeting, COPUOS agreed upon to annex the first set of guidelines to the report of the session and extend the mandate of the Working Group on LTS for two additional years to work on the preamble and a second set of guidelines as a priority. Both sets of guidelines would form a compendium that would be referred in 2018 to the General Assembly (as already advanced, that was the year of the UNISPACE+50 celebration).[1034]

Between 19 and 23 September 2016, the third intersessional meeting took place and a provisional definition of LTS was achieved. However, guideline 7 continued without reaching consensus.

The fourth intersessional meeting was held in the margins of COPUOS at its 60th session in 2017. The examination of the definition of LTS continued but the inclusion of the word 'solely' and the reference to the non-placement of weapons were firmly resisted. The same happened at the fifth intersessional meeting (2 to 6 October 2017) but this time the reference to Article IV of the Outer Space Treaty (incorporated in previous sessions) was deleted.

After five intersessional meetings, the penultimate chance to negotiate was the 55th session of the STSC in 2018. The possibilities of including guideline 7 in the compendium to be referred to the General Assembly were at that stage very limited. The United States was unwilling to address it arguing policy reasons and Brazil did not give up addressing non-weaponisation.

The possibility of including the content of that guideline in the report –with which the compendium would be submitted to COPUOS– was also considered. However, it was clear that in such a case, the contents of guideline 7 would not be part of the compendium itself. The choice between a flexible position and submitting –at least– the partial results of many years of work to COPUOS and a rigid one, remaining without any end-product, became increasingly apparent. That dilemma caused a situation where no decision could be

[1033] Report of the 59th Session of COPUOS (2016), UN Doc. A/71/20, para. 130.
[1034] Ibid, para. 137.

made on a mechanism to submit the guidelines to the General Assembly, to review and incorporate new guidelines and to consider pending guidelines.

In the margins of the 61st session of COPUOS in 2018, the Working Group on LTS continued in session but to no avail. The United States objected treating several guidelines proposed by the Russian Federation and guideline 7. For its part, the Russian Federation was not in a position to agree to adopt a compendium that did not include some of the guidelines considered necessary by that delegation.

Regarding the product of eight years of work, the Russian delegate (after recalling that his country had submitted several working documents) indicated that agreed and pending guidelines should be annexed to the report of COPUOS for consideration of the General Assembly. For its part, the G77 and China made a statement calling for consensus and encouraging the inclusion of the elements discussed in the Working Group on LTS into the Space Agenda 2030. Australia, Canada, France, Germany, Israel, Italy, Japan, the Netherlands, New Zealand, the United Kingdom and the United States submitted a working document expressing their willingness to have the agreed guidelines translated into all the UN official languages and referred to the 73rd General Assembly session in 2018.[1035]

In a tense meeting, COPUOS was unable to reach an agreement on how to proceed. As a result, the work of the previous eight years remained in limbo: the agreed guidelines would not be referred to the General Assembly, nor was there agreement on future work on the seven remaining guidelines[1036] or on a mechanism for its implementation, review and incorporation of new ones.

The issue was taken up again in the 56th session of the STSC in 2019, where the Russian Federation submitted a joint proposal with China to establish a working group to address the pending guidelines. However, other delegations considered that a new working group was not necessary. On the contrary, they argued that States should directly commit to

[1035] Proposal on Long-Term Sustainability of Space Activities (Australia, Canada, France, Germany, Israel, Italy, Japan, the Netherlands, New Zealand, the United Kingdom, and the United States), UN Doc. A/AC.105/2018/CRP.26/Rev.2, 29 June 2018.
[1036] Draft Guidelines for Long-term Sustainability of Activities in Outer Space (submitted by the Chair), UN Doc. A/AC.105/C.1/L.367, 16 July 2018.

implement the 21 agreed guidelines. It was also argued that it was premature to decide on a working group.

In an attempt at conciliation in that meeting, Switzerland proposed organising a workshop at the beginning of the 62nd session of COPUOS in June 2019 to exchange views on the future work and possible mechanisms to address the remaining guidelines. In the same vein, South Africa proposed submitting the 21 agreed guidelines to the upcoming session of the General Assembly for its approval. In addition, that delegation proposed a mechanism to address the remaining ones, revise and implement the existing ones and incorporate others. That delegation also proposed that Brazil, as future Chair of COPUOS together with South Africa initiate informal consultations with interested delegations in order to be able to present a proposal for future work at the 62nd session in 2019.

The COPUOS session of 2019 was decisive for the future of the guidelines. Switzerland organised the proposed workshop on the first day of the session. Then, it became clear that it was necessary to continue working on LTS within the framework of COPUOS and its Subcommittees.[1037] The delegations of Canada, France, Japan, the United Kingdom and the United States submitted a working paper with a proposal to create a working group to implement the 21 agreed guidelines.[1038]

The United Arab Emirates submitted a proposal to establish a working group to continue working on sustainability.[1039] The Russian Federation, China, Nicaragua, Pakistan and Belarus submitted a joint proposal on the working modalities of a future working group on the subject.[1040] The substantial difference between these two proposals was that the latter explicitly included in the mandate the consideration of the seven guidelines that had not reached consensus until then (among which is old guideline 7). COPUOS finally adopted the 21 guidelines and the preamble, which were annexed to the session report, and established a

[1037] Meeting Hosted by Switzerland on Possible Further Work on the Long-Term Sustainability of Outer Space Activities: Background and Chair's Summary, UN Doc. A/AC.105/2019/CRP.16, 18 June 2019.
[1038] Proposal for the Establishment of a Working Group on Implementation of Agreed Guidelines on Long-Term sustainability (Canada, France, Japan, the United Kingdom, and the United States), UN Doc. A/AC.105/2019/CRP.7/Rev.1, 19 June 2019.
[1039] Proposal on Long-Term Sustainability of Outer Space Activities of the Committee on the Peaceful Uses of Outer Space (United Arab Emirates), UN Doc. A/AC.105/2019/CRP.13, 13 June 2019.
[1040] Proposal on the Modalities of the Working Group on the Long-Term Sustainability of Outer Space Activities of the Committee on the Peaceful Uses of Outer Space (Belarus, China, Nicaragua, Pakistan and the Russian Federation), UN Doc. A/AC.105/2019/CRP.10/Rev.2, 20 June 2019.

working group under a five-year work plan.[1041] These 21 guidelines have been labelled by the Chair of the Working Group on LTS as the 'low-hanging fruit of the LTS discussions'.[1042]

The final decision of COPUOS on the setup of a working group struck a balance between the three proposals since the mandate encompasses implementation and incorporation of new guidelines taking into account existing documents, including the seven pending guidelines. The STSC could not make a decision on the composition of the bureau, the terms of reference and work plan in its 57th session in 2020.[1043] Only in its 58th session and after informal consultations facilitated by South Africa, the STSC was finally able to appoint Umamaheswaran R. (India) as Chair of the Working Group on LTS, which was convened under the relevant agenda item.[1044] Until the moment of submitting this thesis, no decision was made on the terms of reference, methods of work and work plan of the working group.

All in all, the balance of the work on LTS is positive since the adopted preamble includes a definition of 'long-term sustainability of outer space activities' and provides for the review and amendment of national space legislation that runs counter to the international governance regime. However, the result is not entirely as expected since the reference to the use of outer space *only, solely* or *exclusively* for peaceful purposes did not reach consensus. Moreover, in the current context, it seems difficult to expect consensus on a clause that goes beyond the terms of Article IV of the Outer Space Treaty to provide for a total ban on the weaponisation of outer space.

### 4.4.2.-THE DRAFT GUIDELINES ON SPACE CYBERSECURITY: A PENDING ISSUE

In addition to the three segments of space systems already identified in chapter 3, this chapter will incorporate the user segment, i.e. the legal or natural person (public or private) that makes use of satellite products, such as imagery, information and reports. Note that there is a difference between data and information, which is clarified in the Principles Relating to Remote Sensing of the Earth from Outer Space: information is the processed

[1041] UN Doc. A/74/20, cit. note 1024, para. 165.
[1042] MARTINEZ, P., *Space Sustainability* (2020), cit. note 953, p. 14.
[1043] Report of the 57th Session of the STSC (2020), UN Doc. A/AC.105/1224, para. 195.
[1044] Report of the 58th Session of the STSC (2021), UN Doc.A/AC.105/1240, para. 195.

data made thus usable.[1045] The identification of these segments in this chapter is crucial to better understand the proposals for additional guidelines on space cybersecurity. Chapter 2 already outlined the role of the Russian Federation in the furtherance of the work on ICTs at UNGA First Committee. Against this backdrop, it is easier to understand the rationale behind the Russian initiatives on space cybersecurity in the framework of LTS at COPUOS.

In 2015, the Russian delegation submitted to the Working Group on LTS a document that built upon the idea that certain actions regarding information and communications technologies in space might qualify as aggressive actions.[1046] In the annex to that document, the Russian Federation expressly mentioned the use of software and hardware to affect functional characteristics of a space object.[1047]

In another document, the Russian delegation proposed the first draft guideline on what this research qualifies as 'space cybersecurity'. The aim of the Russian draft proposal was to discourage embedded instruments or software to interfere or gain unauthorised access into information systems of foreign space objects. It also foresaw a State obligation to provide assurances against that practice. Moreover, the proposal required States controlling the absence of such malicious instruments or software when validating safety and security of operations.[1048] As negotiations evolved, a draft guideline on space cybersecurity was finally incorporated in the (then) draft LTS Guidelines. Although it was apparently based on the Russian proposal, the language differed substantially from it. In effect, draft guideline 9.1 was crafted in terms of prevention of malicious ICT tools or techniques.[1049] The obligations envisaged in the Russian proposal were not included in the draft compendium.

---

[1045] A/RES/41/65, cit. note 839, see principles c) and d). On this issue, see SOUCEK, A., *International Law*, cit. note 545, p. 368.
[1046] Achievement of a Uniform Interpretation of the Right of Self-Defense in Conformity with the United Nations Charter as applied to Outer Space as a Factor in Maintaining Outer Space a Safe and Conflict-Free Environment and Promoting the Long-Term Sustainability of Outer Space Activities (Russian Federation), UN Doc. A/AC.105/C.1/2015/CRP.22, 2 February 2015, p. 2.
[1047] Ibid., Annex.
[1048] Additional Considerations and Proposals aimed at Building up Understanding of the Priority Aspects, Comprehensive Meaning, and Functions of the Concept and Practices of Ensuring the Long-Term Sustainability of Outer Space Activities (Russian Federation), UN Doc. A/AC.105/C.1/2015/CRP.24, 2 February 2015, p. 5.
[1049] UN Doc. A/AC.105/C.1/L.367, cit. note 1036.

The Russian Federation returned to the issue of unauthorised access to hardware or software in other documents.[1050] In a working document submitted in 2016, the Russian Federation pointed at the 2015 report of the GGE on ICTs, in particular paragraph 13 (i), which recommends that States take measures to ensure the security of the supply chain and prevent the proliferation of ICT malicious tools and techniques.[1051] This proposal became reflected in draft guideline 9.2.[1052]

Considering the already referred space systems segments, it is possible to deduce that the focus of draft guideline 9 was the *space segment*. The underlying concern of the Russian delegation appears to have been the protection of spacecraft from malicious software or hardware during the whole supply chain, which includes the production of parts and elements of satellites, launchers, space stations and the assembly construction, launching and operation of space objects.

Yet draft guideline 18 seems to focus on the *ground segment*. Its first paragraph recommends that States recognise that ground infrastructures are critical for the safety of space operations and for the LTS of outer space activities.[1053] The second and third paragraphs aim to strengthen the integrity and resilience of those infrastructures, to improve the ability to recover from disruption and to cooperate for those purposes. Then, the fourth paragraph seeks to avoid that States and international intergovernmental organisations interfere with the other's infrastructures when protecting their own. The fifth paragraph aims to promote cooperation in preventing, identifying, investigating and deterring malicious usage of ICTs and other activities that may endanger or disrupt these infrastructures. The last paragraph encourages information exchange to strengthen integrity and resilience of such infrastructures.

Finally, the Russian Federation made also a proposal to ensure the reliability of the *user segment* (but with the limited scope of information shared by States and international

[1050] Submission of the Russian Federation to the United Nations Committee on the Peaceful Uses of Outer Space on the subject-matter 'Identification of Cross-Links between the Recommendations Contained in the Report of the Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities and the Topic of Developing Guidelines on the Long-Term Sustainability of Outer Space Activities', UN Doc. A/AC.105/C.1/2015/CRP.33, 9 February 2015, para. 4.
[1051] Reviewing Opportunities for Achieving the Vienna Consensus on Space Security Encompassing Several Regulatory Domains (Russian Federation), UN Doc. A/AC.105/C.1/2016/CRP.15, 16 February 2016, p. 10.
[1052] UN Doc. A/AC.105/C.1/L.367, cit. note 1036.
[1053] Ibid.

intergovernmental organisations). Thus, with a great deal of detail, the Russian delegation suggested creating a centre for information on space events and objects under the auspices of the UN. The motivation for such an initiative was explained 'by the desire to safeguard the interests of the international community in obtaining information that may be needed for the analysis and interpretation of events'.[1054] All possible concerns related to the concept of 'information security' that the Russian Federation had addressed at UNGA First Committee were included in this proposal (completeness, reliability and accuracy of information;[1055] and reliability of the software and hardware used for the storage and dissemination of information).[1056] The draft guideline foresaw that data would be hosted in two servers (one for storing information and one for user applications).[1057] It should be underscored that the idea behind this proposal was not a novel issue. Indeed, France had made similar proposals to establish a centre of information at the Conference on Disarmament in the early 90s.[1058] The Russian delegation also contrasted this proposal with the Central Point of Contact proposed in the European draft CoC.[1059] The Europeans had envisaged establishing the referred Central Point of Contact to discharge functions relating to notifications, exchange of information, maintenance of an electronic database and communications system and channel for consultations.[1060] Although the European draft CoC provided that the subscribing parties would designate the Central Point of Contact, it did not provide any criteria for either its composition or its duration. This proposal has not been incorporated as a draft guideline yet.

Beyond the already mentioned proposals made by the Russian Federation, there is no other initiative at the multilateral level seeking to address concretely space cybersecurity.

---

[1054] Long-Term Sustainability of Outer Space Activities (Basic Elements of the Concept of Establishing a Unified Centre for Information on Near-Earth Space Monitoring under the Auspices of the United Nations and the Most Topical Aspects of the Subject Matter) (Russian Federation), UN Doc. A/AC.105/L.290, 4 March 2014, para. 3.

[1055] Considerations on the Sum Total of Prime Requisites and Factors that should shape the Policy of International Information Sharing Serving Safety of Space Operations (Russian Federation), UN Doc. A/AC.105/C.1/2016/CRP.14, 16 February 2016.

[1056] Proposal on the Review and Consideration of the Concept of a United Nations Information Platform Serving Common Needs in Collecting and Sharing Formation on Near-Earth Space Monitoring in the Interests of Safety of Space Operations, and its Architectural and Programmatic Aspects (Russian Federation), UN Doc. A/AC.105/C.1/2015/CRP.32, 9 February 2015.

[1057] UN Doc. A/AC.105/L.290, cit. note 1054.

[1058] Study on the Application of Confidence-Building Measures in Outer Space: Report by the Secretary-General, UN Doc. A/48/305, 15 October, 1993, paras 205 and 292.

[1059] UN Doc. A/AC.105/C.1/2016/CRP.14, cit. note 1055, para. 2.

[1060] See Part 9 of the Draft CoC.

The Russian delegation did not convince the Working Group on LTS about these guidelines. The only consolation prize that the Russian Federation still has is that the mandate of the new Working Group on LTS (see section 4.4.1) includes the consideration of document A/AC.105/C.1/L.367 as a basis for future negotiations. This means that discussions on draft guideline 9, 18 and the information centre might be resumed anytime.

## 4.5.-TRANSPARENCY AND CONFIDENCE-BUILDING MEASURES (TCBMs): POLITICAL COMMITMENTS AS A SOFT LAW TOOL

This section will be broken down into two parts: the first one will explain the security dilemmas as the origin and engine of TCBMs. The second part will outline the evolution of the multilateral mechanisms to address them.

**a) The security dilemmas:**

This chapter has briefly referred to the security dilemma in section 4.2 above. More specifically, the security dilemma explains the fact that when States try to become secure from external threats, they increase their military defence. Thus, they increase the insecurity of others which need in turn to increase their own security, making the former more insecure and so on (in terms of John Herz this is 'the vicious circle of security and power accumulation').[1061] The result is that the international community in general becomes more insecure and the likelihood of conflict increases.

Something similar happens in the cyber domain and is thoroughly explained by Buchanan. That expert in cybersecurity adapted the security dilemma and applied it to the cyber field, creating what he has termed the 'cybersecurity dilemma'.[1062]

Likewise, it is possible to conclude that in the space domain, there is the 'space security dilemma'. Finally, the intersection between the 'space security dilemma' and the 'cybersecurity dilemma' gives rise to the 'space cybersecurity dilemma'. Ultimately, it is all about the chain consisting of actions, perceptions and reactions that affect international

[1061] HERZ, J., *Idealist Internationalism and the Security Dilemma*, in 'World Politics', Vol. 2, No. 2, 1950, p. 157.
[1062] See BUCHANAN, B., *The Cybersecurity Dilemma. Hacking, Trust, and Fear between Nations*, Oxford, 2016.

peace and security. This context information is necessary to understand why NATO considers space and cyberspace operational domains (see chapter 2, section 2.2 and chapter 3, section 3.5) and why several States have set up space forces or commands as military units (see chapter 3, section 3.7). This can be summarised in the Latin adage *si vis pacem, para bellum* (translated as 'if you want peace, prepare for war').

This part started by introducing these dilemmas because it will argue that the security dilemma (in all its variations) can be considered to be the origin and engine of TCBMs. In effect, the security dilemma is built upon a chain of States' perceptions that can effectively be dispelled by TCBMs (see figure 7).

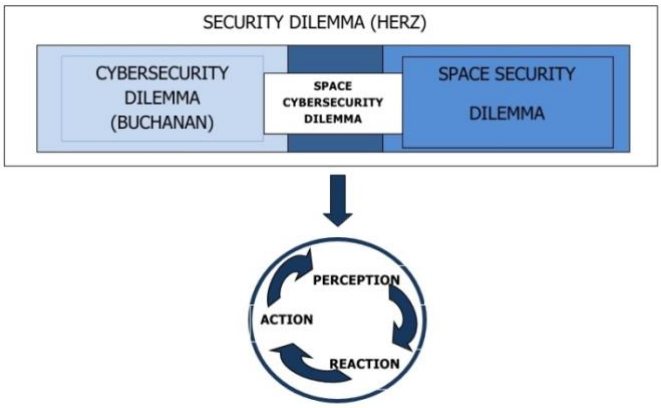


**Figure 7: Security dilemmas as the origin of TCBMs**

**b) Evolution of the mechanisms at the United Nations:**

The concept of 'TCBMs' was introduced by the Russian Federation at UNGA First Committee in 2005.[1063] This tool can be defined as governmental measures to exchange information to enhance trust and reduce misunderstandings, misperceptions and miscalculations, and thus prevent confrontation and military escalation and promote international stability. Such measures can take various forms and names, such as good practices, codes of conduct, guidelines or rules of conduct.[1064] They are in principle non-

[1063] AOKI, S., *Law and Military Uses of Outer Space*, in JAKHU, R. AND DEMPSEY, P. (eds), *Routledge Handbook of Space Law*, London - New York, 2017, p. 213.
[1064] ROBINSON, J., *SpaceTransparency and Confidence-Building Measures,* in SCHROGL, K-U., HAYS, P., ROBINSON, J., MOURA, D. AND GIANNOPAPA, C. (eds), *Handbook of Space Security. Policies, Applications and Programs*, New York, 2015, p. 294.

legally binding and voluntary in nature; however, they might be binding if they are part of a mandatory agreement.

It is possible to discern four moments in the evolution of TCBMs in outer space activities:

1. The first moment: 1990-1993

This period encompasses the years between 1990 and 1993, when UNGA First Committee included the topic of confidence-building measures in outer space (CBMs) on its agenda for the first time and requested the Secretary-General to carry out a study on them with the assistance of governmental experts.[1065] The Secretary-General produced a report in 1993 entitled 'A Study on the Application of Confidence-Building Measures in Outer Space' (hereinafter, '1993 report of the GGE on CBMs').[1066] It is important to note that some of the initiatives that this thesis outlines refresh similar old proposals made at the Conference on Disarmament which were reflected in the 1993 report, such as a space code of conduct proposed originally by France (see section 4.6)[1067] and the setup of a centre on information of space objects (see section 4.4.2).[1068] The General Assembly adopted UNGA Resolution 48/74B taking note of the 1993 report of the GGE on CBMs and commending it to the attention of all Member States.[1069]

2. The second moment: 2005-2008

Later on, a second period started in 2005. Since then, the Russian Federation has tabled a draft resolution on TCBMs in outer space activities yearly, inviting member States to express their views on the advisability of further work. In 2005, UNGA First Committee adopted Resolution 60/66 by a recorded vote of 158 to 1 against (the United States) and 1 abstention (Israel),[1070] which introduced an agenda item to deal with the matter.[1071] The United States voted against successive UNGA resolutions on the topic until 2008.

[1065] United Nations General Assembly, Resolution 45/55B, 4 December 1990, A/RES/45/55B.
[1066] UN Doc. A/48/305, see cit. note 1058.
[1067] Ibid., paras 196-201.
[1068] Ibid., para. 205.
[1069] United Nations General Assembly, UNGA Resolution 48/74B, 16 December 1993, A/RES/48/74B.
[1070] Report of the First Committee of UNGA 60th Session (2005), UN Doc. A/60/463, para. 34.
[1071] United Nations General Assembly, Resolution 60/66, 8 December 2005, A/RES/60/66.

3. The third moment: 2009-2017

A third moment started in 2009 with the changes in the US Administration, which were somehow reflected in a more cooperative position of that country with regard to TCBMs in outer space activities. In 2009, the yearly UNGA Resolution on this matter was adopted without a vote[1072] and in 2010 with the abstention of the United States (see below).[1073] In 2011 and 2012, the resolution on TCBMs was interrupted and resumed in 2013. From 2013 until 2017[1074] all UNGA resolutions on this topic were adopted without a vote.[1075] This position seems to be in line with the US National Security Space Strategy (2011) adopted during the second term of President Obama, which stated: '[t]he United States will support development of data standards, best practices, transparency and confidence-building measures, and norms of behaviour for responsible space operations'.[1076]

During this period, at the annual conference of the Institute of Disarmament Research (UNIDIR) in 2010, the Deputy Permanent Representative at the Permanent Mission of the Russian Federation to the United Nations in Geneva Victor Vasiliev spoke on TCBMs in outer space activities. He proposed creating a GGE on TCBMs in outer space activities as a way to facilitate the ultimate goal that should be a legally binding treaty on the prevention of an arms race in outer space.[1077] This was the prelude to UNGA Resolution 65/68, which was adopted with 183 votes in favour and the abstention of the United States (referred to above). The resolution requested the Secretary-General to establish a GGE with geographical representation to elaborate a report on TCBMs in outer space activities and decided to include a tentative agenda item on that matter.[1078] This was the second GGE on the topic (the first one had been established in 1993 as described above).

[1072] United Nations General Assembly, Resolution 64/49, 2 December 2009, A/RES/64/49.
[1073] United Nations General Assembly, Resolution 65/68, 8 December 2010, A/RES/65/68.
[1074] There were no resolutions on TCBMs in outer space activities activities in 2011 and 2012.
[1075] United Nations General Assembly, Resolution 68/50, 5 December 2013, A/RES/68/50; Resolution 69/38, 2 December 2014, A/RES/69/38; Resolution 70/53, 7 December 2015, A/RES/70/53; Resolution 71/42, 5 December 2016, A/RES/71/42 and Resolution 72/56, 4 December 2017, A/RES/72/56.
[1076] US National Security Space Strategy, January 2011, unclassified summary available at https://www.dni.gov/ (last accessed on 11 August 2021).
[1077] Space Security 2010 from Foundations to Negotiations, UNIDIR Conference Report, Geneva, 29-30 March 2010, pp. 19-20, available at https://www.unidir.org/ (last accessed on 11 August 2021).
[1078] A/RES/65/68, cit. note 1073.

The GGE on TCBMs in outer space activities comprised experts from 15 countries (many of whom were national delegates to COPUOS) [1079] and met three times (one in 2012 and two in 2013). In 2013, it produced a report with recommendations on TCBMs to promote the 3S, including exchange of information on space, promotion of international cooperation, notification and information on launches, space debris, potential collisions and other hazards to space objects.[1080] In the conclusions, the GGE on TCBMs in outer space activities supported efforts to achieve political commitments to encourage responsible behaviour in space; and among the examples cited, it mentioned 'a multilateral code of conduct' (possibly referring to the European initiative).[1081]

The same year, the General Assembly welcomed the report of the GGE on TCBMs in outer space activities, called upon States to review and implement the measures contained therein and referred the recommendations of the report to COPUOS, the Conference on Disarmament and the Disarmament Commission.[1082]As already advanced above, that was the first one of a series of UNGA resolutions on TCBMs in outer space activities that were adopted without a vote.

4. The fourth moment: 2018 till the present

The fourth and last moment in this chronology started in 2018. In terms of voting, this period represents a setback because the annual resolution on TCBMs in outer space activities was no longer adopted without a vote. In 2018, the United States and Israel voted against UNGA Resolution 73/72.[1083] In 2019, UNGA Resolution 74/67[1084] was adopted again with two votes against (the United States and Israel) and 6 abstentions (Australia,

[1079] Brazil, Chile, China, France (Gerard Brachet, former Chair of COPUOS and promoter of the inclusion of sustainability on the agenda of COPUOS), Italy (Sergio Marchisio, former Chair of the Expert Group D on space governance), Kazakhstan, Korea, the Russian Federation, Nigeria, Romania, South Africa (Peter Martinez, former Chair of the Working Group on LTS), Sri Lanka, Ukraine, the United Kingdom, and the United States.
[1080] UN Doc. A/68/189, cit. note 979.
[1081] Ibid., para. 69.
[1082] A/RES/68/50, cit. note 1075 (adopted without a vote).
[1083] United Nations General Assembly, Resolution 73/72, 5 December 2018, A/RES/73/72. Voting record: (180-2-1), United Nations General Assembly 73rd Session (2018), UN Doc. A/73/PV.45, para. 51.
[1084] United Nations General Assembly, Resolution 74/67, 12 December 2019, A/RES/74/67. Voting record: (173-2-6), United Nations General Assembly 74th Session (2019), UN Doc. A/74/PV.46, p. 54.

Georgia, Liberia, Palau, Ukraine and the United Kingdom) and in 2020, also with 2 against and 6 abstentions (Australia, Georgia, Palau, Spain, Ukraine and the United Kingdom).[1085]

If the 1993 report of the GGE on CBMs and the 2013 report of the GGE on TCBMs are compared, it is possible to conclude that the core ideas of the first report remained untouched twenty years later in the second report. One of such untouched considerations is that TCBMs can contribute to, but not act as a substitute for, measures to monitor the implementation of arms limitation and disarmament agreements.[1086] An additional element in common is the need to establish working contacts[1087] and coordination between COPUOS and the Conference on Disarmament.[1088] In fact, the 2013 report kicked off the joint meetings of UNGA First and Fourth Committees[1089] (an issue that will be further addressed in section 4.7.3).

The 2013 report acknowledged that TCBMs contribute to the 3S.[1090] In addition, it reviewed all the endeavours of the international community linked to security, safety and sustainability: the work carried out by COPUOS on LTS, the efforts undertaken by the European Union on a draft CoC, the policy of no first placement of weapons and the Sino-Russian proposal for a Treaty on the Prevention of the Placement of Weapons in Outer Space (the following sections will be devoted to them). The group of governmental experts considered that the LTS Guidelines could be considered TCBMs or might be the technical basis for implementation of other TCBMs.[1091] Finally, the report concluded with a series of recommendations on TCBMs in outer space activities, which mainly address information exchange, capacity-building, outreach, consultations, visits, coordination and cooperation.

[1085] United Nations General Assembly, Resolution 75/69, 7 December 2020, A/RES/75/69. Voting record: (176-2-6), United Nations General Assembly 75th Session (2020), UN Doc. A/75/PV.37, p. 45.
[1086] UN Doc. A/48/305, see cit. note 1058, p. 105; UN Doc. A/68/189, cit. note 979, paras 28 and 33.
[1087] UN Doc. A/48/305, see cit. note 1058, para. 329.
[1088] UN Doc. A/68/189, cit. note 979, para. 72.
[1089] Ibid.
[1090] Ibid., paras 25, 31,
[1091] Ibid., para. 13.

## 4.6.-THE DRAFT EUROPEAN CODE OF CONDUCT ON SPACE ACTIVITIES (CoC): A TOP-DOWN APPROACH

Simultaneously with the process that was going on at COPUOS, the European Union –eager to become an active global space player– was working on a draft code of conduct on space activities. The main difference with the sustainability process at COPUOS was that the European exercise was a top-down initiative; i.e. with a more political rather than technical approach.[1092]

In 2002, after several failed attempts to regulate arms control in outer space at the Conference on Disarmament, the Henry L. Stimson Center proposed a code of conduct containing a roadmap for the responsible use of outer space,[1093] built around the idea of 'no harmful interference' with space objects (that was a simpler concept to define than 'weapons').[1094] Years later, the idea of a code of conduct would be taken up by the European Union.

The origins of the CoC can be traced back to 2006 when UNGA Resolution 61/75 on TCBMs in outer space activities invited Member States to submit concrete proposals to maintain international peace and security, to promote international cooperation and prevent an arms race in outer space.[1095] One year later, the General Assembly renewed its call to Member States to submit concrete proposals on measures of transparency and confidence-building to the Secretary-General through Resolution 62/43.[1096] In 2009, the General Assembly requested the Secretary-General to submit a final report with an annex containing concrete proposals from Member States on TCBMs in outer space activities.[1097]

Another important precedent was a workshop organised in 2007 by Germany (which was holding the Presidency of the Council of the European Union) on security, arms control

[1092] See MARTINEZ, P., *Space Sustainability* (2015), cit. note 1020, p. 271.
[1093] See MUTSCHLER, M., *Security Cooperation in Space and International Relations*, in SCHROGL, K-U., HAYS, P., ROBINSON, J., MOURA, D. AND GIANNOPAPA, C. (eds), *Handbook of Space Security. Policies, Applications and Programs*, New York, 2015, p. 47. See also REMUSS, N., *Space and Security*, cit. note 952, p. 539.
[1094] KREPON, M., *A Code of Conduct for Responsible Space-Faring Nations*, in POWERS, J. (ed.), *Celebrating the Space Age*, UNIDIR Conference Report, Geneva, 2-7 April 2007, p. 172.
[1095] United Nations General Assembly, Resolution 61/75, 6 December 2006, A/RES/61/75, para. 1 (Voting record: 178-1-1).
[1096] United Nations General Assembly, Resolution 62/43, 5 December 2007, A/RES/62/43, para. 2 (Voting record: 179-1-1).
[1097] A/RES/64/49, cit. note 1072, para. 3.

and the role of the European Union.[1098] On that opportunity, the German Ambassador Rüdiger Lüdeking considered that it would be more promising to work first on a code of conduct rather than focus on a treaty banning weapons in outer space.[1099] In March 2007, Italy prepared a working paper entitled 'Food for thought for a Comprehensive Code of Conduct for Outer Space Activities'[1100] and submitted it to the Working Party on Global Disarmament and Arms Control (CODUN).[1101] In September 2007, Portugal –on behalf of the European Union– responded the call made by UNGA Resolution 61/75 with information about the initiative on a code of conduct on space objects and space activities.[1102]

The European draft CoC was initiated and developed outside the multilateral framework of the United Nations, probably to circumvent the negotiating problems that delegations were facing with the discussion on PAROS at the Conference on Disarmament. Moreover, Europe already had experience in negotiating this type of instruments on its own. Clear examples are The Hague Code of Conduct against Ballistic Missile Proliferation (HCOC) and the European Code of Conduct for Space Debris Mitigation, which are successful precedents negotiated in a similar format outside the United Nations.

Although the draft CoC had been negotiated outside the United Nations, the European Union began to report on this initiative to COPUOS in 2008 with the aim of gaining extra-European adherents. Thus, France (which held the rotating Presidency of the Council of the European Union in 2008) mentioned the initiative at the 51st session of COPUOS.[1103] It was exactly that year when the Council of the European Union Ministers endorsed the first draft CoC.

That was precisely a moment when negotiations on the issue of disarmament in outer space were deadlocked at the Conference on Disarmament. At that point, three initiatives on security of outer space coexisted; namely, consultations on the setup of a working group

---

[1098] See RATHGEBER, W., REMUSS, N. AND SCHROGL, K-U., *Space Security and the European Code of Conduct*, cit. note 952, pp. 33-41.
[1099] Quoted in DICKOW, M., *The European Union Proposal for a Code of Conduct for Outer Space Activities*, in ESPI (ed.), *Yearbook on Space Policy 2007/2008*, Vienna-New York, 2009, p. 153.
[1100] See the reference in: Intervention by the Alternate Representative and Charge d'Affaires of Italy to the United Nations, Ambassador Inigo Lambertini in multilateral negotiations on an 'international code of conduct on space activities' (27 July 2015), available at http://www.italyun.esteri.it (last accessed on 11 August 2021).
[1101] REMUSS, N., *Space and Security*, cit. note 1093, p. 540.
[1102] Report of the Secretary-General on Transparency and Confidence-Building in Measures Outer Space Activities (Portugal on behalf of the EU), UN Doc. A/62/114/Add.1, 17 September 2007, paras 9 and 14.
[1103] Report of the 51st Session of COPUOS (2008), UN Doc. A/63/20, para. 296.

on LTS at COPUOS, a draft treaty on non-weaponisation of outer space at the Conference on Disarmament (see section 4.7.1) and the European initiative on a CoC.

Even then, some delegations requested a thorough analysis of the initiative within the United Nations system.[1104] One year later, the draft text (already approved by the Council of the European Union in December 2008)[1105] was submitted to COPUOS by the delegation of the Czech Republic on behalf of the European Union. On that occasion, COPUOS noted in its report that the European Union intended to carry out consultations and afterwards would convene an *ad-hoc* international conference to sign the instrument.[1106]

The initiative reached a higher level of development after the Council of the European Union gave a mandate to the High Representative for Foreign Affairs and Security Policy to conduct a series of consultations with interested third States. The idea was to agree on an acceptable text for a larger number of countries and subscribe it at a diplomatic conference.[1107] On 6 June 2012, the Ambassador and Permanent Representative of Hungary to the International Organisations in Vienna Györgyi Martin Zanathy made a statement at the 55th session of COPUOS explaining the purpose of the initiative and expressing the intention to hold a diplomatic conference the following year. At that session of 2012, Canada and Japan reported to COPUOS that they had participated in a meeting on 5 June 2012 regarding the European initiative organised by UNIDIR.[1108] The delegation of the Russian Federation took the opportunity to express concerns about initiatives that deviated from the principle of jurisdiction to implement measures against foreign space objects without the consent of the State of registry.[1109] The Russian delegate also stressed the close thematic link between the European initiative and the work of COPUOS regarding long-term sustainability.[1110]

---

[1104] Ibid, para. 301.
[1105] Council (EU), Conclusions and Draft Code of Conduct on Space Activities, 17175/08, 17 December 2008.
[1106] UN Doc. A/64/20, cit. note 1011, para. 45.
[1107] Council (EU), Conclusions of 27 September 2010 on a Revised Draft Code of Conduct on Space Activities, 14455/10, 11 October 2010.
[1108] Report of the 55th Session of COPUOS (2012), UN Doc. A/67/20, para. 46.
[1109] Be noted that the Russian Federation had already pointed at the problem of the exercise of jurisdiction over space debris, see Long-term sustainability of activities in outer space (Russian Federation), UN Doc. A/AC.105/L.285, 31 July 2012.
[1110] UN Doc. A/67/20, cit. note 1108, para. 50.

Fundamentally, the envisaged CoC established measures of transparency and confidence-building to safeguard the peaceful and sustainable use of outer space, preserving it for future generations. One of the clauses that raised severe criticism established:

> [t]he responsibility of States to refrain from the threat or use of force against the territorial integrity or political independence of any state, or in any manner inconsistent with the purposes of the Charter of the United Nations, and the inherent right of states to individual or collective self-defense as recognized in the Charter of the United Nations.[1111]

There was no agreement on expressly mentioning Article 51 of the UN Charter in this clause –its inclusion was particularly supported by the United States and the United Kingdom.[1112] Regarding the former country, the previous chapter already advanced the position of the United States regarding self-defence in outer space (see chapter 3, section 3.7). The 'space control' policy introduced during the Clinton Administration[1113] justified the adoption of self-defence measures with the mere purposeful interference with US space systems.[1114] In 2001, the already referred Rumsfeld Commission issued a report which clearly recommended disposing of weapons to protect space assets in the following terms:

> The Commissioners believe the U.S. Government should vigorously pursue the capabilities called for in the National Space Policy to ensure that the President will have the option to deploy weapons in space to deter threats to and, if necessary, defend against attacks on U.S. interests.[1115]

---

[1111] Draft CoC version of 31 March 2014, available at https://eeas.europa.eu/ (last accessed on 11 August 2021).

[1112] Some commentators explained that there were objections from several European countries, including Italy, Germany and the Scandinavian countries. See RATHGEBER, W., REMUSS, N. AND SCHROGL, K-U., *Space Security and the European Code of Conduct*, cit. note 952, p. 37.

[1113] The policy of 'space control' dates from 1995, and consists in the ability to maintain freedom of action in space for the State and its allies, while preventing such freedom of action to adversaries. See the US National Space Policy, 31 August 2006, available at https://history.nasa.gov/ (last accessed on 11 August 2021), which reads in a relevant part: 'Develop capabilities, plans, and options to ensure freedom of action in space, and, if directed, deny such freedom of action to adversaries'. See also Joint Publication 3-14, cit. note 457.

[1114] See PASCO, X., *Controlling the Freedom of Using Space: the White House Space Policy Dilemma,* in SCHROGL, K-U, MATHIEU, C. AND PETER, N. (eds), *Yearbook on Space Policy 2006/2007*, Vienna-New York, 2008, p. 203 (see its footnote 329). It should be recalled that chapter 2 in this thesis addressed the position of the United States in the field of cybersecurity, namely the use of force in case of mere interference, even if there is no destruction.

[1115] Report to the Commission, cit. note 635, p. xvii.

It further concluded that: 'There is no blanket prohibition in international law on placing or using weapons in space, applying force from space to earth or conducting military operations in and through space'.[1116]

President George W. Bush went a step farther and replaced the 'space control' policy with the 'space dominance' policy. In effect, the US National Space Policy of 2006 expressly provided that: 'the United States will oppose the development of new legal regimes or other restrictions that seek to prohibit or limit U.S. access to or use of space'.[1117] This policy has been rejected by China for considering it a 'monopolisation of outer space'.[1118]

In 2012, Secretary of State Hillary Clinton pledged to support the European initiative, although she made it clear that the United States would not adhere to a code that limited the capacity to carry out activities in space or protect the United States or their allies.[1119] This caveat is clearly in line with the Democrats' policy of 'space control'. Likewise, it was in line with the referred Democrats' Space Strategy of 2011 which enabled a supportive position regarding soft law instruments (see section 4.5 above).[1120] The Trump Administration was in line with the 'space dominance' Republican policy –'America first' meant that 'any harmful interference with or attack upon critical components of our space architecture that directly affects this vital interest will be met with a deliberate response at a time, place, manner, and domain of our choosing'.[1121]

The Prime Minister of Australia Kevin Rudd supported the European initiative immediately after the United States.[1122] The elaboration of the report that had to reflect the exchange of views regarding the draft CoC at COPUOS met some difficulties due to the

[1116] Ibid.
[1117] US Space National Policy, 31 August 2006, available at https://www.globalsecurity.org/ (last accessed on 11 August 2021).
[1118] DELPECH, T., *Nuclear Deterrence in the 21st Century*, cit. note 550, p. 148.
[1119] United States Department of State Press Release, Hillary Rodham Clinton, Secretary of State, International Code of Conduct for Space Activities, 17 January 2012, available at https://www.state.gov/ (last accessed on 11 August 2021).
[1120] See US National Security Space Strategy 2011, cit. note 1076.
[1121] White House Fact sheet, 23 March 2018, available at https://www.whitehouse.gov/ (last accessed on 11 August 2021).
[1122] View of the Ministry of Foreign Affairs and Trade of Australia on the Space Sustainability Conference, Beijing, 2012, available at https://swfound.org/ (last accessed on 11 August 2021).

opposing positions. Finally, delegations agreed to express opinions both in favour[1123] and against the European initiative.[1124]

At the 56th session of COPUOS in 2013, the European Union expressed its firm conviction to develop a CoC in an open, transparent and inclusive manner. The European delegate also referred to a first round of consultations in Kyiv that had taken place on 16 and 17 May of that year and a second round of negotiations that would be celebrated on 20 and 22 November later that year in Bangkok. A third one would be in Luxembourg on 27 and 28 May of the following year.[1125] It is possible to believe that this strategy was an attempt to dissipate the idea that the CoC was a 'Western Ploy to limit the activities of other space-faring countries'.[1126]Although the European Union tried to convince a larger number of States within COPUOS to adhere to the initiative in order to close the process in an *ad-hoc* international conference, the truth is that this move created more resistance than adherence. This ambitious strategy was the origin of the difficulties that ushered the initiative into its failed fate. Moreover, this ambition marked an important difference with the European Code of Conduct for Space Debris Mitigation, which was envisaged to be applied by the European Space Agency, by national space agencies within Europe and their contractors and by any other space project conducted in Europe or by any European entity acting outside Europe including operators.[1127] Unlike that initiative, the draft CoC had the aspiration to gain the widest adherence possible (which is already explicitly recognised in the preamble) and become an international code of conduct.

Despite the obstacles, the European Union continued its work towards the CoC, to the point that in 2015 the Council of the European Union issued a decision supporting the initiative.[1128] When the European Union announced during a session of COPUOS that it was time to move from a consultative stage to a negotiating phase, objections became even stronger. The Russian Federation circulated a working document expressing concerns about

[1123] UN Doc. A/67/20, cit. note 1108, para. 48.
[1124] Ibid, paras 51, 53.
[1125] Report of the 56th Session of COPUOS (2013), UN Doc. A/68/20, para. 50.
[1126] RAJESWARI PILLAI RAJAGOPALAN, *The Space Code of Conduct Debate. A View from Delhi*, in 'Strategic Studies Quarterly', 2012, p. 138.
[1127] European Code of Conduct for Space Debris Mitigation, 28 June 2008 (see 'scope and applicability'), available at https://www.unoosa.org/ (last accessed on 11 August 2021).
[1128] Council Decision (CFSP) 2015/203 of 9 February 2015 in support of the Union Proposal for an International Code of Conduct for Outer-Space Activities as a Contribution to Transparency and Confidence-Building Measures in Outer-Space, OJ L 33/38.

legitimating coercive measures against foreign space objects not authorised by the system of the UN Charter.[1129] Such a conduct was labelled by the Russian delegation as 'constructive interventionism', i.e. a use of force beyond the framework provided for in the UN Charter, and described it as ill-founded on space security reasons.[1130] In this regard, most academic commentators concur that the removal of foreign active or inactive space objects would run counter to the principle of jurisdiction and control under the Outer Space Treaty[1131] unless the State of registry agrees to such an action.[1132]

The meeting organised by the European Union with the support of UNIDIR between 27 and 30 July 2015 at the UN headquarters in New York already made it clear that it would not be possible to go ahead with the draft CoC in such a manner if the goal was to achieve a global instrument. A procedural motion at the beginning of the meeting downgraded the level of what was supposed to be a negotiating session to a mere consultative meeting due to the fact that the European Union lacks the UN Member State standing.[1133]

The European Union admitted at the 59th session of COPUOS in 2016 that 'a non-legally binding agreement which is negotiated within the United Nations was the right way to proceed'.[1134] From then on, the European Union concentrated all its efforts and political commitment to carry forward the compendium of LTS Guidelines at COPUOS.

### 4.6.1.-EUROPE AS A SPACE ACTOR: THE END OF BIPOLARITY IN SPACE

The International Geophysical Year in 1957 and the Cold War were the main drivers of the Space Age.[1135] In effect, the space race commenced as a struggle for power superiority

[1129] Additional Considerations and Proposals to Increase Understanding of Priorities, the Overall Meaning and Functions of the Concept and Practice of Ensuring Long-Term Sustainability of Activities in Outer Space (Russian Federation), UN Doc. A/AC.105/L.296, 30 April 2015, paras 4-5.
[1130] UN Doc. A/AC.105/C.1/2015/CRP.22, cit. note 1046, para. 4. See also: Russian Assessment of the Initiative and Actions of the European Union to Advance its Draft Code of Conduct for Outer Space Activities (Russian Federation), UN Doc. A/AC.105/C.1/L.346, 30 July 2015.
[1131] See WILLIAMS, M., *Safeguarding Outer Space,* cit. note 1031, p. 87.
[1132] See also the argument proposed by Popova of claiming a state of necessity to clean up foreign space debris in: POPOVA, R. and SCHAUS, V., *The Legal Framework for Space Debris Remediation'*, cit. note 970.
[1133] PELLEGRINO, M. AND STANG, G., *Space Security for Europe*, cit. note 955, p. 59.
[1134] Digital Recordings of the 59th Session of COPUOS (2016), 8 June 2016, 10 a.m. (EU statement, 1:47:18).
[1135] Sputnik 1 and Explorer 1 (Soviet and American first satellites, respectively) were launched during the International Geophysical Year, a period that expanded from 1 July 1957 until 31 December 1958. One of the most important contributions to the IGY was the discovery of the Van Allen radiation belt, made by the cosmic radiator that flew on Explorer 1.

between the United States and the Soviet Union in the late sixties. The launch of Sputnik 1 was the starting point and was followed by the Apollo 11 Program and the first human being landing on the Moon. At that time, Europe was not yet a space player, although the European countries were both involved and interested in space matters since the early days.

The first steps towards the European space independence were made with the creation of the European Launcher Development Organisation (ELDO) on 29 March 1962 and the European Space Research Organisation (ESRO) on 14 June 1962. ELDO was tasked with the development of a European launcher that would supersede the British failed Blue Streak Missile[1136] and would provide Europe with independence from the American launchers. For its part, ESRO was established to produce scientific satellites.

The second milestone was the creation of ESA merging ESRO and ELDO upon the signature of its founding treaty in 1975 and its entry into force on 30 October 1980. Nowadays, ESA has 22 member States[1137] and concluded agreements with Canada and Slovenia. The preamble of the ESA Convention foresees that one of its aims is to define a European Space Programme '*exclusively* for peaceful purposes', language that was employed again in Article II, which sets out the purposes of the agency.

The idea of achieving space independence was complemented with the goal of achieving sovereignty in certain technologies and their applications.[1138] These were not the only reasons for engaging in endeavours towards a European Space Policy. As early as 1979 (and then again in 1987), the European Parliament stressed the benefits connected to space activities when it addressed the Commission for the first time on the need to develop a space policy.[1139] The Commission also recognised that a space policy would impact on many aspects of the economic, industrial and cultural life of Europe.[1140] Furthermore, space is not

[1136] The Blue Streak was a British medium-range ballistic missile that preceded the launcher developed by ELDO, named 'Europa'.
[1137] Austria, Belgium, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Luxembourg, the Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden, Switzerland and the United Kingdom.
[1138] Commission Working Document (EC), Towards a Coherent European Approach for Space, SEC (1999) 789 final, 7 June 1999, p. 5.
[1139] European Parliament (EC), Resolution on Community Participation in Space Research, OJ C 127/42, 21 May 1979, pp. 1 and 2; European Parliament (EC), Resolution on European Space Policy, OJ C 190/78, 20 July 1987, p. 3.
[1140] Commission Communication (EC), The Community and Space: a Coherent Approach, COM (88) 417 final, 26 July 1988, p. 10.

only a cross-sectorial strategic asset but also a policy instrument.[1141] The Commission acknowledged that space could support European policies and objectives, such as faster economic growth, job creation and industrial competitiveness, enlargement and cohesion, sustainable development and security and defence.[1142] Moreover, space would serve the EU ambitions to become a major player on the international stage.[1143] In sum, Europe became aware of the growing number of emerging stakeholders in space and the need to become a full player at international level.[1144]

The 2004 Framework Agreement signed by the European Community (the predecessor of the EU) and ESA was a turning point in the institutionalisation of the mutual cooperation towards a European Space Policy. Some years later, the Commission crystallised the European Space Policy in Communication (2007) 212.[1145] In addition, the European Council adopted a resolution reaffirming the support of Europe for the ongoing efforts of COPUOS in the mitigation and prevention of space debris.[1146] The European Commission rolled out the European Space Policy during the 51st session of COPUOS on 13 June 2008.[1147] That presentation was made by Ms. Hélène-Diane Dage, from the Space Policy and Coordination Unit, who mentioned four main reasons for the development of a European Space Policy: first, the importance of space systems for critical areas of the economy; second, the benefit that communication satellites bring for every citizen; third, the contribution of space to the knowledge-society; and fourth, the valuable support of space to the European external policies.[1148]

Later on, the entry into force of the Lisbon Treaty in 2009 incorporated the space clause into European Law; namely, Article 189 of the Treaty on the Functioning of the EU

---

[1141] Commission Communication (EC), Towards a European Space Policy, COM (2001) 718, 7 December 2001, p. 30.
[1142] Commission Communication (EC), Space: a new European Frontier for an Expanding Union – An Action Plan for implementing the European Space Policy (White Paper), COM (2003) 673 final, 11 November 2003, p. 5.
[1143] Commission (EU), Towards a Space Strategy for the European Union that Benefits its Citizens, COM (2011) 152 final, 4 April 2011, p. 2.
[1144] European Economic and Social Committee, Opinion on the Communication from the Commission to the Council and the European Parliament: European Space Policy, COM (2007) 212 final, INT/360, 13 February 2008, para. 2.4.
[1145] Commission Communication (EC), European Space Policy, COM (2007) 212, 26 April 2007.
[1146] Council (EC), 10037/07, cit note 682, p. 3.
[1147] UN Doc. A/63/20, cit. note 1103, para. 23.
[1148] The European Space Policy, presentation made on 13 June 2008, Vienna, available at https://www.unoosa.org/ (last accessed on 11 August 2021).

(TFEU). This clause is said to have brought about a 'partial supranationalisation' of the space policy because it achieved the involvement of the EU in the space field without antagonising or displacing existing national space policies of its member States.[1149] On another note, it is worth recalling that the Lisbon Treaty introduced important changes to endow the EU with a diplomatic service, an important element for Europe to become an international player in space matters. With the inclusion of the Common Foreign Security Policy in the Maastricht Treaty, the need for a European Minister of Foreign Affairs became more and more desirable. The Constitutional Treaty failure set in motion new efforts to reform the EU. The Lisbon Treaty circumvented that shortcoming appointing a High Representative of the Union for Foreign Affairs and Security Policy instead of a Union Minister for Foreign Affairs.[1150] Another novelty introduced by the Lisbon Treaty was the modification to Article 27(3) of the Treaty of the European Union (TEU) that provides that the High Representative is assisted by the European External Action Service (EEAS), which has to work in cooperation with the diplomatic services of the Member States.

Before those institutional changes, the Commission represented the European Community in international organisations generally as an observer[1151] and the country holding the rotating Presidency of the Council represented the EU in the field of the Common Foreign Security Policy. The EU representation by the rotating Presidency enabled the EU to take the floor on the same footing as States did. However, its representation by an EU delegate became detrimental to its participation because the EU would then only be able to take the floor with the rights of an observer, i.e. with very limited ones.[1152] This proved to be an important reason to start negotiations on a better deal to ensure a more visible participation of the EU at the United Nations.

The result of these negotiations paved the way to UNGA Resolution 65/276,[1153] which sets out the modalities for the participation of the EU in its capacity as an observer. Indeed, the important note about this resolution is that it did not create any new status or

[1149] SIGALAS, E., *The Role of the European Parliament in the Development of a European Union Space Policy,* in 'Space Policy', Vol. 28, No. 2, 2012, p. 111.
[1150] Council (EC), Presidency Conclusions, 11177/1/07 REV 1, 20 July 2007. Annex I. Draft IGC Mandate, para. 3.
[1151] The EU may be a full member in the international organisations that allow membership of other international organisations, such as the case of the World Trade Organization.
[1152] Observers may not cast a vote, propose candidates or co-sponsor draft resolutions. In addition, they speak after Member States and sit at the back of the room.
[1153] United Nations General Assembly, Resolution 65/276, 3 May 2011, A/RES/65/276.

rights but simply set out the 'modalities' for participation in the work of the General Assembly, its committees and working groups, in international meetings and conferences convened under the auspices of the General Assembly and in UN conferences. Now, the EU takes the floor after regional groups –i.e. before Member States and not after them. Moreover, the UN Secretary-General issued a note that serves as the basis for a further analysis of the modalities.[1154] Since then, the EU has participated as an observer at COPUOS with the particular modalities established in UNGA Resolution 65/276. It is important to highlight that EU representatives are permitted to present proposals and amendments orally but they do not have the right to them for circulation as an official document. EU statements are guided by the arrangements for the EU statements in multilateral organisations,[1155] a document that provides that the EU and its Member States representatives will coordinate their action in international organisations to the fullest extent possible as established in the relevant European treaties.

The European Council and the European Parliament reached an agreement on a text for a new Space Programme 2021-2027 on 13 March 2019.[1156] In May 2021, those EU institutions adopted Regulation 2021/696, which established the European Union Agency for the Space Programme ('the Agency') replacing the European Global Navigation Service System (GNSS) Agency.[1157] This regulation distinguished five components of the EU Programme: Galileo (the European global navigation system), the European Geostationary Navigation Overlay Service or EGNOS (the European regional satellite-based augmentation system, whose aim is to improve the performance of the GNSS), Copernicus (the European Earth observation programme), the Space Situational Awareness, and the European Union Governmental Satellite Communications or GOVSATCOM. The programme also determined a clear distribution of tasks and responsibilities of the entities involved in the

[1154] Participation of the European Union in the Work of the United Nations, UN Doc. A/65/856, 1 June 2011. The representatives of the European Union do not have the right to vote, to co-sponsor draft resolutions or decisions, or to put forward candidates.
[1155] Council (EU), EU Statements in Multilateral Organizations: General Arrangements, 15901/11, 24 October 2011.
[1156] Council (EU), Proposal for a Regulation of The European Parliament and of the Council establishing the space programme of the Union and the European Union Agency for the Space Programme, 15490/18, 14 December 2008 (see its annex).
[1157] Parliament and Council Regulation (EU) 2021/696 of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No. 912/2010, (EU) No. 1285/2013 and (EU) No. 377/2014 and Decision No 541/2014/EU, OJ L 170/69.

implementation of each of these components (i.e. the EU Commission, ESA, EUMETSAT and the Agency).

After this brief introduction into the institutional foundations of Europe as a space actor, it is easier to understand the strong commitment of the EU with the draft CoC –an initiative with the potentiality of bringing Europe to the forefront of space and security matters at a multilateral level.[1158]

### 4.6.2.-THE DRAFT CoC AND THE LTS GUIDELINES: SIMILARITIES AND DIFFERENCES

As already explained, the original scope of the LTS Guidelines was more ambitious than what has been achieved so far. This section will compare them with the draft CoC and will seek to identify similarities and differences.

#### a) The preamble of the draft CoC and the background section of the LTS Guidelines:

- If both are compared, it is possible to conclude that the draft CoC and the LTS Guidelines are similarly inspired in preserving outer space for future generations. The main difference in language is that while the draft CoC used the wording 'peaceful and sustainable use of outer space' in the preamble, the LTS Guidelines employ the language 'long-term sustainability of outer space activities'.

- While both acknowledge the important role of space in the socioeconomic development of the society, the LTS Guidelines expressly mention the Sustainable Development Goals, while the draft CoC does not.

- An important difference is that while the LTS Guidelines underscore the need to ensure long-term sustainability; and in particular, enhance the safety of space operations, the draft CoC referred to sustainability, security and safety.

[1158] See REMUSS, N., *Space and Security*, cit. note 1093, p. 545.

- This chapter has already outlined the negotiations regarding a definition of long-term sustainability of outer space activities in the LTS Guidelines (see setion 4.4.1). For its part, the draft CoC did not provide any definition in its text. Some authors have suggested that the proponents of the European initiative probably selected the CoC format because it avoids extensive discussions on definitions[1159] and its provisions are more likely to become customary international law.[1160]

- Both texts refer to the 2013 report of the GGE on TCBMs in outer space activities. Interestingly, the LTS Guidelines do not mention the prevention of an arms race (this is an issue that did not meet agreement when guideline 7 was discussed as a proposal from GRULAC) but the draft CoC included a preambular paragraph noting the importance of preventing an arms race.

- An element that both texts share is that they were conceived as non-legally binding instruments based on a voluntary commitment (the LTS Guidelines makes that clarification in the background part, whereas the draft CoC did so in the substantive part dealing with the purposes and scope).

- The section entitled 'Definition, objective and scope of the guidelines' foresees that the LTS Guidelines *may* be considered as *potential* TCBMs. For its part, the draft CoC asserts in its Part I (devoted also to the purpose and scope) that its text establishes TCBMs.

- The LTS Guidelines were envisaged as a living instrument, which is the reason why there is a heading in its background part on revision, implementation and update of the guidelines. Likewise, yet in the substantive part entitled 'Organizational Aspects', the draft CoC provided meetings of the subscribing Parties for the review of implementation and modification of its text.

**b) <u>The substantive parts:</u>**

- Both include a series of commitments, such as the need to adopt measures and policies to reduce risks of collision, interference and creation of space debris; the need to

[1159] RATHGEBER, W., REMUSS, N. AND SCHROGL, K-U., *Space security and the European Code of Conduct*, cit. note 952, p. 34.
[1160] See also REMUSS, N., *Space and Security*, cit. note 1093, p. 539.

share information regarding launches into space, space events and space weather (Part II.B of the Guidelines; Part III of the draft CoC).

- In both, international cooperation is guaranteed on an equitable and mutually acceptable basis, according to the 'Declaration on International Cooperation in the Exploration and Use of Outer Space for the benefit and interest of all States, taking particular account of the needs of Developing countries'[1161] (Part I, paragraph 19 of the Guidelines; Part I, paragraph 42 of the CoC).

- While both the LTS Guidelines (Part I, paragraph 22) and the draft CoC (Part III.7) refer to Article IX of the Outer Space Treaty and encourage settling issues with States involved, they differ in that the LTS Guidelines provide that the outcome of such consultations should be presented to COPUOS if consented by the parties involved.

- As to the differences, the draft CoC included the already referred controversial provision relating to the use of force and the destruction of foreign space objects. The LTS Guidelines do not include any such reference nor do they include any mention of the inherent right to self-defence.

In sum, while COPUOS did not reach consensus on a broader scope for the LTS Guidelines that would include security issues, the draft CoC included them but did not become a reality. In both cases formal obstacles led to a governance vacuum in the matter*:* in the case of the CoC one of the reasons was the inappropriateness of such discussions outside the United Nations and in the case of the LTS Guidelines one of the reasons was the mandate of COPUOS. However, it is all about political will. It appears that the international community has created its own 'prisoner's dilemma': whereas the Russian Federation, its allies and the GRULAC were the main objectors of the draft CoC; the United States, its allies and the EU were the main objectors of the security guidelines. None of these groups cooperated and thus the result was the lack of space security governance, which runs counter to the interests of both sides.

[1161] A/RES/51/122, cit. note 584.

## 4.7.-OTHER INITIATIVES RELATING TO SAFETY, SECURITY AND SUSTAINABILITY OF OUTER SPACE ACTIVITIES (3S): SEARCHING FOR A WAY OUT OF THE STALEMATE

Security, safety and long-term sustainability of outer space activities encompass an agenda that does not fit the mandate of a single multilateral body. The next subsections will address three initiatives whose progress (if any) is still to be determined. The evolution of these initiatives range from complete stalemate (the draft PPWT), through certain adherence (no first placement of weapons declarations) to wide support (joint meetings of UNGA First and Fourth Committees).

### 4.7.1.-THE DRAFT TREATY ON THE PROHIBITION OF PLACEMENT OF WEAPONS IN OUTER SPACE (PPWT): THE RISE OF THE SINO-RUSSIAN DUO

The topic of space security is very much interrelated with concepts such as 'weaponisation of outer space' and 'arms race in outer space'. The history of disarmament in connection with outer space did not begin only in 1967 with the Outer Space Treaty (Article IV). There were two precedents already in 1963: a binding one, which was the Partial Test Ban Treaty, and a non-binding one, which was UNGA Resolution 1884 (XVIII). The former (with more than 120 ratifications) was finally signed after years of negotiations in a tense framework marked by the Cuban Missile Crisis. That treaty bans nuclear weapons *tests* and *explosions* in the atmosphere, outer space or underwater but it does not prohibit the *placement* of weapons in outer space. This loophole was filled by Article IV of the Outer Space Treaty, which expressly banned it. However, as already advanced, that provision is also imperfect since it only prohibits the placement of nuclear weapons or weapons of mass destruction, but it does not provide anything regarding the use or placement of conventional weapons.

In an attempt to address these issues, in 1981 Italy tabled a draft resolution on behalf of a group of States at UNGA First Committee.[1162] One of its purposes was to request the

[1162] Preventing an Arms Race in Outer Space (Australia, Belgium, France, the Federal Republic of Germany, Italy, the Netherlands, New Zealand and the United Kingdom), UN Doc. A/C.1/36/L.7, 10 November 1981.

Committee on Disarmament to consider the question of negotiating effective and verifiable agreements on PAROS, which was formally adopted as the already referred UNGA Resolution 36/97C (see section 4.3 above). In 1982, the General Assembly requested the Committee on Disarmament (which was redesignated as the Conference on Disarmament on 7 February 1984),[1163] to establish an *ad hoc* working group on the matter to begin negotiations towards an international agreement.[1164]

The negotiations on PAROS got stuck in 1995. In 2002, China and the Russian Federation tabled a working paper at the Conference on Disarmament, which was entitled 'Possible Elements for a Future International Legal Agreement on the Prevention of the Deployment of Weapons in Outer Space, the Threat or Use of Force Against Outer Space Objects'.[1165] This was the prelude to the future endeavours on a draft treaty. It should be recalled that in the same year, the United States withdrew from the 1972 Anti-Ballistic Missile (ABM) Treaty, which prohibited development, testing or deployment of space-based ABM systems. The stage was already set for the draft PPWT.

The context in 2008 was the following: the draft CoC was at a deliberative stage within the CODUN to be then approved by the Council of the European Union, Brachet submitted his proposal on the long-term sustainability at COPUOS and the Russian Federation and China tabled at the Conference on Disarmament the first version of a draft PPWT. As already outlined above, the draft PPWT supplements the non-weaponisation obligation with the obligation not to use or threat to use force, an issue that the draft CoC attempted to address also unsuccessfully. The idea was not to submit a text on the prevention of an arms race in outer space, something which the Conference on Disarmament had been working on for several years by then. Instead, the goal was to prohibit the weaponisation of outer space as a prior and necessary step to prevent an arms race.[1166] In other terms, the aim

---

[1163] See Report of the Conference on Disarmament (1984), General Assembly 39th Session (1984), UN Doc. A/39/27, p. 1 (see II.A. 'Designation of the Multilateral Negotiating Forum as a Conference').
[1164] United Nations General Assembly, Resolution 37/83, 9 December 1982, A/RES/37/83, op. 6. This request was reiterated in successive UNGA resolutions on PAROS.
[1165] Possible Elements for a Future International Legal Agreement on the Prevention of the Deployment of Weapons in Outer Space, the Threat or Use of Force Against Outer Space Objects (China, the Russian Federation, Vietnam, Indonesia, Belarus, Zimbabwe and the Syrian Arab Republic), CD/1679, 28 June 2002.
[1166] See VASILIEV, A., *The Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force Against Outer Space Objects*, in POWERS, J. (ed.), *Celebrating the Space Age*, UNIDIR Conference Report, Geneva, 2-7 April 2007, p. 115. Cfr. CD/1679, 28 June 2002, cit note 1165.

of the draft PPWT was to prevent an arms race by prohibiting the weaponisation of outer space (the draft treaty referred to *any* weapons).

The draft included a definition of 'weapon in outer space', which did not apply to Earth-based weapons targeting space objects in outer space.[1167] Some authors considered that the inclusion of negative definitions (based on prohibitions) in the PPWT was an important difference compared to the draft CoC, focused rather on positive behaviours.[1168] The draft PPWT also included an article on the exercise of self-defence in accordance with Article 51 of the UN Charter (Article V)[1169] and one referring to the promotion of transparency and confidence-building measures (Article VI).[1170]

The proposal contained two novel elements: the first was the definition of outer space as the space above the Earth over 100 km above sea level[1171] (it is well-known that the delimitation of air and outer space is a thorny issue that COPUOS has not been able to settle in its deliberations). The second one was that the scope of the planned treaty covered not only weaponisation but also the use and threat of use of force in outer space. This means that the draft PPWT covered not only the *placement* but also the *use* of any weapon in outer space, something that was absent in Article IV of the Outer Space Treaty.[1172] However, the draft PPWT did not provide anything regarding testing, storage and development of weapons. Nor did it provide a regime for compliance verification and monitoring.[1173] At the end, the draft did not reach consensus and only led to a general climate of stalemate at the Conference on Disarmament.

---

[1167] HAYS, P., *Developing Agile and Adaptive Space Transparency and Confidence-Building Measures*, in ROBINSON, J., SCHAEFER, M., SCHROGL, K-U., VON DER DUNK, F. (eds), *Prospects for Transparency and Confidence-Building Measures in Space*, ESPI Report No. 27, Vienna, 2010, p. 32.

[1168] See DICKOW, M., *The European Union proposal for a Code of Conduct for Outer Space Activities*, cit 1099, p. 156.

[1169] Draft Treaty on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force against Outer Space Objects, Conference on Disarmament, reproduced in CD/1839, 29 February 2008 (2008 draft PPWT version). Draft Article V reads as follows: 'Nothing in this Treaty may be interpreted as impeding the exercise by the States Parties of their right of self-defence in accordance with Article 51 of the Charter of the United Nations'.

[1170] Draft Article VI first paragraph reads as follows: 'With a view to promoting confidence in compliance with the provisions of the Treaty and ensuring transparency and confidence-building in outer space activities, the States Parties shall implement agreed confidence-building measures on a voluntary basis, unless agreed otherwise'.

[1171] Article 1(a) of the 2008 draft PPWT version.

[1172] FREELAND, S., *The Laws of War in Outer Space*, cit. note 1025, p. 104.

[1173] ROBINSON, J., *SpaceTransparency and Confidence-Building Measures*, in SCHROGL, K-U., HAYS, P., ROBINSON, J., MOURA, D. AND GIANNOPAPA, C. (eds), *Handbook of Space Security. Policies, Applications and Programs*, New York, 2015, p. 294.

A new version of the text was submitted in June 2014[1174] (just a couple of weeks after the third meeting for further discussion on the draft CoC organised by the European Union in Luxembourg). Although this version took note of a part of the objections and improved some controversial aspects (for instance, the definition of outer space was deleted, a detailed mechanism for dispute settlement was put in place and the procedure for amendments was modified), the main problems of the 2008 draft PPWT version were not addressed, notably the lack of a verification mechanism and the inclusion of Earth-based anti-satellites in the definition of 'weapons in outer space'.[1175]

Regarding the last objection, it should be noted that while the definition of 'weapon in outer space' in the draft PPWT comprised 'any outer space object or component thereof', 'use of force' was defined as 'any action intended to inflict damage on an outer space object'. The wording 'intended to' in the latter definition reveals that there was a particular emphasis on the subjective element of the aggressor.

In 2017, a draft resolution entitled 'Further practical measures for the prevention of an arms race in outer space' was tabled by the Russian Federation and China.[1176] The final text was adopted as UNGA Resolution 72/250[1177] with a recorded vote of 121 in favour, 5 against (France, Israel, Ukraine, the United Kingdom and the United States) and 45 abstentions (mostly European countries, Japan and Turkey).[1178] This resolution requested the Secretary-General to establish a GGE on PAROS composed of 25 experts[1179] with the mandate to 'consider and make recommendations on substantial elements of an international legally binding instrument on the prevention of an arms race in outer space, including, *inter alia*, on the prevention of the placement of weapons in outer space'.[1180] The GGE on PAROS met in 2018 and 2019 but could not reach consensus on a report. The only document openly

[1174] Draft Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects, reproduced in CD/1985, 12 June 2014 (2014 draft PPWT version).
[1175] For a detailed analysis and comparison of the two versions, see TRONCHETTI, F. AND HAO, L., *The 2014 updated Draft PPWT: Hitting the Spot or Missing the Mark?,* in 'Space Policy', Vol. 33, 2015.
[1176] See Report of 72nd Session UNGA First Committee (2017), Prevention of an Arms Race in Outer Space, UN Doc. A/72/407, para. 9. This draft resolution was sponsored by several States.
[1177] United Nations General Assembly, Resolution 72/250, 24 December 2017, A/RES/72/250.
[1178] UN Doc. A/72/407, 8 November 2017, cit. note 1176, para. 11.
[1179] Representatives of the following States were members of the GGE on PAROS: Algeria, Argentina, Australia, Belarus, Brazil, Canada, Chile, China, Egypt, France, Germany, India, the Islamic Republic of Iran, Italy, Japan, Kazakhstan, Malaysia, Nigeria, Pakistan, the Republic of Korea, Romania, the Russian Federation, South Africa, the United Kingdom, and the United States.
[1180] A/RES/72/250, cit. note 1177, op. 3.

available is a summary by the Chair of the GGE on PAROS, the Brazilian Ambassador Guilherme de Aguiar Patriota, which reports on an open-ended informal consultative meeting held from 31 January to 1 February 2019.[1181]

In general terms, discussions revolved around whether the Outer Space Treaty was sufficient to regulate current threats and whether lacunae should be filled by a legally binding treaty or by non-binding TCBMs. Views were also exchanged regarding the scope of a potential future instrument; whether only kinetic attacks or also space rendezvous, harmful interferences and other kind of malicious conducts should be foreseen. In this regard, three types of attacks were considered: Earth-to-space, space-to-Earth and space-to-space. Some experts considered it of the utmost importance to provide for a verification system in any potential future treaty as a way of enhancing its credibility, yet others acknowledged that verification methods were difficult to design at the current technological stage.

The last development until the moment of concluding this research is UNGA Resolution 75/36, adopted on the basis of a proposal from the United Kingdom entitled 'Reducing space threats through norms, rules and principles of responsible behaviours'.[1182] This resolution has two main aims: first, it creates a sub-item under the UNGA agenda item on PAROS with the same title of the resolution. Second, it encourages Member States to study existing and potential threats and security risks to space systems, characterise actions and activities as responsible, irresponsible or threatening and share views on further development and implementation of norms, rules and principles of responsible behaviours and on the reduction of misunderstandings in outer space. On the one hand, this initiative appears to come back to the approach envisaged in the draft CoC based on 'positive behaviours' rather than on prohibitions. On the other hand, the bottom-up approach in the proposal of the United Kingdom offers as an alternative to the PPWT and the European CoC.[1183]

---

[1181] See Report by the Chair of the Group of Governmental Experts on Further Practical Measures for the Prevention of an Arms Race in Outer Space, New York, 31 January 2019, available at https://www.un.org/ (last accessed on 11 August 2021).
[1182] United Nations General Assembly, Resolution 75/36, 7 December 2020, A/RES/75/36 (Voting record: 164-12-6).
[1183] RAJESWARI PILLAI RAJAGOPALAN, *Assessing the British Proposal on Space Security*, 10 December 2020, available at https://thediplomat.com/ (last accessed on 11 August 2021).

In sum, although some delegations are still very reluctant to negotiate a binding treaty banning any type of weapons and the use or threat of use of force in outer space, the proponents of the PPWT achieved to keep the topic of a binding instrument on the agenda since 2002. Even if they have not gained enough traction in the furtherance of negotiations, they have skillfully managed to introduce references to the draft PPWT in a number of UNGA resolutions (see next sub-section) and in the 2013 report of the GGE on TCBMs in outer space activities. It is adventurous to conclude that the PPWT ousted the European draft CoC because it is not possible to conclude either that the draft PPWT is completely alive or that the draft CoC is completely dead. Even if there are other space powers that play a significant role in the negotiating arena, such as Europe and China, the global space governance (at least in security matters) still remains a matter of old bipolar antagonisms.

### 4.7.2.-NO FIRST PLACEMENT OF WEAPONS IN OUTER SPACE (NFP): THE CHINESE 'SHARED FUTURE' POLICY

In 2004, the Russian Federation committed itself not to be the first one to place weapons in outer space and called upon other States to join that political commitment as an interim measure towards a PPWT. Until the moment of writing, there are 22 countries that have joined that initiative.[1184] There is a precedent of a similar policy in the nuclear domain, the 'No First Use', which mandated not to be the first one to use nuclear weapons. China was the first one to make such a commitment in 1964[1185] and the Soviet Union made a similar unilateral pledge in 1982[1186] but the Russian Federation withdrew it in 1993.[1187]

Ten years after, upon an initiative tabled by the Russian Federation in 2014, the General Assembly adopted Resolution 69/32[1188] 'No first placement of weapons in outer space' with 126 votes in favour, four against (the United States, Israel, Georgia and Ukraine) and 46 abstentions (mainly European countries, Australia and Canada). In that resolution,

[1184] Statement by Representative of the Russian Federation Andrei Belousov in the First Committee of the 74th Session of the UNGA on cluster 3 Outer Space (disarmament aspects), available at https://russiaun.ru (last accessed on 11 August 2021).
[1185] ZHENQIANG, P., *A Study of China's No-First-Use Policy on Nuclear Weapons,* in 'Journal for Peace and Nuclear Disarmament', Vol. 1, No. 1, 2018, p.115. See also PANDA, A., *'No First Use' and Nuclear Weapons*, 17 July 2018, available at https://www.cfr.org/ (last accessed on 11 August 2021).
[1186] FEIVESON, H. AND HOGENDOORN, E., *No First Use of Nuclear Weapons*, in 'The Nonproliferation Review', Summer 2003, p. 3, available at https://www.nonproliferation.org/ (last accessed on 11 August 2021).
[1187] Ibid.
[1188] United Nations General Assembly, Resolution 69/32, 2 December 2014, A/RES/69/32 (Voting record: 126-4-46).

the General Assembly urged States to start substantive work on the updated draft PPWT (operative paragraph no. 3) and encouraged States to make a political commitment not to be the first to deploy weapons in outer space (operative paragraph no. 5). Although the Russian Ambassador Victor Vasiliev has characterised the NFP pledge as a TCBM to be implemented individually,[1189] some authors have pointed out that the unilateral declaration of not being the first to deploy weapons in space does not meet the necessary conditions to be considered a TCBM since it is not possible to demonstrate its implementation nor verify its compliance.[1190]

UNGA Resolution 69/32 started the practice of passing a resolution on NFP with wide support annually since 2014,[1191] although without universal adherence. Some academic commentators have argued that support for NFP resolutions could be interpreted as an indirect recognition of a possible acceptance of the PPWT.[1192] Some of the concerns that were mentioned during the vote were that that NFP is unverifiable and that there is no definition of 'weapon'; hence, it would be difficult to make an undefined element the scope of a commitment.[1193]

In 2017, a controversial new wording was included in preambular paragraph no. 4 of the draft NFP resolution at the request of China, which reads: '[…] in a common effort towards a community *of shared future* for humankind' (emphasis added). This language was included in UNGA Resolution 72/27 (2017), UNGA Resolution 73/31 (2018), UNGA Resolution 74/33 (2019) and UNGA Resolution 75/37 (2020). In the explanation of their vote in 2018, the United States, France and the United Kingdom opposed to this draft

[1189] UNIDIR, Space Security 2010 from Foundations to Negotiations, cit. note 1077, p. 18.
[1190] MARTINEZ, P., CROWTHER, R., MARCHISIO, S. AND BRACHET, G., *Criteria for Developing and Testing Transparency and Confidence-Building Measures (TCBMs) for Outer Space Activities',* in 'Space Policy', 2014, p. 2.
[1191] United Nations General Assembly, Resolution 70/27, 7 December 2015, A/RES/70/27; Resolution 71/32, 5 December 2016, A/RES/71/32; Resolution 72/27, 4 December 2017, A/RES/72/27; Resolution 73/31, 5 December 2018, A/RES/73/31; Resolution 74/33, 12 December 2019, A/RES/74/33; Resolution 75/37, 16 December 2020, A/RES/75/37. All these resolutions welcome the draft PPWT submitted by the Russian Federation and China at the Conference on Disarmament.
[1192] LIU, H. AND TRONCHETTI, F., *United Nations Resolution 69/32 on the "No First Placement of Weapons in Space": A Step Forward in the Prevention of an Arms Race in Outer Space'*, in 'Space Policy', 2016, p. 4.
[1193] EU Explanation of Vote – UNGA First Committee: No First Placement of Weapons in Outer Space, New York, 2 November 2018, available at https://eeas.europa.eu/ (last accessed on 11 August 2021).

resolution[1194] expressing that 'this phrase has been promoted by China to insert its own view of multilateralism and world geopolitics on the international system'.[1195]

A similar phrase had already brought about several shortcomings during the negotiation of the UNISPACE+50 Resolution.[1196] There, the original proposal of the Chinese delegation had been to insert in one of the preambular paragraphs the following language: '[…] for the objective of shaping *a shared future* for humankind...' (emphasis added). This language was not accepted and thus was replaced by: '[...] and contribute to realizing *a shared vision* for the future in the exploration and use of outer space for peaceful purposes and for the benefit and in the interest of all humankind' (emphasis added).[1197] The Head of the Chinese Delegation, Ambassador Shi Zhongjun, delivered a speech entitled 'Strengthening the governance of and promoting cooperation and win-win in outer space, in a joint effort to build *a shared future* in space exploration and use' (emphasis added) at the high level segment of UNISPACE+50.[1198]

In order to understand the underlying reasons for this language, it is necessary to refer back to the 18th National Congress of the Communist Party of China in 2012, where the concept of 'a community of shared future' was launched for the first time –marking the transition from the 'hide-and-bide' policy to one where China became an active player.[1199]

The 'community of shared future' was subsequently included in several statements of the Chinese President Xi Jinping, who transformed that phrase into his new diplomacy motto. On different opportunities at a multilateral level, he introduced the five underlying goals behind this seemingly philosophical phrase, which are peace; security; prosperity; inclusion and sustainable development. In 2015 the Chinese President elaborated on this policy in his statement at the 70th session of the General Assembly. Quoting an ancient

---

[1194] Working Document of the 73rd Session of UNGA First Committee (2018), UN Doc. A/C.1/73/L.51, 19 October 2018.
[1195] US Explanation of Vote in the First Committee on Resolution: L.50, 'No First Placement of Weapons in Outer Space' (on behalf of the United States, France and the United Kingdom), New York, 5 November 2018, available at https://geneva.usmission.gov/ (last accessed on 11 August 2021).
[1196] A/RES/73/6, cit. note 1021.
[1197] Ibid., preambular paragraph 12.
[1198] Statement by Head of the Chinese Delegation, H. E. Ambassador Shi Zhongjun at the UNISPACE+50 High-Level Segment 20 June 2018, Vienna, Austria, available at https://www.unoosa.org/ (last accessed on 11 August 2021).
[1199] See XIACHUNG, Z., *In Pursuit of a Community of Shared Future. China's Global Activism in Perspective*, in 'China Quarterly of International Strategic Studies', Vol. 4, No. 1, 2018, p. 24.

Chinese adage, he expressed the following: '...[t]he greatest ideal is to create a world truly *shared* by all' (emphasis added). Jinping called upon the international community to 'build a new type of international relations featuring win-win cooperation, and create a community *of shared future* for mankind' (emphasis added).[1200]

It is not the aim of this section to review the Chinese diplomacy in detail; however, these references are a crucial element in the background of current negotiations. It is a fact that China is increasing its political weight in the international arena. The NATO final declaration at the London Summit in 2019 for the first time recognised the growing influence of China and also acknowledged that its international policies provide both opportunities and challenges for the Alliance.[1201] In 2021, NATO referred again to the growing influence of China, but this time concerned about the challenges that such a fact poses.[1202]

In a nutshell, it is safe to conclude that China was skilled in infiltrating its domestic policy of a 'shared future' into its diplomatic action and –through it– added an explicit Chinese footprint in the global space governance relating, *inter alia*, to NFP and UNISPACE+50 UNGA resolutions.

### 4.7.3.-JOINT MEETINGS OF UNGA FIRST AND FOURTH COMMITTEES: THE SEEDS FOR A SOLUTION?

It is not possible to conclude this section without referring to the joint work of UNGA First Committee ('Disarmament and International Security') and UNGA Fourth Committee ('Special Political and Decolonization'). At the outset, it is necessary to recall that pursuant to Article 21 of the UN Charter, the General Assembly adopts its own rules of procedure. According to Article 11.1 of the UN Charter, that organ is mandated to consider the principle of disarmament and the regulation of armaments. In addition, in 1952 UNGA

[1200] Working Together to Forge a New Partnership of Win-win Cooperation and Create a Community of Shared Future for Mankind, Statement by H.E. Xi Jinping President of the People's Republic of China At the General Debate of the 70th Session of the UN General Assembly, New York, 28 September 2015, available at https://www.fmprc.gov.cn/mfa_eng/ (last accessed on 11 August 2021).
[1201] NATO London Declaration (2019), cit. note 561.
[1202] NATO Brussels Summit Communiqué (2021), cit. note 884, paras 3, 55 and 56.

Resolution 502 (VI)[1203] established the Disarmament Commission to report to the Security Council.

A proposal to divide the work of UNGA Main Committees was submitted in 1971 so as to allocate the discussion of certain conflicts within the Special Political Committee and to address disarmament, arms control and international peace and security in UNGA First Committee.[1204] In 1978, the General Assembly held its Tenth Special Session, which concluded with substantial inputs for the purposes of this thesis. One of them was that UNGA First Committee should deal only with questions of disarmament and international security in the future.[1205] It also replaced the Disarmament Commission that reported to the Security Council with the Disarmament Commission that became a subsidiary organ of the General Assembly (Article 22 of the UN Charter establishes the competence of the General Assembly to establish its own subsidiary bodies). Finally, it established the Committee on Disarmament as a negotiating body to be convened in 1979 in Geneva.[1206] This committee was redesignated in 1984 as the Conference on Disarmament (see section 4.7.1).

Turning the attention to UNGA Fourth Committee, the 90s marked a diverse geopolitical map due to the decolonisation process. Aware of this fact, in 1993 the General Assembly passed a resolution entitled 'Revitalization of the work of the General Assembly',[1207] which recognised the need to rationalise the Committees' structure of the General Assembly 'to respond better to the requirements of a new phase of international relations'.[1208] With this resolution, UNGA Fourth Committee (until then only discharging functions in matters related to decolonisation) absorbed the Special Political Committee, which became the 'Special Political and Decolonization Committee'.[1209] Rule 98 of the Rules of Procedure of the General Assembly enshrines the current six-tier configuration (six Committees) of this UN organ. As a subsidiary organ of the General Assembly, COPUOS used to report to the Special Political Committee until its 35th session (1992).[1210] Due to the changes just explained, the annual resolution on international cooperation in the peaceful

[1203] United Nations General Assembly, Resolution 502 (VI), 11 January 1952, A/RES/502(VI).
[1204] See PETERSON, M., *The UN General Assembly* (Global Institutions Series), London-New York, 2005.
[1205] United Nations General Assembly, Resolution Tenth Special Session, UN Doc. S-10/2, 30 January 1978, para. 117.
[1206] Ibid., para. 120.
[1207] United Nations General Assembly, Resolution 47/233, 17 August 1993, A/RES/47/233.
[1208] Ibid., preambular paragraph 8.
[1209] Ibid., op. 4.
[1210] A/RES/47/67, cit note 962. This resolution was the last one to be tabled at the Special Political Committee.

uses of outer space that endorses the report of COPUOS is since then tabled at UNGA Fourth Committee.[1211]

Given the interconnectedness between safety, security and LTS, the General Assembly decided to convene a joint meeting of its First and Fourth Committees in Resolution 69/38 on TCBMs in outer space activities (2014).[1212] In this joint meeting, the Director of OOSA Simonetta Di Pippo enhanced the notion that there is a complex and evolving agenda in the field of space affairs. In particular, she expressed that '[w]ith the evolution of the space awareness in society, COPUOS is positioning itself at the forefront of the overarching global sustainable development process by addressing *challenges to space security and sustainability'* (emphasis added).[1213]

After that first milestone, in 2016 the General Assembly decided to convene a joint half-day panel discussion of UNGA First and Fourth Committees as a contribution to the 50th anniversary of the Outer Space Treaty.[1214] The panel discussion took place in 2017 under a provisional agenda item during the 72nd session of the General Assembly. On that occassion, several challenges to security, safety and sustainability of activities in outer space were addressed, such as space debris, near-Earth objects; the emergence of new space actors, the development of anti-ballistic missiles, the practice of surveillance satellites and the extraction of natural resources in space.[1215] In addition, some States expressed that the right to self-defence enshrined in Article 51 of the UN Charter applied to the context of outer space. There was a delegation expressing that the resort to that right required further study.[1216]

Based on the positive experience of 2015 and 2017, COPUOS decided to propose a joint panel discussion of UNGA First and Fourth Committees to be convened in October

---

[1211] United Nations General Assembly, Resolution 48/39, 10 December 1993, A/RES/48/39. This resolution was the first one to be tabled at the Fourth Committee.
[1212] UN Doc. A/RES/69/38, cit. note 1075, para. 6. The joint meeting took place in 2015.
[1213] Joint Ad Hoc Meeting of the GA 1st /4th Committee – 'Possible Challenges to Space Security and Sustainability, by the Director of OOSA, 22 October 2015, available at http://www.unoosa.org/ (last accessed on 11 August 2021).
[1214] A/RES/71/90, cit. note 628, para. 15.
[1215] Joint Panel Discussion of the First and Fourth Committees 'Possible Challenges to Space Security and Sustainability', Co-Chairs Summary, 12 October 2017, para. 13, available at https://www.unoosa.org/ (last accessed on 11 August 2021).
[1216] Ibid., para. 15. Although the summary does not mention the Russian Federation, it is possible to infer that the view reflected in this paragraph is from that delegation.

2019.[1217] UNGA Resolutions 73/72[1218] and 73/91[1219] decided to convene a joint half-day panel discussion and thus gave a hint that the trend for the future would be to enhance their joint work. The mandate of this joint meeting had four indicative aims: 1) identify intersections between security and sustainability, 2) take stock of the ongoing processes on the matter, 3) exchange views on international cooperation and 4) identify approaches that help achieve targets for safety and sustainability.[1220]

From the precedents outlined above, it is safe to conclude that UNGA First and Fourth Committees are attuned to the need for more coordination and joint work in several topics that have a point of contact. It should be underscored, however, that such interconnectedness is not a new finding. As already pointed out, the 1993 report of the GGE on CBMs and the 2013 report of the GGE on TCBMs in outer space activities had already hinted the possibility of establishing working contacts between the Conference on Disarmament and COPUOS (see section 4.5).

The 2019 UNIDIR Conference on Space Security recognised the value of the joint meetings of both Committees to address cross-cutting issues that have civil and security-related aspects. It also considered that those meetings should have 'to progress beyond a largely symbolic half-day affair, to a longer session with a specific thematic focus and serious preparation'.[1221] By the same token, Theresa Hitchens and Joan Johnson-Freese assessed that the division of the peaceful purposes of outer space (addressed by COPUOS and the Fourth Committee) and the disarmament approach (addressed by the Conference on Disarmament and the First Committee) is a 'false dichotomy' due to the very nature of space technology as dual-use.[1222] Moreover, the Outer Space Treaty is the central instrument governing space

[1217] Report 61st Session of COPUOS (2018), UN Doc. A/73/20, para. 385.
[1218] A/RES/73/72, cit. note 1083, para. 10 (TCBMs). This resolution welcomes the previous joint *ad hoc* meetings of the First and Fourth Committees, held on 22 October 2015 and 12 October 2017 (para. 10).
[1219] United Nations General Assembly, Resolution 73/91, 7 December 2018, A/RES/73/91, para. 15.
[1220] Draft Concept Note on the Joint Panel Discussion of the First and Fourth Committees of the General Assembly on Possible Challenges to Space Security and Sustainability, UN Doc. A/AC.105/2019/CRP.19, 21 June 2019.
[1221] Supporting Diplomacy: Clearing the Path for Dialogue, UNIDIR Space Security Conference 2019, 28-29 May, Geneva, 2019, p. 7, available at https://www.unidir.org/ (last accessed on 11 August 2021).
[1222] HITCHENS, T. AND JOHNSON-FREESE, J., *Toward a New National Security Space Strategy: Time for a Strategic Rebalancing*, in Atlantic Council Strategy Paper No. 5, 2017, p. 32, available at https://www.atlanticcouncil.org/ (last accessed on 11 August 2021).

activities and the principles enshrined in it were envisaged to advance peace and security.[1223] Even if that instrument is the cornerstone of the peaceful uses of outer space, it also encompasses a (partial) non-weaponisation clause in Article IV. Furthermore, annual PAROS resolutions also reaffirm the fundamental principles of the Outer Space Treaty. These elements could be read as a clear sign of the interconnection of the agendas of COPUOS and the Conference on Disarmament.

The precedent of merging the 'Special Political Committee' and the 'Decolonization Committee' as outlined in this section, coupled with the General Assembly practice of establishing subsidiary bodies, gives a hint of possible mechanisms that might be examined with a degree of originality to overcome (at least) procedural shortcomings. This is exactly what this research attempts to achieve.

## 4.8.-CONCLUSIONS

The international community faces new threats that arise out of increasing space activities, congested orbits and new stakeholders with space and cyber capabilities. The need to strike a balance between economic development, environmental protection and responsible use of outer space is a necessary premise to allow the benefits of space applications to extend to present and future generations.

The analysis in this chapter of various initiatives has attempted to illustrate that matters concerning 3S are interconnected despite their fragmented treatment in different UN bodies or UN connected bodies. Moreover, it has shown that work in silos is not contributing to the overall goal of ensuring security, safety and sustainability of outer space activities. The underlying idea is to convey that it is not possible to conceive the long-term sustainability of space activities without a commitment to ensure safety and security in space. The current 'mandates conflict' between COPUOS and the Conference on Disarmament described above has proven to be an effective obstacle to address security, safety and LTS in an integrated manner.

[1223] See KAVANATH, C., *New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?*, in Carnegie Endowment for International Peace, August 2019, p. 33, available at https://carnegieendowment.org/ (last accessed on 11 August 2021).

On another note, this chapter provided a clear picture of different space policies and their impact on international negotiations. While the space age made its debut with the United States and the Soviet Union as unique space powers, successive years opened the doors to Europe, China and India, whose technological development transformed them into new international space actors. Although the Latin American and the Caribbean countries have not reached such technological level yet, their involvement in the negotiations on LTS has demonstrated that they are willing to continue making their voice heard and crystallised in the global space governance.

Until a definitive solution for the stalemate in negotiations is found at a multilateral intergovernmental level and the 3S is finally addressed holistically, the biggest challenge that COPUOS faces is to continue its future work on sustainability without waiting for progress to be made in other fora. To this end, it is necessary to design an agenda on LTS as a renewed effort to break deadlocks that prevent progress on space security. Ultimately, the interim strategy should be to leverage the work of COPUOS on LTS as a facilitator of dialogue to achieve consensus in other bodies and not take the failures of other venues to block the work at COPUOS.

By providing an overview of different institutional mechanisms and the shortcomings in negotiations regarding space matters, this chapter provided important inputs to answer the first part of **research question 5** (relating to the best way to address cyber threats in the space domain), which will be complemented in chapter 5. Likewise, it has contributed to partially answering the second part of **research question 5** (why a binding instrument is not –for the time being– the appropriate means to address space cyber threats). Additional inputs to answer this research question will be provided in chapter 5. Last but not least, this chapter has put together the necessary elements to complete the analysis made in chapter 3 to answer **research question 6** (how the regulation of space cybersecurity can contribute to the long-term sustainability of outer space activities and the governance of outer space).

# CHAPTER 5:
# REGULATION OF SPACE CYBERSECURITY

## 5.1.-INTRODUCTION

The two previous chapters addressed space debris as a worrying consequence of certain malicious space cyber activities. Hence, the preservation of space systems from that risk is a necessary premise for the safety of space missions and the long-term sustainability of outer space activities. The previous chapter also described the 'mandates conflict' between COPUOS and the Conference on Disarmament as a situation that has forced the international community into a deadlock on the 3S agenda.

This chapter will look into the venues that are available to circumvent the space security stalemate and provide a possible normative solution for space cybersecurity, taking into consideration the mandates' boundaries and the limited political will in future negotiations. Before that, this chapter will scrutinise relevant provisions of the UN space treaties to determine whether there is already a regulatory framework applicable to space cyber activities. In addition, an account of the doctrinal interpretation –mainly made by the Tallinn and the IISL experts– will be analysed.

The third section of this chapter will address certain principles of international law to shed light on whether they might apply to space cyber activities to complement the international space law regime, and if so to what extent. Ultimately, this assessment will allow determining which are the lacunae in the current legal system, and how they might or should be addressed in light of a set of scenarios that envisage the classification proposed in chapter 3 (section 3.4).

The final proposal of this chapter is to negotiate a draft UNGA resolution within COPUOS with principles on space cybersecurity. In that regard, a draft text will be put forward to allow the engagement of UNGA First and Fourth Committees, on the understanding that the topics addressed fall under the mandates of both of them.

The contents of this chapter served as valuable sources for the following two publications: JAMSCHON MAC GARRY, L., *The Particularities of the Responsibility and Liability Regimes in Space Law: Reality or Myth?,* in 'Revista de Derecho Espacial', No. 5, 2021 and JAMSCHON MAC GARRY, L., *Seguridad cibernética de los sistemas espaciales: el dilema de contribuir a la gobernanza global de las actividades en el espacio o dejar un vacío legal,* Revista Iberoamericana de Derecho Internacional y de la Integración, No. 14, June 2021.

## 5.2.-RELEVANT PROVISIONS OF INTERNATIONAL SPACE LAW APPLICABLE TO SPACE CYBERSECURITY

This section is broken down into two main sub-sections: the first one will focus on the regimes of responsibility and liability under space law. The second one will examine the interpretation of existing space law made by scholars and their assessment regarding its possible application to space cybersecurity.

### 5.2.1.- SPACE LAW

Space activities have repeatedly been depicted as ultra-hazardous.[1224] In this regard, they are only comparable with nuclear and oil pollution. This particular characterisation requires a special and unique regime of liability and responsibility. As to the former, it is one that provides for liability based on the activities at stake, regardless of the existence of a violation of a rule of international law,[1225] and which is not limited in time, amount and location.[1226] Regarding the latter, this regime of responsibility deviates from the general regime of State responsibility and establishes direct responsibility of the State for non-governmental activities in outer space.[1227]

---

[1224] See MARCHISIO, S., *International Legal Regime on Outer Space*, cit. note 740, p. 19; TRONCHETTI, F., *Fundamentals of Space Law and Policy*, cit. note 545, pp. 10 and 26; VON DER DUNK, F., *International Space Law*, cit. note 545, p. 89; SOUCEK, A., *International Law*, cit. note 545, pp. 311 and 342; KERREST, A. AND SMITH, J., *Article VII* (Outer Space Treaty), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. I), Cologne, 2009, p. 129 (para. 6).

[1225] KOPAL, V., *Origins of Space Law and the Role of the United Nations*, cit. note 690, p. 227.

[1226] KERREST, A. AND SMITH, J., *Article VII* (Outer Space Treaty), cit. note 1224, pp. 130-131 (para. 6) and p. 136 (para. 35).

[1227] See MARCHISIO, S., *Space Law and Governance*, cit. note 685, p. 4; BLOUNT, P., *Renovating Space: The Future of International Space Law,* cit. note 720; p. 518. See CHENG, B., *Article VI of the 1967 Space Treaty Revisited: 'International Responsibility', 'National Activities', and 'The Appropriate State'*, in 'Journal of Space Law', Vol. 26, No. 1, 1998, p. 12; MARCHISIO, S., *National Jurisdiction for Regulating Space Activities Of Governmental and Non-*

The particularity of the responsibility regime in space law is already traceable in the language chosen in Article VI of the Outer Space Treaty; namely, 'international responsibility' instead of 'State responsibility'. The rationale behind this language was to enhance the idea that a State is also responsible for national activities that are not carried out by the State concerned (or its agents), i.e. activities undertaken by private entities and by international organisations.[1228] However, it should be underscored that the expression 'international responsibility' makes it clear that the regime applies to inter-State controversies.

It is important to differentiate responsibility from liability in space law: while the *appropriate* State is responsible for *national activities*, the *launching* State is liable for *damage* caused by its *space object*. Thus, it is crucial to elucidate what 'national activities' and 'appropriate State' mean in Article VI (responsibility) and what 'launching State', 'damage' and 'space object' mean in Article VII (liability).

**a) Responsibility of the appropriate State for national activities:**

The first sentence of Article VI of the Outer Space Treaty refers to 'national activities' to distinguish it from the case regulated in the third sentence, which deals with responsibility for activities of international organisations.[1229] National activities include governmental and non-governmental ones,[1230] i.e. the appropriate State is directly responsible for private activities as well. This is why the second sentence of Article VI of the Outer Space Treaty includes the State obligation to authorise and continuous supervise space activities – a provision that is considered to be the legal basis for domestic space legislation.[1231] Domestic space law has three important purposes: to call on private entities to adapt their activities to the standards required by international obligations, to establish a mechanism to recover compensation paid by the State for damages caused by a private entity and to regulate matters related to insurance. This is an issue that was further enhanced in UNGA Resolution 59/115

*Governmental Entities*, United Nations/Thailand Workshop On Space Law, 16-19 November 2010, Bangkok, Thailand, p. 3, available at https://unoosa.org/ (last accessed on 11 August 2021).

[1228] See VON DER DUNK, F., *International Space Law*, cit. note 545, p. 46.

[1229] GERHARD, M., *Article VI* (Outer Space Treaty), cit. note 686, p. 109 (para. 31). This provision is complemented by Article XIII of the Outer Space Treaty, which deals with international intergovernmental organisations.

[1230] Ibid., pp. 110-111 (paras 35-36).

[1231] Ibid., p. 120 (para. 72).

on the 'Application of the concept of "Launching State"',[1232] where the General Assembly recommended States, *inter alia,* to consider enacting and implementing national laws authorising and providing for continuing supervision of the activities in outer space of non-governmental entities under their jurisdiction.[1233]

Revisiting the meaning of 'national activities' in the first sentence of Article VI of the Outer Space Treaty, it is possible to argue that governmental activities are easily identifiable as national because they are conducted by State entities or agencies.[1234] Regarding non-governmental entities, it is safe to conclude that national activities are those carried out by nationals from a State or activities conducted from its territory or with space objects registered with it.[1235] The Cologne Commentary to the Outer Space Treaty focused on the term 'national' but it did not address what is meant by 'activities' in this provision. It should be further analysed if the concept is broad enough to also include space cyber activities (see section 5.4 below).

The clarification regarding 'national activities' contributes to understanding the concept of the 'appropriate State': that is the State represented by the relevant agency (in the case of governmental activities) or the State that has jurisdiction based on nationality, territory or registry (in other cases concerning private entities).

**b) Liability for damage caused by the space object of the launching State:**

The liability regime is governed by the Liability Convention, which complements Article VII of the Outer Space Treaty. The regime is victim-oriented,[1236] which means that it is designed to strike a balance between the advancement of space exploration and the protection of victims of space activities.[1237]

---

[1232] United Nations General Assembly, Resolution 59/115, 10 December 2004, A/RES/59/115.
[1233] Ibid., op. 1.
[1234] GERHARD, M., *Article VI* (Outer Space Treaty), cit. note 686, p. 111 (para. 37).
[1235] Ibid., p. 113 (para. 46); VON DER DUNK, F., *International Space Law*, cit. note 545, p. 54.
[1236] MARCHISIO, S., *International Legal Regime on Outer Space*, cit. note 740, p. 19; CHRISTOL, C., *International Liability for Damage Caused by Space Objects,* in 'The American Journal of International Law', Vol. 74, No. 2, 1980, p. 359; KERREST, A. AND SMITH, J., *Article VII* (Outer Space Treaty), cit. note 1224, p. 136 (para. 35).
[1237] BURKE, J., *Convention on International Liability for Damage Caused by Space Objects: Definition and Determination of Damages After the Cosmos 954 Incident*, in 'Fordham International Law Journal', Vol. 8, No. 2, 1984, p. 257.

The Liability Convention enshrines a two-pronged approach: one of object and absolute liability for damage caused by a space object of a launching State on the surface of Earth or to aircraft in flight (Article II of the Liability Convention) and one based on fault (understood either as *culpa* or *dolus*)[1238] for damages caused elsewhere (Article III of the Liability Convention). Pursuant to Article VI(1) of the Liability Convention, the absolute liability may only be exonerated in case of damage resulted either wholly or partially from gross negligence or from an act or omission done with intent to cause damage on the part of a claimant State or of the natural or juridical persons it represents. However, liability cannot be exonerated when damage results from illegal activities conducted by a launching State (Article VI(2) of the Liability Convention). The Convention does not apply to damage caused to nationals of the launching State or foreigners in the space object of the launching State (Article VII of the Liability Convention).

Pursuant to Article VIII of the Liability Convention, three States are entitled to submit a claim: the State of the nationality of the victims, the State on whose territory the damage occurred and the State whose permanent residents are affected. In any case, the decision of granting or not its diplomatic protection to the victim is a discretionary power to be determined on political or other reasons by the State concerned, as acknowledged by the ICJ in the Barcelona Traction case.[1239]

The purpose of the liability regime is that the victim State be paid a compensation agreed upon the principles of equity and justice, as provided for in Article XII of the Liability Convention. Unlike the Draft Principles on the Allocation of Loss in the Case of Transboundary Harm Arising out of Hazardous Activities that require 'prompt and adequate' compensation,[1240] the Liability Convention only provides for 'compensation' in the operative part, although a reference to a 'prompt' compensation was inserted in the fourth paragraph of the preamble. The compensation under the liability regime follows the principle of *restitutio in integrum*.[1241] Article XII of the Liability Convention provides that compensation has to

[1238] STUBBE, P. AND SCHROGL, K-U., *The Legal Significance of the COPUOS SDM Guidelines* (SDM Guidelines), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. III), 2015, p. 648 (para. 82).
[1239] *Barcelona Traction, Light and Power Company, Limited (Belgium v. Spain),* Judgement, [1970] ICJ Reports 3, 5 February 1970, para. 79.
[1240] A/61/10, cit. note 807, p. 140 (see Principle 3 and the commentary thereto).
[1241] KERREST, A. AND SMITH, J., *Article VII* (Outer Space Treaty), cit. note 1224, p. 141 (para. 55).

restore the victim to the state that *would* have existed before the damage.[1242] To claim compensation there must be a causal link between the damage and the space object; however, this does not necessarily need be immediate. It is important in this latter case that the causal chain or nexus is not interrupted.[1243]

The parties to the controversy have one year after the notification from the claim to conduct negotiations and reach a settlement. As a fall back solution, Article XIV of the Liability Convention provides for the establishment of a Claims Commission whose decision will only be final and binding if the parties so agree. Indeed, the recommendatory character of the Claims Commission is the general rule. However, States may accept the opposite rule on the basis of reciprocity –in such a case the decisions of the Claims Commission are binding. It is important to highlight that there is no requirement to exhaust local remedies under the national jurisdiction, yet the choice of one mechanism precludes submitting a claim regarding the same damage before a different settlement mechanism (Article XI). Up to the moment of writing this thesis, there is no precedent of a compensation claim via a Claims Commission.

Unlike the Outer Space Treaty, the Liability Convention provides for some definitions; most importantly, 'damage', 'launching State' and 'space object'.

Article I(a) of the Liability Convention defines damage as 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'. The definition of the concept of 'damage' has been subject to much scholarship, which is divided between a literal and an evolutionary interpretation of the definition contained in Article I(a) of the Liability Convention. Despite the divergent opinions, it is generally understood that damage to property only includes physical damage and that damage to persons includes moral damage.[1244] Some academic commentators argued that damage under the Liability

---

[1242] Cfr. 'the state that existed before the damage': *Case Concerning the Factory at Chorzow (Germany v. Poland),* PCIJ (Ser. A), No. 9, 26 July 1927, p. 28.
[1243] KERREST, A. AND SMITH, J., *Article VII* (Outer Space Treaty), cit. note 798, p. 142 (para. 57).
[1244] VON DER DUNK, F., *The 1972 Liability Convention. Enhancing Adherence and Effective Application,* in Proceedings of the Forty-First Colloquium on the Law of Outer Space, Vienna, 23 March 1998, p. 369, available at https://digitalcommons.unl.edu/ (last accessed on 11 August 2021); CHRISTOL, C., *International Liability for Damage Caused by Space Objects*, cit. note 1236, p. 370; KERREST, A. AND SMITH, J., *Article VII* (Outer Space Treaty), cit. note 1224, p. 141 (para. 55).

Convention only covers material and physical damage.[1245] Mental and social well-being has also been considered covered under damage to health.[1246]

Regarding direct and indirect damage, some pundits have explained that the course of negotiations and the underlying spirit of justice and equity at the core of the Liability Convention would allow including indirect damage.[1247] Yet other writers have a different view.[1248] Experts like Stephen Gorove have interpreted that consequential damage which does not flow directly and immediately from the act but from its consequences would not be covered.[1249] Negotiations do not appear to back the inclusion of indirect and remote damage with hypothetical causation nexus.[1250] The determination of what type of damage would be covered (direct and/or indirect) was left open on purpose by considering it a matter of causality not to be defined in the instrument.[1251] It is appropriate to underscore that the one year limit provided for the settlement mechanism under the Liability Convention was envisaged bearing in mind damage that does not manifest immediately.[1252]

Damage to the space environment caused by space debris is not covered by the notion of 'damage'.[1253] It falls under the prohibition of harmful contamination contained in Article IX of the Outer Space Treaty,[1254] although there is seldom practice confirming this

---

[1245] CHRISTOL, C., *International Liability for Damage Caused by Space Objects*, cit. note 1236, pp. 354 and 355. Also VON DER DUNK, F., *International Space Law*, cit. note 545, pp. 48, 53, 86; CHRISTOL, C., *Satellite Power System (SPS) White Paper on Inter-National Agreements,* National Technical Information Service, 1978, pp. 138-141, available at https://www.osti.gov/ (last accessed on 11 August 2021); KERREST, A. AND SMITH, J., *Article VII* (Outer Space Treaty), cit. note 1224, p. 139 (para. 51). See also MENDES DE LEON, P. AND VAN TRAA, H., *The Practice of Shared Responsibility and Liability in Space Law*, SHARES Research Paper 70 (2015), p. 21-22; MOUNTIN, S., *The Legality and Implications of Intentional Interference*, cit. note 521, p. 146.

[1246] GOROVE, S., *Cosmos 954: Issues of Law and Policy*, cit. note 842, p. 140.

[1247] CHRISTOL, C., *International Liability for Damage Caused by Space Objects*, cit. note 1236, p. 370; KERREST, A. AND SMITH, J., *Article VII* (Outer Space Treaty), cit. note 1224, p. 141 (para. 55); BURKE, J., *Convention on International Liability for Damage Caused by Space Objects,* cit. note 1237, p. 282.

[1248] CARPANELLI, E. AND COHEN, B., *Interpreting "Damage Caused by Space Objects" under the 1972 Liability Convention*, p. 10, IAC paper available at www.iislweb.org/ (last accessed 11 August 2021).

[1249] GOROVE, S., *Cosmos 954: Issues of Law and Policy*, cit. note 842, p. 141.

[1250] LSC Summary Records 10th Session, UN Doc. A/AC.105/C.2/SR.168, p. 141.

[1251] SMITH, J. AND KERREST, A., *Article I* (Liability Convention), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), Cologne Commentary on Space Law (Vol. II), Cologne, 2013, pp. 105-106 (para 33) and p. 113 (para. 56).

[1252] SMITH, J. AND KERREST, A., *Article II* (Liability Convention), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), Cologne Commentary on Space Law (Vol. II), Cologne, 2013, pp. 126-127 (para 107).

[1253] SMITH, J. AND KERREST, A., *Article I* (Liability Convention), cit. note 1251, p. 111 (para. 48) and p. 113 (para. 55). See also SMITH, J. AND KERREST, A., *Article XII* (Liability Convention), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), Cologne Commentary on Space Law (Vol. II), Cologne, 2013, p. 175 (para. 298); SMITH, J. AND KERREST, A., *Article XVIII* (Liability Convention), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), Cologne Commentary on Space Law (Vol. II), Cologne, 2013, p. 192 (paras 352-354).

[1254] MARCHISIO, S., *Article IX* (Outer Space Treaty), cit. note 799, pp. 176-177 (para. 29).

approach.[1255] Economic loss[1256] and damage to humanity[1257] are generally not included in this definition of 'damage'. Regarding damage to the environment on Earth, Marchisio considered that it is also not covered under the concept at stake,[1258] but Elena Carpanelli and Brendan Cohen pointed out that a joint interpretation of Articles I and XXI of the Liability Convention would allow for a broader interpretation of damage that would encompass significant damage to the environment on Earth as well.[1259] Paul Dembling came to a similar conclusion based on Article XII of the Liability Convention, which stipulates compensation based on justice and equity.[1260]

Some academic commentators have also argued that the definition of 'damage' does not cover interference.[1261] They tend to refer to the hearings of the Senate of the United States before the Committee on Foreign Relations relating the ratification of the Outer Space Treaty. At that time, Senator Albert Gore posed the question to the American Ambassador to the United Nations Arthur Goldberg if damage caused by jamming or other electronic means fell under 'damage' in the terms of the Liability Convention. Ambassador Goldberg replied that such damage was not covered by Article VII of the Outer Space Treaty but by Article IX of the same instrument.[1262] Furthermore, he also considered that liability under Article VII did not cover liability for any ground-based activity.[1263] Sarah Mountin argued that the concept of 'harmful interference' in the Outer Space Treaty is broader than in the ITU regime,[1264] which is limited to radiocommunication. Even if it is apparent that a legal regime governing harmful interference already exists both in telecommunications and space law, Samuel Black considered it necessary to negotiate a code of conduct defining and

---

1255 SU, J., *Control over Activities Harmful to the Environment*, in JAKHU, R. AND DEMPSEY, P. (eds), *Routledge Handbook of Space Law*, London - New York, 2017, p. 76.
1256 VON DER DUNK, F., *International Space Law*, cit. note 545, pp. 48, 53, 86. For a different view, see SMITH, J. AND KERREST, A., *Article I* (Liability Convention), cit. note 1251, p. 112 (para. 51).
1257 See CARPANELLI, E. AND COHEN, B., *Interpreting "Damage Caused by Space Objects"*, cit. note 1248, p. 4.
1258 MARCHISIO, S., *International Legal Regime on Outer Space*, cit. note 740, p. 20.
1259 See CARPANELLI, E. AND COHEN, B., *Interpreting "Damage Caused by Space Objects"*, cit. note 1248, p. 5.
1260 DEMBLING, P., *Cosmos 954 and the Space Treaties*, in 'Journal of Space Law', Vol. 6, No. 2, 1978, p. 135.
1261 VON DER DUNK, F., *International Space Law*, cit. note 545, pp. 53 and 86.
1262 Treaty on Outer Space: Hearings before the Committee on Foreign Relations, United States Senate, Ninetieth Congress, first session, on Executive D, 90th Congress, First Session, March 7, 13, and April 12, 1967, pp. 38-39.
1263 Ibid., p. 54.
1264 MOUNTIN, S., *The Legality and Implications of Intentional Interference*, cit. note 521, p. 150.

banning 'harmful interference' as a way of overcoming difficulties defining and banning 'space weapons'.[1265]

Article IX of the Outer Space Treaty is an important provision for the purposes of this research because it stipulates that States Parties shall conduct all their activities in outer space with *due regard* to the corresponding interests of all other States Parties to the Treaty. Due regard in the context of space law is one of the restrictions to space freedoms (see section 5.4). It entails the obligation to act with a certain degree of care, attention or observance[1266] and seems to be a necessary limitation in the use of global commons[1267] and a requirement for ultra-hazardous activities.[1268] In the words of a Soviet delegate during the treaty negotiations: 'States must refrain from any experiment likely to interfere with the space activities of other States'.[1269] In its third and fourth sentences, Article IX establishes a mechanism for consultations in the event of *potential* harmful interference but there is no compulsory settlement mechanism for harmful interference or any obligation to reach an agreed solution as a result of the consultations. Nor is there a definition of what 'appropriate' consultations mean under Article IX of the Outer Space Treaty.

Another important definition in Article I(c) of the Liability Convention is the concept of 'launching State'. As already indicated, the term is envisaged to include the State which launches or procures the launching of a space object and the State from whose territory or facility a space object is launched.

Last but not least, although Article I(d) of the Liability Convention does not define what a 'space object' is, it clarifies at least what is included in the concept: component parts of a space object as well as its launch vehicle and parts thereof. The fact that the liability regime only covers 'damage caused by the space object' makes this wording of vital importance. This aspect will be revisited in section 5.4 below.

There is a final issue that deserves attention: although the Outer Space Treaty distinguishes *de jure* the responsibility and liability regimes under two different provisions

[1265] BLACK, S., *No Harmful Interference with Space Objects: The Key to Confidence-Building*, Stimson Center Report No. 69, July 2008, p. 15, available at https://www.stimson.org/ (last accessed on 11 August 2021).
[1266] MARCHISIO, S., *Article IX* (Outer Space Treaty), cit. note 799, pp. 175-176 (para. 25).
[1267] Ibid., p. 176 (para. 26).
[1268] Ibid., p. 176 (para. 28).
[1269] LSC Summary Records 5th Session (1966), A/AC.105/C.2/SR. 57, p. 12.

(Article VI for responsibility and Article VII for liability), such a distinction does not always exist *de facto* because there is a connection point between both (see figure 8 below). As von der Dunk correctly pointed out, there is an intersection of regimes when there is a violation of an international obligation (international responsibility) that additionally causes damage (liability).[1270]

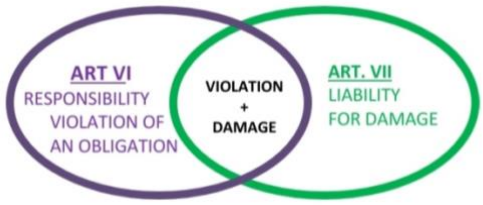


**Figure 8: Intersection between Articles VI and VII of the Outer Space Treaty**

### 5.2.2.- DOCTRINAL INTERPRETATION:

This section will endeavour to examine the considerations made by the Tallinn Experts in the second version of the Tallinn Manual (2017), and by the IISL in the 61st Colloquium of the Law of Outer Space (2018).

Yet, before getting into the details of those materials, this introductory part will make reference to a previous contribution in the field. As early as 2013, Martha Mejía-Kaiser –a current member of the IISL Board– wrote a seminal paper within a publication by the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) that reached several conclusions regarding the application of current telecommunications and space law to space cybersecurity. First, she argued that Article 45 of the ITU Constitution prohibits electromagnetic harmful interference but not malicious space cyber activities.[1271] Second, that author considered that neither the responsibility nor the liability regimes under space law offer a solution to a victim of a space cyber threat because neither is it clear that a cyber activity is a space activity under Article VI of the Outer Space Treaty, nor does damage caused by a space cyber activity fit into the definition of 'damage' under Article 1(a) of the

[1270] VON DER DUNK, *International Space Law*, in VON DER DUNK, F. (ed.), *Handbook of Space Law*, Cheltenham-Northampton, 2015, pp. 51-52.
[1271] MEJÍA-KAISER, M., *Space Law and Unauthorised Cyber Activities*, in ZIOLKOWSKI, K., (ed.), *Peacetime Regime for State Activities in Cyberspace*, NATO CCD COE, 2013, p. 355.

Liability Convention.[1272] She further explained that pursuant to Article III of the Liability Convention, damage by a space object to another one would make the launching State liable if there is fault. For fault to exist, there should be either a protective rule that was breached or an intentional or negligent act that causes damage.[1273] In the event that the damage was caused on Earth, the launching State would be absolutely liable, even if the space object was beyond its control.[1274]

**a) Tallinn Manual 2.0:**

Tallinn Manual 2.0 addressed what it named 'space-enabled space cyber operations' (in other terms, malicious space cyber activities taking control of a satellite or its payload) in Rules 58 to 64.

At the outset it is necessary to recall the notion of 'cyber operations' which this thesis explained in chapter 2 (section 2.2). A harmful activity –whether destructive or not– is implicit in every cyber operation. This clarification is of the utmost importance because under that terminological precision, and considering that according to the glossary of the Tallinn Manual a 'cyber operation' is meant in an operational context, the language chosen in Tallinn Manual 2.0. is not always the appropriate one. For instance, Rule 58(a) stipulates: 'Cyber operations on the moon and other celestial bodies may be conducted only for peaceful purposes'. The more appropriate language for that Rule would be 'space cyber activities' because due to the complete demilitarisation of the Moon and the celestial bodies established in Article IV of the Outer Space Treaty, cyber operations shall be understood to be forbidden (see chapter 3, section 3.9.1). Rule 58(b) will be scrutinised in the next section.

Rule 59 clearly reproduces core provisions of the Outer Space Treaty, notably Articles VIII and IX. In effect, Rule 59(a) provides that States have to respect the jurisdiction and control of the State of registry. For its part, paragraph (b) imports the duty of due regard contained in Article IX of the Outer Space Treaty and merges it with a second obligation contained in the same provision: the one that calls upon States to avoid (harmful) interference. The rule reads as follows: 'A State must conduct its cyber operations involving

[1272] Ibid., p. 360.
[1273] Ibid., p. 364.
[1274] Ibid., p. 366.

outer space with due regard for the need to avoid interference with the peaceful space activities of other States'. It should be noted that the wording in this rule deviates from the language enshrined in the telecommunications and space law regimes, which is 'harmful interference', and replaces it with 'interference with the peaceful space activities of other States'. Moreover, the wording that this rule employs conveys the idea that there are certain interferences caused by malicious cyber activities that might be allowed– these can be read to be the interferences with non-peaceful space activities of other States. It should be recalled that the due regard obligation and the obligation to consult in case of harmful interference are two different obligations. A more appropriate wording for this rule would have been: 'A State must conduct its space cyber activities with due regard to the interests of other States and avoiding harmful interference'.

The commentary clarifies that malicious space cyber activities that create space debris might violate the right of other States to conduct their space activities[1275] yet there is no thorough analysis of the connection between space debris creation and the obligation of due regard (see section 5.4 below).

Rule 60 uses a different wording in paragraphs (a) and (b). The former reads: 'A State must authorise and supervise the *cyber "activities* in outer space" of its non-governmental entities' (emphasis added), which appears to assume the idea that 'cyber activities in outer space' are tantamount to 'activities in outer space', which is the wording used in the second sentence of Article VI of the Outer Space Treaty.[1276] Paragraph (b) reads: '*Cyber operations* involving space objects are subject to the responsibility and liability regime of space law' (emphasis added). One reading of this paragraph is that, by asserting that the regime of responsibility applies to 'cyber operations', Tallinn Manual 2.0 implicitly admits that they (or some of them) may constitute a wrongful act –the necessary requirement for responsibility to arise. An additional reading is that, by affirming that the regime of liability applies to 'cyber operations', Tallinn Manual 2.0 hints that certain space cyber activities are legal but may cause damage in the terms of the liability regime. Unfortunately, broad interpretations of permissible activites in outer space may even include the use 'cyber warfare technologies'.[1277]

[1275] *Tallinn Manual 2.0,* cit. note 40, Rule 59, commentary, para. 6.
[1276] *Tallinn Manual 2.0,* cit. note 40, Rule 60, commentary, para. 1.
[1277] See RAJESWARI PILLAI RAJAGOPALAN, *Electronic and Cyber Warfare in Outer Space*, cit. note 477, p. 13, available at www.unidir.org (last accessed on 11 August 2021).

The experts of Tallinn Manual 2.0 examined the concept of 'damage' in light of the liability regime and excluded two types of damage from its scope: 1) deletion or alteration of data unless it leads to physical damage and 2) economic loss for the space object damaged. However, they considered permanent loss of functionality of the space object to be 'damage' compensable under the liability regime.[1278]

The analysis made in Tallinn Manual 2.0 regarding the applicability of the liability regime can be summarised as follows:

1. Damage on Earth:

The commentary foresees the case of absolute liability of a launching State for a 'cyber operation' of that State deorbiting its own space object and causing damage on Earth.[1279] In addition, it addresses the case of damage caused by a 'cyber operation' carried out by a State other than the launching State. If there is gross negligence or an intentional act by the victim State, Article VI of the Liability Convention exonerates absolute liability of the launching State.[1280] However, if there is no exoneration, the victim State will seek compensation from the launching State –even if it was unable to control the space object registered with it as a consequence of the 'cyber operation'. In such a case –the commentary continues– the launching State might claim responsibility of the State that carried out the 'cyber operation' under the assumption that such an 'operation' is 'an activity in outer space' under Article VI of the Outer Space Treaty.[1281]

2. Damage in flight:

In this case, the commentary again distinguishes two scenarios:[1282] one where a State conducts a 'cyber operation' against a foreign space object causing damage to a third space object in flight, and a 'cyber activity' of the launching State that causes its own space object to damage a foreign space object in flight. In the former case, the commentary assumes that the launching State is not at fault (this conclusion would only hold true if there is no obligation to protect own space assets against malicious space cyber activities or a duty to

[1278] *Tallinn Manual 2.0,* cit. note 40, Rule 60, commentary, para. 9.
[1279] Ibid., para. 5.
[1280] Ibid., para. 6
[1281] Ibid, para. 7.
[1282] Ibid., para. 8.

minimise the effects of an ongoing malicious cyber activity). In the latter case, the commentary assessed that the launching State would be liable for failing to properly test the software it executed (this conclusion would only hold true if there is an obligation of due regard that encompasses testing own software). This means that the commentary assumes an obligation of due diligence for own space cyber activities in outer space but does not assume an obligation to protect space objects registered with it from third States' malicious cyber activities.

Although this section is devoted only to space law, a brief reference should be made to chapter 11 of Tallinn Manual 2.0, which is dedicated to telecommunications law. In that context, it is relevant to refer to Rule 63 dealing with 'harmful interference' based on Article 45(1) of the ITU Constitution.

**b) <u>The International Institute of Space Law:</u>**

In 2017, the IISL decided to look into the question of whether cyber law should be included as a topic for future work. For that purpose, a working group on cyber law composed of 22 IISL members was divided into five sub-working groups (SWGs) to discuss the following issues:

SWG 1) The technical architecture of cyberspace;

SWG 2) Whether there is a self-contained regime for cyberspace;

SWG 3) Who should regulate cyberspace;

SWG 4) Whether space law is applicable to cyber activities in outer space;

SWG 5) The legal aspects of space cybersecurity.

The aspects addressed by SWGs 3 to 5 are very much connected to the subject matter of the present research. SWG 3 concluded that there are three possible alternative answers to the question of who should regulate cyberspace: a) nobody –no regulation is required, b)

international law is applicable on the grounds that cyberspace is a global commons or 3) cyberspace should be self-regulated by manufacturers, companies and other users.[1283]

SWG 4 concluded that cyber-enabled operations should be clarified and –for such purposes– existing space law terminology should be interpreted or its scope should be expanded or new rules should be created to address them.[1284]

Last but not least, SWG 5 assessed that cyber threats should be identified and legally classified. In addition, the application of space law and international law (notably *jus ad bellum* and *jus in bello*) should be examined.[1285]

Upon the conclusions of the five SWGs, the IISL Working Group on Cyber Law decided to include the topic in future colloquia starting from 2018 onwards. Thus, the IISL addressed space cybersecurity matters in the 61st Colloquium on the Law of Outer Space in Bremen, Germany (2018). On that opportunity, a set of papers regarding the relationship between space law and cyber law were presented. There are several points that deserve attention in the present section.

Rada Popova reflected on the improper generalisation of the term 'cyberattack', and expressed preference for the wording 'malicious cyber activities' to refer to the wide range of cyber threats –which encompass the gravest form (cyberattacks).[1286] She considered that by virtue of the 'principles' of due regard and non-interference emanating from Article IX of the Outer Space Treaty, cyber activities in outer space should not damage the rights that other States have to conduct space activities peacefully, which otherwise would entail State responsibility.[1287] Following up on the prior investigation conducted by Mejía-Kaiser in 2013 (already examined *supra)*, Popova concluded that it is questionable whether the liability regime of space law is applicable to damage caused by cyber threats.[1288]

---

[1283] IISL Working Group on Cyber Law, Report by Stephan Hobe, Cologne 2018, pp. 4-5, available at https://iislweb.org/ (last accessed on 11 August 2021).
[1284] Ibid. p. 5.
[1285] Ibid.
[1286] POPOVA, R., *Cyber Law and Outer Space (Activities): Legal and Regulatory Challenges*, in Proceedings of the International Institute of Space Law 2018, The Hague, 2019, p. 660.
[1287] Ibid., p. 668.
[1288] Ibid.

For its part, Stefan Kaiser identified several principles of space law that might be applicable to cyber activities, such as the principles of peaceful purposes, benefit and interest of all countries, non-discrimination, international cooperation and international peace and security.[1289]

Setsuko Aoki put together several covert malicious threats under the umbrella of 'malicious cyber activities'; namely, jamming, hijacking, hacking, spoofing and control seizure of TT&C. She equated the latter with 'a premature type of anti-satellite (ASAT)'.[1290] On another note, she concluded that the ITU regime only addresses harmful interference in the event of activities conducted by non-State actors and advanced that the fusion of telecommunications and space law is foreseeable in the future.[1291] Finally, she expressed doubts about the applicability of the liability regime under space law for intangible damage.[1292]

The analysis made by P.J. Blount started from the assumption that certain cyber threats might amount to an ASAT. He continued considering that cyber-ASATs are a watershed because the technology they employ changes the traditional restrains that States used to have with other ASAT technologies –notably, the creation of space debris and easy attribution.[1293] He pointed at the legal framework applicable to the limitation of traditional ASATs, which includes the Partial Test Ban Treaty of 1963 and Articles I, IV and IX of the Outer Space Treaty.[1294]

Gina Petrovici and Antonio Carlo argued that according to the responsibility that Article VI of the Outer Space Treaty imposes on States, they should refrain from 'accepting, encouraging and engaging in un-authorized cyber-attacks'.[1295] For his part, Roy Balleste held that a State not involved in a conflict would violate Article III of the Outer Space Treaty if

---

[1289] KAISER, S., *In Search of an International Public Order for Cyber Activities*, in Proceedings of the International Institute of Space Law 2018, The Hague, 2019, p. 685.
[1290] AOKI, S., *Identifying the Scope of the Applicable International Law Rules towards Malicious Cyber Activities against Space Assets*, in Proceedings of the International Institute of Space Law 2018, The Hague, 2019, p. 688.
[1291] Ibid., p. 699.
[1292] Ibid.
[1293] BLOUNT, P. J., *That Escalated Quickly: The Cyber-ASAT Conundrum*, in Proceedings of the International Institute of Space Law 2018, The Hague, 2019, p. 707.
[1294] Ibid., pp. 703 – 704.
[1295] PETROVICI, G. AND CARLO, A., *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 Proceedings of the International Institute of Space Law 2018, The Hague, 2019, p. 85.

it engages in malicious space cyber activities aimed at disabling or destroying space objects that belong to another State when it knowingly allows its territory to be used for such acts.[1296]

From the review made above, it is possible to reaffirm the conclusion reached earlier in this research; namely, that there is no agreement in the literature as to the terminology (cyber operations, cyber activities, malicious cyber activities, unauthorised cyberattacks). For a part of the literature there is an assumption that needs to be further looked into: if space cyber activities are space activities for the purposes of the space treaties. Moreover, it should be elucidated if there is an obligation to protect own space objects and prevent malicious cyber activities from third parties. Finally, it should be determined whether the responsibility and the liability regimes apply to malicious space cyber activities. All these issues will be further examined in section 5.4.

## 5.3.-RELEVANT PROVISIONS OF INTERNATIONAL LAW APPLICABLE TO SPACE CYBERSECURITY

This section will move away from space law towards the more general regime of international law. Thus, it will seek to describe how scholars have assessed that international law might apply to space cybersecurity.

The only rule in chapter 10 of Tallinn Manual 2.0 that deals with the application of international law to space cybersecurity is Rule 58(b), which provides the following: 'Cyber operations in outer space are subject to international law limitations on the use of force'. The commentary clarifies that the underlying idea was to confirm that the use of force is forbidden in outer space.[1297] Nonetheless, the manual acknowledges that generally accepted exceptions apply in outer space as well: the Security Council might authorise the use of force in outer space, and States may exercise the right to self-defence in that domain. The Tallinn experts also considered the exercise of self-defence in outer space to be lawful, even as a response to armed attacks occurring on Earth.[1298]

[1296] BALLESTE, R., *Reconsidering Rules of Engagement in Outer Space*, in Proceedings of the International Institute of Space Law 2018, The Hague, 2019, p. 734.
[1297] *Tallinn Manual 2.0,* cit. note 40, Rule 58, commentary, para. 3.
[1298] Ibid., para. 4.

**a) Non-intervention:**

Mountin mentioned some examples of interferences that would constitute a violation of the non-intervention principle (although she referred to electromagnetic interference, the conclusions may be transposable to cyber interference).[1299] She pointed out the cases where interference was aimed at forcing a political change or the manipulation of elections. For its part, Aoki considered that it is 'clear' that overtaking the control of a satellite's TT&C is a violation of the principle of non-intervention.[1300]

**b) Sovereignty:**

Popova argued that cyber activities in outer space should not interfere with a State's jurisdiction and control over a space object; otherwise, they would violate its sovereignty.[1301] Aoki was of the view that overtaking the control of a satellite is also a violation of the principle of sovereignty.[1302]

**c) Use of force:**

Thomas Wingfield distinguished two types of malicious cyber activities: those carried out *through* satellites affecting a target on Earth and those undertaken *against* satellites. As to the former, he pointed out that the more attenuated the role of the satellite in the malicious space cyber activity at stake, the greater the possibility that international law will not be violated.[1303] Regarding the latter, he discerned five types of malicious cyber activities *against* satellites: blinding, shutdown, movement, destruction and appropriation, and impressment. On that basis, he assessed that a destructive cyber activity 'is the closest fit with traditional terrestrial military uses of force'.[1304] Jackson Maogoto and Steven Freeland acknowledged that there are several activities in space that might meet the threshold of the use of force; however, they might only be easily identifiable as such in a context of hostilities but not in a peaceful one.[1305] Blount also considered that cyberattacks of 'a certain magnitude' might be

[1299] MOUNTIN, S., *The Legality and Implications of Intentional Interference*, cit. note 521, p. 157.
[1300] AOKI, S., *Identifying the Scope of the Applicable International Law Rules*, cit. note 1290, p. 687.
[1301] Ibid., p. 668.
[1302] Ibid., p. 687.
[1303] WINGFIELD, T., *Legal Aspects of Offensive Information Operations in Space*, Department of Defense Washington DC, 2005, available at https://apps.dtic.mil/ (last accessed on 11 August 2021).
[1304] Ibid.
[1305] MAOGOTO, J. AND FREELAND, S., *Space Weaponization and the United Nations*, cit. note 858, pp. 1112.

considered a use of force; although, he acknowledged that there is no clarity when such threshold is met.[1306]

**d) Armed attacks and self-defence:**

Christopher Petras argued that a cyberattack against a satellite can be equated with a use of armed force because the effect is similar to what an ASAT or any other kinetic means would have.[1307] In analogy with the right to self-defence of vessels in the high seas, he explained that the State of registry –which is the State that retains jurisdiction and control pursuant to Article VIII of the Outer Space Treaty– would have the right to protect the space asset over which it has jurisdiction because such jurisdiction may be understood as equivalent to 'sovereignty' when it comes to outer space.[1308] He quoted Ian Brownlie to support the argument that space assets would be –as vessels are– analogous to the territory of the State; hence, the State of registry might use force in self-defence to protect them.[1309] Maogoto and Freeland considered that a cyberattack in outer space can objectively be likened to armed force.[1310] Rajagopalan assessed that, in a context of privatisation of outer space activities, it would be difficult to determine if a cyberattack against a satellite that is privately owned and operated could be equated to a State-to-State attack.[1311]

Despite the views outlined above, whether a malicious space cyber activity constitutes a use of force or an armed attack is an unresolved issue.[1312] The Russian Federation and China already expressed the view that the application of the relevant provisions of the Charter 'requires further elaboration and clarification through negotiation between States' in COPUOS,[1313] particularly taking into account the wide range of

---

1306 BLOUNT, P.J., *That Escalated Quickly,* cit. 1293, p. 706.
1307 PETRAS, C., *The Use of Force in Response to Cyber-Attack,* cit. note 632, p. 1259.
1308 Ibid., pp. 1255-1256.
1309 Ibid., pp. 1257-1258.
1310 MAOGOTO, J. AND FREELAND, S., *Space Weaponization and the United Nations*, cit. note 858, p. 1113.
1311 See RAJESWARI PILLAI RAJAGOPALAN, *Electronic and Cyber Warfare in Outer Space*, cit. note 477, p. 14.
1312 See HOUSEN-COURIEL, D., *Cybersecurity Threats to Satellite Communications: Towards a Typology of State Actor Responses*, in 'Acta Astronautica', Vol. 128, 2016, p. 411.
1313 Letter dated 11 September 2015 from the Permanent Representative of China to the Conference on Disarmament and the Charge d'affaires a.i. of the Russian Federation addressed to the Secretary-General of the Conference transmitting the comments by China and the Russian Federation regarding the United States of America analysis of the 2014 updated Russian and Chinese texts of the draft treaty on prevention of the placement of weapons in outer space and of the threat or use of force against outer space objects (PPWT), CD/2042, 14 September 2015, paras 9-10.

possibilities to affect space systems with malware.[1314] Several academic commentators agree that there is a need for complementary instruments to address space cyber threats.[1315] The question is whether it is feasible to address all aspects in a singular instrument or if the regulatory task needs to be progressive.

## 5.4.-IDENTIFICATION OF LEGAL LACUNAE

Focusing on legal lacunae requires reflecting on the fact that international law has a consensual nature; i.e. States are bound as long as they have consented to be bound. Some authors contend that when neither treaty nor customary law regulates a situation, the general principles of law as per Article 38(1)(c) of the ICJ Statute apply and fill the gap avoiding a *non liquet*.[1316] One of such principles of particular importance for this thesis is the principle that no State should knowingly allow its territory (or its infrastructures) to be used by others contrary to the rights of third States.[1317]

Traditionally, the doctrine refers to the Lotus principle as one of the building blocks of the international law system, whereby States are allowed to do all that is not prohibited. In other words, lacunae mean the lack of an obligation regarding a certain conduct. On the basis of the principle that 'everything that is not prohibited by international law is permitted', the PCIJ examined in the referred case whether there was a rule of international law forbidding Turkey to criminally prosecute a foreigner on board of a French ship when the effects of the offence were produced on the Turkish vessel.[1318] The tribunal held that 'restrictions upon the independence of States cannot be presumed'[1319] –there needs to be a prohibitive rule accepted by the State to limit its action.[1320]

This principle, however, is not free from criticism and revisionism attempts. Judge Simma criticised the majority vote in the Kosovo advisory opinion, where the Court

---

[1314] Ibid., para. 8.
[1315] RAJESWARI PILLAI RAJAGOPALAN, *Electronic and Cyber Warfare in Outer Space*, cit. note 477, p. 17; FALCO, G., *The Vacuum of Space Cybersecurity*, cit. note 510, p. 11; MAOGOTO, J. AND FREELAND, S., *Space Weaponization and the United Nations*, cit. note 858, p. 1118.
[1316] ZHUKOV, G. AND KOLOSOV, Y., *International Space Law*, cit. note 688, p. 23; STEER, C., *Sources and Law-Making Processes*, cit. note 793, p. 8. See also UN Doc. A/CN.4/732, cit. note 358, para. 144.
[1317] STEER, C., *Sources and Law-Making Processes*, cit. note 793, p. 9.
[1318] *Lotus,* cit. note 155, pp. 22-23.
[1319] Ibid, p. 18.
[1320] Ibid, p. 19. See also *Nicaragua*, cit. note 154, para. 269; *Nuclear Weapons*, cit. note 188, para. 52.

reinterpreted the question put by the General Assembly on whether the declaration of independence of Kosovo was 'in accordance with international law' as whether international law prohibited the independence declaration.[1321] In his declaration, Simma characterised the approach based on the Lotus principle whereby the Court considered that –since there was no prohibition– the declaration was in accordance with international law, as an 'anachronist, extremely consensualist vision of international law'.[1322] He concluded that there is a difference between the existence of a permissive rule and the inexistence of or silence on a rule.[1323] Simma continued arguing that the inexistence of a prohibition does not necessarily mean that the conduct is legal[1324] but that 'that there are areas where international law has not yet come to regulate or indeed will never come to regulate'.[1325]

Space law experts do not hold a uniform position either. In a recent publication (2021), von der Dunk argued that the clauses of the Outer Space Treaty that crystallise the use and exploration of outer space as the province of all mankind and the relevant freedoms have inserted the Lotus principle into space law.[1326] To the contrary, other legal academic commentators rule out the application of the Lotus principle to space law because the limit imposed to what is not prohibited is the interest and the rights of other States pursuant to the principle of the global public interest in outer space.[1327]

With this discussion as a backdrop, and taking into consideration the analysis made previously in this chapter, it is crucial to answer the following questions: 1) whether malicious space cyber activities are prohibited by a primary rule (in order to determine the applicability of the responsibility regime), 2) whether damage by cyber means can be interpreted as damage by the space object (in order to assess the applicability of the liability regime) and 3) whether the creation of space debris as a result of a space cyberattack would be compensable under the liability or responsibility regimes.

---

1321 *Kosovo*, cit. 200, para. 56.
1322 Ibid., Declaration of Judge Simma, para. 3.
1323 Ibid.
1324 Ibid., para. 9.
1325 Ibid.
1326 VON DER DUNK, F., *Armed Conflicts in Outer Space*, cit. note 870, pp. 196.
1327 See JAKHU, R., *Legal Issues relating to the Global Public Interest*, cit. note 815, pp. 42-43.

**(Q1) Whether malicious space cyber activities are prohibited by a primary rule (responsibility):**

**a) Under international law:**

This chapter has already argued that there is no explicit obligation under international law that expressly mandates not engaging in malicious space cyber activities, no matter where they take place. However, they may violate for instance the obligation of non-intervention, the principle of sovereignty and the obligation to refrain from the use of force. Thus, it is not the malicious space cyber activity *per se* that would breach an international rule but rather *how* the conduct has been carried out, i.e. if it meets certain requirements or reaches a certain threshold. For the time being, it is difficult to imagine that an instrument (rather than future practice) would provide more clarity on this in the short term.

**b) Under space and telecommunications law:**

Likewise, this thesis has already demonstrated that there is no explicit prohibition under space law not to engage in malicious space cyber activities as such. However, certain primary rules are relevant to determine responsibility for such conducts: the obligation to use and explore outer space for the benefit and in the interests of all countries (Article I of the Outer Space Treaty) in accordance with international law and in the interest of maintaining international peace and security (Article III of the Outer Space Treaty), to consult in case of potential harmful interference (Article IX of the Outer Space Treaty), to avoid harmful interference to the radio services or radiocommunications (Article 45(1) of the ITU Constitution), to avoid harmful contamination (Article IX of the Outer Space Treaty) and to conduct space activities with due regard (Article IX of the Outer Space Treaty).

It should be underscored that at the time of the negotiations of the Outer Space Treaty, the space activities that were in the minds of the drafters were launching satellites, landing on the Moon and sending astronauts into outer space. Since space law emerged in a different technological context where space cyber activities were not even foreseeable, there are three issues that currently need some clarity and interpretation for the application of the Outer Space Treaty provisions referred above:

1) If space cyber activities are 'exploration and use of outer space' in the terms of Article I of the Outer Space Treaty.

2) If space cyber activities are 'activities in the exploration and use of outer space' in the terms of Article III of the Outer Space Treaty.

3) If space cyber activities are 'activities in outer space' in the terms of Article IX of the Outer Space Treaty.

While the language in the three provisions differs slightly, it is possible to infer from the *travaux préparatoires* that they were employed with the same meaning throughout the text of the treaty.

Article I of the Outer Space Treaty is generally considered to enshrine the freedom of use and exploration of outer space; however, that freedom has certain limitations. One of them is that the interest of all mankind shall be taken into consideration.[1328] Similarly, Articles III and IX also establish limitations to space freedoms –the former based on international law and the latter based on the exercise of due regard.

The wording in Article I of the Outer Space Treaty not only refers to the exploration but also to the use of outer space. This formula was introduced at an early stage of treaty negotiations by a Soviet draft.[1329] For its part, the American draft only made reference to the 'exploration of the moon and other celestial bodies'.[1330] At that time, the French delegate emphasised that the term 'use' required further clarification in order to determine whether it included 'exploitation'[1331] –to which the Soviet delegate reacted referring to the provision of non-appropriation.[1332] In the same line, the Hungarian delegate indicated that the terms 'use'

[1328] HOBE, S., *Article I* (Outer Space Treaty), cit. note 541, p. 38-39 (para. 52).
[1329] Draft Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, the Moon and Other Celestial Bodies (Soviet Union), letter dated 11 July 1966 reproduced in A/AC.105/C.2/L.13, 11 July 1966.
[1330] Draft Treaty Governing the Exploration of the Moon and other Celestial Bodies (United States), letter dated 16 June 1966 reproduced in UN Doc. A/AC.105/C.2/L.12, 11 July 1966.
[1331] LSC Summary Records 5th Session (1966), UN Doc. A/AC.105/C.2/SR.63, p. 8; UN Doc. A/AC. 105/C.2/SR.69, p. 5
[1332] LSC Summary Records 5th Session (1966), UN Doc. A/AC/.105/C.2/SR. 63, p. 10.

and 'exploration' needed to be defined.[1333] On another opportunity, France directly expressed reservations regarding the term 'use'.[1334]

Although the treaty did not clarify those terms, the Cologne Commentary to the Outer Space Treaty tried to shed some light on the meaning of 'exploration', explaining that it is the activity that seeks to find out whether any use is possible.[1335] It also described the term 'use' as a broad concept that includes '[a]ll kinds of activities that purport to make use of space in one way or another, including launch activities on Earth or the usage of satellites'.[1336]

While Article III employs the phrase 'activities in the exploration and use of outer space', there is not much difference in the meaning with regard to the expression employed in Article I.

A more simplified language is used in Article IX, which speaks of 'activities in outer space'. Chapter 3 (section 3.8) already clarified that the term 'activities in outer space' –used repeatedly in the treaty– encompasses the launching, the operation and the return of space objects. In the analysis of Article VI of the Outer Space Treaty –which employs the same expression– Michael Gerhard distinguished two currents of interpretation: one that considers an activity in outer space to be any activity aimed at accessing, exploring or using outer space.[1337] The other one is broader and considers activities in outer space to be any activity even taking place on Earth that is intentionally directed towards outer space.[1338] Soviet experts, like Gennady Zhukov and Yuri Kolosov, represent the latter interpretative current –they consider space activities also those that are 'organically' linked with the launching, operation and return of space objects, even if they are carried out on the ground.[1339] Gerhard further provided a non-exhaustive list of activities in outer space, which includes the operation and control of a satellite, a probe, a platform or a space station; the use of such objects; the launching of space objects into outer space; manufacturing of

[1333] LSC Summary Records 5th Session (1966), UN Doc. A/AC.105/C.2/SR. 66, p. 4.
[1334] UN Doc. A/AC.105/C.2/SR.70, cit. note 861, p. 14.
[1335] HOBE, S., *Article I* (Outer Space Treaty), cit. note 541, p. 34 (para. 34).
[1336] Ibid., p. 35 (para. 37).
[1337] GERHARD, M., *Article VI* (Outer Space Treaty), cit. note 686, p. 107 (para. 20).
[1338] Ibid., pp. 107-108 (para. 21).
[1339] ZHUKOV, G AND KOLOSOV, Y., *International Space Law*, cit. note 688, p. 12.

elements in outer space and exploration, exploitation and use of celestial bodies.[1340] Some authors even include 'any space-related activity that is yet to develop in the future'.[1341]

When Stephan Hobe fleshed out Article I of the Outer Space Treaty, he interpreted that there are basically three activities which are the scope of the Outer Space Treaty: use, exploration and scientific investigation.[1342] The concepts of 'use' and 'exploration' were already elucidated above, but the reference to scientific investigation as a separate third category is novel until now. The ICJ had the chance to elucidate the meaning of a similar concept –'scientific research'– in the Whaling case. In that opportunity, the Court had to determine whether lethal methods for purposes of scientific research were in accordance with the Convention for the Regulation of Whaling. The criteria presented by an Australian expert to interpret the concept of 'scientific research' in the context of the Convention were dismissed by the Court, which did not even consider it necessary to define the term at all.[1343] The separate opinion of Judge Cançado Trindade made a significant contribution to the understanding of the sustainable use of living resources by rejecting an 'unfettered discretion to decide the meaning of "scientific research"'.[1344] He agreed with the majority vote that it was not necessary to define 'scientific research' for all purposes but emphasised that those conducting scientific research shall abide by the principle of prevention and the precautionary principle.[1345]

In sum, although there is no definition in the treaty of any of the formulations that were just reviewed, and even if the language slightly differs throughout the provisions, it is safe to conclude that launching, operation and control of a space asset for use, exploration or scientific research are covered by the terminology under study.

Now, it should be examined whether such activities include space cyber activities. As already explained in chapter 3 (section 3.8.2), the Outer Space Treaty was drafted with vague terms to allow for its flexibility and adaptation to the course of technological development.

---

[1340] GERHARD, M., *Article VI* (Outer Space Treaty), cit. note 686, p. 109 (para. 28).
[1341] HOBE, S. AND CHEN, K-W., *Legal Status of Outer Space and Celestial Bodies*, in JAKHU, R. AND DEMPSEY, P. (eds), *Routledge Handbook of Space Law*, London - New York, 2017, p. 26.
[1342] HOBE, S., *Article I* (Outer Space Treaty), cit. note 541, p. 41 (para. 60).
[1343] *Whaling in the Antarctic (Australia v. Japan. New Zealand: intervening)*, Judgement, [2014] ICJ Reports 226, 31 March 2014, para. 86.
[1344] Ibid., Separate Opinion of Judge Cançado Trindade, para. 24.
[1345] Ibid., para. 23.

The statements made by the representatives of Argentina Aldo Cocca and Mario Campora during the negotiations is a clear reflection of a forward-looking approach requiring caution in drafting a binding instrument to avoid it becoming obsolete due to the rapid pace of technological progress.[1346] In addition, the findings of the ICJ in the Namibia advisory opinion should be borne in mind. There, the tribunal concluded that certain concepts are 'not static, but [are] by definition evolutionary'.[1347] Consequently, the activities referred above –regardless of whether they are undertaken by the use of ICTs– should also comply with the limitations that the Outer Space Treaty establishes to the freedom of use and exploration of outer space, in particular those laid out in Articles I, III and IX as explained. A malicious space cyber activity would run counter to the obligations enshrined in the Outer Space Treaty and thus might entail international responsibility.

**(Q2) Whether damage by cyber means can be interpreted as damage caused by the space object (liability):**

The previous part has reached the conclusion that space cyber activities might be unlawful if they breach certain provisions of space and telecommunications law, or of international law in general. However, it should be acknowledged that there are some space cyber activities that are legal and; therefore, no responsibility arises from them. In such a case, it is appropriate to build upon the premise that even if a space cyber activity is legal, it might cause damage anyway. Thus, the question arises as to whether damage caused by cyber means would be compensable under the liability regime.

As already clarified in section 5.2.1, the liability regime applies to damage 'caused by the space object'. In effect, Article VII of the Outer Space Treaty provides that the State that launches or procures the launching of a space object and each State Party from whose territory or facility an object is launched is internationally liable for damage to another State Party by such object. In line with that, the Liability Convention also makes the launching State liable for 'damage caused by its space object'.

[1346] LSC Summary Records 3rd Session (1964), UN Doc. A/AC.105/C.2/SR.29-37, pp. 42-43. See also LSC Summary Records 4th Session (1965), UN Doc. A/AC.105/C.2/SR.43, p. 4.
[1347] *Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970),* Advisory Opinion, [1971] ICJ Reports 16, 21 June 1971, para. 53. See also UN Doc. A/61/10, cit. note 807, p. 416 (para. 23).

The language 'damage caused by the space object' –instead of broader formulations like 'damage caused by exploration'[1348] or 'damage caused by accidents to space vehicles'[1349]– can be traced back to the early negotiations of UNGA Resolution 1962 (XVIII). After UNGA Resolution 1348 (XIII) requested to set up an *ad hoc* committee to report, *inter alia,* on the nature of legal problems that might arise in the exploration of outer space, the United States submitted a working document that already employed similar wording: 'damage caused by space vehicles'.[1350]

According to customary law on treaty interpretation embodied in Article 31 of the Vienna Convention on the Law of the Treaties, '[a] treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose'. A textual reading of the Liability Convention provides the first element for interpretation: there is a coherent language used in the title, the preamble and the clauses of the Liability Convention –they all refer to damage caused by the space object. Similar language was used in Article VII of the Outer Space Treaty and in UNGA Resolution 1962 (XVIII) ('for damage [...] by such object or its component parts').

According to the commentary of the ILC to the Draft Articles on the Law of the Treaties, the object and purpose of a treaty is often stated in its preamble.[1351] In the particular case of the Liability Convention, the fourth paragraph of its preamble reads:

> *Recognizing* the need to elaborate effective international rules and procedures concerning liability for *damage caused by space objects* and to ensure, in particular, the prompt payment under the terms of this Convention of a full and equitable measure of compensation to victims of such damage,[1352] (emphasis added)

In addition, Article 31(3) of the Vienna Convention on the Law of the Treaties foresees that in the interpretative task, subsequent agreements between the parties regarding the interpretation of the treaty or its application and subsequent practice in its application should be taken into account as part of the context of the treaty. The Liability Convention

[1348] LSC Summary Records 2nd Session (1962), UN. Doc. A/AC.105/C.2/SR.2, p. 5 (Mexico).
[1349] LSC Summary Records 2nd Session (1962), UN Doc. A/AC.105/C.2/SR.04, p. 11 (Romania).
[1350] Report under Paragraph 1(d) of the GA Res 1348 (XIII), UN Doc. A/AC.98/L.7, 27 May 1959, p. 3.
[1351] See Draft Articles on the Law of the Treaties with commentaries, *Yearbook of the International Law Commission, 1966*, vol. II, commentary to Article 27 (para. 12).
[1352] Liability Convention, cit. note 753, preamble.

can be considered a subsequent agreement on the interpretation and application of Article VII of the Outer Space Treaty (Article 31(3)(a) of the Vienna Convention on the Law of the Treaties) since it provides evidence of the understanding of the parties as to the meaning of that provision.

However, if national space law is examined under Article 31(3)(b) of the Vienna Convention on the Law of the Treaties, it can be inferred that there is a differing State practice regarding the language used to refer to liability. For instance, the Dutch Space Activities Act regulates 'liability arising from the space activities'.[1353] The Law of the Russian Federation about Space Activity establishes full compensation for 'direct damage inflicted as a result of accidents while carrying out space activity'.[1354] The Swedish Act on Space Activities foresees liability 'for damage which has come about as a result of space activities'.[1355] The Outer Space Act 1986 of the United Kingdom refers to liability for the activities authorised by the license.[1356] The French Space Operations Act envisages liability 'for damages caused to third parties by the space operations'.[1357]

Some legal experts have assessed that 'damage' includes either the harm caused by kinetic or virtual (cyber) means.[1358] In the latter case, the argument could be made that the OBC or the software is an integral part of the space object; and in the case of a space cyber activity in a satellite targeting another satellite in orbit, the condition of 'damage by the space object' might be fulfilled. However, it should be underscored that in such a case, it would not be a lawful cyber space activity, but an illegal one and thus would fall under the regime of responsibility (Q1). Moreover, the Cologne Commentary to the Liability Convention argued that the ordinary meaning of the treaty would favour the interpretation that the treaty only covers damage resulting from impact but not from an immaterial origin (such as a virus would be) –although the Commentary acknowledged that the discussion is not yet settled.[1359]

---

[1353] See Selected Examples of National Laws Governing Space Activities: Netherlands, available at https://www.unoosa.org/(last accessed on 11 August 2021). See Section 1(3)(4).
[1354] See Selected Examples of National Laws Governing Space Activities: Russian Federation, Article 30, available at https://www.unoosa.org/(last accessed on 11 August 2021).
[1355] See Selected Examples of National Laws Governing Space Activities: Sweden, Section 6, available at https://www.unoosa.org/(last accessed on 11 August 2021).
[1356] See Outer Space Act 1986 of the UK, available at https://www.legislation.gov.uk/ (last accessed on 11 August 2021).
[1357] See unofficial translation of France's 'LOI no 2008- 518 du 3 juin 2008 relative aux opérations spatiales', ar.t 13, available at https://aerospace.org/ (last accessed on 11 August 2021).
[1358] See HOUSEN-COURIEL, D., *Cybersecurity Threats to Satellite Communications*, cit. note 1312, p. 412.
[1359] SMITH, J. AND KERREST, A., *Article II* (Liability Convention), cit. note 1252, p. 129 (para. 113).

Likewise, some authors considered that the liability regime of space law does not cover damage caused by signals[1360] or interference caused by telecommunication satellites (see section 5.2.1).[1361]

From the analysis and opinions exposed above, it is safe to conclude that a literal interpretation of the Liability Convention does not make room for damage caused by other than space objects as defined in the same instrument. However, State practice seems to confirm the existence of a broader interpretation in the domestic law of certain States. The latter does not mean that the treaty text became modified –not until a customary rule emerges– but only that certain States will apply a broader standard domestically, although they will not be entitled to request its application at international level.

**(Q3) Whether the creation of space debris as a result of a space cyber activity would be compensable under the liability or responsibility regimes:**

Since section 3.4 argued that certain space cyberattacks create space debris (even if this is not always intentional, it is at least foreseeable), this begs the question of which the applicable regime should be. Whereas unintentional space debris would give rise to liability for damage caused with the space object, some authors have considered that intentionally created space debris additionally would involve responsibility for space activities.[1362] However, it should be recalled that for the general framework of the ILC Draft Articles on State responsibility, the intentional element is not necessary to determine responsibility unless it is an element of the primary obligation that gives rise to the internationally wrongful act.[1363]

Furthermore, section 5.2.1 has already discussed different opinions regarding what academic commentators consider to be covered by damage under the liability regime. In a nutshell, it depends on whether a restrictive or an evolutionary interpretation of the concept 'damage' is adopted.[1364] In the former case, damage will only include direct and physical

[1360] MENDES DE LEON, P. AND VAN TRAA, H., *The Practice of Shared Responsibility and Liability*, cit. note 1245, pp. 21-22.
[1361] VIIKARI, L., *The Environmental Element in Space Law,* cit. note 921, p. 69.
[1362] HOBE, S., *Environmental Protection in Outer Space: Where We Stand and What is Needed to Make Progress with Regard to the Problem of Space Debris*, in 'The Indian Journal of Law and Technology', Vol. 8, 2012, p. 9.
[1363] *Draft Articles on State Responsibility,* cit. note 219, commentary to Article 2, para. 10.
[1364] See CARPANELLI, E. AND COHEN, B., *Interpreting "Damage Caused by Space Objects"*, cit. note 1248, p. 4.

damage. To the contrary, with an evolutionary interpretation, damage will cover a broader variety of harm, including indirect and environmental and even such damage that could not be envisaged by the drafters at the time of negotiations.[1365]

Depending on the scenario, space debris may have a direct or an indirect cause and the effects may be immediate or remote. The scrutiny of how straightforward cause and effect connect with each other is not only important to determine whether damage is recoverable –and if so under which regime– but also who is accountable.

As explained in chapter 3 (section 3.4), if a malicious space cyber activity transforms a functional space object into a defunct satellite, it will be more straightforward to link the effect with the cyber cause. However, if a malicious cyber activity interferes with the communication between the ground station and the satellite and thus the space object delays an avoidance manoeuvre and consequently it collides with an asteroid, with another space object or with space debris, then the cause of the space debris creation will be indirect, although the effect may be immediate or not. While direct damage (the delay in the manoeuvre) would allow the victim to be compensated by the subject that conducted the cyber activity under the responsibility regime (Q1), indirect damage (space debris creation) would allow the victim State to claim compensation to the other launching State in the collision if impact is against another functional satellite or with identifiable space debris (Q2). Likewise, the other launching State affected by the collision in flight could claim compensation for damage caused by the victim of the malicious cyber activity. In this case, each of them should prove who acted with fault. However, if the collision is against an asteroid, there will not be any possibility of the victim claiming compensation under the liability regime. In other words, there will be two situations in which the victim of a malicious cyber activity causing space debris will remain legally unprotected in a space debris-creating event: if fault from the other launching State in the collision cannot be proved and if the satellite collides with an asteroid or with a non-registered space object. The only possible solution out of this conundrum would be the victim arguing that space debris is direct damage from the malicious space cyber activity, recoverable under the responsibility regime for the violation of Articles I (respect for the interests of other States), III (environmental

[1365] Ibid., p. 9.

principles incorporated into space law) and IX (due regard and no harmful contamination obligations) of the Outer Space Treaty (Q1).

Yet another scenario is where a malicious space cyber activity permanently disables a satellite and five years later it collides with another State's functional space object in orbit or falls down within the territory of a third State. Here, it is possible to discern two moments in the creation of space debris: an immediate one (the permanent disability of the space object) and a remote one (the subsequent collision). While the former might only be examined under the responsibility regime against the relevant State (Q1), the latter would be studied under the liability regime against the other launching State involved in the collision (Q2).

Chapter 4 reviewed two soft law instruments dealing with space debris and safety in outer space: the Space Debris Mitigation Guidelines of COPUOS (see section 4.3) and the Guidelines for the Long-term Sustainability of Outer Space Activities (see section 4.4). In addition, chapter 3 (section 3.9.2) referred to Recommendation ITU-R S.1003.2. These instruments –although not binding in nature– provide a significant tool to interpret the obligation of due regard under Article IX of the Outer Space Treaty (Q1) and the concept of 'fault' under Article III of the Liability Convention (Q2). The former confirms through its language that States should avoid the creation of space debris and that they should take measures to reduce space debris in orbit, to dispose and to foresee potential break-ups, and avoid 'intentional destruction' or 'other harmful activities that generate long-lived space debris' (guideline 4). In addition, the LTS Guidelines foresee several recommendations, notably the prompt resolution of identified harmful radio frequency interference, the controlled removal and/or disposal of non-functional spacecraft (guideline A.4), information exchange on space objects, their operation and status, appropriate responses and means to avoid collisions (guideline B.1), conjunction assessments (guideline B.4), better registration practices (guideline A.5) and provision of information on uncontrolled re-entry of space objects (guideline B.9).

A final point that deserves attention here is State responsibility for obligations owed to the international community as a whole. It has been argued that the preservation of the

environment of outer space is, *inter alia*,[1366] an obligation *erga omnes*.[1367] Thus, Articles 42 and 48(1)(b) of the Draft Articles on State Responsibility would be applicable to the harm that space debris cause to a global commons. In effect, customary environmental law –applicable in the space domain pursuant to Article III of the Outer Space Treaty as already indicated in chapter 3 (section 3.9)– crystallised the principle which establishes that States are responsible for pollution in *areas beyond their jurisdiction*.[1368] Although certain obligations might be considered *erga omnes*, it should be recalled that not all *erga omnes* obligations are necessarily established by peremptory norms.[1369] It exceeds the purpose of this thesis to examine the nature of certain principles of environmental law.[1370]

In the end, an evolutionary interpretation of Article VI of the Outer Space Treaty in light of art IX of the same instrument along with customary international law on State responsibility and on environmental protection introduced into space law via Article III of the Outer Space Treaty would allow the conclusion that reparation for injury to the outer space environment should be a possible scenario.

On the basis of the three-tier analysis made above, the following cases will depict practical scenarios that might arise from the classification proposed in chapter 3 (section 3.4).

**CASE A:** State A conducts a malicious cyber activity that causes interference with the space object of State B. Due to that interference, State B delays an avoidance manoeuvre which leads to a conjunction with a space object of State C (see section (a) of the classification proposed in chapter 3, section 3.4).

[1366] Some authors have considered that 'most of the obligations' under the five UN treaties are *erga omnes*. See STEER, C., *Sources and Law-Making Processes*, cit. note 793, p. 7.
[1367] MARCHISIO, S., *Article IX* (Outer Space Treaty), cit. note 799, p. 181 (para. 50).
[1368] Declaration of the United Nations Conference on the Human Environment, Stockholm, 16 June 1972, Principle 22; Rio Declaration on Environment and Development, Rio de Janeiro, 14 June 1992, Principle 16.
[1369] A/61/10, cit. note 807, para. 251 (38).
[1370] For a further analysis on what is considered by the ILC as *jus cogens*, see UN Doc. A/CN.4/727, cit. note 809, paras 122 -123 (the right to life, the principle of non-refoulement, the prohibition of human trafficking, the right to due process (the right to a fair trial), the prohibition of discrimination, environmental rights, and the prohibition of terrorism).

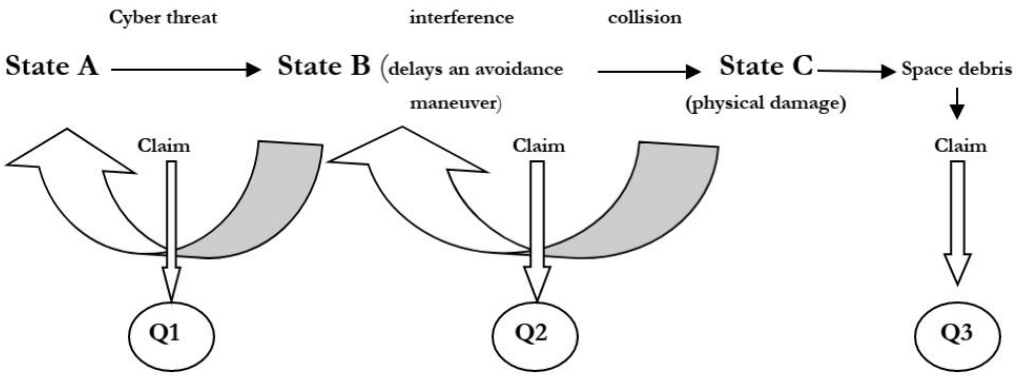


**Figure 9: interference with a satellite**

**CASE B:** State A conducts a malicious cyber activity against the space object of State B. State A overtakes the control of the satellite and commands it to collide with a space object of State C. As a consequence, the population of space debris increases (see case b.1.1. of the classification proposed in chapter 3, section 3.4).

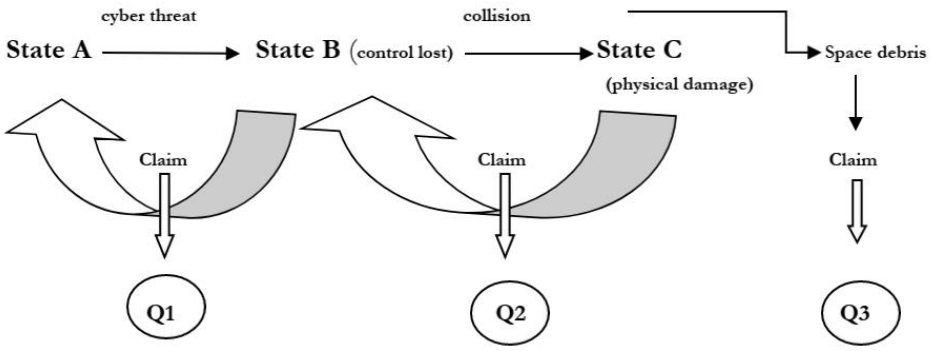


**Figure 10: cyberattack against a satellite**

**CASE C**: A variation of cases A and B above is when State A conducts a malicious cyber activity against the space object of State B and, as a consequence, it collides with the space object of State C. As a chain consequence, the space debris produced by that collision causes material damage to the satellite of State D. In this case, State D might claim joint and severe liability against States B and C (Article IV of the Liability Convention).

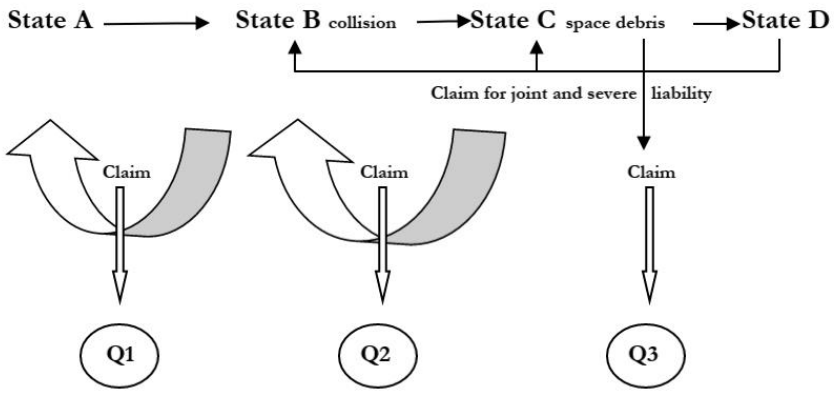


**Figure 11: malicious space cyber activity and joint liability**

**CASE D:** A malicious cyber activity of State A damages a critical instrument for the space mission of State B. Control of the space satellite is still possible but State B leaves it orbiting as it is no longer functional. It collides with an asteroid and the population of space debris grows (see case b.1.3. of the classification proposed in chapter 3, section 3.4).

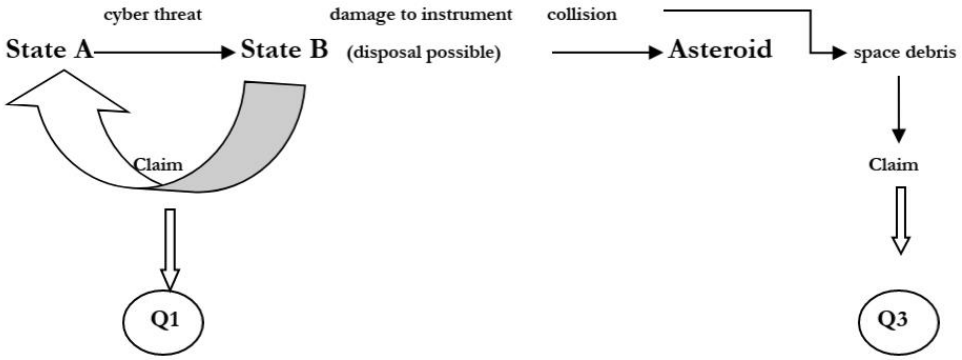


**Figure 12: cyberattack and collision with an asteroid**

**CASE E:** State A conducts a malicious cyber activity against a space object of State B. As a consequence of it, important data collected by its satellite is destroyed (see case (b.1.4) of the classification proposed in chapter 3, section 3.4).

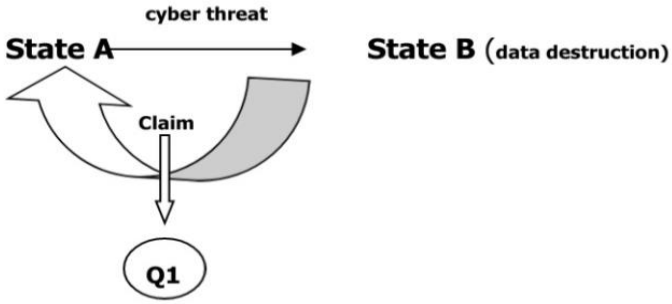


**Figure 13: cyberattack destroying data**

**CASE F:** State A conducts a malicious cyber activity against the space object of State B and exhausts its energy until no more control over it is possible (see case (b.3) of the classification proposed in chapter 3, section 3.4). Finally, this uncontrolled space object collides with the space object of State C creating space debris.

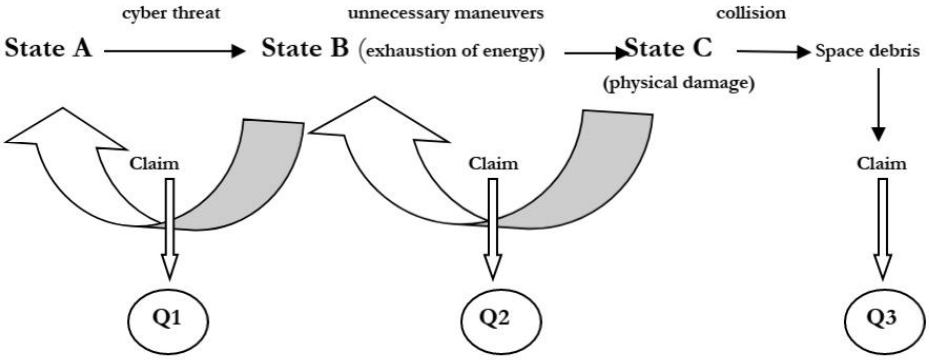


**Figure 14: cyberattack causing energy exhaustion**

**CASE G:** State A conducts a malicious cyber activity against the space object of State B and the remnants of the satellite fall in the territory of State C.

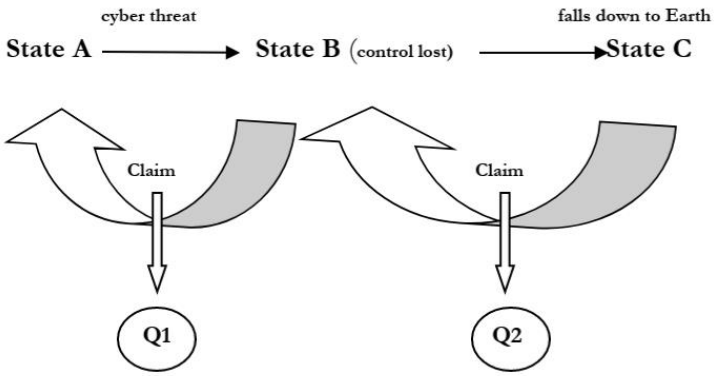


**Figure 15: cyberattack against a satellite causing damage on Earth**

In conclusion, while there seems to be a gap to apply the responsibility regime of space law since there is no explicit primary rule prohibiting malicious space cyber activities *per se*, a State might still have the opportunity to make a case arguing that they violate existing primary rules of space and telecommunications law, such as Articles I, III or IX of the Outer Space Treaty or Article 45(1) of ITU Constitution. Likewise, under the general regime of international law, a State might claim State responsibility for the violation of the principle of non-intervention or the use of force. However, the victim State will have a hard time trying to attribute the malicious space cyber activity due to the attribution problem, as explained in chapter 2 (section 2.3).

The application of the liability regime to malicious space cyber activities has several shortcomings: first, it should only apply to indirect effects because direct ones do not involve damage by the space object as required by the regime; second, the liability regime would not hold liable the subject that conducted the malicious space cyber activity but the launching State which was not necessarily able to control the space object registered with it; and third, if there is no identifiable launching State (for instance, in case of a collision with an asteroid) or if fault from a third launching State cannot be proved for damage caused in spaceflight, there will not be grounds for compensation for the victim of a malicious space cyber activity for damage.

Thus, any future endeavour to address space cybersecurity should: 1) confirm that space cyber activities are 'activities' in the terms of the Outer Space Treaty to allow the responsibility regime to be activated for violations of Articles I, III and IX; b) delineate some

interpretation of the due regard obligation and the concept of fault in connection with the prevention of cyber threats effects.

The most difficult gaps to fill are: (if it were desirable) to extend the liability regime to 'damage caused by space activities', which would require amending the space treaties or negotiating an additional protocol; study how to compensate indirect damage where no launching State is identifiable or when fault is impossible to be proved; the exoneration of liability of the launching State that did not control the space object due to a malicious space cyber activity, and some guidance regarding the attribution problem. These should be the subject matter of further research.

## 5.5.-POSSIBLE MECHANISMS TO ADDRESS SPACE CYBERSECURITY

The debate on what kind of instrument best suits the regulation of a certain matter in the international arena is an old discussion –not only in international law in general but it has also accompanied international space law since its inception. There is vast scholarship dealing with this issue –it is not the intention to reproduce it here but to succinctly extract the arguments in favour and against binding and non-binding instruments in the space field. This exercise aims at evaluating the pros and cons of both solutions and concludes with a concrete assessment on what is legally feasible (i.e. a solution that adapts to the legal framework of competences and mandates), technologically realistic (i.e. a solution that adapts to current technological challenges) and politically desirable (i.e. a solution that might overcome political antagonisms).

### 5.5.1.-THE BINDING SOLUTION

How feasible a binding instrument would be to regulate space cybersecurity is only answerable if reference is made to the factors that ushered into the negotiations of the five UN space treaties. At the time of the negotiations of the Outer Space Treaty, the Soviet delegate to the UN argued in favour of a binding instrument explaining that it was necessary to 'prevent a great technical achievement from being used against the interests of peace'.[1371]

[1371] LSC Summary Records 5th Session (1966), UN Doc. A/AC.105/C.2/SR. 57, p. 13

Soviet space experts have regarded the binding solution 'the best suited to assuring a legal order in space'.[1372] In the event of a legal lacuna in international space law, the Soviet doctrine advocates for the application of the general principles of international law to regulate space activities.[1373]

Freeland and Anja Pecujlic acknowledged that the geopolitical context during the Cold War and the increasing tensions between the United States and the Soviet Union were a fertile ground for the conclusion of binding treaties.[1374] That was the context of what has been called Space Age 1.0 (see chapter 3, section 3.5), which is far from being what is now called Space 4.0, an era of interaction among governments, the private sector, the society and politics.[1375] In effect, Pecujlic explained that beyond the geopolitical context there are other factors that contribute to misgivings about binding instruments, such as the increasing participation of the private sector and the resulting competitiveness in the commercial sector, the neoliberal paradigm with its resulting deregulation of markets, lobby from the private sector to avoid binding instruments and shortcomings of the law-making process.[1376]

While Zhang Ju'nan acknowledged that TCBMs in space activities might build up trust, that author assessed that 'good will is far from being enough'.[1377] Stephan Hobe considered that even if the golden treaty era might be closed, States are still willing to continue working on binding instruments; therefore, he concluded (although with certain caution) that States would be likely to agree to a binding instrument to regulate vital security or commercial interests.[1378]

One of the voices in favour of a binding instrument to supplement Article IV of the Outer Space Treaty has been the Canadian Ambassador (ret.) Paul Meyer, who was actively

---

[1372] ZHUKOV, G. AND KOLOSOV, Y., *International Space Law*, cit. note 688, p. 22.
[1373] Ibid., p. 23.
[1374] FREELAND, S. AND PECUJLIC, A., *How do you like your Regulation – hard or soft? The Antarctic Treaty and the Outer Space Treaty compared*, in 'National Law School of India Review', Vol. 30, No. 1, 2018, p. 31.
[1375] This is a concept coined by the European Union, see BOHLMAN, U., *Space 4.0*, in FERRETTI, S. (ed.), *Space Capacity Building in the XXI Century*, Vienna, 2020, p. 34.
[1376] See PECUJLIC, A., *European Space Policy Institute's Comprehensive Analysis on Adopting New Binding International Norms Regarding Space Activities,* in VENCATA RAO, R., GOPALKRISHNAN, V. AND ABHIJEET, K. (eds), *Recent Developments in Space Law. Opportunities & Challenges*, Bengaluru, 2017, pp. 144-145.
[1377] JU'NAN, Z., *Fundamental Ways to Ensure Outer Space Security: Negotiating and Concluding a Legally Binding International Instrument*, in POWERS, J. (ed.), Celebrating the Space Age, UNIDIR Conference Report, Geneva, 2-7 April 2007, p. 110.
[1378] HOBE, S., *The Impact of New Developments on International Space Law (New Actors, Commercialisation, Privatisation, Increase in the Number of 'Space-Faring Nations')*, in 'Uniform Law Review', Vol. 15, 2010, p. 878.

involved in the discussions of PAROS. In a webinar organised by McGill University in December 2020, he embraced the idea of extending the ban on weapons of mass destruction to all types of weapons with an additional protocol to the Outer Space Treaty. He made a case for a binding instrument since it would be a simpler tool than the proposed PPWT and would not entail opening up the Outer Space Treaty. With regard to the inclusion of a definition of 'weapon', he assessed that it should not be too difficult to define the term. However, due to the shortcomings that such definition posed politically, he pointed at other instruments that enjoy wide support and yet do not include core definitions, like 'nuclear weapons' in the Treaty on the Non Proliferation of Nuclear Weapons and 'nuclear explosion' in the Comprehensive Nuclear Test Ban Treaty.[1379]

It should be recalled that the proposal for an additional protocol to the Outer Space Treaty is about thirty years older than the PPWT –and even older than the origin of PAROS itself. In effect, as early as 1979 Italy submitted a draft to the Conference on Disarmament in reaction to the recommendation made by the General Assembly in its Tenth Special Session of 1978 to further measures to prevent an arms race in outer space.[1380] The Italian draft for an additional protocol extended the prohibition on weapons of mass destruction to 'any other types of devices designed for offensive purposes, the conduct of military manoeuvres, as well as the testing of any type of weapons'.[1381]Article III of that proposal foresaw the possibility of lodging a complaint with the Security Council in case of breach.

### 5.5.2.-THE NON-BINDING SOLUTION

Another part of the doctrine has put forward several positive aspects in favour of non-binding instruments to contribute to the global space governance. Some scholars have considered non-binding instruments the best solution for a field of law that needs flexibility. In this group of scholars is Marchisio who supported the idea that non-binding instruments are more adaptable to the technological evolution.[1382] In the same vein, Cassandra Steer[1383]

[1379] IASL-IAASS Webinar Series IV, 'Constraints on Military Uses of Outer Space: What Might International Law Offer?', Panel by Paul Meyer, available at https://www.mcgill.ca/ (last accessed on 11 August 2021).
[1380] A/RES/S-10/2, cit. note 1205, para. 80.
[1381] Additional Protocol to the 1967 'Outer Space Treaty, formally the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies', CD/9, 26 March 1979.
[1382] MARCHISIO, S., *The Evolutionary Stages of the Legal Subcommittee,* cit. note 707, p. 242.
[1383] STEER, C., *Sources and Law-Making Processes*, cit. note 793, p. 24.

and Valentina Vecchio[1384] assessed that the role of soft law in space law will be increasing not only due to the development in technology, but also due to the proliferation of space actors. Brian Wessel postulated that changes in space technology require flexibility in space law to allow space actors to adapt their practices without breaching binding instruments.[1385]

It is possible to identify another factor with leverage when selecting this type of instrument: the subject matter. Legal experts like Jennifer Urban considered that non-binding instruments best suit space security matters and may bring about stability in the era of globalisation.[1386] In the same vein, Wessel argued that non-binding instruments are more adequate to address technical areas of space law than rather vague binding instruments.[1387] Space activities seem to provide a fertile ground for non-binding instruments –at least some space law experts consider this kind of instrument 'essential and necessary',[1388] 'well-accepted'[1389] and performing an 'indispensable function' in international space law.[1390]

Another aspect in favour of non-binding instruments in the space field is the legal impact they have in the future. Some scholars contended that even if this type of instrument is not binding, it might be a first step in the consolidation of binding rules, either of a treaty or customary nature. As to the former alternative, it is useful to point at the statements made by some delegations during the negotiations of the space treaties. Those delegations argued that the most appropriate method to develop space law should be deductive: from clear and unambiguous general principles to the codification of detailed rules.[1391] Regarding the second alternative (customary law), Blount has underscored that soft law instruments may crystallise into general international law if States behave as if they were bound to.[1392] Building upon the 'incidents genre methodology' of Michael Risman, he argued that since space law is very

---

1384 VECCHIO, V., *Customary International Law in the Outer Space Treaty: Space Law as Laboratory for the Evolution of Public International Law,* in 'Zeitschrift fur Luft und Weltraumrecht', Vol. 66, No. 3, 2017, p. 501.
1385 WESSEL, B., *The Rule of Law in Outer Space*, cit note 825, p. 315.
1386 URBAN, J., *Soft Law: The Key to Security in a Globalized Outer Space*, in 'Transportation Law Journal', Vol. 43, 2016, p. 49.
1387 WESSEL, B., *The Rule of Law in Outer Space,* cit note 825, pp. 316-317.
1388 FERRAZZANI, M., *Soft law in Space Activities*, Presentation in the Conference 'Soft Law in Outer Space. The Function of Non-binding Norms in International Space Law' at the Faculty of Law of the University of Vienna, 2 April 2011, available at https://www.spacelaw.at/ (last accessed on 11 August 2021).
1389 FREELAND, S., *A Natural System of Law - Andrew Haley and the International Legal Regulation of Outer Space*, in 'Journal of Space Law', Vol. 39, 2013, p. 97.
1390 VON DER DUNK, F., *Contradictio in Terminis or Realpolitik*?, cit. note 545, p. 56.
1391 UN Doc. A/AC.105/C.2/SR.29-37, cit. note 1346, p. 17 (Poland); se also UN Doc. A/AC.105/C.2/SR.57, cit. note 1371, p. 10 (USSR).
1392 BLOUNT, P.J., *The Development of International Norms to Enhance Space Security Law in an Asymmetric World,* Proceedings of the 52nd Colloquium on the Law of Outer Space, 2010, p. 5.

permissive and States can interpret it to their best advantage, they might be willing to use incidents as 'a norm generator' or as 'norm-indicator' to enhance space security.[1393] Moreover, some authors agreed that even if these instruments are not legally binding, they nevertheless have a special legal importance[1394] –they have a moral and political value or even a legal one.[1395] Brünner and Königsberger posited that soft law instruments do not just have a moral and political value but may have an 'indirect normative power'.[1396] In the same line of thought, Martinez pointed out that States can transform them into legal instruments at a domestic level (this is why 'non-binding' is not necessarily synonymous with 'non-legal').[1397]

Non-binding instruments are considered by some authors the 'most workable',[1398] the 'most viable',[1399] the 'most likely'[1400] or the simplest[1401] track in international negotiations. From a practical standpoint, it is adventurous to make a general assessment regarding all non-binding instruments. In effect, attention should be drawn to the two initiatives already addressed in this research: the LTS Guidelines took around a decade of work and is not yet a complete endeavour, and the European draft CoC took –without counting the preparatory work– from 2008 until 2015 and reached no agreement. Moreover, Jack Beard argued that the EU draft CoC is a case study in the limitations of soft law.[1402]

Despite the arguments in favour that have been just laid out, there is a part of the literature that is very critical regarding non-binding instruments. When Beard wrote on the limitations of soft law for arms control mechanisms, he argued that non-binding instruments are not the best tool to regulate military activities and the use of weapons in such an unstable environment as outer space.[1403] He pointed at the vagueness and ambiguity of the terms, and

---

[1393] Ibid., p. 3. 'Norms are then derived from the interpretations of the actors involved as well as the international community as a whole'.
[1394] JANKOWITSCH, P., *The Background and History of Space Law*, cit. note 707, p. 25; TRONCHETTI, F., *Soft Law*, cit. note 708, p. 619.
[1395] SCHACHTER, O., *The Twilight Existence of Non-Binding International Agreements*, in 'The American Journal of International Law, Vol. 71, 1977, pp. 296–304 quoted in TRONCHETTI, F., *Soft Law*, cit. note 708, p. 620.
[1396] BRÜNNER, C. AND KÖNIGSBERGER, G., *'Regulatory Impact Assessment' — A Tool to Strengthen Soft Law Regulations*, in MARBOE, I. (ed.), S*oft Law in Outer Space: The Function of Non-Binding Norms in International Space Law*, Vienna, 2012, p. 90.
[1397] See MARTINEZ, P., *Space Sustainability* (2020), cit. note 953, p. 20.
[1398] TRONCHETTI, F., *Fundamentals of Space Law and Policy*, cit. note 545, p. 19.
[1399] Ibid., p. 85.
[1400] BLOUNT, P. J., *Renovating Space: The Future of International Space Law,* cit. note 720, p. 532.
[1401] See CHENG, B., *United Nations Resolutions on Outer Space*, cit. note 702, p. 135.
[1402] BEARD, J., *Soft Law's Failure on the Horizon: The International Code of Conduct for Outer Space Activities,* in 'University of Pennsylvania Journal of International Law', Vol. 38, No. 2, 2016, p. 344.
[1403] Ibid., p. 344.

the lack of a well-established mechanism for interpretation (like the one provided in the Vienna Convention on the Law of the Treaties for binding instruments).[1404]

The 2016 ESPI report mentioned two dangers posed by soft law instruments. The argument was put forward that they may downgrade already binding obligations, and that they might be considered as the end of the law-making process instead of the beginning where binding rules can derive from them.[1405] Although some scholars see non-binding instruments playing a role in the formation of customary law, other academic commentators like Beard are of the view that such a process of transformation is indeed a disadvantage because it brings about a 'democratic deficit' in the formation of such rules.[1406]

### 5.5.3. STATES' VIEWS:

The previous sub-sections provided an overview of the opinions in the academic circles in favour and against the *alternative* between binding *or* non-binding instruments, the *antagonism* of binding *vs.* non-binding instruments and the *complementarity* between binding *and* non-binding instruments.[1407] This sub-section will rely on official State views from two different sources: a) discussions within the LSC and b) discussions within the Working Group on the Status and Application of the Five United Nations Treaties on Outer Space.

#### a) Discussions within the LSC:

In 2013 Japan, sponsored by Austria, Canada, France, Nigeria and the United States, submitted a proposal to include an agenda item entitled 'General exchange of information on practices in relation to non-legally binding instruments for outer space activities' with a three-year work plan.[1408] The title of the agenda was renamed 'General exchange of information on non-legally binding United Nations instruments on outer space' and has been retained until the present day. Although the purpose of the agenda item was 'to assess to

---

[1404] Ibid., p. 363.
[1405] See FROEHLICH, A. AND PECUJLIC, A. (eds), *Mechanisms for the Development of International Norms regarding Space Activities*, ESPI Report No. 57, Vienna, May 2016, pp. 38-39, available at https://espi.or.at/ (last accessed on 11 August 2021).
[1406] BEARD, J., *Soft Law's Failure on the Horizon:* cit. note 1402, p. 345.
[1407] The approach of binding and non-binding instruments as complementary, antagonists and alternatives is taken from: SHAFFER, G. AND POLLACK, M., *Hard Versus Soft Law in International Security*, in 'Boston College Law Review', Vol. 52, 2011.
[1408] New agenda Item on General Exchange of Information on Practices in Relation to Non-Legally Binding Instruments for Outer Space Activities, UN Doc. A/AC.105/C.2/L.291, 11 April 2013.

what extent and how those instruments have been put into practice by individual States in their domestic dealings and in international activities',[1409] it provided enough room for States expressing their views regarding non-legally binding instruments altogether.

As a result of that work, a compendium of mechanisms adopted by Member States and international organisations in relation to non-legally binding instruments on outer space was made available on a dedicated web page of the OOSA.[1410] In the exchange of views within this agenda item 26 national delegations made statements until the moment of concluding this research.[1411] The LSC agreed to a common ground which is the assertion that UN non-legally binding instruments related to outer space activities *complement* and support the UN space treaties.[1412]

**b) Discussions within the Working Group on the Status and Application of the Five United Nations Treaties on Outer Space:**

This part will set out the individual opinions of some COPUOS Member States in reaction to a set of questions put by the Chair of the Working Group on the Status and Application of the Five United Nations Treaties on Outer Space (withing the LSC) in the lead-up to UNISPACE+50.[1413] The relevant answers provided by a small group of States to the following three issues will be reviewed below: 1) the impact of non-binding instruments on the UN space treaties, 2) the need for other instruments beyond non-binding ones and 3) prospects for the space treaties.

- **Armenia:** As to the second issue, Armenia replied that non-binding instruments 'are sufficient; no additional actions are required'.[1414]

[1409] Ibid, para. 4.
[1410] UN Doc. A/71/20, cit. note 1033, para. 197; Report of 60th Session of COPUOS (2017), A/72/20, para. 217; UN Doc. A/73/20, cit. note 1217, para. 268; UN Doc. A/74/20, cit. note 1024, para. 235.
[1411] From 2014 until 2021 the following States made statements under this agenda item: Austria, Belgium, Brazil, Canada, Chile, China, Colombia, Cuba, the Czech Republic, France, Germany, Greece, Iran, Israel, Italy, Japan, Mexico, the Netherlands, the Republic of Korea, the Russian Federation, Pakistan, Poland, Spain, the United Kingdom, the United States and Venezuela.
[1412] Report of the 58th Session of the LSC (2019), UN Doc. A/AC.105/1203, para. 190; Report of the 56th Session of the LSC (2017), UN Doc. A/AC.105/1122, para. 180.
[1413] UN Doc. A/AC.105/1122, cit note 1412, Annex I, Appendix I.
[1414] Responses to the Set of Questions Provided by the Chair of the Working Group on the Status and Application of the Five United Nations Treaties on Outer Space, UN Doc. A/AC.105/C.2/2019/CRP.18, 2 April 2019, question 1.2.

- **Austria:** Regarding the first point, Austria answered that non-binding instruments 'can specify and concretize the provisions contained in the existing United Nations space treaties'.[1415] They 'give guidance to space actors with regard to the interpretation, application and implementation of the treaties'.[1416]

With regard to the second point, that country argued that 'non-binding principles, resolutions and guidelines seem to be a practically feasible and implementable solution to complement the treaties and specify their meaning to facilitate their application'.[1417]

Finally, regarding the third point, Austria stated that a non-binding instrument 'currently appears to be a more practicable option to further develop the application of the treaties'.[1418]

- **Czech Republic:** In reference to the first issue, the Czech Republic asserted that 'non-binding instruments cannot stipulate new legal rights and obligations'; however, they may 'facilitate the application of the treaties and are more suited to react to current developments in outer space activities'.[1419]

As to the second matter, that country acknowledged that a new treaty or an amendment of existing one seems today to be 'unlikely'.[1420]

- **Germany:** Germany acknowledged 'the reasonable complementary relation' between binding and non-binding instruments and considered the latter to be 'more suited to react to current developments in outer space activities'.[1421] However, that country considered that the negotiation of a treaty regulating traffic management should be assessed.[1422]

---

[1415] Responses to the Set of Questions Provided by the Chair of the Working Group on the Status and Application of the Five United Nations Treaties on Outer Space, UN Doc. A/AC.105/C.2/2017/CRP.6 (Austria), 23 March 2017, question 1.1.
[1416] Ibid.
[1417] Ibid., question 1.2.
[1418] Ibid., question 1.3.
[1419] Responses to the Set of Questions Provided by the Chair of the Working Group on the Status and Application of the Five United Nations Treaties on Outer Space, UN Doc. A/AC.105/C.2/2018/CRP.12, 6 April 2018, question 1.2.
[1420] Ibid., question 1.3.
[1421] UN Doc. A/AC.105/C.2/2017/CRP.6 (Germany), cit. note 1415, question 1.
[1422] Ibid.

- **Greece:** The answer from Greece referred to the three points in common and stated that 'soft law instruments particularize and complement the five Treaties'. '[...] the persistence of the international community to the adoption of "Principles", "Guidelines", "Practices" and "Codes of conduct" adversely affect the progressive development of space law'. The statement continues: 'There is, therefore, a clear need either for an effective revision of the existing space treaties or for the creation of a new, updated contractual framework for the regulation of outer space activities'.[1423]

- **Indonesia:** Indonesia replied to the first point that 'resolutions guidelines regarding outer space may also be needed to provide further clarification in the implementation of the existing United Nations Treaties on Outer Space provisions in practice'.[1424]

As to the second issue, Indonesia manifested that 'non-legally binding instruments are a way to fill the gaps on the existing legally binding treaties on the outer space'.[1425] Finally, the comment to the third point was that 'the development of space law by adding or amending the five United Nations Treaties is almost impossible'.[1426]

Although this review represents only a small group of States in relation to COPUOS membership (these are the States that have so far replied to the questionnaire),[1427] it is possible to draw some conclusions: first, most of them consider binding and non-binding instruments complementary with each other. Second, while some States considered it necessary to negotiate further treaties, others assessed that such endeavour would not be feasible or practicable nowadays. And third, there are highly conflicting positions: those who consider a non-binding instrument as the only appropriate mechanism when it comes to the

[1423] Responses to the Set of Questions Provided by the Chair of the Working Group on the Status and Application of the Five United Nations Treaties on Outer Space, UN Doc. A/AC.105/C.2/2017/CRP.17, 28 March 2017, Common Answer to 1.1, 1.2 and 1.3.
[1424] Responses to the Set of Questions Provided by the Chair of the Working Group on the Status and Application of the Five United Nations Treaties on Outer Space, UN Doc. A/AC.105/C.2/2018/CRP.16, 11 April 2018, question 1.1.
[1425] Ibid., question 1.2.
[1426] Ibid., question 1.3.
[1427] Although Pakistan also replied to the set of questions, that State did not articulate a position on the topic at stake.

regulation of technological developments and those who perceive non-binding instruments as a threat to the progressive development of space law.

In sum, even if this group of States is neither quantitatively (6 out of 95 COPUOS member States) nor qualitatively representative (none of them is among the top spacefaring nations), this sample clearly shows that it will not be easy to agree on a binding treaty in the short term. However, a more positive conclusion can also be drawn from these sparse replies: at this early stage States may still hesitate to define a position on the need for new treaties to tackle emerging challenges.

## 5.6.-THE RIGHT FORUM

A desirable premise to any negotiation is to comply with the requirement of universal inclusiveness. The United Nations is the multilateral forum *par excellence* that undoubtedly fulfils this condition. This section aims to discuss the mandate of two different fora that the international system offers for discussions on space matters, depending on the approach: COPUOS and the Conference on Disarmament. The purpose of this section is to analyse the evolution of their mandates in order to determine which would be the right forum to address an initiative on space cybersecurity.

### 5.6.1.- COPUOS:

Pursuant to Article 22 of the UN Charter and Article 161 of the UNGA Rules of Procedure, the General Assembly may establish the subsidiary organs that it deems necessary. As already explained, the Legal Subcommittee of COPUOS is the forum where the five UN treaties were negotiated (see chapter 3, section 3.8.1). In order to better elucidate the mandate of COPUOS, it is necessary to review the background of UNGA Resolution 1348 (XIII), which established this body as an *ad hoc* committee in 1958 with the aim, *inter alia,* 'to study the nature of legal problems which may arise from the exploration of outer space'. This mandate was reiterated in UNGA Resolution 1472 (XIV), which established COPUOS as a permanent committee.

In August 1958, the American Ambassador Henry Cabot Lodge was instructed to submit an agenda item to the General Assembly. The item was entitled 'Program for

International Cooperation in the Field of Outer Space' and was intended to be presented before the Soviets did it. The telegram from the Department of State directed to the Permanent Mission of the United States in New York explained that such an agenda item 'would consider peaceful uses aspects of outer space and not disarmament aspects which would be discussed within framework of usual disarmament item which is already on GA agenda'.[1428]

However, the discussion of an agenda item on the uses of outer space took place within UNGA First Committee on the basis of a Soviet draft that also banned the military uses of outer space, and whose aim was to ensure that the use of outer space would be *exclusively* for peaceful purposes.[1429] Finally, the Soviet delegation agreed to focus on international cooperation in the peaceful uses of outer space in spirit of consensus[1430] but reserved its right to bring up the matter again at another moment.[1431]

In 1983, the General Assembly requested COPUOS to consider the militarisation of outer space as a matter of priority and, in that task, to coordinate the efforts with the Committee on Disarmament (predecessor of the Conference on Disarmament), dealing with the prevention of an arms race in outer space at that time.[1432] That same year coincided with the already referred 'Strategic Defense Initiative' (see chapter 3), announced by the Reagan administration. In 1984, under the agenda item 'Questions relating to the militarization of outer space', some delegations expressed that it had been a serious mistake to have given COPUOS the mandate related to arms control.[1433] It should be recalled that when that topic was discussed at COPUOS, the United States did not participate in the debate and threatened to withdraw from COPUOS if there was no agreement on the mandate.[1434] From then on, the language of the annual resolution on international cooperation at COPUOS did not refer to that mandate (neither derogating nor reconfirming it) but limited itself to *urge* States to

[1428] Telegram 443 from the Department of State to the Mission at the United Nations, Washington, August 18, 1958—9:53 p.m., available at https://history.state.gov/(last accessed on 11 August 2021).
[1429] General Assembly 13th Session (1958), UN Doc. A/PV.792, paras 103, 105, 115.
[1430] It should be noted that this resolution was adopted with a recorded vote of 53-93-19. However, it should be underscored that the obstacle for its adoption without a vote was the composition of the committee and not the substance.
[1431] UN Doc. A/PV.792, cit. note 1429, para. 131.
[1432] United Nations General Assembly, Resolution 38/80, 15 December 1983, A/RES/38/80, op. 15.
[1433] Report of the 27th Session of COPUOS (1984), UN Doc. A/39/20, para. 25.
[1434] JASENTULIYANA, N., *Consideration of Space Activities by the UN General Assembly*, in 'Space Policy', May 1985, p. 219.

contribute actively to preventing an arms race in outer space as an essential condition for the promotion of international cooperation.[1435] The consensus language regarding the mandate of COPUOS is that it has a 'unique' role in international cooperation in space matters.[1436]

The Cologne Commentary to the Outer Space Treaty explained that during the past years there has been a 'silent consensus' not to discuss military issues in COPUOS.[1437] However, it could be argued that the current practice seems to deviate from that assessment if consideration is taken to the content of States' statements under the COPUOS agenda item entitled 'Ways and means of maintaining outer space for peaceful purposes'.[1438] This practice demonstrates that it has usually been difficult to disassociate the maintenance of outer space for peaceful purposes from security aspects, such as the prohibition of weaponisation and the prevention of an arms race in outer space.

Moreover, it has been argued that the work done within COPUOS in 2007 regarding the already referred Space Debris Mitigation Guidelines does not strictly fall within its 'peaceful uses' mandate.[1439] Furthermore, it has been interpreted as an indication of the possibility for COPUOS to deal with security matters if the Conference on Disarmament is unable to carry out its work.[1440]

In the same vein, a note by the UNOOSA Secretariat –issued in the context of the process leading up to UNISPACE+50– described one of the objectives of the thematic priority 2 relating to the legal regime of outer space and the global space governance, in the following terms: 'Studying legal mechanisms to foster an international regime of

---

[1435] United Nations General Assembly, Resolution 39/96, 14 December 1984, A/RES/39/96, op. 13; Resolution 40/162, 16 December 1985, A/RES/40/162, op. 13; Resolution 41/64, 3 December 1986, A/RES/41/64, op. 15; Resolution 42/68, 2 December 1987, A/RES/42/68, op. 18; Resolution 43/56, 6 December 1988, A/RES/43/56, op. 18; A/RES/44/46, cit. note 962, op. 24; A/RES/45/72, cit. note 962, op. 24; A/RES/46/45, cit. note 962, op. 27; A/RES/47/67, cit note 962, op. 28; Resolution 48/39, 10 December 1993, A/RES/48/39, op. 34; Resolution 49/34, 9 December 1994, A/RES/49/34, op. 35; Resolution 50/27, 6 December 1995, A/RES/50/27, op. 38. This is a paragraph that is included annually in all UNGA resolutions on international cooperation until the present days.

[1436] For instance, A/RES/73/6, cit. note 1021 (op. 7 reads as follows: 'Reaffirms the unique role of the Committee on the Peaceful Uses of Outer Space and its subcommittees'); A/RES/71/90, cit. note 628, preambular paragraph 2.

[1437] SCHROGL, K-U. AND NEUMANN, J., *Article IV* (Outer Space Treaty), cit. note 567, p. 87 (para. 72).

[1438] See for instance, UN Doc. A/74/20, cit. note 1024, paras 42-79.

[1439] RAJESWARI PILLAI RAJAGOPALAN, *Beyond Outer Space Treaty,* cit. note 498, p. 179.

[1440] Ibid., p. 180.

responsibility and liability to cope with present and future challenges to the *safety, security and sustainability* of outer space activities' (emphasis added).[1441]

In sum, the discussion at COPUOS of the military aspects of the use of outer space is as old as the origin of COPUOS itself and reflects the bipolarisation between the United States and the Russian Federation. Attempts to include topics related to those issues have never been given up; however, nothing seems to promise a modification of their respective positions. The understanding of this context reinforces the argument made in this thesis that space cybersecurity addressed from a military standpoint will not be welcome by some delegations at COPUOS.

### 5.6.2.- THE CONFERENCE ON DISARMAMENT:

Unlike COPUOS, the Conference on Disarmament is not a permanent subsidiary organ of the General Assembly, but only a 'disarmament negotiating forum'.[1442] Nonetheless, the Rules of the Conference on Disarmament foresee several connections between this forum and the United Nations: 1) the Secretary-General of the United Nations appoints the Secretary-General of the Conference, 2) the Conference on Disarmament reports to the General Assembly (UNGA First Committee), 3) the General Assembly provides staff and the necessary assistance to the Conference on Disarmament, 4) the Conference on Disarmament meets at the Office of the United Nations in Geneva and 5) the General Assembly may propose matters to be addressed by the Conference on Disarmament.

In the context of the latter capacity, the General Assembly requested the Committee on Disarmament in 1981 'to embark on negotiations with a view to achieving agreement on the text' of an international treaty on the prevention an arms race.[1443] UNGA Resolution 37/83 requested the Committee on Disarmament to establish an *ad hoc* working group in 1983 to *negotiate* an agreement on PAROS.[1444] It should be recalled that some years before; the General Assembly Tenth Special Session had concluded that in order to prevent an arms race, international *negotiations* should be held in accordance with the spirit of the Outer Space

[1441] Thematic priority 2. Legal regime of outer space and global governance: current and future perspectives, UN Doc. A/AC.105/1169, 13 November 2017, para. 4 c).
[1442] Rules of Procedure of the Conference on Disarmament, CD/8/Rev.9, 19 December 2003, I.1.
[1443] United Nations General Assembly, Resolution 36/99, 9 December 1981, A/RES/36/99.
[1444] A/RES/37/83, cit. note 1164.

Treaty.[1445] The reference to 'negotiations' is important because that is the core issue that has taken the Conference on Disarmament to a stalemate: the lack of agreement between those States that are only willing to *discuss* the topic and those that are determined to undertake genuine *negotiations*.[1446] The *ad hoc* group was finally established with the limited mandate 'to examine as a first step [...], through substantive and general consideration, issues relevant to the prevention of an arms race in outer space'.[1447]

The adoption of the work programme and any decision in the Conference on Disarmament is also made by consensus.[1448] It has been considered that the rule of consensus was used to give a voice in the decision of sensitive issues, such as security, to new States incorporated to the international community after their decolonisation processes.[1449] The Conference on Disarmament was unable to adopt its work programme most of the years due to the difficulties that the consensus rule brings about.[1450]

As already advanced in chapter 4 section 4.7.1, the first UNGA Resolution on PAROS was in 1981 (UNGA Resolution 36/97C). In that year, the General Assembly requested the Committee on Disarmament to consider the question of negotiating effective and verifiable agreements aimed at preventing an arms race in outer space.[1451] Although neither the PAROS Resolution of 1981 or 1982 expressed anything in that regard, the annually PAROS Resolution from 1983 onwards 'reiterates that the Conference on Disarmament, as the *single* multilateral disarmament negotiating forum, has a *primary* role in the negotiation' of an instrument on prevention of an arms race (emphasis added).[1452]

The Conference on Disarmament has a 'primary' role in the negotiations on PAROS,[1453] and not an 'exclusive' one. This is not a minor detail if examined in light of the

[1445] A/RES/S-10/2, cit. note 1205, para. 80.
[1446] See generally MEYER, P., *The CD and PAROS. A Short History*, UNIDIR Resources, April 2011, available at https://www.unidir.org/ (last accessed on 11 August 2021).
[1447] Report of the Ad Hoc Committee on Prevention of an Arms Race in Outer Space, CD/641, 6 August 1985, para. 1.
[1448] CD/8/Rev. 9, cit. note 1442, Article 18.
[1449] CARTAGENA, I., *Mandate and Working Methods in the Conference of Disarmament. A Historical Perspective*, UNIDIR, 2019, p. 12, available at https://unidir.org/ (last accessed on 11 August 2021).
[1450] Ibid., p. 9.
[1451] A/RES/36/97C, cit. note 988, op. 3.
[1452] A/RES/38/70, cit. note 1029, op. 4; see also subsequent PAROS resolutions.
[1453] For example, A/RES/72/250, cit. note 1177, preambular paragraph 5; United Nations General Assembly, Resolution 72/26, 4 December 2017, A/RES/72/26, op. 5 reads as follows: 'Reiterates that the Conference on Disarmament, as the sole multilateral disarmament negotiating forum, has the primary role in the negotiation

findings of the ICJ in the Certain Expenses Advisory Opinion. There, the Court had to determine whether the General Assembly was competent to control the finances of the Organisation pursuant to Article 17(2) of the UN Charter, even if they were related to operations for the maintenance of international peace and security. The ICJ acknowledged that Article 24 of the UN Charter had conferred upon the Security Council the 'primary' responsibility for the maintenance of international peace and security, but not an 'exclusive' one.[1454]

While certain States object to discussing security issues at COPUOS arguing that such topics fall under the remit of the Conference on Disarmament and UNGA First Committee, others try to include references to LTS and international cooperation in space activities (issues that fall under the mandate of COPUOS) in the PAROS process. This is clear evidence that efforts to divide issues regarding safety, security and long-term sustainability of space activities will probably always fail.

Voices have been raised sustaining that if the Conference on Disarmament is unable to do something that is patently necessary; other fora should be able to perform the task.[1455] A well-known scholar sharing a similar view is Jakhu.[1456] However, it seems unfeasible to reach an agreement on discussing topics with explicit warfare language (including references to weapons and arms) at COPUOS. An alternative solution is avoiding references to such terminology to circumvent the stalemate of the Conference on Disarmament and to enhance how certain activities affect the rights and freedoms that States have under the UN space treaties. This is the approach that is followed in the present thesis.

---

of a multilateral agreement or agreements, as appropriate, on the prevention of an arms race in outer space in all its aspects'; UNGA Resolutions on NFP employ the following language: '[…] that the Conference on Disarmament, as the single multilateral negotiating forum on this subject, has the primary role in the negotiation of a multilateral agreement, or agreements[…]'.

1454 *Certain Expenses of the United Nations (Article 17, paragraph 2, of the Charter),* Advisory Opinion, [1962], ICJ Reports 151, 20 July 1962, p. 163.

1455 See PALIHAKKARA, H., *Space Security: Perspectives of Developing Countries*, in POWERS, J. (ed.), *Celebrating the Space Age*, UNIDIR Conference Report, Geneva, 2-7 April 2007, p. 83.

1456 JAKHU, R., *Legal Issues relating to the Global Public Interest*, cit. note 815, p. 102.

## 5.7.- A POSSIBLE NORMATIVE SOLUTION:

This chapter has revealed that for the time being there is no conclusive political will to engage in a treaty negotiation in space security matters. Although this hurdle might be circumvented by exporting the negotiation either to the General Assembly under a specific mandate where no consensus rule governs or to an *ad hoc* diplomatic conference for a treaty, the question arises as to whether such an effort is really worthy, efficient and promising.

This chapter has provided important inputs to shed some light on this question. First, the conclusion was reached that Articles I, III, VI, VII and IX of the Outer Space Treaty are a substantive and robust legal framework to address malicious cyber activities in outer space. In addition, building upon the previous debate on binding and non-binding instruments, abundant literature and State practice support the argument that non-binding instruments complement and provide some guidance as to the application of treaty law.

Thus, practical and theoretical evidence leads to propose a non-binding solution, either in the format of a set of guidelines (see section 5.7.1 below) or an UNGA resolution (see section 5.7.2 and section 5.7.3). In either case, it is proposed that it be negotiated at COPUOS since the subject matter would not involve disarmament issuses. Now, regarding the referral to the General Assembly of any endeavour at COPUOS, there is no discussion that issues relating to the peaceful uses of outer space fall under the remit of UNGA Fourth Committee. However, as already explained in chapter 2 (see section 2.8.1) the topic of ICTs in the context of international security falls under the mandate of UNGA First Committee; hence, it would not be sensible to disassociate the use of ICTs in outer space in the context of international security from the same Committee. In addition, TCBMs in outer space is a topic on the agenda of UNGA First Committeee (see section 4.5).

The following sub-sections will study three models that will provide a basis to decide on a mechanism to negotiate a normative solution for space cybersecurity: either a set of guidelines or an UNGA resolution. The first one is based on the procedural mechanism adopted for the LTS Guidelines, i.e. a three-stage process that involves COPUOS, an UNGA Main Committee and the Plenary of the General Assembly to adopt an omnibus resolution on international cooperation. The second one is built upon the procedural mechanism followed for the UNISPACE+50 resolution; i.e. a two-stage process that begins with

COPUOS and ends directly at a plenary meeting of the General Assembly for adoption. The third model follows the example of the 'launching State'UNGA resolution. This is again a three-stage process that involves COPUOS, an UNGA Main Committee and a plenary meeting of the General Assembly for the adoption of a resolution negotiated at COPUOS on a specific matter.

### 5.7.1.-A SET OF GUIDELINES: THE LTS MODEL

As already described in chapter 4 (see section 4.4), the negotiations for the LTS Guidelines took place in a particular working group of the STSC with the inputs of four expert groups. After several years of discussions, the working group agreed on a set of 21 guidelines and a preamble, which was adopted by COPUOS in 2019 and annexed to the report of the 62nd session of COPUOS.

The delegate of Brazil, in his capacity as Chair of COPUOS, submitted the draft omnibus resolution on international cooperation to UNGA Fourth Committee. The final version of the resolution 'welcomes with appreciation the adoption by the Committee of the preamble and 21 guidelines for the long-term sustainability of outer space activities, as contained in annex II to the report of the Committee'. The text was endorsed by UNGA Fourth Committee without a vote[1457] and adopted as UNGA Resolution 74/82[1458] in a plenary meeting also without a vote.[1459]

It should be recalled that even if there were joint meetings of UNGA First and Fourth Committees as explained in chapter 4 (see section 4.7.3.), the report containing the draft LTS Guidelines was not submitted to a joint committee but only to UNGA Fourth Committee.

This is the same procedure that the 2007 Space Debris Guidelines followed. In effect, those guidelines were referred to in UNGA Resolution 62/217 –the guidelines themselves

[1457] Report of the Special Political and Decolonization Committee (Fourth Committee), UN Doc. A/74/408, 7 November 2019, paras 7-9.
[1458] United Nations General Assembly, Resolution 74/82, 13 December 2019, A/RES/74/82.
[1459] General Assembly 74th Session, 47th plenary meeting, 13 December 2019, 10 a.m. New York, A/74/PV.47, p. 4.

were annexed to the COPUOS report. The process can be summarised in the following figure:

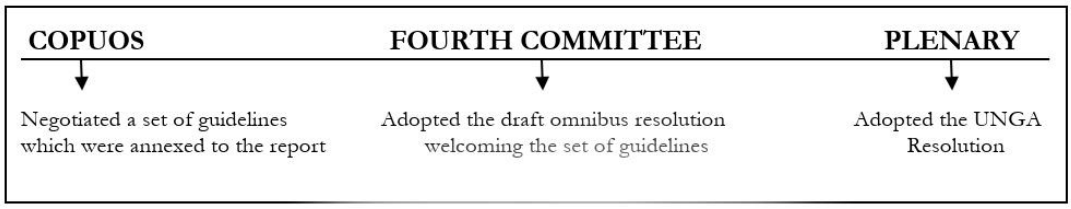


**Figure 16: The LTS model**

### 5.7.2.-A DRAFT UNGA RESOLUTION: THE UNISPACE+50 MODEL

The text of UNGA resolution for UNISPACE+50 was negotiated in COPUOS and there was a long process behind the result. In effect, in 2017 COPUOS made several decisions regarding the procedure: First, it gave the mandate to the Working Group of the Whole (within the STSC) and the Working Group on the Status and Application of the Five United Nations Treaties on Outer Space (within the LSC) to consider an initial draft to be submitted early in 2018 for consideration of Member State delegations.[1460] Second, COPUOS decided that Canada –in its capacity as Chair– would submit a draft resolution to UNGA Fourth Committee whereby the General Assembly would decide to address UNISPACE+50 as a separate item in a plenary meeting.[1461]

Thus, in 2017 UNGA Fourth Committee considered and adopted without a vote not only the annual traditional draft resolution on international cooperation in the peaceful uses of outer space but also the draft resolution submitted by Canada entitled 'Consideration of the fiftieth anniversary of the United Nations Conference on the Exploration and Peaceful Uses of Outer Space'.[1462]UNGA Fourth Committee recommended to the General Assembly the adoption of the draft resolutions at its plenary meeting.[1463] On that basis, UNGA

[1460] UN Doc. A/72/20, cit. note 1410, para. 324.
[1461] Ibid.
[1462] Consideration of the Fiftieth Anniversary of the United Nations Conference on the Exploration and Peaceful Uses of Outer Space, UN Doc. A/C.4/72/L.4, 20 September 2017. In addition, there was a third resolution adopted, entitled 'Declaration on the Fiftieth Anniversary 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'.
[1463] Report of the Special Political and Decolonization Committee (Fourth Committee), UN Doc. A/72/446, 27 October 2017, para. 19.

Resolution 72/79[1464] was adopted without a vote.[1465] That resolution is the legal basis for the consideration of the UNISPACE+50 draft resolution directly by the plenary of the General Assembly under the agenda item entitled 'Space as a driver of sustainable development'.

With regard to the substantive content of the draft resolution of UNISPACE+50, discussions were held within COPUOS during 2018, as originally mandated. The draft resolution[1466] was endorsed at the high level meeting during the 61st session of COPUOS in the same year.[1467] Then, the draft was submitted to the plenary meeting of the General Assembly in 2018 by Mexico, in its capacity as Chair of COPUOS at the time.[1468] As decided and formalised by the already referred UNGA Resolution 72/79, the draft resolution was addressed under the agenda item 'Space as a driver of sustainable development' in the plenary meeting and was adopted as UNGA Resolution 73/6[1469] without a vote.[1470]

In sum, the process of this resolution can be divided into a procedural and a substantive path, which can be illustrated as follows:

[1464] United Nations General Assembly, Resolution 72/79, 7 December 2017, A/RES/72/79.
[1465] General Assembly 72nd Session 66th plenary meeting, 7 December 2017, 10 a.m. New York, A/72/PV.66, p. 5.
[1466] Draft resolution entitled 'Fiftieth Anniversary of the first United Nations Conference on the Exploration and Peaceful Uses of Outer Space: Space as a Driver of Sustainable Development', UN Doc. A/AC.105/L.313, 16 May 2018.
[1467] UN Doc. A/73/20, cit. note 1217, para. 31.
[1468] Fiftieth Anniversary of the first United Nations Conference on the Exploration and Peaceful Uses of Outer Space: Space as a Driver of Sustainable Development, UN Doc. A/73/L.6, 12 October 2018.
[1469] A/RES/73/6, cit. note 1021.
[1470] General Assembly 73rd Session, 26th plenary meeting, 26 October 2018, 10 a.m. New York, UN Doc. A/73/PV.26.

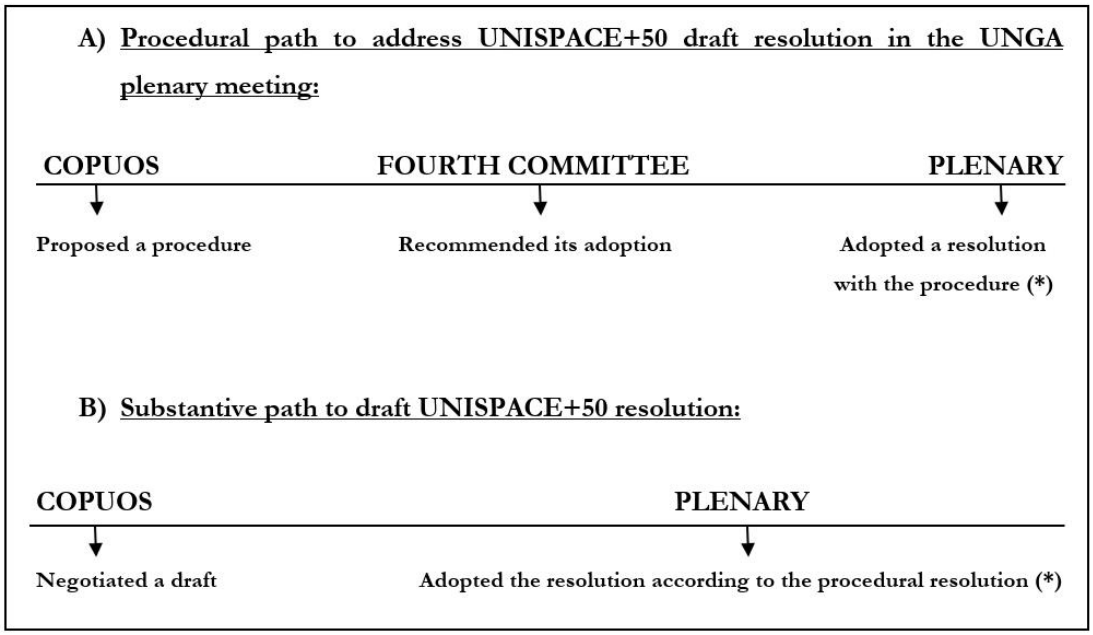


**Figure 17: The UNISPACE+50 model**

### 5.7.3.- A DRAFT UNGA RESOLUTION: THE 'LAUNCHING STATE' MODEL

The final model that will be proposed for consideration here is the one of UNGA Resolution 59/115. In this case, discussions on the topic were initially carried out in a particular working group established in 2002 under a relevant agenda item of the LSC to review the concept of 'launching State'.[1471] Building upon that work and on the basis of a proposal submitted by Germany on behalf of a group of States, the Working Group on the Status and Application of the Five UN Treaties (within the LSC) reached consensus on a draft resolution in 2004 on the concept of the 'launching State'.[1472] COPUOS approved the draft resolution and agreed to submit it to the General Assembly.[1473] Nigeria, in its capacity as Chair of COPUOS, submitted to UNGA Fourth Committee the draft resolution entitled

[1471] Report of the 41st Session of the LSC (2002), UN Doc. A/AC.105/787, Annex IV.
[1472] Report of the Chairman of the Working Group on agenda item 6, entitled 'Status and Application of the five United Nations Treaties on Outer Space' contained in the Report of the 47th Session of COPUOS (2004), UN Doc. A/AC.105/826, 16 April 2004, Annex I, para.7.
[1473] Report of COPUOS 59th Session (2004), UN Doc. A/59/20, para. 149. The draft resolution is contained in Annex II.

'Application of the concept of the 'launching State"', which was adopted without a vote.[1474] That draft resolution was referred to the plenary meeting of the General Assembly in the report of UNGA Fourth Committee and was adopted as UNGA Resolution 59/115 without a vote.[1475]

Unlike the LTS model, this model produced an UNGA resolution negotiated in COPUOS that is independent of the omnibus resolution on international cooperation. However, unlike the UNISPACE model, this resolution went through UNGA Fourth Committee and was then adopted by the plenary meeting of the General Assembly. The process can be summarised as follows:

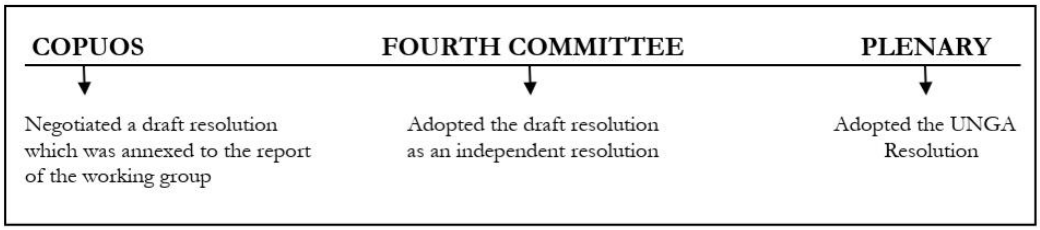


**Figure 18: The 'launching State' model**

## 5.8.- A CONCRETE PROPOSAL:

The previous section boiled down the options of negotiation to two alternatives: either a set of guidelines or an UNGA draft resolution. While both are non-binding instruments, they differ in substance and procedure.

**a) A set of guidelines:**

A set of guidelines tends to be a more technical and lengthy endeavour. In order to substantiate that assertion, it suffices to examine the two sets of guidelines negotiated in

[1474] Report of the Special Political and Decolonization Committee (Fourth Committee), UN Doc.A/59/469, 8 November 2004, paras 8-9.
[1475] General Assembly 59th Session, 71st plenary meeting, 10 December 2004, at 3 p.m. New York, UN Doc. A/59/PV.71, p. 5.

COPUOS that bear a connection to this thesis: the 2007 Space Debris Mitigation Guidelines and the LTS Guidelines, both already referred to in chapter 4.

The former was the result of a long process that started with the inclusion of the topic on the agenda of the STSC in 1994. In 2001 a corresponding working group was established with a four-year work plan to consider the proposals on debris mitigation made by the IADC.[1476] Finally, in 2004 the Working Group on Space Debris agreed to develop a set of guidelines on space debris mitigation making reference to the IADC Guidelines.[1477] This means that the topic was on the agenda of the STSC almost fourteen years until the endorsement of the guidelines by the General Assembly in 2007. In addition, the technical work of the IADC contributed tremendously to them. The final outcome was not a stand-alone UNGA resolution, but the guidelines were merely endorsed in the omnibus resolution on international cooperation.[1478]

The latter also originated from a technical and lengthy process. Indeed, the process leading to the LTS Guidelines began in 2009 with the inclusion of the topic on the agenda of the STSC and continued with the setup of a corresponding working group in 2010. Finally, four expert groups were established to provide inputs to the working group. In other terms, the topic was on the agenda of the STSC ten years until the endorsement of the guidelines by the General Assembly in 2019.

In sum, according to the practice examined, a set of guidelines on space cybersecurity would require: a) an agreement on the inclusion of an agenda item in the STSC and b) the establishment of a corresponding working group. An alternative path for point b) might be to mandate an existing working group with the task of drafting a set of guidelines on space cybersecurity (for instance, the LTS Working Group).

**b) A draft UNGA resolution:**

Chapter 3 has already briefly reviewed a set of core UNGA resolutions (see section 3.8.3), and this chapter has already referred to two additional ones (see section 5.7.2 and section 5.7.3). Beyond the annually adopted resolution on international cooperation, roughly

[1476] Report of the 38th Session of the STSC (2001), UN Doc. A/AC.105/761, para. 130.
[1477] Report of the 42nd Session of the STSC (2005), UN Doc. A/AC.105/848, Annex II, paras 5- 6.
[1478] A/RES/62/217, cit. note 963, para. 26.

speaking it is possible to divide UNGA resolutions relating to outer space matters into three main categories: principles,[1479] declarations[1480] and recommendations.[1481] In addition to these categories, there are five UNGA resolutions that annex the five UN space treaties.[1482]

These UNGA resolutions have several points in common: first, they were drafted within the LSC and not in the STSC. Second, they are independent from the omnibus resolution on international cooperation. Third, those negotiated after 1993 were endorsed by the UNGA Fourth Committee without a vote (see chapter 4, section 4.7.3 on the revitalisation of the work of the General Assembly). Finally, they were adopted by a plenary meeting of the General Assembly also without a vote (the only exception is UNGA Resolution 37/92 on direct television broadcasting, which was adopted with a vote).

Following the practice at COPUOS, a draft UNGA resolution on space cybersecurity would require: a) an agreement on adding an agenda item for consideration by the LSC and b) the establishment of a corresponding working group. An alternative path for point b) might be to mandate an existing working group (for instance, the Working Group on the Status and Application of the Five UN Treaties) with the task of drafting an UNGA resolution with principles on space cybersecurity.

In conclusion, taking into consideration that there was already an unsuccessful attempt to address space cybersecurity in the Working Group on LTS, that the substance of negotiations on space cybersecurity is legal in nature and that –as already explained in chapter 3– UNGA resolutions may sometimes have a normative value, and that they may also reflect the existence or contribute to the formation of a customary rule if adopted without a vote, the normative solution proposed in this thesis is to draft an UNGA resolution in the LSC.

[1479] A/RES/1962(XVIII), cit. note 582; A/RES/37/92, cit. note 836; A/RES/41/65, cit. note 839; A/RES/47/68, cit. note 841.
[1480] A/RES/51/122, cit. note 584; United Nations General Assembly, Resolution 72/78, 7 December 2017, A/RES/72/78 ('Declaration on the fiftieth anniversary 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').
[1481] A/RES/59/115, cit. note 1232; A/RES/62/101, cit. note 765; United Nations General Assembly, Resolution 68/74, 11 December 2013, A/RES/68/74 ('Recommendations on national legislation relevant to the peaceful exploration and use of outer space').
[1482] A/RES/2222 (XXI), cit. note 729; A/RES/2345 (XXII), cit. note 748; A/RES/2777 (XVI), cit. note 754; A/RES/3235 (XXIX), cit. note 757; A/RES/34/68, cit. note 773.

### 5.8.1.- FOURTH COMMITTEE, JOINT COMMITTEES OR UNGA PLENARY?:

According to the analysis made above, it appears to be irrefutable that space cybersecurity has aspects that fall under UNGA First and Fourth Committees. To shed some light on which should be the best way to refer a draft resolution to the General Assembly for its adoption, it is necessary to resort to the methods of work and rules of procedure of that organ to elucidate how overlapping mandates can be dealt with. Reference can be made to UNGA Resolution 362 (IV), which amended the Rules of Procedure of the General Assembly in 1949. On that opportunity, the Special Committee recommended changing the practice in the allocation of topics to the UNGA Main Committees, which was according to the category to which a certain topic belonged (current Rule 97). Such a manner of allocation led to overloading certain UNGA Committees more than others; thus, it was proposed referring the subject to the UNGA Committee with the lightest agenda when a topic could fall under the mandate of two Committees.[1483]

If the agendas of UNGA First and Fourth Committees are compared with each other, it will become clear that UNGA First Committee[1484] has a far more loaded agenda than UNGA Fourth Committee. [1485] Hence, following the above mentioned recommendation, UNGA Fourth Committee might be allocated the topic, even if the proposed draft resolution falls also under UNGA First Committee's mandate due to the international security matters involved.

A second alternative option is to follow the recommendation of the General Assembly suggesting the consideration of an agenda item in plenary meetings without prior referral to any of the Main Committees.[1486] However, it should be underscored that such a course of action would be extraordinary because pursuant to the Rules of Procedure of the General Assembly, the ordinary procedure is that this organ makes a final decision on an

[1483] United Nations General Assembly, Resolution 362 (IV), 22 October 1949, A/RES/362(IV), Annex II, para. 22.
[1484] See for instance: Allocation of Items to the First Committee, UN Doc. A/C.1/75/1, 21 September 2020.
[1485] See for instance: Allocation of Agenda Items to the Special Political and Decolonization Committee (Fourth Committee), UN Doc. A/C.4/75/1, 18 September 2020.
[1486] A/RES/362(IV), cit. note 1483, para. 23. See also United Nations General Assembly, Resolution 48/264, 29 July 1994, A/RES/48/264, Annex I, para. 2.

agenda item once it has received the report of an UNGA Committee on that item, unless it decides otherwise (Rule 65).

The third alternative option is to consider the possibility of establishing an UNGA joint Committee. The recommendations on the methods of work of the General Assembly do not expressly envisage such a possibility for any combination of Committees but only for any combination that requires the involvement of UNGA Sixth Committee due to the legal matters concerned. This particular recommendation was the result of lengthy discussions upon a proposal submitted by the United Kingdom in 1951 that, *inter alia*, proposed submitting to UNGA Sixth Committee matters dealt with by another UNGA Committee when they involved legal aspects.[1487]

In practice, there was such joint cooperation also between UNGA Second and Third Committees in the sixtieth and sixty-first session.[1488] Moreover, it should be borne in mind that the General Assembly during several years has reminded of 'the need to enhance synergies and coherence and reduce overlap where it is found to exist in the agendas of the General Assembly'.[1489] In this regard, chapter 4 (see section 4.7.3) already reviewed the practice of joint discussions of UNGA First and Fourth Committees. Such a practice may be grounded on an UNGA resolution of 2004, which decided that the practice of interactive debates and panel discussions shall be implemented and expanded to bring together experts from different fields without prejudicing the progress of the substantive work of UNGA Main Committees.[1490]

On the basis of the analysis made above, this thesis proposes the following three-stage procedure for drafting an UNGA resolution on space cybersecurity:

1.- Following the UNISPACE+50 model, a working group under the LSC (and eventually under a specific agenda item) should draft a procedural UNGA resolution to

[1487] For a complete analysis on the proposal and the evolution of the negotiation of this recommendation, see LIANG, Y., *Methods and Procedures of the General Assembly for Dealing with Legal and Drafting Questions*, in 'The American Journal of International Law', Vol. 47, No. 1, 1953.
[1488] Updated Inventory Chart of General Assembly Resolutions on the Revitalization of the Work of the General Assembly, issued pursuant to Resolution 74/303, draft as of 3 February 2021. https://www.un.org/ (last accessed on 11 August 2021).
[1489] United Nations General Assembly, Resolution 70/305, 13 September 2016, A/RES/70/305, para. 22; Resolution 71/323, 8 September 2017, A/RES/71/323; Resolution 72/313, 17 September 2018, A/RES/72/313, para. 29.
[1490] United Nations General Assembly, Resolution 58/316, 1 July 2004, A/RES/58/316, op. 3(c).

decide that a substantive draft resolution on space cybersecurity (point 2 below) will be addressed jointly by UNGA First and Fourth Committees. That draft resolution on procedural matters should be considered and endorsed by UNGA Fourth Committee and then adopted in a plenary meeting of the General Assembly.

2.- Following the 'launching State' model with a variation, the same working group under the LSC should draft a substantive UNGA resolution on space cybersecurity to be submitted to a joint meeting of UNGA First and Fourth Committees according to UNGA resolution of point 1 above.

3.-The substantive draft resolution should be considered jointly by UNGA First and Fourth Committees. In that instance, UNGA First Committee will be entitled to, on the one hand, add all necessary references and aspects emanating from its work on the use of ICTs and international security that are deemed appropriate and, on the other hand, the inputs regarding TCBMs in outer space activities. Since the preliminary draft to be submitted will be negotiated within COPUOS with the necessary legal and technical expertise, it is desirable that UNGA Fourth Committee does not reopen the draft text referred by COPUOS but only for minor editions. Its main task should be to take up the role of coordinator with UNGA First Committee to ensure a proper merge of the technical inputs under the competence of the latter with the contents falling under the competence of the former.

4.- UNGA First and Fourth Committees should jointly refer the draft resolution as amended to the plenary of the General Assembly meeting for adoption.

### 5.8.2.- A TEXT FOR A DRAFT UNGA RESOLUTION

The resolution text proposed in this section is drafted on the basis of the background information and findings arising out from this thesis. For the sake of clarity, the layout of this section is divided into two parts: one with the draft text and the other one with the substantiation of the wording selected. For a better individualisation, inputs that fall under the remit of UNGA First Committee are in red.

**a) Draft text:**

The General Assembly,

*Recalling* its resolutions 1962 (XVIII) of 13 December 1963; 2222 (XXI) of 19 December 1966; on 2777 (XXVI) of 29 November 1971; 3235 (XXIX) of 12 November 1974; 62/217 of 22 December 2007 and 74/82 of 13 December 2019; [75/32 of 7 December 2020]; [73/27 of 5 December 2018]; 70/237 of 23 December 2015; 64/49 of 2 December 2009, 69/38 of 2 December 2014, 70/53 of 7 December 2015, 71/42 of 5 December 2016, 72/56 of 4 December 2017 and 68/50 of the 5 December 2013. (1)

*Reaffirming* that outer space shall be free for exploration and use by all States without any discrimination of any kind, on the basis of equality and in accordance with international law, (2)

*Convinced* that the use of existing space technology, including ICTs, can play a vital role in supporting disaster management by providing accurate and timely information for decision-making and re-establishing communication in case of disasters, (3)

*Mindful* that space systems are critical infrastructures and support other Earth-based critical infrastructures, (4)

*Seriously concerned* about the malicious use of ICTs against space systems and the harmful impact of malicious space cyber activities in the normal functioning of critical infrastructures, (5)

*Reaffirming* the importance of international cooperation in developing the rule of international law, including the relevant norms of space law and their important role in international cooperation for the exploration and use of outer space for peaceful purposes, and of the widest possible adherence to international treaties that promote the peaceful uses of outer space in order to meet emerging new challenges, especially for developing countries, (6)

*Seriously concerned* about the possibility of an arms race in outer space and bearing in mind the importance of Article IV of the Outer Space Treaty, (7)

*Deeply concerned* about the fragility of the space environment and the challenges to the long-term sustainability of outer space activities, in particular the impact of space debris, which is an issue of concern to all nations, (8)

*Recalling* the fact that the United Nations Conference on Sustainable Development and the 2005 World Summit recognized the important role that science and technology play in promoting sustainable development, (9)

[*Welcoming* the effective work of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and the relevant outcome reports transmitted by the Secretary-General, and also welcoming the productive work of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security] (10)

*Noting* that nothing in the conclusions of the Working Group of the Legal Subcommittee [name to be added] or in the present resolution constitutes an [authoritative interpretation of or] a proposed amendment either to the Outer Space Treaty or to the Liability Convention, (11)

*Adopts* the Principles governing space cyber activities set forth in the annex to the present resolution (12)

## ANNEX

## PRINCIPLES GOVERNING SPACE CYBER ACTIVITIES

### PRINCIPLE I (13)

For the purposes of these principles governing space cyber activities,

(a) The term 'space cyber activities' means activities in outer space or directed to outer space, including the Moon and other celestial bodies, which are carried out by the use of ICTs.

(b) The term 'malicious space cyber activities' means space cyber activities, [aimed at interfering] [which interfere] with the normal operation of a functional space object registered with a third State by:

a) taking control of it,

b) affecting any of its constituent parts and/or payload,

c) stealing, degrading, altering or destroying images and/or data obtained or produced by it,

d) reducing its lifespan, or

e) acting in any other manner contrary to Article IX of the Outer Space Treaty.

**PRINCIPLE II** (14)

Space cyber activities shall be carried out for the benefit and in the interests of all countries, irrespective of their degree of economic or scientific development. They shall also be conducted with due regard to the corresponding interests of other States and shall be in accordance with international law, including the Charter of the United Nations, the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, and the relevant instruments of the International Telecommunication Union, in the interest of maintaining international peace and security and promoting international cooperation and understanding.

**PRINCIPLE III** (15)

In conducting their space cyber activities, it is essential that Member States pay more attention to the problem of collisions of space objects, especially those with nuclear power sources.

**PRINCIPLE IV** (16)

Transparency and confidence-building measures in outer space can reduce or even eliminate misunderstandings, mistrust and miscalculations with regard to space cyber activities and intentions of States in outer space and thus enhance space security, safety and long-term sustainability of space activities.

**PRINCIPLE V** (17)

States shall cooperate in developing and applying measures to increase stability and security in space cyber activities and in preventing practices that are acknowledged to be harmful or that may pose threats to international peace and security.

**PRINCIPLE VI** (18)

States shall not knowingly allow their territory or space objects registered with them to be used for malicious space cyber activities contrary to the rights of other States.

**PRINCIPLE VII** (19)

Any international dispute that may arise from space cyber activities shall be settled through established procedures for the peaceful settlement of disputes agreed upon by the parties to the dispute in accordance with the provisions of the Charter of the United Nations.

**PRINCIPLE VIII** (20)

In compliance with Article VI 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, States conducting space cyber activities shall bear international responsibility for them and assure that such activities are conducted in accordance with these principles and the norms of international law, irrespective of whether such activities are carried out by governmental or non-governmental entities or through international organisations to which such States are parties. This principle is without prejudice to the applicability of the norms of international law on State responsibility for malicious space cyber activities.

**PRINCIPLE IX** (21)

These Principles [may/shall] be reopened for revision by the Committee on the Peaceful Uses of Outer Space and joint consideration of UNGA First and Fourth Committees no later than two years after their adoption.

**b) Substantiation:**

1. Preambular part:

**(1)** The preamble of UNGA resolutions usually makes reference to previous resolutions particularly significant for the topic at stake. In the present case, the resolutions that have a significant bearing on the matter are:

- **Resolutions regarding international space law within COPUOS (see chapter 3 section 3.8.2, section 3.8.3 and chapter 4 section 4.4):**

-UNGA Resolution 1962 (XVIII): the Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space.

-UNGA Resolution 2222 (XXI): Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies.

-UNGA Resolution 2777 (XXVI): Convention on International Liability for Damage Caused by Space Objects.

-UNGA Resolution 3235 (XXIX): Convention on Registration of Objects Launched into Outer Space.

-UNGA Resolution 62/217: International cooperation in the peaceful uses of outer space (this resolution endorses the Space Debris Mitigation Guidelines).

-UNGA Resolution 74/82: International cooperation in the peaceful uses of outer space (this resolution welcomes the LTS Guidelines).

In addition, UNGA First Committee might include:

- **Resolutions regarding ICTs (see chapter 2, section 2.8.1):**

-A reference to UNGA Resolution 75/32, which calls upon States to be guided by the **2010, 2013 and 2015** reports of the GGEs on ICTs, would be desirable but it might meet objections because it was adopted with a recorded vote of 163 to 10, with 7 abstentions. For this reason this proposal is in brackets.

- A reference to UNGA Resolution 73/27, which welcomes the recommendations of the **2013 and 2015** reports of the GGEs on ICTs. Since that resolution was adopted with a recorded vote of 119-46-14, its inclusion might probably meet some objections (this is the reason why it is between square brackets).

-A reference to UNGA Resolution 70/237, which calls upon States to be guided by the **2015** report of the GGE on ICTs. From these three resolutions on the matter, this is the minimum that should be acceptable because it was adopted without a vote but on the other hand it is the least ambitious.

- **Resolutions regarding TCBMs (see chapter 4 section 4.5)**

-A reference to the resolutions on TCBMs that were adopted without a vote: UNGA Resolution 48/74B (which takes note of the 1993 report of the GGE on CBMs); Resolution 64/49 (2009), Resolution 68/50 (welcomes the 2013 report of the GGE on TCBMs and encourages States to implement the recommendations contained therein), Resolution 69/38 (2014), Resolution 70/53 (2015), Resolution 71/42 (2016) and Resolution 72/56 (2017).

**(2)** This is a paragraph that refers to one of the most fundamental principles of space law. Such a paragraph can be found in several UNGA resolutions, such as UNGA Resolution 73/6 (UNISPACE+50 Resolution).

**(3)** A paragraph referring to space technology including ICTs is a variation from UNGA Resolution 62/217 (which endorses the 2007 Space Debris Mitigation Guidelines). This variation intends to adapt the wording to the particular subject matter making reference to ICTs.

**(4)** A paragraph asserting that space systems are critical infrastructures and also support other critical infrastructures on Earth is a paragraph specially crafted for this draft resolution, built upon the premises and conclusions of this thesis.

**(5)** A paragraph expressing concern about the malicious use of ICTs and introducing the language of 'space cyber activities' is also specially crafted for this draft resolution, taken from the findings of this thesis.

**(6)** The paragraph reinforcing the importance of international cooperation and international space law to promote the peaceful uses of outer space was taken from UNGA Resolution 73/6 (UNISPACE+50 Resolution) and UNGA Resolution 74/82 (which welcomes the LTS Guidelines).

**(7)** As already explained in chapter 5 (see section 5.6.1), a reference to the prevention of an arms race became commonplace in COPUOS texts. The paragraph inserted in the proposed draft resolution is a traditional paragraph on the prevention of an arms race that is included in most UNGA resolutions regarding space matters.

**(8)** A paragraph devoted to the concerns regarding LTS was taken from UNGA Resolution 74/82 (which welcomes the LTS Guidelines).

**(9)** A paragraph referring to the relation between space science and sustainable development was built upon certain paragraphs from UNGA Resolution 74/82 (which welcomes the LTS Guidelines) and UNGA Resolution 62/217 (which endorses of the 2007 Space Debris Mitigation Guidelines).

**(10)** A paragraph welcoming the work of the GGEs on ICTs and of the OEWG in line with UNGA Resolution 75/32. Since this resolution was adopted with a recorded vote of 163-10-7, its inclusion might probably meet some objections (this is the reason why it is in square brackets).

**(11)** A paragraph that clarifies that the resolution does not intend to serve as an interpretative or amending instrument to the treaties is a caveat that can be found in UNGA Resolution 59/115 (Application of the concept of the 'launching State'). An alternative would be to allow this resolution indeed to become an authoritative source of interpretation, like UNGA Resolution 51/122 (Declaration on Space Benefits). In such a case, the wording in brackets should be eliminated and only state that the principles do not constitute an amendment to the treaties.

**(12)** The last paragraph is a closing clause adapted to the present case, usually inserted in UNGA resolutions that annex a set of principles on a certain matter, for instance, UNGA Resolution 51/122 (Space Benefits Declaration), UNGA Resolution 37/92 (Principles for Direct Television Broadcasting) and UNGA Resolution 41/65 (Principles relating to remote

sensing). An alternative option is to follow the model of UNGA Resolution 47/68 (Nuclear Power sources), which adopts the principles directly (and not as an annex).

2. Operative part:

**(13)** This paragraph is the glossary that usually clarifies the terms to be used in a set of principles adopted in an UNGA resolution. Examples of such a format can be found in UNGA Resolution 41/65 (Principles Relating to Remote Sensing of the Earth from Outer Space) and in UNGA Resolution 47/68 (Principles Relevant to the Use of Nuclear Power Sources in Outer Space).

In this case, there are two concepts that need to be defined at the outset: 'space cyber activities' which is mainly the use of ICTs in space activities and 'malicious space cyber activities', which includes the full range of interferences as covered by Article IX of the Outer Space Treaty, from mere incidents to cyberattacks. For the latter, there are two options to be examined in square brackets: whether there is a need for an intentional element or not.

**(14)** The source of inspiration of this paragraph is UNGA Resolution 47/68 (Principles Relevant to the Use of Nuclear Power Sources in Outer Space) and UNGA Resolution 37/92 (Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting). If the text is examined closely, it will be clear that it reproduces essential elements of the three core provisions of the Outer Space Treaty that this thesis addressed as limitations to space cyber activities: Articles I, III and IX. It should be recalled that, according to the conclusions reached in this research, the reference to the application of international law includes the preventive and precautionary principles applicable to relevant environmental matters. Finally, it also includes an explicit reference to the ITU regime.

**(15)** The reference to the concern about space debris in Principle III is mainly extracted from UNGA Resolution 62/217 (which endorses of the 2007 Space Debris Mitigation Guidelines) and UNGA Resolution 74/82 (which welcomes the LTS Guidelines).

**(16)** This is a paragraph that should be considered by UNGA First Committee since it concerns issues under its mandate. It is a reformulation of a wording adopted in the 2013 report of the GGE on TCBMs in outer space activities (A/68/189). It should be recalled

that this report was adopted by consensus and endorsed by UNGA Resolution 68/50 without a vote (which welcomes the report). This draft principle enshrines the interconnection of space safety, security and long-term sustainability of space activities.

**(17)** Like the previous draft principle, this one also falls under the remit of UNGA First Committee. The wording is an adaptation of a paragraph from UNGA Resolution 73/27 (which welcomes the norms, principles and recommendations made in the 2013 and 2015 reports of the GGEs on ICTs) to the concept of 'space cyber activities'.

**(18)** This paragraph has been specially crafted for this draft resolution and enshrines an important principle that has already been acknowledged by ICJ jurisprudence and by the conclusions of the GGEs on ICTs. It also equates a space object registered with a State with its territory, as suggested by a part of the literature reviewed in this thesis.

**(19)** The wording of this paragraph is extracted from UNGA Resolution 37/92 (Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting) and UNGA Resolution 47/68 (Principles Relevant to the Use of Nuclear Power Sources in Outer Space). The main purpose of this draft principle is to discourage the resort to forceful measures in response to malicious space cyber activities and to enhance the principle of peaceful settlement of disputes enshrined in Article 2(3) of the UN Charter.

**(20)** A similar paragraph regarding responsibility under Article VI of the Outer Space Treaty and State responsibility under general international law can be found in UNGA Resolution 41/65 (Principles Relating to Remote Sensing of the Earth from Outer Space) and in UNGA Resolution 47/68 (Principles Relevant to the Use of Nuclear Power Sources in Outer Space). The variation in this case is the employment of the expression 'malicious space cyber activities'.

**(21)** This paragraph envisages the evolutionary and flexible nature of the principles and the idea that they should not be envisaged as a one-shot solution but rather as a progressive endeavour. The essence of this draft principle is imported from UNGA Resolution 47/68 (Principles Relevant to the Use of Nuclear Power Sources in Outer Space). The novelty in this paragraph is that it acknowledges and preserves the joint role of UNGA

First and Fourth Committees in this matter and thus in the revision of the principles. Furthermore, this might be the legal ground for a more specific and expansive work on the topic.

## 5.9.-CONCLUSIONS

Although there is no specific rule either under space law or under international law in general prohibiting expressly malicious space cyber activities *per se*, there is a legal framework that is applicable to space cyber activities. In effect, this chapter concluded that those activities have to comply with the limitations that the Outer Space Treaty establishes, most importantly in Articles I, III and IX. In addition, space cyber activities have to comply with the principles and obligations under international law in general, in particular the prohibition on the use of force, the non-intervention principle and the obligation to respect State sovereignty.

The responsibility regime under Article VI of the Outer Space Treaty, the liability regime under Article VII of the same instrument complemented by the Liability Convention and the regime of State responsibility under customary international law were examined in order to determine whether the existing normative framework provides a legal ground on which to seek compensation, either for a wrongful act or for damage. In the former case (responsibility), the argument was put forward that when a space activity is not compensable under the space law regime, the customary rules on State responsibility apply. Moreover, it was argued that where global commons are impaired, any State might claim under such customary regime for the violation of the *erga omnes* obligation not to cause pollution in areas beyond a State's jurisdiction, which is a principle enshrined in the international law regime applicable via Article III of the Outer Space Treaty.

In the latter case (liability), the conclusion was reached that the liability regime does not provide any assistance to the victim State of a malicious space cyber activity on two counts: first, the liability regime applies only to legal and permitted activities; and second, because the understanding of 'damage' in the context of this regime is limited to the damage caused by the impact of a space object. The direct and indirect damages resulting from a malicious space cyber activity were examined and in that context, it was concluded that the liability regime does provide a remedy for the indirect damage (if caused), i.e. the creation of

space debris. However, such a remedy is very limited because it provides a mechanism for compensation from the launching State and not from the State responsible for the malicious space cyber activity. In addition, it does not provide any exoneration when the launching State lost control of the space object as a consequence of the malicious space cyber activity and a third State claims compensation for damage.

The other part of the analysis carried out in this chapter was the normative one. Chapter 4 already presented the concept of the 'mandates conflict' between COPUOS and the Conference on Disarmament as an introductory note. It also explained the interconnection of security, safety and LTS. Moreover, it reviewed the achievements and defeats in the negotiations in the field. In sum, chapter 4 set the scene to the examination made in this chapter, where the arguments in favour and against binding and non-binding instruments were put forward, not only from a doctrinal standpoint but more importantly from a State's practice perspective. The attempt to unravel the 'mandates conflict' led to the conclusion that when the lack of political will is disguised as a limitation in the mandate, the only solution to circumvent the stalemate is to avoid the warfare language that enables a body to make a specific subject matter its own.

The examination of which should be the normative solution that is simultaneously legally feasible, technologically realistic and politically desirable (international space law as a triad) led to the conclusion that for the time being a non-binding instrument should be the preferable solution. However, that instrument should not be envisaged as a one-shot normative solution but rather as progressive normative evolution.

Upon the examination of the practice of COPUOS in drafting non-binding instruments, the options for a normative solution were reduced to either a set of guidelines or an UNGA draft resolution. Taking into consideration the normative value that an UNGA resolution may have and the effects that it may produce, this chapter proposed to draft an UNGA resolution with principles.

The analysis of the competences of UNGA First and Fourth Committees reaffirmed that work in silos has some limitations that are not impossible to overcome. In effect, original solutions are required to fully implement the recommendations on the revitalisation of the work of that body, in particular those suggestions relating to coordination and cooperation

among UNGA Main Committees. In that vein, this thesis proposed a draft resolution that should start being negotiated in COPUOS to then become under the joint examination of UNGA First and Fourth Committees. This would take the practice that already exists in the field of space security of joint *ad hoc* meetings to a higher level.

In sum, this chapter has completed the analysis started in previous chapters to answer the six questions proposed in the introductory chapter. The research findings will be laid out in the next and final chapter.

# CHAPTER 6:
# FINAL CONCLUSIONS

This chapter does not intend to restate the findings that were already presented in each preceding chapter. Furthermore, most of the sections have their own concluding remarks and partial summaries. Rather, the aim of this chapter is to provide the reader with an overall assessment on three issues: a) the research problem and findings, b) implications of the research and c) recommendations for future work.

## 6.1. THE RESEARCH PROBLEM AND FINDINGS:

The research problem was stated in chapter 1 (see section 1.4) as a research problem based on a 'how' question (how international space law applies to space cybersecurity, how international law in general may fill the gaps and how the international community may address the topic in future negotiations). It should be underscored that this is a problem of interest not only within academic circles but notably of policy-makers. Likewise, it provides important tools for diplomats assigned with multilateral functions in space and security bodies, including in the United Nations ('space diplomacy'[1491] and 'science diplomacy'[1492]).

In order to better understand the problem, four aspects of particular concern should be brought to the forefront: the 'mandates conflict' between COPUOS and the Conference on Disarmament, the limited progress made in PAROS, the desire to expand space applications and space exploration for the betterment of present and future generations, and the need to extend the global space governance to the new technological challenges and the threats emerging from the malicious use of space assets.

[1491] It should be recalled that 'space diplomacy' was one of the four pillars of UNISPACE+50 and is also one of the four objectives of the Space2030 Agenda.
[1492] 'Science diplomacy' has three possible interpretations: science for diplomacy – the use of science to further diplomatic aims; diplomacy for science – the use of diplomatic endeavours to promote scientific and technological progress; and science in diplomacy – the direct involvement of scientific actors in diplomatic initiatives, see www.science-diplomacy.eu

The hypothesis that had to be confirmed or refuted was that there are provisions of space and telecommunications law that apply as *lex specialis* to the threats stemming from the convergence of the cyber and space domains, and that the broader universe of international law would anyway be applicable in accordance with Article III of the Outer Space Treaty. However, since those regimes do not fully address the challenges that space cybersecurity poses nowadays, the gaps should be filled in future negotiations specifically focused on the matter.

In the introduction, six research questions were identified as the common thread to reach the conclusions and establish the findings of this study. Each chapter contributed partially to replying them. At this more comprehensive stage, it is possible to conclude that there is a regulatory framework applicable to the convergence of space and cyber domains; however, it does not explicitly regulate space cyber security (**research question 1**). Space law and telecommunications law provide the necessary legal basis to regulate space cyber activities (**research question 2**). Space cyber activities are space activities under the Outer Space Treaty and therefore have to comply with its provisions (**Research question 3 a**). The concept of damage under the liability regime does not apply to the direct damage caused by malicious cyber activities (**Research question 3 b**). Even if the operating system/software is part of a space object, the concept of damage under the liability regime applies only to material and physical damage caused by impact in the course of a lawful space activity (**Research question 3 c**). COPUOS is the right body to undertake negotiations to draft a guiding instrument in the field, which should be addressed jointly by UNGA First and Fourth Committees (**Research question 4**). A non-binding instrument is for the time being the most appropriate solution, although the work on space cybersecurity should be progressive. The negotiation of binding instruments in the field of space security has proven to be difficult due to conflicting positions around them (**Research question 5**). The regulation of space cybersecurity contributes to the long-term sustainability of space activities since it addresses the legal problems emerging from space cyber activities that increase the space debris population. Any instrument that contributes to the regulation of the activities in outer space enhances the global space governance (**Research question 6**).

## 6.2. IMPLICATIONS OF THIS RESEARCH:

This section will be broken down into two sub-sections that will aim to reply two 'why' questions: why this research is original and why it is significant and contributes to knowledge.

### 6.2.1. THE ORIGINALITY OF THIS THESIS:

This research builds upon existing academic, political and legal sources. This means that the originality of this research does not lie on drafting *new* treaties of space law or proposing *revolutionary* models deviating from previous research or *imaginary* solutions deviating from international practice. To the contrary, this research intends to strike a balance between originality and pragmatism. In this regard, particular attention was paid to the focus on 'who' are interested in this problem and 'who' would be in charge of implementing the proposed solution: the answer is States, policy-makers and diplomats. Overly innovative solutions might not be a practical solution since States tend to be led by precedents and policy caution. On the understanding that the field of 3S requires a 'stepping stones' approach, the proposed solution in this research is more balanced than ambitious; and intends to be a first step in a progressive task of regulation in an environment that is more than reluctant to new regulations.

In such a context, originality needs to adopt a different shape. Estelle Phillips and Derek Pugh explained the concept of originality and laid down fifteen different ways to fulfil that aim.[1493] Some of these criteria will be employed below to explain the originality of this thesis:

**a) 'continuing a previously original piece of work':**

The intersection between cyberspace and outer space is an issue that was originally addressed by the Chatham House Royal Institute, and was also dealt with by the IISL and Tallinn Manual 2.0. This thesis built upon those inputs and continued that work in the field. However, what is new in this research is a clear statement about the need for different

[1493] PHILLIPS, E. AND PUGH, D., *How to Get a PhD. A Handbook for Students and their Supervisors*, Open University Press, Maidenhead, 2010, pp. 69-70.

language that avoids any reference to war, military operations, weapons and the like. In that vein, the language chosen is 'space cyber activities' and 'malicious space cyber activities'.

An additional novel element in this thesis is the endeavour to distinguish between cyber and electromagnetic activities in layman's language, for those with little command of physics and IT knowledge. In that vein, the distinction between a possible target for electromagnetic and cyber activities and where their effects materialise was the necessary result of this distinction (see chapter 3, section 3.3). Ultimately, this distinction is useful to understand the role of telecommunications law when it comes to harmful interference.

**b) 'carrying out empirical work that has not been done before':**

The idea that space systems are critical infrastructures and that they are 'systems-of-systems' was originally developed and stated by Romanian experts. This thesis examined and put together State positions, domestic law and literature providing evidence of such an assessment. State practice of a limited group of stakeholders was selected on the basis of their level of development in space and cyber domains (see chapter 3, section 3.7).

The discussion on binding and non-binding instruments has been an integral part of international space law since its very origin. Considerable ink has already been spilled on this; however, this thesis put together official opinions of certain States at COPUOS regarding both space governance solutions. In addition, it made the case that the small group of States providing inputs on this issue might be read as the absence of a clear-cut position by the rest of the international community regarding the need (or not) for new treaties to tackle emerging challenges (see chapter 5, section 5.5.3).

**c) 'being cross-disciplinary and using different methodologies':**

The preface and the epilogue intend to be an original way of starting and closing this research. Ph.D. theses are a formal display of scientific information laid out in a structured logical manner from the beginning to the end. In this thesis, those two sections break the rules: the preface and the epilogue embody an imaginary dialogue among three women living in different historical periods having a conversation three years ago (preface) and today (epilogue) in a real context. Those sections are pieces of a unique fictional narrative that summarises some underlying ideas of the thesis (preface), describes the research process and

sets out the ultimate goal of this research (the epilogue) in a ludic and unrealistic manner. All the previously mentioned elements are inserted in an atmosphere that reveals certain *clichés*, such as those relating to women and lawyers. Thus, this intertemporal dialogue conveys two implicit messages in a persuasive manner: the role of women in science now and in the past; and that 'science' should not be understood to include only STEM but also political and legal sciences. The ultimate purpose of this dialogue is to describe the interdisciplinary nature of this research, which combines cyber and space technology with law and policy.

**d) 'making a synthesis that has not been made before':**

This thesis identified a series of problems or contradictions and synthesised them as dilemmas. Hence, it created the concept of 'cyber regulatory dilemma' to refer to the contradictory willingness of digitally dependent States to set limits on others in the use of digital capacities while they remain reluctant to curtail own capacities (see chapter 2, section 2.3). Another dilemma that was identified and labelled is the 'techno dependence dilemma', i.e. the more dependent a State is on the 'system-of-systems', the more vulnerable it becomes (see chapter 2, section 2.3). Building upon the 'security dilemma', this thesis termed 'space cybersecurity dilemma' the intersection between the 'space security dilemma' and the 'cybersecurity dilemma' (see chapter 4, section 4.5 and figure 7). It also described as a 'prisoner's dilemma' the opposing positions between those against the LTS Guidelines on space security and those against the CoC, which led to a stalemate in the governance of space security (see chapter 4, section 4.6.2).

The idea of international space law as a 'triad' synthesise in an innovative manner the idea that the origin of international space law was the result of the intersection of three types of phenomena: legal, technological and geopolitical. These three elements permeate and give shape to international space law even today (see chapter 3, section 3.8.2).

The concept of 'mandates conflict' is once again another way to synthesise an old discussion about the appropriate body to *discuss* and *negotiate* space security matters. It was crafted with the aim of making visible the disagreement among States regarding the mandates of COPUOS and the Conference on Disarmament (see chapter 4, section 4.8 and chapter 5, section 5.9).

**e) 'looking at areas that people in the discipline have not looked at before':**

Integrating security matters into the agenda of COPUOS tends to be resisted and rejected. It might be difficult to read the title of this thesis and envisage a governance solution emanating from COPUOS. Moreover, the proposed solution goes even beyond the alternative between COPUOS and the Conference on Disarmament and brings the discussion to a possible joint mandate of UNGA First and Fourth Committees, taking into consideration rules of procedure of the General Assembly and certain practice of that body (see chapter 5, section 5.8.1).

Another element that needs to be underscored under this criterion of originality is that looking into manifold sources and materials regarding space security, space cybersecurity and LTS, not even a single article was found examining the space cybersecurity guidelines proposed by the Russian Federation within the LTS process. Although this thesis does not make any judgment on the appropriateness or not of those guidelines, it examined their content and their current status as inputs that are on the table for future discussions (see chapter 4, section 4.4.2).

**f) 'adding to knowledge in a way that has not been done before':**

None of the materials found during the research provided for taxonomy of malicious space cyber activities. The classification proposed in chapter 3 is not an expansion of an already existing categorisation but is a way to systematise the collected information (see chapter 3, section 3.4).

As already noted, the discussion on which is the preferred instrument to regulate an aspect in international space law is an old issue. The innovative element that this thesis added in that discussion is the definition of such an instrument as the 'legally feasible, technologically realistic and politically desirable solution' (see chapter 5, section 5.5 and section 5.9). This expression was created to respond to the idea of international space law as a triad, which was developed in chapter 3, section 3.8.2).

The shift from the discussion regarding the appropriate body for discussions on space security to a proposal for consideration jointly by UNGA First and Fourth Committees to deal with 3S has not ever been suggested. However, that solution is not isolated from

practice and rules of procedure of the General Assembly. To the contrary, it is drawn from precedents in the more general context of rationalisation of the General Assembly work, and from the recent practice of joint *ad hoc* meetings of UNGA First and Fourth Committees to address 3S. Furthermore, this thesis based that solution on the recommendations made by UNGA First Committee in the context of its work on TCBMs in outer space activities –the initial promoter of joint meetings in the field of 3S– and on relevant UNGA resolutions on international cooperation on the peaceful uses of outer space (see chapter 4, section 4.7.3 and chapter 5, section 5.8.1).

### 6.2.2. THE SIGNIFICANCE OF THIS RESEARCH:

In order to better explain the significance of this thesis, this section will build upon the four lines of argument laid down by David Evans, Paul Gruba and Justin Zobel:[1494]

**a) 'theory development':**

As explained in the previous section, this research does not create a new theory; it develops already existing studies in different interconnected fields. In this regard, paraphrasing Patrick Dunleavy, it is a 'value-added' contribution to knowledge.[1495]

**b) 'tangible solution':**

The proposal to table a draft resolution at COPUOS for the joint consideration of UNGA First and Fourth Committees is a tangible (though preliminary) solution. The draft text contains consensus language that has mostly been accepted in previous resolutions and reports negotiated at governmental level. The proposal to avoid warfare language is also a tangible solution to overcome the stalemate that the topic and the 'mandates conflict' create.

**c) 'innovative methods':**

A novelty in the approach of international space law is the departure from the traditional way of studying its formation in stages or periods. To the contrary, this research

[1494] EVANS, D., GRUBA, P. AND ZOBEL, J., *How to Write a Better Thesis*, Melbourne, 2014, pp. 66-67, 72.
[1495] DUNLEAVY, P., *Authoring a PhD. How to Draft, Plan, Write and Finish a Doctoral Thesis or Dissertation*, New York, 2003, p. 31.

employed a different methodology to avoid linking binding and non-binding instruments to a specific period of time, which clearly does not seem to reflect the more complex reality. Thus, this research reviews law, customary law, *jus cogens spatialis* and soft law, regardless of temporal criteria (see chapter 3, section 3.8.2 and section 3.8.3).

**d) 'policy extension':**

The research problem has practical rather than theoretical relevance; its solution is built upon already existing practice in multilateral bodies of negotiation. Moreover, it is envisaged as a policy solution and thus takes into consideration existing difficulties and opposing positions in negotiations, both in procedure and substantive matters.

### 6.2.3. LIMITATIONS OF THIS RESEARCH:

With regard to the limitations, chapter 1 (see section 1.4) already made reference to some limitations regarding the methodology (i.e. vagueness of international instruments, confidential documents and ongoing mechanisms). In addition, there are several limitations that emerged during the research process, which had an impact on the final outcome:

**a) Lack of universal definitions:** since there is no agreement on the terminology, this research had to establish its own glossary. It generally used the term 'malicious cyber activities' which encompasses all cyber threats, regardless of the scale and effects, the duration and the intention (chapter 2, section 2.2). In addition, for practical reasons the terminology used is 'space cybersecurity'; however, it would have been more appropriate to use the expression 'security in the use of ICTs in outer space', but such an expression would have led to a discussion on what is meant by 'in outer space' (chapter 3, section 3.2).

**b) Lack of sufficient State practice:** Since the practice of States in the qualification of malicious cyber activities is so far limited, few inductive conclusions could be drawn. Likewise, there is no State practice regarding the threshold that is necessary to determine the qualification of a malicious cyber activity as a mere use of force or as an armed attack (see chapter 2, section 2.4). Furthermore, there is no practice on the application of the international law governing non-intervention, use of force and self-defence to outer space activities (see chapter 3, section 3.9.1).

**c) Inconclusive definitions on how international law applies:** At governmental level, there is as yet no consensus on how international law applies to security in the use of ICTs and the literature is not uniform on how the rules on non-intervention, use of force and armed attacks apply to the cyber domain. In this case, the value-added approach of this thesis encountered serious difficulties to build upon a robust foundation.

**d) Ongoing endeavours with pending outcomes:** Since this thesis relies mainly on multilateral negotiations and some of the mechanisms in place are still ongoing, the findings of the research are partial (see chapter 2, section 2.8.1 and chapter 4, section 4.4.2). Likewise, there are at least two academic initiatives that are still in the pipeline, which would have been useful to consult but they are not yet available: the Woomera Manual on the International Law of Military Space Operations and the Milamos Manual on International Law Applicable to Military Uses of Outer Space.

**e) Materials with a preponderantly military approach**: Most of the literature on security in the use of ICTs has a military approach because the topics relating to State and international security are mainly addressed by military branches or military alliances. This thesis attempted to extract the relevant notions from such literature and 'neutralise' them in order to make them fit into the non-warfare approach proposed here.

## 6.3. RECOMMENDATIONS FOR FURTHER STUDY:

**a) Consensus definitions on specific concepts:** The first difficulty encountered in the research was to understand the multiplicity of concepts and their differing meanings. Future research into the topic might encounter a similar difficulty unless there is agreement on core concepts at a multilateral level. In particular, this research identified three concepts that require an urgent definition: cyberspace, cyber operations and cyberattacks. Moreover, definitions should be established regarding whether cyberspace encompasses the electromagnetic spectrum as well; whether cyber operations are also conducted in times of peace and by civil personnel and if cyberattacks require deliberation and certain duration. Likewise, it should be further determined if non-destructive effects might be encompassed (such as economic damage and loss of functionality).

As long as the international community does not adopt a uniform understanding, this research recommends starting any future research by stating how those concepts are understood and employed because the current state of the art is not crystal clear in that regard (see chapter 2, section 2.2).

**b) Practice of NATO:** A greater focus on the practice of NATO regarding Earth-based conflicts could produce interesting findings to account for the determination of the threshold a malicious cyber activity should reach to be a 'cyberattack' and thus activate the collective defence provided in Article 5 of the NATO treaty (see chapter 2, section 2.4). A follow-up of future summit declarations regarding cyberspace and outer space will be of the utmost importance. Particular attention should be given to Article 6 of the NATO treaty, which does not expressly include attacks against space objects. Hence, it will be useful to delve into how NATO's practice shapes and gives content to the description of 'armed attack' for the purposes of the application of Article 5.

**c) Other obligations of international law**: the scope of this research stuck to a limited group of international obligations (non-intervention, non-use of force and due diligence); hence, further research on other wrongful acts that might give rise to State responsibility would complement this research (see chapter 2, section 2.6). Particular attention should be given to the consequences of attacks against CNI. Since this research argued that space systems are CNI, any future endeavour examining the application of the right to self-defence should start from that premise and balance the findings with the obligations enshrined in the space treaties, notably the peaceful uses of outer space including the Moon and other celestial bodies (see chapter 3, section 3.9.1).

**d) The attribution test for activities by non-State actors in outer space**: Currently, scholars are divided between applying the effective control, the overall control or a more flexible approach. Furthermore, the literature on this aspect is scarce and is rather superficial (see chapter 2, section 2.6). This is an area that needs further exploration taking into consideration the jurisprudence of international tribunals.

**e) Human damage and compensation:** In the face of a new era of human spaceflight and taking into consideration the shortcomings that the current liability regime presents for compensation to the victim of space cyber activities, further research and

solutions will be needed to address injury, death and psychological damage as a consequence of such threats. Any such research will need to take into consideration and study a governance solution applicable to astronauts and space tourists according to their particularities.

**f) Follow-up on the development and activities of space forces**: At the moment of concluding this research, space forces or units within the military are only at an embryonic stage. In some cases, they are not yet completely operative; and in others, there is as yet no concrete practice at all. Constitutive instruments and statements of governments regarding their functions and competences would eventually provide evidence of State practice regarding how States envisage the prohibition of the threat or use of force in outer space (see chapter 3, section 3.7, part b)).

**g) Space cybersecurity from a private standpoint:** While this research focused on State security and international stability, there might be issues that need further research within the domestic or private international law remits; for instance, malicious space cyber activities carried out by non-State actors with private aims, such as competence in the space industry market within a State or internationally (see chapter 3, section 3.8.2).

**h) General international law of outer space:** Although this research briefly reviewed the views within the specialised literature regarding space customary law and *jus cogens*, the assessments made by scholars should be tested and verified against concrete State practice and *opinio juris*. The ILC has not included any norm of space law in its future study of *jus cogens* –there should be a thorough analysis of the criteria that such UN body of experts takes into consideration for including *jus cogens* 'candidates' on its agenda (see chapter 3, section 3.8.2, parts b) and c)).

**i) Space debris mitigation, supply chain and space cybersecurity**: A thorough analysis of the different instruments of space debris mitigation (including COPUOS Guidelines of 2007 and the LTS Guidelines) is required in order to determine if it would be appropriate to include specific guidelines on measures to protect space assets along the whole supply chain from vulnerabilities and make them more resilient. In addition, implementation guidance at a domestic level should further complete the research in that field (see chapter 4, section 4.3 and section 4.4.2).

**j) International security and 'mandates conflicts' in international organisations**: Another topic that might deserve some attention is whether the 'mandates conflict' in security matters is exclusive for the outer space field or if there are other examples within the United Nations or even in other international organisations that confirm the pattern. In such a case, the examination of other concrete solutions enabled by relevant rules of procedure and practice would enrich the present research and open up other avenues of study (see chapter 4, section 4.7.3 and chapter 5, section 5.6).

**k) Malicious space cyber activities and non-intervention:** Possible concrete scenarios in which the principle of non-intervention could be violated by malicious space cyber activities should be further explored and compared with iconic cases of unlawful intervention on Earth (see chapter 5, section 5.3).

**l) The role of soft law in the interpretation of fault and due regard in the Outer Space Treaty:** A part of the literature supported the role of soft law in the interpretation of binding instruments. Based on that premise, it would be of particular interest to further explain to which extent the 2007 Guidelines on Space Debris and the LTS Guidelines give content to the notion of fault under the liability regime, and how they shape the obligation of due regard enshrined in Article IX of the Outer Space Treaty (see chapter 5, section 5.4).

## 6.4. RECOMENDATIONS IN TERMS OF POLICY:

In any future regulatory endeavour on security in the use of ICTs, States should strike a balance between State security and human rights, in particular the exercise of the freedom of opinion and expression and the right to development and digital access for everybody (see chapter 2, section 2.3).

States should redouble their efforts to agree on the necessary threshold for the qualification of a use of force and when it becomes an armed attack in the cyber domain (see chapter 2, section 2.5). In particular, it is desirable to determine the need for an intentional and temporal requirement for a cyberattack. Agreement is imperative on how to deal with malicious cyber activities that cause economic damage and loss of functionality. Likewise, a clear stance is necessary regarding malicious cyber activities that target CNI. The determination of these aspects will shed some light on possible responses thereto, also in

cases where malicious cyber activities are conducted by non-State actors (see chapter 2, section 2.7)

States should further work to provide clear elements to give content to the due diligence obligation in the context of the use of ICTs. The literature is not conclusive regarding the applicability of the obligation to prevent malicious cyber activities and what it would imply (see chapter 2, section 2.6).

In future initiatives in the field of space cybersecurity, it is recommended that States refer back to the work conducted by UNGA First Committee and promote the liaison between UNGA First and Fourth Committees.

## ANNEX:

| | ICTs | TCBMs | NFP | PAROS | | | LTS | CoC |
|---|---|---|---|---|---|---|---|---|
| **ORIGIN** | 1998 | 1990/2005 | 2014 | 1981 | 2002 | 2017 | 2009 | 2007 |
| **FORUM** | UNGA FIRST COMMITTEE | UNGA FIRST COMMITTEE | UNGA FIRST COMMITTEE | UNGA FIRST COMMITTEE-CONFERENCE ON DISARMAMENT | | | UNGA FOURTH COMMITTEE-COPUOS | OUTSIDE THE UN |
| **INICIATOR** | RUSSIAN FEDERATION | RUSSIAN FEDERATION | RUSSIAN FEDERATION | ITALY | RUSSIAN FEDERATION+CHINA | | FRANCE | ITALY |
| **MECHANISM** | GGEs ON ICTs | GGEs ON (T)CBMs | - | - | - | GGE on PAROS | WG on LTS | INTERNATIONAL CONSULTATIONS |
| **OUTCOME** | REPORTS 2010 2013 2015 | REPORTS 1993 2013 | UNGA RES ON NFP | | DRAFT PPWT 2008 2014 | - | 21 GUIDELINES | DRAFT CoC 2008 2014 |
| **CURRENT STATUS** | GGE+OEWG | UNGA RES ON TCBMs | UNGA RES ON NFP | UNGA RES 75/36 (Responsible Behaviour) | | | NEW WG on LTS | - |

# EPILOGUE

## *The dialogue among Ada, Valentina and Eilene (cont.): Goodbye*

During the last three years, the friendship of Ada, Valentina and Eilene became stronger day by day. The idea of sharing their own expertise with each other created an atmosphere of exoticism, where the 'Queen of Computing' became the 'Princess of Negotiations', the 'Queen of Spaceflights' became the 'Princess of Binaries' and the 'Queen of the Multilateralism' became the 'Princess of Gravity Zero'. Their reign was a self-constructed fiction that aimed at deliberating on space cybersecurity and the future of space activities in a context were space safety, security and long-term sustainability of outer space activities would be warranted.

Valentina: *I would have never thought that flying into space would have ever had such an impact on what governments discuss at the UN...*

Ada: *You know...I had a similar feeling...I would have never thought that computer programmes would be under the spotlight of policy-makers...*

It turned out that after having spent three years together, these ladies had created a parallel reality, where they researched and wrote in the middle of a pandemic that changed the rules of our coexistence. Thus, they became used to working remotely at home, to wearing a mask and receiving daily reports on the lethality of a (biological) virus.

Ada: *I still recall that while everyone was complaining about staying at home, we had the chance to get to know each other closer and learn a lot from our XL reading sessions...*

Valentina: *While everyone was commenting about the 'new normality', we made our best of the absolute silence in the deepest concentration mode...*

Eilene: *While everyone was learning about the origin, mutations and vaccines against Covid-19, we were investigating about attribution, scenarios and potential policies to address (cyber) viruses affecting space activities...*

Valentina: *I recall reading in the newspapers about the 'vaccine race' with the Sputnik V while we were discussing the 'space race' and Sputnik 1...*

Eilene: *It's crazy...but while bipolarity is nowadays the history of the past, the present resembles the past in a different world...*

In effect, the world has changed but it did not stop revolving around the progress of science. Whatever the field might be, whatever the reality in which the reader might have been living, the truth is that in the most adverse context of humanity, in which policy-makers used to point at the 'invisible enemy', thousands of scientists and PhD students continued carrying out their research with libraries and universities closed and with travel bans everywhere.

Ada: *Oh, we have to be thankful for the Internet. I intend to be humble, but this time let me congratulate myself for having contributed to computing!*

Valentina: *Of course that was awesome...but allow me to share with you a part of the honours because thanks to the space race that my Soviet friends started in 1957, we can communicate with each other via satellite applications...*

Eilene: *Well...it's not all about science and technology here, girls...Of course ICTs and space systems are critical for our well-being, but bear in mind that universal access to digitalisation and satellite services is a victory of States coming together at the UN and gathering their efforts for the betterment of humankind...*

This thesis intends to be a contribution to scientific knowledge and a useful tool for policy-makers and 'space diplomats' to continue working to bring more stability and well-being to our world. I hope to have made one small step towards that goal.

# BIBLIOGRAPHY

## BOOKS:


AMOROSO, S., *Cyberattacks: Protecting National Infrastructure*, Burlington, 2011.

BIRNIE, P., BOYLE, A. AND REDGWELL, C., *International Law & the Environment*, Oxford, 2009.

BRAUSE, R., *Writing your Doctoral Dissertation: Invisible Rules for Success*, New York, 1999.(*)

BUCHANAN, B., *The Cybersecurity Dilemma. Hacking, Trust, and Fear between Nations*, Oxford, 2016.

CRAWFORD, J., *The International Law Commission's Articles on State Responsibility: Introduction, Text, and Commentaries*, Cambridge, 2002.

DIEDERIKS-VERSCHOOR, I. AND KOPAL, V., *An Introduction to Space Law*, Alphen aan den Rijn, 2008.

DINSTEIN, Y., *War, Aggression and Self-Defence,* Cambridge, 2005.

DÖRR, O. AND SCHMALENBACH, K. (eds), *Vienna Convention on the Law of the Treaties. A Commentary*, Berlin-Heidelberg, 2012.

DUNLEAVY, P., *Authoring a PhD. How to Draft, Plan, Write and Finish a Doctoral Thesis or Dissertation*, New York, 2003.

ECO, U., *Come si fa una Tesi di Laurea*, Milano, 2001.(*)

ESSINGER, J., *Ada's Algorithm: How Lord Byron's Daughter Ada Lovelace Launched the Digital Age,* Brooklyn, 2014.(*)

EVANS, D., GRUBA, P. AND ZOBEL, J., *How to Write a Better Thesis*, Melbourne, 2014.

GARNER, B. (ed), *Black's Law Dictionary*, St. Paul, 2009.

GEORGESCU, A., GHEORGHE, A., PISO, M. AND KATINA, P., *Critical Space Infrastructures. Risk, Resiliency and Complexity*, Cham, 2019.

JIMENEZ DE ARECHAGA, E., *International Law in the Past Third of a Century*, Recueil des Cours, Alphen aan den Rijn, 1978.

JOHNSON-FREESE, J., *Space Warfare in the 21st Century*, London-New York, 2017.

LYALL, F. AND LARSEN, P., *Space Law. A Treatise*, Farnham-Furlington, 2009.

MARCHISIO, S. AND MONTUORO, U. (eds), *Lo spazio cyber e cosmico. Risorse dual use per il sistema Italia in Europa*, Torino, 2019.(*)

MEADOWS, D.&D., RANDERS, J. AND BEHRENS, W., *Limits to Growth*, New York, 1972.

MURRAY, R., *How to Write a Thesis*, Berkshire, 2011.(*)

OAKLEY, J., *Cybersecurity for Space: Protecting the Final Frontier*, Alabama, 2020.

OSTROM, E., *Governing the Commons: The Evolution of Institutions for Collective Action (Political Economy of Institutions and Decisions),* Cambridge, 1990.

PALTRIDGE, B. AND STARFIELD, S., *Thesis and Dissertation Writing in a Second Language: A Handbook for Supervisors*, New York, 2007.(*)

PETERSON, M., *The UN General Assembly* (Global Institutions Series), London-New York, 2006.

PHILLIPS, E. AND PUGH, D., *How to get a PhD. A Handbook for Students and their Supervisors*, Maidenhead, 2010.

ROSCINI, M., *Cyber Operations and the Use of Force in International Law,* Oxford, 2014.

RUYS, T., '*Armed attack' and Article 51 of the UN Chater. Evolution in Customary Law and Practice*, New York, 2010.

SCHMITT, M. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge, 2017 ('Tallinn Manual 2.0').

SCHMITT, M. (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare,* New York, 2013.

SHARP, W., *Cyberspace and the Use of Force*, Virginia, 1999.

SHAW, M., *International Law,* Cambridge, 2015.

SIMMA, B., *The Charter of the United Nations. A Commentary*, Oxford, 2012.

STAMP, M., *Information Security: Principles and Practice*, New Jersey, 2011.

TERESHKOVA, V.*, The First Lady of Space. In her Own Words,* 2015.

TRONCHETTI, F., *Fundamentals of Space Law and Policy*, Harbin, 2013.

VIIKARI, L., *The Environmental Element in Space Law. Assessing the Present and Charting the Future*, Leiden-Boston, 2008.

VON CLAUSEWITZ, C., *On War*, New York, 2007.

ZHUKOV, G. AND KOLOSOV, Y., *International Space Law*, Moscow, 2014 (translated by Boris Belitzky).

**CHAPTERS IN COLLECTIVE WORKS:**

AOKI, S., *Law and Military Uses of Outer Space*, in JAKHU, R. AND DEMPSEY, P. (eds), *Routledge Handbook of Space Law*, London-New York, 2017, pp. 197-224.

BANDYOPADHYAY, R., *Qualitative Research and Its Application in Organizational Management and Social Research*, in HEDGE, D. (ed.), *Essays on Research Methodology*, New Delhi, 2015.(*)

BARDIN, J., *Satellite Cyberattack Search and Destroy*, in VACCA, J. (ed.), *Computer and Information Security,* Cambridge, 2017, pp. 1173-1181.

BATSANOV, S., *The Outer Space Treaty: Then and Now*, in POWERS, J. (ed.), *Celebrating the Space Age*, UNIDIR Conference Report, Geneva, 2-7 April 2007, pp. 51-56.

BOHLMAN, U., *Space 4.0*, in FERRETTI, S. (ed.), *Space Capacity Building in the XXI Century*, Vienna, 2020, 33-38.

BRÜNNER, C. AND KÖNIGSBERGER, G., *'Regulatory Impact Assessment' — A Tool to Strengthen Soft Law Regulations*, in MARBOE, I. (ed.), S*oft Law in Outer Space: The Function of Non-Binding Norms in International Space Law*, Vienna, 2012, pp. 87-97.

CHENG, B., *The 1967 Space Treaty*, Oxford, 1997, in CHENG, B., *Studies in International Space Law*, Oxford, 1997.Oxford Scholarship Online Version: March 2012.

CHENG, B., *The Extraterrestrial Application of International Law,* in CHENG, B., *Studies in International Space Law*, Oxford, 1997. Oxford Scholarship Online Version: March 2012.

CHENG, B., *The United Nations and Outer Spac*e, in CHENG, B., *Studies in International Space Law*, Oxford, 1997. Oxford Scholarship Online Version: March 2012.

CHENG, B., *The United Nations and the Development of International Law Relating to Outer Space,* in CHENG, B., *Studies in International Space Law*, Oxford, 1997. Oxford Scholarship Online Version: March 2012.

CHENG, B., *United Nations Resolutions on Outer Space: 'Instant' International Customary Law?*, in CHENG, B., *Studies in International Space Law*, Oxford, 1997. Oxford Scholarship Online Version: March 2012.

DICKOW, M., *The European Union Proposal for a Code of Conduct for Outer Space Activities*, in ESPI (ed.), *Yearbook on Space Policy 2007/2008*, Vienna-New York, 2009, pp. 152-163.

ESCOLAR, G. AND REYNDERS, M., *Historical Background and Context* (NPS Principles), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. III), Cologne, 2015, pp. 196-202.

FREELAND, S. AND JAKHU, R., *Article II* (Outer Space Treaty), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. I), Cologne, 2009, pp. 44-63.

FREELAND, S., *The Laws of War in Outer Space*, in SCHROGL, K-U., HAYS, P., ROBINSON J., MOURA, D. AND GIANNOPAPA, C. (eds), *Handbook of Space Security. Policies, Applications and Programs*, New York, 2015, pp. 81-112.

FREELAND, S., *The Role of 'Soft Law' in Public International Law and its Relevance to the International Legal Regulation of Outer Space, in* MARBOE, I. (ed.), *Soft Law in Outer Space: The Function of non-binding Norms in International Space Law,* Vienna, 2012, pp. 9-30.

FROEHLICH, A., *The Right to (Anticipatory) Self-Defence in Outer Space to Reduce Space Debris*, in FROEHLICH, A. (ed.) *Space Security and Legal Aspects of Active Debris Removal*, Cham, 2019, pp. 71-92.

GERHARD, M., *Article VI* (Outer Space Treaty), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. I), Cologne, 2009, pp. 103-125.

GRAY, C., *The Use of Force and the International Legal Order*, in EVANS, M. (ed.), *International Law*, Oxford, 2003, pp. 589-622.

HAYS, P., *Developing Agile and Adaptive Space Transparency and Confidence-Building Measures*, in ROBINSON, J., SCHAEFER, M., SCHROGL, K-U., VON DER DUNK, F. (eds), *Prospects for Transparency and Confidence-Building Measures in Space*, ESPI Report No. 27, Vienna, 2010, pp. 30-35.

HEGDE, D. AND HARI, L., *Writing a Doctoral Dissertation, in Hedge, D., Essays on Research Methodology*, New Delhi, 2015.(*)

HESSE, M. AND HORNUNG, M., *Space as a Critical Infrastructure*, in SCHROGL, K-U., HAYS, P., ROBINSON, J., MOURA, D. AND GIANNOPAPA, C. (eds), *Handbook of Space Security. Policies, Applications and Programs*, New York, 2015, pp. 187-202.

HOBE, S. AND CHEN, K-W., *Legal Status of Outer Space and Celestial Bodies*, in JAKHU, R. AND DEMPSEY, P. (eds), *Routledge Handbook of Space Law*, London-New York, 2017, pp. 25-41.

HOBE, S. AND TRONCHETTI, F., *Future Perspectives* (SB Declaration), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law*, (Vol. III), Cologne, 2015, pp. 355-357.

HOBE, S. AND TRONCHETTI, F., *Historical Background and Context* (SB Declaration), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. III), Cologne, 2015, pp. 306-318.

HOBE, S., *Article I* (Outer Space Treaty), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. I), Cologne, 2009, pp. 25-43.

HOBE, S., *Space Law- an Analysis of its Development and its Future*, in BRÜNNER, C. AND SOUCEK, A. (eds), *Outer Space in Society, Politics and Law*, Vienna-New York, 2011, p. 476-490.

JAKHU, R., *Evolution of the Outer Space Treaty*, in LELE, A. (ed.), *50 years of the Outer Space Treaty. Tracing the Journey, Institute for Defense Studies & Analyses*, New Delhi, 2017, pp. 13-19.

JAKHU, R., *Iridium-Cosmos Collision and its Implications for Space Operations*, in SCHROGL, K-U., RATHGEBER, W., BARANES, B. AND VENET, C. (eds), *Yearbook on Space Policy 2008/2009*, Vienna-New York, 2010, pp. 254-299.

JAKHU, R., *The future of the Outer Space Treaty*, in LELE, A., *50 years of the Outer Space Treaty. Tracing the Journey, Institute for Defense Studies & Analyses,* New Delhi, 2017, pp. 185-200.

JANKOWITSCH, P., *The Background and History of Space Law*, in VON DER DUNK, F. (ed.), *Handbook of Space Law*, Cheltenham-Northampton, 2015, pp. 1-28.

JU'NAN, Z., *Fundamental Ways to Ensure Outer Space Security: Negotiating and Concluding a Legally Binding International Instrument*, in POWERS, J. (ed.), Celebrating the Space Age, UNIDIR Conference Report, Geneva, 2-7 April 2007, pp. 109-111.

KERREST, A. AND SMITH, J., *Article VII* (Outer Space Treaty), in HOBE S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. I), Cologne, 2009, pp. 126-145.

KERREST, A., *Space Law and the Law of the Sea*, in BRÜNNER, C. AND SOUCEK, A. (eds), *Outer Space in Society*, *Politics and Law*, Vienna-New York, 2011, pp. 247-256.

KOPAL, V. AND HOFMANN, M., *Vladimir Mandl,* in HOBE, S. (ed.), *Pioneers of Space Law*, Leiden-Boston, 2013, pp. 57-70.

KOPAL, V., *Origins of Space Law and the Role of the United Nations*, in BRÜNNER, C. AND SOUCEK, A. (eds), *Outer Space in Society, Politics and Law*, Vienna-New York, 2011, pp. 221-233.

KREPON, M., *A Code of Conduct for Responsible Space-Faring Nations*, in POWERS, J. (ed.), *Celebrating the Space Age*, UNIDIR Conference Report, Geneva, 2-7 April 2007, pp. 165-173.

LALÁ, P., *Study on Space Traffic Management by the International Academy of Astronautics,* in POWERS, J. (ed.), *Celebrating the Space Age*, UNIDIR Conference Report, Geneva, 2-7 April 2007, pp. 179-187.

MARBOE, I., NEUMANN, J. AND SCHROGL, K-U, *Historical Background and Context* (Rescue Agreement), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. II), Cologne, 2013, pp. 9-30.

MARCHISIO, S., *Article IX* (Outer Space Treaty), in HOBE, S., SCHMIDT-TED B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. I), Cologne, 2009, pp. 169-182.

MARTINEZ, P., *Space Sustainability*, in SCHROGL, K-U., HAYS, P., ROBINSON, J., MOURA, D. AND GIANNOPAPA, C. (eds), *Handbook of Space Security. Policies, Applications and Programs*, New York, 2015, pp. 257-272.

MARTINEZ, P., *Space Sustainability*, in SCHROGL, K-U., HAYS, P., ROBINSON J., MOURA, D. AND GIANNOPAPA, C. (eds), *Handbook of Space Security. Policies, Applications and Programs*, New York, 2020, pp. 1-22.

MAYENCE, J., *Space Security: Transatlantic Approach to Space Governance*, in ROBINSON, J., SCHAEFER, M., SCHROGL, K-U., VON DER DUNK, F. (eds), *Prospects for Transparency and Confidence-Building Measures in Spac*e, ESPI Report No. 27, Vienna, 2010, pp. 35-36.

MEJÍA-KAISER, M., *Space Law and Unauthorised Cyber Activities*, in ZIOLKOWSKI, K., (ed), *Peacetime regime for State Activities in Cyberspace*, NATO CCD COE, 2013, pp. 349-372.

MEYER, P., *Outer Space and Cyberspace: a Tale of Two Security Realms*, in OSULA, A. AND RÕIGAS, H. (eds), *International Cyber Norms*, Tallinn, 2016, pp. 155-169.

MUTSCHLER, M., *Security Cooperation in Space and International Relations*, in SCHROGL, K-U., HAYS, P., ROBINSON J., MOURA, D. AND GIANNOPAPA, C. (eds), *Handbook of Space Security. Policies, Applications and Programs*, New York, 2015, pp. 41-56.

NEGER, T. AND WALTER, E., *Space Law- an Independent Branch of the Legal System*, in BRÜNNER, C. AND SOUCEK, A. (eds), *Outer Space in Society, Politics and Law*, Vienna-New York, 2011, pp. 234-245.

PAIKOWSKY, D., BEN-ISRAEL, I. AND AZOULAY, T., *Israeli Perspective on Space Security*, in SCHROGL, K-U., HAYS, P., ROBINSON J., MOURA, D. AND GIANNOPAPA, C. (eds), *Handbook of Space Security. Policies, Applications and Programs*, New York, 2015, pp. 493-505.

PAKHARENKO, G., *Cyber Operations at Maidan: A First-Hand Account*, in GEERS, K. (ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, Tallinn, 2015, pp. 59-66.

PALIHAKKARA, H., *Space Security: Perspectives of Developing Countries*, in POWERS, J. (ed.), *Celebrating the Space Age*, UNIDIR Conference Report, Geneva, 2-7 April 2007, pp. 83-87.

PASCO, X., *Controlling the Freedom of Using Space: the White House Space Policy dilemma,* in SCHROGL, K.-U., MATHIEU, C. AND PETER, N. (eds), *Yearbook on Space Policy 2006/2007*, Vienna-New York, 2008, pp. 197-210.

PECUJLIC, A., *European Space Policy Institute's Comprehensive Analysis on Adopting New Binding International Norms Regarding Space Activities,* in VENCATA RAO, R., GOPALKRISHNAN, V.

AND ABHIJEET, K. (eds), *Recent Developments in Space Law. Opportunities & Challenges*, Bengaluru, 2017, pp. 141-154.

PYNNÖNIEMI, K., *The Evolution of Russian Policy on Critical Infrastructure Protection,* in PYNNÖNIEM, K., (ed.), *Russian Critical Infrastructures. Vulnerabilities and Policies*, Helsinki, 2012, pp. 31-53.

RAJESWARI PILLAI RAJAGOPALAN, *Beyond Outer Space Treaty – Time for New Mechanisms?*, in LELE, A. (ed.), *50 years of the Outer Space Treaty. Tracing the Journey*, New Delhi, 2017, pp. 172-184.

REMUS, N., *Space and Security*, in BRÜNNER, C. AND SOUCEK, A. (eds), *Outer Space in Society, Politics and Law*, Vienna, 2011, pp. 519-568.

RIBBELINK, O., *Article III* (Outer Space Treaty), in HOBE S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. I), Cologne, 2009, pp. 64-69.

ROBINSON, J., *SpaceTransparency and Confidence-Building Measures,* in SCHROGL, K-U., HAYS, P., ROBINSON, J., MOURA, D. AND GIANNOPAPA, C. (eds), *Handbook of Space Security. Policies, Applications and Programs*, New York, 2015, pp. 291-297.

ROBINSON, J., *The Status and Future Evolution of Transparency and Confidence-Building Measures,* in ROBINSON, J., SCHAEFER, M., SCHROGL, K-U., VON DER DUNK, F. (eds), *Prospects for Transparency and Confidence-Building Measures in Space*, ESPI Report No. 27, Vienna, 2010, pp. 5-8.

SACHDEVA, G., *Outer Space Treaty: An Appraisal*, in LELE, A., *50 years of the Outer Space Treaty. Tracing the Journey,* Institute for Defense Studies & Analyses, New Delhi, 2017, pp. 24-47.

SACHDEVA, G., *Select Tenets of Space Law as Jus Cogens*, in RAO, V., GOPALKRISHAN, V AND ABHIJEET, K. (eds), *Recent Developments in Space Law. Opportunities & Challenges*, Bengaluru, 2017, pp. 7-26.

SADEH, E., *Evolution of Policy and Law for International Space Governance*, in LELE, A. (ed.), *50 years of the Outer Space Treaty. Tracing the Journey*, New Delhi, 2017, pp. 153-171.

SCHMIDT, Y., *International Space Law and Developing Countries*, in BRÜNNER, C. AND SOUCEK, A. (eds), *Outer Space in Society, Politics and Law*, Vienna-New York, 2011, pp. 690-725.

SCHMIDT-TEDD, B. AND MICK, S., *Article VIII* (Outer Space Treaty), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U.(eds), *Cologne Commentary on Space Law* (Vol. I), Cologne, 2009, pp. 146-168.

SCHMIDT-TEDD, B., MALYSHEVA, N., STELMAKH, O., TENNEN, L. AND BOHLMANN, U., *Article II* (Registration Convention), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U.(eds), *Cologne Commentary on Space Law* (Vol. II), Cologne, 2013, pp. 249-297.

SCHMITT, M., *International Law and Military Operations in Space*, in BONGDANDY, A. AND WOLFRUM, R. (eds), *Max Planck Yearbook of United Nations Law*, Vol. 10, 2006, pp. 89-125.

SCHROGL, K-U. AND NEUMANN, J., *Article IV* (Outer Space Treaty), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. I), Cologne, 2009, pp. 70-93.

SEGURA-SERRANO, A., *Internet Regulation and the Role of International Law',* in BONGDANDY, A. AND WOFLRUM, R. (eds), *Max Planck Yearbook of United Nations Law*, Vol. 10, Leiden-Boston, 2006, pp. 191-272.

SHEEHAN, M., *Defining Space Security*, in SCHROGL, K-U., HAYS, P., ROBINSON, J., MOURA, D. AND GIANNOPAPA, C. (eds), *Handbook of Space Security. Policies, Applications and Programs*, New York, 2015, pp. 7-21.

SMITH, J. AND KERREST, A., *Article I* (Liability Convention), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), Cologne Commentary on Space Law (Vol. II), Cologne, 2013, pp. 104-115.

SMITH, J. AND KERREST, A., *Article II* (Liability Convention), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), Cologne Commentary on Space Law (Vol. II), Cologne, 2013, pp. 116-130.

SMITH, J. AND KERREST, A., *Article XVIII* (Liability Convention), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), Cologne Commentary on Space Law (Vol. II), Cologne, 2013, pp. 190-193.

SOUCEK, A., *International Law*, in BRÜNNER, C. AND SOUCEK, A. (eds), *Outer Space in Society, Politics and Law*, Vienna-New York, 2011, pp. 294-405.

SOUCEK, A., *Negotiation and Drafting History* (SDM Guidelines), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. III), 2015, pp. 612-616.

STEER, C., *Sources and Law-Making Processes Relating to Space Activities*, in JAKHU, R. AND DEMPSEY, P. (eds), *Routledge Handbook of Space Law*, London-New York, 2017, pp. 3-24.

STUBBE, P., *Historical Background and Context* (DBS Principles), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. III), Cologne, 2015, pp. 6-19.

STUBBE, P. AND SCHROGL, K-U., *The Legal Significance of the COPUOS SDM Guidelines* (SDM Guidelines), in HOBE, S., SCHMIDT-TEDD, B. AND SCHROGL, K-U. (eds), *Cologne Commentary on Space Law* (Vol. III), 2015, pp. 643-648.

SU, J., *Control over Activities Harmful to the Environment*, in JAKHU, R. AND DEMPSEY, P. (eds), *Routledge Handbook of Space Law*, London - New York, 2017, pp. 73-89.

TRONCHETTI, F., *Legal Aspects of The Military Uses of Outer Space*, in VON DER DUNK, F. (ed.), *Handbook of Space Law*, Cheltenham-Northampton, 2015, pp. 331-381.

TRONCHETTI, F., *Soft Law*, in BRÜNNER, C. AND SOUCEK, A. (eds), *Outer Space in Society, Politics and Law*, Vienna-New York, 2011, pp. 619-637.

VASILIEV, A., *The Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force Against Outer Space Objects*, in POWERS, J. (ed.), *Celebrating the Space Age*, UNIDIR Conference Report, Geneva, 2-7 April 2007, pp. 113-117.

VENET, C., *The Political Dimension*, in BRÜNNER, C. AND SOUCEK, A. (eds), *Outer Space in Society, Politics and Law*, Vienna-New York, 2011, pp. 73-91.

VON DER DUNK, F., *International Space Law*, in VON DER DUNK, F. (ed.), *Handbook of Space Law*, Cheltenham-Northampton, 2015, pp. 29-126.

VON DER DUNK, F., *Legal Aspects of Satellite Communications*, in VON DER DUNK, F. (ed.), *Handbook of Space Law*, Cheltenham-Northampton, 2015, pp. 456-500.

WOLFF, J., *'Peaceful Uses' of Outer Space has permitted its Militarization—Does it also mean its Weaponization?*, in VIGNARD, K. (ed.), *Making Space for Security*, UNIDIR Disarmament Forum, 2003, pp. 1-13.

WRIGHT, D., *Orbital Debris Produced by Kinetic-Energy Anti-Satellite Weapons*, in POWERS, J. (ed.), *Celebrating the Space Age*, UNIDIR Conference Report, Geneva, 2-7 April 2007, pp. 155-164.

**ARTICLES**:

ABOU YEHIA, J., *Threats, Risks, and Sustainability—Answers from Space: Results of the ESPI Conference*, in '*Space Policy*', Vol. 24, 2008, pp. 113-115.

ALDRICH, R., *The International Legal Implications of Information Warfare*, in 'Airpower Journal', Vol. 10, No. 3, 1996, pp. 99-110.

ANTOLIN-JENKINS, V., *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places*, in 'Naval Law Review', Vol. 51, 2005, pp. 132-174.

AOKI, S., *Identifying the Scope of the Applicable International Law Rules towards Malicious Cyber Activities against Space Assets*, in Proceedings of the International Institute of Space Law 2018, The Hague, 2019, pp. 687-699.

BALLESTE, R., *Reconsidering Rules of Engagement in Outer Space*, in Proceedings of the International Institute of Space Law 2018, The Hague, 2019, pp. 727-734.

BARKHAM, J., *Information Warfare and International Law on the Use of Force,* in 'New York University Journal of International Law and Politics', Vol. 34, 2001, pp. 57-113.

BEARD, J., *Soft Law's Failure on the Horizon: The International Code of Conduct for Outer Space Activities,* in 'University of Pennsylvania Journal of International Law', Vol. 38, No. 2, 2016, pp. 335-424.

BLAKE, D. AND IMBURGIA, J., '*Bloodless Weapons'? The Need to Conduct Legal Review of Certain Capabilities and the Implications of Defining Them as 'Weapons'*, in 'Air Force Law Review', Vol. 66, 2010, pp. 157-203.

BLANK, L., *International Law and Cyber Threats from Non-State Actors*, in 'International Law Studies', Vol. 89, 2013, pp. 406-437.

BLOUNT, P. J., *Renovating Space: The Future of International Space Law*, in 'Denver Journal of International Law and Policy', Vol. 40, 2011, 515-532.

BLOUNT, P.J., *That Escalated Quickly: The Cyber-ASAT Conundrum*, in Proceedings of the International Institute of Space Law 2018, The Hague, 2019, pp. 701-707.

BLOUNT, P.J., *The Development of International Norms to Enhance Space Security Law in an Asymmetric World,* Proceedings of the 52nd Colloquium on the Law of Outer Space, 2010.

BOCKSTIEGEL, K-H., *ILA Draft Convention on Space Debris / ILA Konventions-Entwurf zu Weltraumtrummern / Un Projet de Convention de l'ILA sur les Debris Spatiaux*, in 'German Journal of Air and Space Law', Vol. 43, No. 4, 1994, pp. 395-400.

BOOTHBY, W., *Some Legal Challenges Posed by Remote Attack*, in 'International Review of the Red Cross', Vol. 94, 2012, pp. 579-595.

BOWMAN, M., *Is International Law Ready for the Information Age?*, in 'Fordham International Law Journal', Vol. 19, 1995, pp. 1935-1946.

BRACHET, G., *The origins of the Long-term Sustainability of Outer Space Activities*, in 'Space Policy', Vol. 28, 2012, pp. 161-165.

BRECCIA, P., *Article III of Outer Space Treaty and its Relevance in the International Space Legal Framework*, 67th International Astronautical Congress (IAC), Guadalajara, 26-30 September 2016.

BRENNER, S., *At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare*, in 'The Journal of Criminal Law and Criminology', Vol. 97, 2007, pp. 379-476.

BROWN, G. AND POELLET, K., *The Customary International Law of Cyberspace*?, in 'Strategic Studies Quarterly', Vol. 6, No. 3, 2012, pp. 126-145.

BROWN, G., *International Law applies to Cyber Warfare! Now, What*?, in 'Southwestern Law Review', Vol. 46, 2017, pp. 355-377.

BUCHAN, R., *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions*?, in 'Journal of Conflict and Security Law', Vol. 17, 2012, pp. 211-227.

BURKE, J., *Convention on International Liability for Damage Caused by Space Objects: Definition and Determination of Damages After the Cosmos 954 Incident*, in 'Fordham International Law Journal', Vol. 8, No. 2, 1984, pp. 255-285.

CEPELKA, C. AND GILMOUR, J., *The Application of General International Law in Outer Space*, in 'Journal of Air Law and Commerce', Vol. 36, No. 1, 1970, pp. 30-49.

CHENG, B., *Article VI of the 1967 Space Treaty Revisited: "International Responsibility", "National Activities", and "The Appropriate State"*, in 'Journal of Space Law', Vol. 26, No. 1, 1998.

CHENG, B., *United Nations Resolutions on Outer Space: "Instant" International Customary Law?',* in 'Indian Journal of International Law', Vol. 5, 1965, pp. 23-112.

CHENG, D., *China's Military Role in Space*, in 'Strategic Studies Quarterly', Vol. 6, No. 1, 2012, pp. 55-77.

CHOW, B., *Space Arms Control: A Hybrid Approach,* in 'Strategic Studies Quarterly', Vol. 12, No. 2, 2018, pp. 107-132.

CHOW, B., *Stalkers in Space: Defeating the Threat*, in 'Strategic Studies Quarterly', Vol. 11, No. 2, 2017, pp. 82-116.

CHRISTOL, C., *International Liability for Damage Caused by Space Objects,* in 'The American Journal of International Law', Vol. 74, No. 2, 1980, pp. 346-371.

CHRISTOL, C., *The Common Heritage of Mankind Provision in the 1979 Agreement Governing the Activities of States on the Moon and Other Celestial Bodies*, in 'The International Lawyer', Vol. 14, No. 3, 1980, pp. 429-483.

CLANCY, E., *The Tragedy of the Global Commons*, in 'Indiana Journal of Global Legal Studies', Vol. 5, No 2, 1998, pp. 601-619.

COCCA, A., *The Advances in International Law through the Law of Outer Space*, in 'Journal of Space Law', Vol. 9, 1981, pp. 13-20.

CONDRON, S., *Getting It Right: Protecting American Critical Infrastructure in Cyberspace*, in 'Harvard Journal of Law and Technology', Vol. 20, 2007, pp. 403-422.

COX, S., *Confronting Threats Through Unconventional Means: Offensive Information Warfare as Covert Alternative to Preemptive War,* in 'Houston Law Review', Vol. 42, 2005, pp. 881-909.

D'AMATO, A., *International Law, Cybernetics and Cyberspace*, in 'International Law Studies', Vol. 76, 2002, pp. 59-71.

DANILENKO, G., *International Law-Making for Outer Space*, in 'Space Policy', Vol. 37, 2016, pp. 179-183.

DE MAN, P., *State Practice, Domestic Legislation and the Interpretation of Fundamental Principles of International Space Law*, in 'Space Policy', 2017, pp. 1-11.

DEL MONTE, L., *Towards a Cybersecurity Policy for a Sustainable, Secure and Safe Space Environment*, Proceedings of the 64th International Astronautical Congress (IAC), 2013.

DELIBASIS, D., *State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century,* in 'Peace Conflict and Development: An Interdisciplinary Journal', Vol. 8, 2006, pp. 1-50.

DEMBLING, P., *Cosmos 954 and the Space Treaties*, in 'Journal of Space Law', Vol. 6, No. 2, 1978, pp. 129-136.

DENNING, D., *Stuxnet: What has Changed?*, in 'Future Internet', Vol. 2, 2012, pp. 672-687.

DINSTEIN, Y., *Computer Network Attacks and Self-Defense*, in 'International Law Studies', Vol. 76, 2002, pp. 99-119.

DINSTEIN, Y., *Cyber War and International Law: Concluding Remarks at the 2012 War Naval College International Law Conference*, in 'International Law Studies', Vol. 89, 2013, pp. 276-287.

FALCO, G., *Cybersecurity Principles for Space Systems*, in 'Journal or Aerospace Information Systems', 2018, pp. 1-10 (article in advance).

FARWELL, J. AND ROHOZINSKI, R., *Stuxnet and the Future of Cyber War*, in 'Survival', Vol. 53, No 1, 2011, pp. 23-40.

FIDLER, D., *Tinker, Tailor, Soldier, Duqu: Why Cyber espionage is More Dangerous Than You Think,* in 'International Journal of Critical Infrastructure Protection', Vol. 5, 2012, pp. 28-29.

FREELAND, S. AND PECUJLIC, A., *How do you like your Regulation – hard or soft? The Antarctic Treaty and the Outer Space Treaty compared*, in 'National Law School of India Review', Vol. 30, No. 1, 2018, pp. 11-36.

FREELAND, S., *A Natural System of Law - Andrew Haley and the International Legal Regulation of Outer Space*, in 'Journal of Space Law', Vol. 39, 2013, pp. 77-98.

FRITZ, J., *Satellite Hacking: a Guide for the Perplexed*, in 'Bulletin of the Centre for East-West Cultural and Economic Studies', Vol. 10, No. 1, December 2012- May 2013, pp. 21-50.

GALLOWAY, E., *Consensus Decisionmaking by the United Nations Committee on the Peaceful Uses of Outer Space,* in 'Journal of Space Law', Vol. 7, No 1, 1979, pp. 3-14.

GILL, P. AND DOLAN, G., *Originality and the PhD: What is it and How can it be Demonstrated?*, in 'Nurse Researcher', Vol. 22, No. 6, 2015, pp. pp. 11-15.(*)

GLENNON, M., *The Dark Future of International Cybersecurity Regulation*, in 'Journal Of National Security Law & Policy', Vol. 6, 2013, pp. 563-570.

GLENNON, M., *The Road Ahead: Gaps, Leaks and Drips',* in 'International Law Studies'*,* Vol. 89, 2013, pp. 362-386.

GOH, G., *Keeping the Peace in Outer Space: a Legal Framework for the Prohibition of the Use of Force*, in 'Space Policy', Vol. 20, 2004, pp. 259-278.

GOROVE, S., *Cosmos 954: Issues of Law and Policy*, in 'Journal of Space Law', Vol. 6, 1978, pp. 137-146.

GRAHAM, D., *Cyber Threats and the Law of War*, in 'Journal of National Security Law and Policy', Vol. 4, 2010, pp. 87-102.

GRIMAL, F. AND SUNDARAM, J., *Cyber-Warfare and Autonomous Self-Defense*, in 'Journal on the Use of Force and International Law'*,* 2017, pp. 1-26.

GRIMAL, F. AND SUNDARAM, J., *The Incremental Militarization of Outer Space: A Threshold Analysis*, in 'Chinese Journal of International Law', Vol. 17, 2018, pp. 45-72.

GROVER, K., *Jamming and Anti-jamming Techniques in Wireless Networks: A Survey,* in 'International Journal of Ad Hoc and Ubiquitous Computing', Vol. 17, No. 4, 2014, pp. 1-16.

HARDIN, G., *The Tragedy of the Commons*, in 'Science', Vol. 162, No. 3859, 1968, pp. 1243-1248.

HATHAWAY, O., *The Law of Cyber-attack*, in 'California Law Review'*,* Vol. 100, 2012, pp. 817-886.

HERZ, J., *Idealist Internationalism and the Security Dilemma*, in 'World Politics', Vol. 2, No. 2, 1950, pp. 157-180.

HINKLE, K., *Countermeasures in the Cyber Context: One More Thing to Worry About*, in 'Yale Journal of International Law Online*',* Fall 2011, pp. 11-21.

HOBE, S., *Environmental Protection in Outer Space: Where We Stand and What is Needed to Make Progress with Regard to the Problem of Space Debris*, in 'The Indian Journal of Law and Technology', Vol. 8, 2012, pp. 1-10.

HOBE, S., *The Impact of New Developments on International Space Law (New Actors, Commercialisation, Privatisation, Increase in the Number of "Space-Faring Nations")*, in 'Uniform Law Review', Vol. 15, 2010, pp. 869-882.

HOISINGTON, M., *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense,* in 'Boston College International and Comparative Law Review', Vol. 32, 2009, 439-454.

HOLLIS, D., *Cyberwar Case Study: Georgia 2008*, in 'Small Wars Journal', 2011, pp. 1-10.

HOLLIS, D., *Why States Need an International Law for Information Operations*, in 'Lewis and Clark Law Review', Vol. 11, 2007, pp. 1023-1061.

HOUSEN-COURIEL, D., *Cybersecurity Threats to Satellite Communications: Towards a Typology of State Actor Responses*, in 'Acta Astronautica', Vol. 128, 2016, pp. 409-415.

HURWITZ, R., *Depleted Trust in the Cyber Commons*, in 'Strategic Studies Quarterly', Vol. 6, No. 3, 2012, pp. 20-45.

INTOCCIA, G. AND MOORE, J., *Communications Technology, Warfare, and the Law: Is the Network a Weapon System?*, in 'Houston Journal of International Law', Vol. 28, 2006, pp. 467-489.

JAKHU, R., *Legal Issues relating to the Global Public Interest in Outer Space*, in 'Journal of Space Law', Vol. 32, No. 1, 2006, pp. 31-110.

JASENTULIYANA, J., *Ensuring Equal Access to the Benefits of Space Technologies for all Countries*, in 'Space Policy', Vol. 10, No. 1, 1994, pp. 7-18.

JASENTULIYANA, N., *Consideration of Space Activities by the UN General Assembly,* in 'Space Policy', May 1985, pp. 218-219.

JASENTULIYANA, N., *The UN Space Treaties and the Common Heritage Principle*, in 'Space Policy', 1986, pp. 296-301.

JENSEN, E., *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense,* in 'Stanford Journal of International Law', Vol. 38, 2002, pp. 207-240.

JOHNSON, P., *Is It Time for a Treaty on Information Warfare?*, in 'International Law Studies', Vol. 76, 2002, pp. 439-455.

JOHNSON-FREESE, J., *A Space Force Mission for the Global Commons of Space*, in 'SAIS Review of International Affairs', Vol. 36, No. 2, Summer-Fall 2016, pp. 5-13.

JOYNER, C. AND LOTRIONTE, C., *Information Warfare as International Coercion: Elements of a Legal Framework*, in 'European Journal of International Law', Vol. 12, 2001, pp. 825-865.

KAISER, S., *In Search of an International Public Order for Cyber Activities*, in Proceedings of the International Institute of Space Law 2018, The Hague, 2019, pp. 671-685.

KALLBERG, J., *Designer Satellite Collisions from Covert Cyber War*, in 'Strategic Studies Quarterly', Vol. 6, No. 1, 2012, pp. 124-136.

KALLENDER, P., *Waking Up to a New Threat: Cyber Threats and Space*, in 'Trans. JSASS Aerospace Tech. Japan', Vol. 12, 2014, pp. 1-10.

KANUCK, S., *Sovereign Discourse on Cyber Conflict Under International Law,* in 'Texas Law Review', Vol. 88, 2010, pp. 1571-1597.

KESAN, J. AND HAYES, C., *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, in 'Harvard Journal of Law and Technology', Vol. 25, 2012, pp. 429-543.

KESSLER, D. AND COUR-PALAIS, B., *Collision Frequency of Artificial Satellites: The Creation of a Debris Belt*, in 'Journal of Geophysical Research', Vol. 83, No A6, 1978, pp. 2637-2646.

KOH, H., *International Law in Cyberspace*, in 'Harvard International Law Journal', Vol. 54, 2012, pp. 1-12.

KOPAL, V., *International Legal Regime on Outer Space: Outer Space Treaty, Rescue Agreement and the Moon Agreement,* in Proceedings of United Nations/Nigeria Workshop on Space Law, Vienna, 2006.

KUEHL, D., *Information Operations, Information warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age*, in 'International Law Studies', Vol. 76, 2002, pp. 35-58.

LACHS, M., *Some Reflections on the State of the Law of Outer Space*, in 'Journal of Space Law', Vol. 9, No. 1&2, 1981, pp. 3-12.

LEE, R., *The Jus ad Bellum in Outer Space: The Interrelation between Article 103 of the Charter of the United Nations and Article IV of the Outer Space Treaty*, in 'Proc. on L. Outer Space', Vol. 45, 2002, pp. 139-148.

LENTZ, C., *A State's Duty to Prevent and Respond to Cyberterrorist Acts,* in 'Chicago Journal of International Law', Vol. 10, 2010, pp. 799-823.

LIANG, Y., *Methods and Procedures of the General Assembly for Dealing with Legal and Drafting Questions*, in 'The American Journal of International Law', Vol. 47, No. 1, 1953, pp. 70-83.

LIN, H., *Offensive Cyber Operations and the Use of Force*, in 'Journal of National Security Law and Policy', Vol. 4, 2010, pp. 63-86.

LIU, H. AND TRONCHETTI, F., *United Nations Resolution 69/32 on the "No First Placement of Weapons in Space": A Step Forward in the Prevention of an Arms Race in Outer Space'*, in 'Space Policy', 2016, pp. 1-4.

MANULIS, M., BRIDGES, C.P., HARRISON, R., SEKAR, V. AND DAVIS, A., *Cyber Security in New Space*, in 'International Journal of Information Security', 2020.

MAOGOTO, J. AND FREELAND, S., *Space Weaponization and the United Nations Charter Regime on Force: A Thick Legal Fog or a Receding Mist?*, in 'The International Lawyer', Vol. 41, No. 4, 2007, pp. 1091-1119.

MARCHISIO, S., *International Legal Regime on Outer Space: Liability Convention and Registration Convention*, in Proceedings of United Nations/Nigeria Workshop on Space Law, Vienna, 2006.

MARCHISIO, S., *Security in Space: Issues at Stake*, in 'Space Policy', 2015, pp. 67-69.

MARCHISIO, S., *The Evolutionary Stages of the Legal Subcommittee of the United Nations Committee on the Peaceful Uses of Outer Space (COPUOS*), in 'Journal of Space Law', Vol. 31, 2005, pp. 219-242.

MARKOV, M., *Against the So-Called 'Broader' Interpretation of the Term 'Peaceful' in International Space Law*, in Proceedings of the Eleventh Colloquium on the Law of Outer Space, 1968.

MARTINEZ, M., *Challenges for Ensuring the Security, Safety and Sustainability of Outer Space Activities,* in 'Journal of Space Safety Engineering', Vol. 6, No. 2, 2019, pp. 1-4.

MARTINEZ, P., CROWTHER, R., MARCHISIO, S. AND BRACHET, G., *Criteria for Developing and Testing Transparency and Confidence-Building Measures (TCBMs) for Outer Space Activities',* in 'Space Policy', 2014, pp. 1-7.

MARTINEZ, P., *Development of an International Compendium of Guidelines for the Long-Term Sustainability of Outer Space Activities'*, in 'Space Policy', Vol. 43, 2018, pp. 13-17.

MATTE, N., *Environmental Implications and Responsibilities in the Use of Outer Space*, in 'Annals Air & Space L.', Vol. 14, 1989, pp. 419-448.

MENDES DE LEON, P. AND VAN TRAA, H., *The Practice of Shared Responsibility and Liability in Space Law*, SHARES Research Paper 70 (2015), pp. 1-25.

MILLER, G., *Space Pirates, Geosynchronous Guerrillas, and Nonterrestrial Terrorists. Nonstate Threats in Space*, in 'Air & Space Power Journal', Fall 2019, pp. 33-51.

MORTH, T., *Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter',* in 'Case Western Reserve Journal of International Law', Vol. 30, 1998, pp. 567-600.

MOUNTIN, S., *The Legality and Implications of Intentional Interference with Commercial Communication Satellite Signals*, in 'International Law Studies', Vol. 90, 2014, pp. 100-197.

MUIR, L., *The Case Against an International Cyber Warfare Convention,* in 'Wake Forest Law Review Online', Vol. 5, 2011, pp.1-10.

MUREŞAN, L. and GEORGESCU, A., *The Road to Resilience in 2050,* in 'The RUSI Journal', 2015,pp. 58-66.

NEWMAN, C. AND WILLIAMSON, M., *Space Sustainability: Reframing the Debate*, in 'Space Policy', Vol. 46, 2018, pp. 30-37.

PETRAS, C., *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 'Journal of Air Law and Commerce', Vol. 67, No. 4, 2002, pp. 1213-1268.

PETROVICI, G. AND CARLO, A., *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 Proceedings of the International Institute of Space Law 2018, The Hague, 2019, pp. 71-87.

POPOVA, R. and SCHAUS, V., *The Legal Framework for Space Debris Remediation as a Tool for Sustainability in Outer Space*, in 'Aerospace', Vol. 5, 2018, pp. 1-17.

POPOVA, R., *Cyber Law and Outer Space (Activities): Legal and Regulatory Challenges*, in Proceedings of the International Institute of Space Law 2018, The Hague, 2019, pp. 659-670.

PORRAS, D., *The "Common Heritage" of Outer Space: Equal Benefits For Most of Mankind,* in 'California Western International Law Journal', Vol. 37, No. 1, 2006, pp. 143-176.

PURSIAINEN, C., *Russia's Critical Infrastructure Policy: What do we Know about it*?, in 'European Journal for Security Research', Vol. 6, 2020, pp. 21-38.

PRASAD, D., *Relevance of the Sustainable Development Concept for International Space Law: An Analysis*, in 'Space Policy', Vol. 47, 2019, pp. 166-174.

RABOIN, B., *Corresponding Evolution: International Law and the Emergence of Cyber Warfare,* in 'Journal of the National Association of Administrative Law Judiciary', Vol. 31, No 2, 2011, pp. 602-668.

RAJESWARI PILLAI RAJAGOPALAN, *The Space Code of Conduct Debate. A View from Delhi*, in 'Strategic Studies Quarterly', 2012, pp. 137-148.

RATHGEBER, W., REMUSS, N. AND SCHROGL, K-U., *Space Security and the European Code of Conduct for Outer Space Activities*, in 'Disarmament Forum', Vol. 4, 2009, pp. 33-41.

RATHORE, E. AND GUPTA, B., *Emergence of Jus Cogens Principles in Outer Space Law*, in 'Astropolitics', Vol. 18, No. 1, 2020, pp. 1-21.

ROBBAT, M., *Resolving the Legal Issues Concerning the Use of Information Warfare in the International Forum: The Reach of the Existing Legal Framework, and the Creation of a New Paradigm*, in 'Journal of Science & Technology Law', Vol. 6, 2000.

ROSCINI, M., *World Wide Warfare: Jus ad Bellum and the Use of Cyber Force*, in '*Max Planck Yearbook of United Nations Law',* Vol. 14, 2010, pp. 85-130.

SCHACHTER, O., *The Twilight Existence of Non-Binding International Agreements*, in 'The American Journal of International Law, Vol. 71, 1977, pp. 36-39.

SCHMITT, M. AND VIHUL, L., *Proxy Wars in Cyberspace: the Evolving International Law of Attribution*, in 'Fletcher Security Review', Vol. 1, No 2, 2014, pp. 55-73.

SCHMITT, M. AND WATTS, S., *Beyond State-Centrism: International Law and Non-State Actors in Cyberspace*, in 'Journal of Conflict & Security Law', 2016, pp. 1-17.

SCHMITT, M., *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, in 'Columbia Journal of Transnational Law', Vol. 37, 1999, pp. 885-937.

SCHMITT, M., *Cyber Operations and the Jus Ad Bellum Revisited*, in 'Villanova Law Review', Vol. 56, 2011, pp. 569-606.

SCHMITT, M., *In Defense of Due Diligence in Cyberspace*, in 'The Yale Journal Forum', 2015, pp. 68-81.

SCHMITT, M., *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, in 'Harvard International Law Journal Online', Vol. 54, 2012, pp. 13-37.

SCHMITT, M., *Peacetime Cyber Responses and Wartime Cyber Operations under International Law: An Analytical Vade Mecum'*, in 'Harvard National Security Journal', Vol. 8, 2017, pp. 239-282.

SCHMITT, M., *Wired Warfare: Computer Network Attack and the Jus in Bello*, in 'International Review of the Red Cross', Vol. 84, 2002, pp. 365-399.

SHACKELFORD, S. AND RUSSELL, S., *Above the Cloud: Enhancing Cybersecurity in the Aerospace Sector*, in 'FIU Law Review', Vol. 10, No. 2, 2015, pp. 635-667.

SHACKELFORD, S., *From Nuclear War to Net War: Analogising Cyber Attacks in International Law*, in 'Berkeley Journal of International Law', Vol. 27, 2009, pp. 192-251.

SHAFFER, G. AND POLLACK, M., *Hard Versus Soft Law in International Security*, in 'Boston College Law Review', Vol. 52, 2011, pp. 1147-1241.

SIGALAS, E., *The Role of the European Parliament in the Development of a European Union Space Policy,* in 'Space Policy', Vol. 28, No. 2, 2012, pp. 110-117.

SILVER, D., *Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter*, in 'International Law Studies', Vol. 76, 2002, pp. 73-97.

SIMMA, B. AND PULKOWSKI, D., *Of Planets and the Universe: Self-contained Regimes in International Law,* in 'European Journal of International Law, Vol. 17, No. 3, 2006, pp. 483–529.

SINGH, A., GUPTA, M. AND OJHA, A., *Identifying Critical Infrastructure Sectors and their Dependencies: An Indian Scenario*, in 'International Journal of Critical Infrastructure Protection', 2014, pp. 1-15.

SKLEROV, M., *Solving the Dilemma of State Responses to Cyber-attacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, in 'Military Law Review', Vol. 201, 2009, pp. 1-85.

TRONCHETTI, F. AND HAO, L., *The 2014 Updated Draft PPWT: Hitting the Spot or Missing the Mark?,* in 'Space Policy', Vol. 33, 2015, pp. 38-49.

TSAGOURIAS, N., *Cyber Attacks, Self-Defence and the Problem of Attribution*, in 'Journal of Conflict and Security Law', Vol. 17, 2012, pp. 229-244.

URBAN, J., *Soft Law: The Key to Security in a Globalized Outer Space*, in 'Transportation Law Journal', Vol. 43, 2016, pp. 33-50.

VARMA, T. AND UPADHYAY, A., *Meaconing and Spoofing Attacks Evaluation with Enhancement in Security for Satellite Communication*, in 'International Open Access Journal', Vol. 2, No. 3, 2018, pp. 520-524.

VECCHIO, V., *Customary International Law in the Outer Space Treaty: Space Law as Laboratory for the Evolution of Public International Law,* in 'Zeitschrift für Luft und Weltraumrecht', Vol. 66, No. 3, 2017, pp. 491-502.

VERESHCHETIN, V. AND DANILENKO, G., *Custom as a Source of International Law of Outer Space*, in 'Journal of Space Law', Vol. 13, No. 1, 1985, pp. 22-35.

VON DER DUNK, F., *Armed Conflicts in Outer Space: Which Law Applies*?, in '*International Law Studies*', Vol. 97, 2021, pp. 188-231.

WALKNER, P., *Organizing for Cyberspace Operations: Selected Issues*, in 'International Law Studies', Vol. 89, 2013, pp. 341-361.

WESSEL, B., *The Rule of Law in Outer Space: The Effects of Treaties and Nonbinding Agreements on International Space Law*, in 'Hastings Int'l & Comp. L. Rev.', Vol. 35, No. 2, 2012, pp. 289-322.

WILLIAMS, R., *(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action*, in 'The George Washington Law Review', Vol. 79, 2011, pp. 1162-1200.

WILLIAMSON, M., *Space Ethics and Protection of the Space Environment*, in 'Space Policy', Vol. 19, 2003, pp. 47-52.

WILLIAMSON, R., *Assuring the Sustainability of Space Activities*, in 'Space Policy', Vol. 28, 2012, pp. 154-160.

WOLTAG, J., *Computer Network Operations below the Level of Armed Force',* in 'European Society of International Law Conference', Paper Series 1, 2011, pp. 1-18.

WOLTER, D., *The Peaceful Purpose Standard of the Common Heritage of Mankind Principle in Outer Space Law*, in 'ASILS Journal of International Law', Vol. 9, 1985, pp. 117-146.

XIACHUNG, Z., *In Pursuit of a Community of Shared Future. China's Global Activism in Perspective*, in 'China Quarterly of International Strategic Studies', Vol. 4, No. 1, 2018, pp. 23-37.

ZHENQIANG, P., A, *Study of China's No-First-Use Policy on Nuclear Weapons,* in 'Journal for Peace and Nuclear Disarmament', Vol. 1, No. 1, 2018, pp. 115-136.

**UNITED NATIONS RESOLUTIONS:**

United Nations General Assembly, Resolution 362 (IV), 22 October 1949, A/RES/362 (IV).

United Nations General Assembly, Resolution 502 (VI), 11 January 1952, A/RES/502(VI).

United Nations General Assembly, Resolution 1148 (XII), 14 November 1957, A/RES/1148 (XII).

United Nations General Assembly, Resolution 1348 (XIII), 13 December 1958, A/RES/1348 (XIII).

United Nations General Assembly, Resolution 1472A (XIV), 12 December 1959, A/RES/1472 (XIV).

United Nations General Assembly, Resolution 1721 (XVI), 20 December 1961, A/RES/1721 (XVI).

United Nations General Assembly, Resolution 1802 (XVII), 14 December 1962, A/RES/1802 (XVII).

United Nations General Assembly, Resolution 1884 (XVIII), 17 October 1963, A/RES/1884 (XVIII).

United Nations General Assembly, Resolution 1962 (XVIII), 13 December 1963, A/RES/1962 (XVIII).

United Nations General Assembly, Resolution 2131 (XX), 21 December 1965, A/RES/2131 (XX).

United Nations General Assembly, Resolution 2222 (XXI), 19 December 1966, A/RES/2222 (XXI).

United Nations General Assembly, Resolution 2345 (XXII), 19 December 1967, A/RES/2345 (XXII).

United Nations General Assembly, Resolution 2625 (XXV), 24 October 1970, A/RES/2625 (XXV).

United Nations General Assembly Resolution 2777 (XXVI), 29 November 1971, A/RES/2777 (XVI).

United Nations General Assembly, Resolution 3201 (S-VI), 1 May 1974, A/RES/3201 (S-VI).

United Nations General Assembly, Resolution 3235 (XXIX), 12 November 1974, A/RES/3235 (XXIX).

United Nations General Assembly, Resolution 3314 (XXIX), 14 December 1974, A/RES/3314 (XXIX).

United Nations General Assembly, Resolution S-10/2, 30 June 1978, A/RES/S-10/2.

United Nations General Assembly, Resolution 34/68, 5 December 1979, A/RES/34/68.

United Nations General Assembly, Resolution 36/99, 9 December 1981, A/RES/36/99.

United Nations General Assembly, Resolution 36/97C, 9 December 1981, A/RES/36/91C.

United Nations General Assembly, Resolution 37/7, 28 October 1982, A/RES/37/7.

United Nations General Assembly, Resolution 37/83, 9 December 1982, A/RES/37/83.

United Nations General Assembly, Resolution 37/92, 10 December 1982, A/RES/37/92.

United Nations General Assembly, Resolution 38/70, 15 December 1983, A/RES/38/70.

United Nations General Assembly, Resolution 38/80, 15 December 1983, A/RES/38/80.

United Nations General Assembly, Resolution 38/161, 19 December 1983, A/RES/38/161.

United Nations General Assembly, Resolution 39/96, 14 December 1984, A/RES/39/96.

United Nations General Assembly, Resolution 40/87, 12 December 1985, A/RES/40/87.

United Nations General Assembly, Resolution 40/162, 16 December 1985, A/RES/40/162.

United Nations General Assembly, Resolution 41/64, 3 December 1986, A/RES/41/64.

United Nations General Assembly, Resolution 41/65, 3 December 1986, A/RES/41/65.

United Nations General Assembly, Resolution 42/33, 30 November 1987, A/RES/42/33.

United Nations General Assembly, Resolution 42/68, 2 December 1987, A/RES/42/68.

United Nations General Assembly, Resolution 43/56, 6 December 1988, A/RES/43/56.

United Nations General Assembly, Resolution 44/46, 8 December 1989, A/RES/44/46.

United Nations General Assembly, Resolution 44/112, 15 December 1989, A/RES/44/112.

United Nations General Assembly, Resolution 45/55B, 4 December 1990, A/RES/45/55B.

United Nations General Assembly, Resolution 45/72, 11 December 1990, A/RES/45/72.

United Nations General Assembly, Resolution 46/45, 9 December 1991, A/RES/46/45.

United Nations General Assembly, Resolution 47/67, 14 December 1992, A/RES/47/67.

United Nations General Assembly, Resolution 47/68, 14 December 1992, A/RES/47/68.

United Nations General Assembly, Resolution 47/233, 17 August 1993, A/RES/47/233.

United Nations General Assembly, Resolution 48/74B, 16 December 1993, A/RES/48/74B.

United Nations General Assembly, Resolution 48/39, 10 February 1994, A/RES/48/39.

United Nations General Assembly, Resolution 48/264, 29 July 1994, A/RES/48/264.

United Nations General Assembly, Resolution 50/27, 6 December 1995, A/RES/50/27.

United Nations General Assembly, Resolution 51/122, 13 December 1996, A/RES/51/122.

United Nations General Assembly, Resolution 53/70, 4 December 1998, A/RES/53/70.

United Nations General Assembly, Resolution 56/19, 29 November 2001, A/RES/56/19.

United Nations General Assembly, Resolution 56/183, 21 December 2001, A/RES/56/183.

United Nations General Assembly, Resolution 58/199, 23 December 2003, A/RES/58/199.

United Nations General Assembly, Resolution 58/316, 1 July 2004, A/RES/58/316.

United Nations General Assembly, Resolution 59/115, 10 December 2004, A/RES/59/115.

United Nations General Assembly, Resolution 60/45, 8 December 2005, A/RES/60/45.

United Nations General Assembly, Resolution 60/66, 8 December 2005, A/RES/60/66.

United Nations General Assembly, Resolution 61/75, 6 December 2006, A/RES/61/75.

United Nations General Assembly, Resolution 62/43, 5 December 2007, A/RES/62/43.

United Nations General Assembly, Resolution 62/101, 17 December 2007, A/RES/62/101

United Nations General Assembly, Resolution 62/217, 22 December 2007, A/RES/62/217.

United Nations General Assembly, Resolution 64/49, 2 December 2009, A/RES/64/49.

United Nations General Assembly, Resolution 65/41, 8 December 2010, A/RES/65/41.

United Nations General Assembly, Resolution 65/68, 8 December 2010, A/RES/65/68.

United Nations General Assembly, Resolution 65/276, 3 May 2011, A/RES/65/276.

United Nations General Assembly, Resolution 66/288, 27 July 2012, A/RES/66/288.

United Nations General Assembly, Resolution 68/50, 5 December 2013, A/RES/68/50.

United Nations General Assembly, Resolution 68/74, 11 December 2013, A/RES/68/74.

United Nations General Assembly, Resolution 68/75, 11 December 2013, A/RES/68/75.

United Nations General Assembly, Resolution 68/243, 27 December 2013, A/RES/68/243.

United Nations General Assembly, Resolution 69/32, 2 December 2014, A/RES/69/32.

United Nations General Assembly, Resolution 69/38, 2 December 2014, A/RES/69/38.

United Nations General Assembly, Resolution 69/85, 5 December 2014, A/RES/69/85.

United Nations General Assembly, Resolution 70/27, 7 December 2015, A/RES/70/27.

United Nations General Assembly, Resolution 70/53, 7 December 2015, A/RES/70/53.

United Nations General Assembly, Resolution 70/82, 9 December 2015, A/RES/70/82.

United Nations General Assembly, Resolution 70/237, 23 December 2015, A/RES/70/237.

United Nations General Assembly, Resolution 70/305, 13 September 2016, A/RES/70/305.

United Nations General Assembly, Resolution 71/32, 5 December 2016, A/RES/71/32.

United Nations General Assembly, Resolution 71/41, 5 December 2016, A/RES/71/41.

United Nations General Assembly, Resolution 71/90, 6 December 2016, A/RES/71/90.

United Nations General Assembly, Resolution 71/323, 8 September 2017, A/RES/71/323.

United Nations General Assembly, Resolution 72/27, 4 December 2017, A/RES/72/27.

United Nations General Assembly, Resolution 72/26, 4 December 2017, A/RES/72/26.

United Nations General Assembly, Resolution 72/56, 4 December 2017, A/RES/72/56.

United Nations General Assembly, Resolution 72/78, 7 December 2017, A/RES/72/78.

United Nations General Assembly, Resolution 72/79, 7 December 2017, A/RES/72/79.

United Nations General Assembly, Resolution 72/250, 24 December 2017, A/RES/72/250.

United Nations General Assembly, Resolution 72/313, 17 September 2018, A/RES/72/313.

United Nations General Assembly, Resolution 73/6, 26 October 2018, A/RES/73/6.

United Nations General Assembly, Resolution 73/27, 5 December 2018, A/RES/73/27.

United Nations General Assembly, Resolution 73/31, 5 December 2018, A/RES/73/31.

United Nations General Assembly, Resolution 73/72, 5 December 2018, A/RES/73/72.

United Nations General Assembly, Resolution 73/91, 7 December 2018, A/RES/73/91.

United Nations General Assembly, Resolution 73/206, 22 December 2018, A/RES/73/266.

United Nations General Assembly, Resolution 74/33, 12 December 2019, A/RES/74/33.

United Nations General Assembly, Resolution 74/67, 12 December 2019, A/RES/74/67.

United Nations General Assembly, Resolution 74/82, 13 December 2019, A/RES/74/82.

United Nations General Assembly, Resolution 75/32, 7 December 2020, A/RES/75/32.

United Nations General Assembly, Resolution 75/36, 7 December 2020, A/RES/75/36.

United Nations General Assembly, Resolution 75/69, 7 December 2020, A/RES/75/69.

United Nations General Assembly, Resolution 75/37, 16 December 2020, A/RES/75/37.

United Nations General Assembly, Resolution 75/240, 31 December 2020, A/RES/75/240.

United Nations Security Council, Resolution 1368, 12 September 2001.

United Nations Security Council, Resolution 1373, 28 September 2001.

**UN DOCUMENTS:**


Achievement of a Uniform Interpretation of the Right of Self-Defense in Conformity with the United Nations Charter as Applied to Outer Space as a Factor in Maintaining Outer Space a Safe and Conflict-Free Environment and Promoting the Long-Term Sustainability of Outer Space Activities (Russian Federation), UN Doc. A/AC.105/C.1/2015/CRP.22, 2 February 2015.

Addendum - Eighth Report on State responsibility by Mr. Roberto Ago, Special Rapporteur - the Internationally Wrongful Act of the State, Source of International Responsibility (part 1), UN Doc. A/CN.4/318/Add.5-7, 1980.

Additional Considerations and Proposals aimed at Building up Understanding of the Priority Aspects, Comprehensive Meaning, and Functions of the Concept and Practices of Ensuring the Long-Term Sustainability of Outer Space Activities (Russian Federation), UN Doc. A/AC.105/C.1/2015/CRP.24, 2 February 2015.

Additional Considerations and Proposals to Increase Understanding of Priorities, the Overall Meaning and Functions of the Concept and Practice of Ensuring Long-Term Sustainability of Activities in Outer Space (submitted by the Russian Federation), UN Doc. A/AC.105/L.296, 30 April 2015.

Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, UN Doc. A/C.1/73/L.37, 18 October 2018.

Allocation of Agenda Items to the Special Political and Decolonization Committee (Fourth Committee), UN Doc. A/C.4/75/1, 18 September 2020.

Allocation of Items to the First Committee, UN Doc. A/C.1/75/1, 21 September 2020.

Comments and Proposed Amendments to the Updated set of Draft Guidelines for the Long-term Sustainability of Outer Space Activities (submitted by GRULAC), UN Doc. A/AC.105/C.1/2015/CRP.19/Rev.1, 9 February, 2015.

Compendium of Space Debris Mitigation Standards adopted by States and International Organizations, UN Doc. A/AC.105/C.2/2019/CRP.14, 5 April 2019.

Consideration of the Fiftieth Anniversary of the United Nations Conference on the Exploration and Peaceful Uses of Outer Space, UN Doc. A/C.4/72/L.4, 20 September 2017.

Considerations on the Sum Total of Prime Requisites and Factors that Should Shape the Policy of International Information Sharing Serving Safety of Space Operations (Russian Federation), UN Doc. A/AC.105/C.1/2016/CRP.14, 16 February 2016.

Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/54/213, 10 August 1999.

Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/55/140, 10 July 2000.

Developments in the field of information and telecommunications in the context of international security, UN Doc. A/58/373, 17 September 2003.

Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/59/116/Add.1, 28 December 2004.

Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/60/95/Add.1, 21 September 2005.

Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/61/161, 18 July 2006.

Developments in the field of information and telecommunications in the context of international security, UN Doc. A/62/98, 2 July 2007.

Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/65/154, 20 July 2010.

Developments in the Field of Information and Telecommunications in the Context of International Security, UN. Doc. A/68/156, 16 July 2013.

Developments in the field of information and telecommunications in the context of international security, UN Doc A/68/156/Add.1, 9 September 2013.

Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/69/112, 30 June 2014.

Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/69/112/Add.1, 18 September 2014.

Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/172, 22 July 2015.

Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/71/172, 19 July 2016.

Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/72/315, 11 August 2017.

Developments in the field of information and telecommunications in the context of international security, UN Doc. A/C.1/73/L.27/Rev.1, 29 October 2018.

Digital Recordings of the 59th Session of COPUOS (2016), 8 June 2016.

Draft Agreement on the Moon and other Celestial Bodies (Argentina), UN Doc. A/AC.105/C.2/L.54, 13 June 1969.

Draft Concept Note on the Joint Panel Discussion of the First and Fourth Committees of the General Assembly on Possible Challenges to Space Security and Sustainability, UN Doc. A/AC.105/2019/CRP.19, 21 June 2019.

Draft Guidelines for Long-term Sustainability of Activities in Outer Space (submitted by the Chair of the Working Group), UN Doc. A/AC.105/C.1/L.367, 16 July 2018.

Draft Resolution entitled 'Fiftieth Anniversary of the first United Nations Conference on the Exploration and Peaceful Uses of Outer Space: Space as a Driver of Sustainable Development', UN Doc. A/AC.105/L.313, 16 May 2018.

Draft Treaty Governing the Exploration of the Moon and other Celestial Bodies (United States), letter dated 16 June 1966 reproduced in UN Doc. A/AC.105/C.2/L.12, 11 July 1966.

Draft Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, the Moon and Other Celestial Bodies (the Soviet Union), letter dated 11 July 1966 reproduced in UN Doc. A/AC.105/C.2/L.13, 11 July 1966.

Fiftieth Anniversary of the First United Nations Conference on the Exploration and Peaceful Uses of Outer Space: space as a driver of sustainable development, UN Doc. A/73/L.6, 12 October 2018.

First Report on General Principles of Law by Marcelo Vázquez-Bermúdez, Special Rapporteur, UN Doc. A/CN.4/732, 5 April 2019.

Fourth Report on Peremptory Norms of General International Law (*jus cogens*) by Dire Tladi, Special Rapporteur, Official Records of the General Assembly, Seventy First Session, UN Doc. A/CN.4/727.

Future Role and Activities of COPUOS (submitted by the Chair), UN Doc. A/AC.105/L.268, 10 May 2007

Future Role and Activities of the Committee on the Peaceful Uses of Outer Space (submitted by the Chair), UN Doc. A/AC.105/L.268 Corr. 1, 1 June 2007.

General Assembly 13th Session (1958), UN Doc. A/PV.792.

General Assembly 59th Session (2004), UN Doc. A/59/PV.71.

General Assembly 72nd Session (2017), UN Doc. A/72/PV.66.

General Assembly 73rd Session (2018), UN Doc. A/73/PV.26.

General Assembly 74th Session (2019), UN Doc. A/74/PV.47.

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/65/201, 30 July 2010.

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98, 24 June 2013.

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174, 22 July 2015.

Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities, UN Doc. A/68/189, 29 July 2013.

Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, UN Doc. HRC/29/32, 22 May 2015.

Ideas for the Way Forward on the Draft Set of Guidelines for the Long-Term Sustainability of Outer Space Activities (submitted by the Chair), UN Doc. A/AC.105/C.1/2016/CRP.3, 28 January 2016.

Information on the Activities of International Intergovernmental and Non-Governmental Organizations Relating to Space Law, UN Doc. A/AC.105/C.2/L.265, 16 January 2007.

Information on the Activities of International Intergovernmental and Non-Governmental Organizations Relating to Space Law, UN Doc. A/AC.105/C.2/L.270, 25 January 2008.

Inter-Agency Space Debris Coordination Committee Space Debris Mitigation Guidelines, UN Doc. A/AC.105/C.1/L.260, 29 November 2002.

International Code of Conduct for Information Security (China, the Russian Federation, Tajikistan and Uzbekistan), reproduced in Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, UN Doc. A/66/359, 14 September 2011.

International Law Commission, Sixty-ninth Session, Fourth Report on the Protection of the Atmosphere by Shinya Murase, UN Doc. A/CN.4/705, 31 January 2017.

Letter dated 11 September 2015 from the Permanent Representative of China to the Conference on Disarmament and the Charge d'affaires a.i. of the Russian Federation addressed to the Secretary-General of the Conference transmitting the comments by China and the Russian Federation regarding the United States of America analysis of the 2014 updated Russian and Chinese texts of the draft treaty on prevention of the

placement of weapons in outer space and of the threat or use of force against outer space objects (PPWT), CD/2042, 14 September 2015.

Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General, reproduced in UN Doc. A/C.1/53/3, 30 September 1998.

Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, UN Doc. A/69/723, 13 January 2015.

Long-term sustainability of activities in outer space (Russian Federation), UN Doc. A/AC.105/L.285, 31 July 2012.

Long-term Sustainability of Activities in Outer Space (France), UN Doc. A/AC.105/C.1/L.303, 9 February 2010.

Long-term Sustainability of Outer Space Activities (United States), UN Doc. A/AC.105/C.1/2011/CRP.17, 7 February 2011.

Long-Term Sustainability of Outer Space Activities (basic elements of the concept of establishing a unified Centre for Information on Near-Earth Space Monitoring under the auspices of the United Nations and the most topical aspects of the subject matter) (Russian Federation), UN Doc. A/AC.105/L.290, 4 March 2014.

Long-term Sustainability, UN Doc. A/AC.105/C.1/2011/CRP.17, 7 February 2011.

LSC Summary Records 2nd Session (1962), UN. Doc. A/AC.105/C.2/SR.2.

LSC Summary Records 3rd Session (1964), UN Doc. A/AC.105/C.2/SR.29-37.

LSC Summary Records 5th Session (1966), UN Doc. A/AC.105/C.2/SR.57.

LSC Summary Records 5th Session (1966), UN Doc. A/AC.105/C.2/SR.64.

LSC Summary Records 5th Session (1966), UN Doc. A/AC.105/C.2/SR.66.

LSC Summary Records 5th Session (1966), UN Doc. A/AC.105/C.2/SR.69.

LSC Summary Records 5th Session (1966), UN Doc. A/AC.105/C.2/SR.70.

LSC Summary Records 5th Session (1966), UN Doc. A/AC.105/C.2/SR.71.

LSC Summary Records 5th Session (1966), UN Doc. A/AC/.105/C.2/SR.63.

LSC Summary Records 10th Session (1971), UN Doc. A/AC.105/C.2/SR.154.

LSC Summary Records 10th Session (1971), UN Doc. A/AC.105/C.2/SR.168.

LSC Summary Records 17th Session (1978), UN Doc. A/AC.105/C.2/SR.291.

Meeting Hosted by Switzerland on Possible Further Work on the Long-Term Sustainability of Outer Space Activities: Background and Chair's Summary, UN Doc. A/AC.105/2019/CRP.16, 18 June 2019.

New Agenda Item on General Exchange of Information on Practices in Relation to non-legally Binding Instruments for Outer Space Activities, UN Doc. A/AC.105/C.2/L.291, 11 April 2013.

Nominations of Members of Expert Groups and List of Points of Contact Communicated to the Secretariat as of 9 June 2011, UN Doc. A/AC.105/2011/CRP.15 and Add. 1, 9 June 2011.

Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Final Substantive Report, UN Doc. A/AC.290/2021/CRP.2, 10 March 2021.

Participation of the European Union in the Work of the United Nations, UN Doc. A/65/856, 1 June 2011.

Preventing an Arms Race in Outer Space (Australia, Belgium, France, Federal Republic of Germany, Italy, The Netherlands, New Zealand and the United Kingdom), UN Doc. A/C.1/36/L.7, 10 November 1981.

Proposal for the Establishment of a Working Group on Implementation of Agreed Guidelines on Long-Term sustainability (Canada, France, Japan, the United Kingdom and the United States), UN Doc. A/AC.105/2019/CRP.7/Rev.1, 19 June 2019.

Proposal on Long-Term Sustainability of Outer Space Activities of the Committee on the Peaceful Uses of Outer Space (United Arab Emirates), UN Doc. A/AC.105/2019/CRP.13, 13 June 2019.

Proposal on Long-Term Sustainability of Space Activities (Australia, Canada, France, Germany, Israel, Italy, Japan, the Netherlands, New Zealand, the United Kingdom and the United States), UN Doc. A/AC.105/2018/CRP.26/Rev.2, 29 June 2018.

Proposal on the Modalities of the Working Group on the Long-Term Sustainability of Outer Space Activities of the Committee on the Peaceful Uses of Outer Space (submitted by Belarus, China, Nicaragua, Pakistan and the Russian Federation), UN Doc. A/AC.105/2019/CRP.10/Rev.2, 20 June 2019.

Proposal on the Review and Consideration of the Concept of a United Nations Information Platform Serving Common Needs in Collecting and Sharing Formation on Near-Earth Space Monitoring in the Interests of Safety of Space Operations, and its Architectural and Programmatic Aspects (Russian Federation), UN Doc. A/AC.105/C.1/2015/CRP.32, 9 February 2015.

Report of the 60th Session UNGA First Committee (2005), UN Doc. A/60/463.

Report of the 72nd Session UNGA First Committee, Prevention of an Arms Race in Outer Space (2017), UN Doc. A/72/407.

Report of the 2nd Session of COPUOS (1962), UN Doc. A/5181.

Report of the 27th Session of COPUOS (1984), UN Doc. A/39/20.

Report of the 50th Session of COPUOS (2007), UN Doc. A/62/20.

Report of the 51st Session of COPUOS (2008), UN Doc. A/63/20.

Report of the 52nd Session of COPUOS (2009), UN Doc. A/64/20.

Report of the 55th Session of COPUOS (2012), UN Doc. A/67/20.

Report of the 56th Session of COPUOS (2013), UN Doc. A/68/20.

Report of the 57th Session of COPUOS (2014), UN Doc. A/69/20.

Report of the 59th Session of COPUOS (2016), UN Doc. A/71/20.

Report of the 60th Session of COPUOS (2017), UN. Doc. A/72/20.

Report of the 61st Session of COPUOS (2018), UN Doc. A/73/20.

Report of the 62nd Session of COPUOS (2019), UN Doc. A/74/20.

Report of the 41st Session of the LSC (2002), UN Doc. A/AC.105/787.

Report of the 47th Session of the LSC (2008), UN Doc. A/AC.105/917.

Report of the 49th Session of the LSC (2010), UN Doc. A/AC.105/942.

Report of the 50th Session of the LSC (2011), UN Doc. A/AC.105/990.

Report of the 56th Session of the LSC (2017), UN Doc. A/AC.105/1122.

Report of the 58th Session of the LSC (2019), UN Doc. A/AC.105/1203.

Report of the 31st Session of the STSC (1994), UN Doc. A/AC.105/571.

Report of the 38th Session of the STSC (2001), UN Doc. A/AC.105/761.

Report of the 42nd Session of the STSC (2005), UN Doc. A/AC.105/848.

Report of the 46th Session of the STSC (2009), UN Doc. A/AC.105/933.

Report of the 47th Session of the STSC (2010), Doc. A/AC.105/958.

Report of the 57th Session of the STSC (2020), UN Doc. A/AC.105/1224.

Report of the 58th Session of the STSC (2021), UN Doc. A/AC.105/1240.

Report of the Chairman of the Working Group on agenda item 6, entitled 'Status and application of the five United Nations treaties on outer space' contained in the Report of the 47th Session of COPUOS (2004), UN Doc. A/AC.105/826, 16 April 2004.

Report of the International Law Commission 53rd Session (2001), Draft Articles on Responsibility of States for Internationally Wrongful Acts, UN Doc. A/56/10.

Report of the International Law Commission 58th Session (2006), Conclusions of the work of the Study Group on the Fragmentation of International Law: Difficulties arising from the Diversification and Expansion of International Law, UN Doc. A/61/10.

Report of the International Law Commission 67th Session (2015), Other Decisions and Conclusions of the Commission, UN Doc. A/70/10.

Report of the International Law Commission 70th Session (2018), Draft Conclusions on Identification of Customary International Law with commentaries, UN Doc. A/73/10.

Report of the International Law Commission 71st Session (2019), Peremptory norms of general international law (*jus cogens*), UN Doc. A/74/10.

Report of the Second United Nations Conference on the Exploration and Peaceful Uses of Outer Space, UNISPACE II, UN Doc. A/CONF.101/10, 9-21 August 1982.

Report of the Secretary-General on Transparency and Confidence-Building in Measures Outer Space Activities (Portugal on behalf of the EU), UN Doc. A/62/114/Add.1, 17 September 2007.

Report of the Special Political and Decolonization Committee (Fourth Committee), UN Doc. A/59/469, 8 November 2004.

Report of the Special Political and Decolonization Committee (Fourth Committee), UN Doc. A/72/446, 27 October 2017.

Report of the Special Political and Decolonization Committee (Fourth Committee), UN Doc. A/74/408, 7 November 2019.

Report of the Third UN Conference on Space Exploration and Peaceful Uses of Outers Space, UN Doc. A/CONF. 184/6, 18 October 1999.

Report of the United Nations Conference on the Human Environment, Stockholm, 5-16 June 1972, UN Doc. A/CONF.48/14/Rev.1.

Report of the Working Group on the Review of International Mechanisms for Cooperation in the Peaceful Exploration and Use of Outer Space on the work conducted under its multi-year workplan, UN Doc. A/AC.105/C.2/112, 13 April 2017.

Report of the World Summit on Sustainable Development, including the Plan of Implementation of the World Summit on Sustainable Development, UN Doc. A/CONF.199/20, 4 September 2002.

Report of the World Commission on Environment and Development (Brundtland Commission), UN Doc A/42/427, 4 August 1987.

Report under Paragraph 1(d) of the GA Res 1348 (XIII), UN Doc. A/AC.98/L.7, 27 May 1959.

Request for the Inclusion of an Item in the Provisional Agenda of Twenty Sixth Session (USSR), A/8391, 4 June 1971.

Russian Assessment of the Initiative and Actions of the European Union to Advance its Draft Code of Conduct for Outer Space Activities (Russian Federation), UN Doc. A/AC.105/C.1/L.346, 30 July 2015.

Reviewing Opportunities for Achieving the Vienna Consensus on Space Security encompassing several regulatory domains (Russian Federation), UN Doc. A/AC.105/C.1/2016/CRP.15, 16 February 2016.

Responses to the Set of Questions provided by the Chair of the Working Group on the Status and Application of the Five United Nations Treaties on Outer Space, UN Doc. A/AC.105/C.2/2017/CRP.6, 23 March 2017.

Responses to the Set of Questions provided by the Chair of the Working Group on the Status and Application of the Five United Nations Treaties on Outer Space, UN Doc. A/AC.105/C.2/2017/CRP.17, 28 March 2017.

Responses to the Set of Questions provided by the Chair of the Working Group on the Status and Application of the Five United Nations Treaties on Outer Space, UN Doc. A/AC.105/C.2/2018/CRP.12, 6 April 2018.

Responses to the Set of Questions provided by the Chair of the Working Group on the Status and Application of the Five United Nations Treaties on Outer Space, UN Doc. A/AC.105/C.2/2018/CRP.16, 11 April 2018.

Responses to the Set of Questions provided by the Chair of the Working Group on the Status and Application of the Five United Nations Treaties on Outer Space, UN Doc. A/AC.105/C.2/2019/CRP.18, 2 April 2019.

Study on the Application of Confidence-Building Measures in Outer Space: Report / by the Secretary-General, UN Doc. A/48/305, 15 October 1993.

Submission of the Russian Federation to the United Nations Committee on the Peaceful Uses of Outer Space on the subject-matter 'Identification of Cross-Links between the Recommendations Contained in the Report of the Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities and the Topic of Developing Guidelines on the Long-Term Sustainability of Outer Space Activities', UN Doc. A/AC.105/C.1/2015/CRP.33, 9 February 2015.

Technical Report on Space Debris, UN Doc. A/AC.105/720, New York, 1999.

Terms of Reference and Methods of Work of the Working Group on the Long-term Sustainability of Outer Space Activities of the Scientific and Technical Subcommittee, UN Doc. A/AC.105/C.1/L.307, 24 January 2011.

Thematic priority 2. Legal Regime of Outer Space and Global Governance: Current and Future Perspectives, UN Doc. A/AC.105/1169, 13 November 2017.

United Nations General Assembly 73rd Session (2018), UN Doc. A/73/PV.45.

United Nations General Assembly 74th Session (2019), UN Doc. A/74/PV.46.

United Nations General Assembly 75th Session (2020), UN Doc. A/75/PV.37.

Working Document of the 73rd Session of UNGA First Committee (2018), UN Doc. A/C.1/73/L.51, 19 October 2018.

**INTERNATIONAL INSTRUMENTS AND DECLARATIONS:**

Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, adopted on 5 December 1979, entered into force on 11 July 1984, 1363 UNTS 3.

Agreement on the Rescue of Astronauts, the Return of Astronauts and Return of Objects Launched into Outer Space, adopted on 19 December 1967, and entered into force on 3 December 1968, 672 UNTS 119.

Convention on International Liability for Damage Caused by Space Objects, adopted on 29 November 1971, and entered into force on 1 September 1972, 961 UNTS 187, preamble.

Convention on Registration of Objects Launched into Outer Space, concluded on14 January 1975 in New York, and entered into force on 15 September 1976, 1023 UNTS 15.

Constitution and Convention of the International Telecommunication Union, concluded on 22 December 1992, and entered into force on 1 July 1994, 1825 UNTS 331.

Declaration of the United Nations Conference on the Human Environment, Stockholm, 16 June 1972.

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, adopted on 8 June 1977, and entered into force on 7 December 1978, 1125 UNTS 3.

Rio Declaration on Environment and Development, Rio de Janeiro, 14 June 1992.

The Space Millennium: Vienna Declaration on Space and Human Development, (UNISPACE III), held in Vienna from 19 to 30 July 1999.

The Space Millennium: Vienna Declaration on Space and Human Development, Third United Nations Conference on the Exploration and Peaceful Uses of Outer Space (UNISPACE III), held in Vienna from 19 to 30 July 1999.

Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water, concluded on 5 August 1963, and entered into force on 10 October 1963, 480 UNTS 43.

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, adopted on 16 December 1966, and entered into force on 10 October 1967, 610 UNTS 205.

United Nations Environment Programme: the Cocoyoc Declaration adopted by the participants in the UNEP/UNCTAD Symposium on 'Patterns of Resource Use, Environment and Development Strategies' held at Cocoyoc, Mexico, from 8 to 12 October 1974.

United Nations, Charter of the United Nations, signed on 26 June 1945, and entered into force on 24 October 1945.

Vienna Convention on the Law of Treaties, concluded on 23 May 1969, and entered into force on 27 January 1980, 1155 UNTS 331.

**INTERNATIONAL JURISPRUDENCE:**

*Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo*, Advisory opinion, Judgement, [2010] ICJ Reports 403, 22 July 2010 and Declaration of Judge Simma.

*Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Hersegovina v. Serbia and Montenegro),* Judgement, [2007] ICJ Reports 43, 26 February 2007.

*Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda),* Judgement, [2005] ICJ Reports 168, 19 December 2005.

*Barcelona Traction, Light and Power Company, Limited (Belgium v. Spain),* Judgement, [1970] ICJ Reports 3, 5 February 1970.

*Case Concerning the Factory at Chorzow (Germany v. Poland),* PCIJ (Ser. A), No. 9, 26 July 1927.

*Certain Expenses of the United Nations (Article 17, paragraph 2, of the Charter),* Advisory Opinion, [1962] ICJ Reports 151, 20 July 1962.

*Corfu Channel (United Kingdom v Albania),* Judgment, [1949] ICJ Reports 4, 9 April 1949.

*Gabčíkovo-Nagymaros Project (Hungary/Slovakia),* Judgement, [1997] ICJ Reports 7, 25 September 1997.

*Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970),* Advisory Opinion, [1971] ICJ Reports 16, 21 June 1971.

*Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory,* Advisory opinion, [2004] ICJ Reports 136, 9 July 2004, and Separate declaration of Judge Buergenthal.

*Legality of the Threat or Use of Nuclear Weapons, Legality of the Threat or Use of Nuclear Weapons,* Advisory Opinion, [1996] ICJ Reports 126, 8 July 1996.

*Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America),* Judgement, [1986] ICJ Reports 14, 27 June 1986.

*North Sea Continental Shelf Cases (Federal Republic of Germany v. Denmark; Federal Republic of Germany v. Netherlands)*, [1969] ICJ Reports 3, 20 February 1969, and Dissenting opinions of Judge Lachs and Sorensen.

*Oil Platforms (Islamic Republic of Iran v. United States of America),* Judgement, [2003] ICJ Reports 161, 6 November 2003.

*Prosecutor v Tadic*, Case No IT-94-1, Appeals Chamber Judgment 15 July 1999.

*Pulp Mills on the River Uruguay (Argentina v. Uruguay),* Judgement [2010] ICJ Reports 14, 20 April 2010 and Separate Opinion of Judge Cançado Trindade.

*SS 'Lotus' (France v. Turkey),* PCIJ (Ser. A) No. 10, 7 September 1927.

*United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)*, Judgement, [1980] ICJ Reports 3, 24 May 1980.

*Whaling in the Antarctic (Australia v. Japan. New Zealand: intervening*), Judgement, [2014] ICJ Reports 226, 31 March 2014.

**ONLINE RESOURCES:**

ALBRIGH, D., STRICKER, J. AND WALROND, C., *IAEA Iran Safeguards Report: Shutdown of Enrichment at Natans Result of Stuxnet Virus?*, ISIS Report, 23 November 2010. Available at http://isis-online.org/

ALSHAER, M., *Cyberattacks On Satellites Review & Solutions*. Available at www.academia.edu

BAYLON, C., *Challenges at the Intersection Cyber Security and Space Security*, Chatham House, December 2014. Available at https://www.chathamhouse.org/

BEN-ISRAEL, I. AND KAPLAN, Z., *Out of this World: Israel's Space Program*. Available at https://mfa.gov.il/

BLACK, S., *No Harmful Interference with Space Objects: The Key to Confidence-Building*, Stimson Center Report No 69, July 2008. Available at https://www.stimson.org/

BORGER, J., *Pentagon Kept the Lid on Cyberwar in Kosovo,* 9 November 1999. Available at https://www.theguardian.com/

BROWN, G. AND HARRIS, W., *How Much do Satellites Cost.* Available at https://science.howstuffworks.com/

BROWN, O, COTTOM, T., GLEASON, M., HALLEX, M., LONG, A., RIVERA, E., FINKLEMAN, D., HITCHENS, T., JAH, M., KOPLOW, D., SEDWICK, R., *Orbital Traffic Management Study – Final Report*, National Aeronautics and Space Administration (NASA) and Science applications International Corporation (SAIC), 21 November 2016. Available at https://www.spacepolicyonline.com/

CARPANELLI, E. AND COHEN, B., *Interpreting "Damage Caused by Space Objects" under the 1972 Liability Convention*, 2014, IAC paper. Available at www.iislweb.org/

CARTAGENA, I., *Mandate and Working Methods in the Conference of Disarmament. A Historical Perspective*, UNIDIR, 2019. Available at https://unidir.org/

CHRISTOL, C., *Satellite Power System (SPS) White Paper on Inter-National Agreements,* National Technical Information Service, 1978. Available at https://www.osti.gov/

COLBY, E., *From Sanctuary to Battlefield: a Framework for a U.S. Defense and Deterrence Strategy for Space*, published by Center for a New American Security, January 2016. Available at https://www.cnas.org/

COMAN, M. AND BADEA, D., *The Critical Space Infrastructure and its Importance to Military Operations*, International Conference Knowledge-Based Organization, Vol. XXV, No. 1, 2019. Available at https://sciendo.com/

CONTANT-JORGENSEN, C., LÁLA, P. AND SCHROGL, K-U., (eds), *Cosmic Study on Space Traffic Management*, Paris, 2006. Available at www.iaaweb.org/

DEKEL, T. AND LEVI, R., *Space Security Capabilities and Trends,* in *Space Security Conference 2011: Building on the Past, Stepping Towards the Future*, UNIDIR, 2011. Available at https://swfound.org/

DELPECH, T., *Nuclear Deterrence in the 21st Century: Lessons from the Cold War for a New Era of Strategic Piracy, Santa Monica*, 2012. Available at https://www.rand.org/

DILLOW, D., LIN, J. AND SINGER, S., *China's Race to Space Domination*, 20 September 2016. Available at www.popsci.com

DÖRR, O., Encyclopedia of Public International Law, Use of force, prohibition of, Introduction. Availabe at https://opil.ouplaw.com/

ELLIMAN , W., *Israel in Space*, January 2003. Available at https://mfa.gov.il/

FALCO, G., *The Vacuum of Space Cybersecurity*, AIAA Space Forum, Orlando, 18 September 2018. Available at https://arc.aiaa.org/

FEIVESON, H. AND HOGENDOORN, E., *No First Use of Nuclear Weapons*, in 'The Non proliferation Review', Summer 2003. Available at https://www.nonproliferation.org/

FERRAZZANI, M., *Soft law in Space Activities*, Presentation in the Conference "Soft Law in Outer Space. The Function of Non-binding Norms in International Space Law" at the Faculty of Law of the University of Vienna, 2 April 2011. Available at https://www.spacelaw.at/

FERRETTI, S., FEUSTEL BÜECHL, J., GIBSON, R., HULSROJ, P., PAPP, A., VEIT, E., *Space for Sustainable Development*, ESPI Report No. 59, Vienna, June 2016. Available at https://espi.or.at/

FIDLER, D., *Cybersecurity and the New Era of Space Activities,* Articles by Maurer Faculty, 2018. Available at https://www.repository.law.indiana.edu/

FILDES, J., *Stuxnet Virus Targets and Spread Revealed*, 15 February 2011. Available at https://www.bbc.com/

FISK, L., *Space as a Global Commons*. Presentation available at https://www.unoosa.org/

FROEHLICH, A. AND PECUJLIC, A. (eds), *Mechanisms for the Development of International Norms regarding Space Activities*, ESPI Report N° 57, Vienna, May 2016. Available at https://espi.or.at/

GARINO, B. AND GIBSON, J., *Space System Threats*, Air University Press, 2009. Available at https://aerospace.csis.org/

GASPARINI ALVES, P., *Prevention of an Arms Race in Outer Space. A Guide to the Discussions in the Conference of Disarmament*, UNIDIR/91/79, New York, 1991. Available at https://www.unidir.org/

GEERS, K., *Cyberspace and the Changing Nature of Warfare*, Tallinn, CCDCOE, Keynote Speech. Available at https://ccdcoe.org/

GOEHRING, J., *Why isn't Outer Space a Global Commons*?, in 'Journal of National Security Law and Policy', Vol. 11 __ (forthcoming 2021). Available at https://jnslp.com/

GRAHAM, B., *Military Grappling with Rules for Cyber Warfare*, 8 November 1999. Available at http://www.washingtonpost.com/

HARRISON, T., JOHNSON, K. AND ROBERTS, T., *Space Threats Assessment 2018*, CSIS, 2018. Available at https://www.csis.org/

HARRISON, T., JOHNSON, K. AND ROBERTS, T., *Space Threats Assessment 2019,* CSIS, 2019. Available at https://www.csis.org/

HENRI, Y., *Presentation entitled Frequency Management and Space Traffic Management*. Available at https://www.unoosa.org/

HERTZFELD, H., WEEDEN, B. AND JOHNSON, C., *How Simple Terms Mislead Us: The Pitfalls of Thinking about Outer Space as a Commons,* 2015. Available at https://swfound.org/

HITCHENS, T. AND JOHNSON-FREESE, J., Toward a New National Security Space Strategy: Time for a Strategic Rebalancing, in Atlantic Council Strategy Paper No. 5, 2017. Available at https://www.atlanticcouncil.org/

HITCHENS, T., *NSC Makes Cyber Security For Space Industry 'Top Priority'*, 23 October 2019. Available at https://breakingdefense.com/

HOFFMAN, D., *Reagan Approved Plan to Sabotage Soviets*, 27 February 2004. Available at https://www.washingtonpost.com/

HUTCHINS, R., *Cyber Defense of Space Assets*, Tufts University, 2016. Available at www.cs.tufts.edu

HYTEN, H., *Space Mission Force: Developing Space Warfighters for Tomorrow,* Air Force Space Command, White Paper, 29 June 2016. Available at https://www.afspc.af.mil/

JAKHU, R. AND FREELAND, S., *The Relationship between the Outer Space Treaty and Customary International Law*, 67th International Astronautical Congress 2016. Available at https://ssrn.com/

JAKHU, R., *United Nations Principles on Outer Space, in Proceedings of United Nations/Nigeria Workshop on Space Law*, Vienna, 2006. Available at https://unoosa.org/

JONES, S., *Russian Group Accused of Hacking Satellites*, 9 September 2015. Available at https://www.ft.com/

JONG-CHEN, J. AND O'BRIEN, B., *A Comparative Study: The Approach to Critical Infrastructure Protection in the U.S., E.U., and China*, Digital Future Project, November 2017. Available at https://www.wilsoncenter.org/

KAVANATH, C., *New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?*, in Carnegie Endowment for International Peace, August 2019. Available at https://carnegieendowment.org/

LANGER, R., *Stuxnet und die Folgen*, Munich, 2017. Available at https://www.langner.com/

LEE, D., *Los Niños que lograron hackear el Sistema Electoral de los Estados Unidos*, 13 August 2018. Available at https://www.bbc.com/

LEE, R., ASSANTE, M. AND CONWAY, T., *Analysis of the Cyber Attack on the Ukrainian Power Grid*, 18 March 2016. Available at https://ics.sans.org/

LEWIS, P. AND LIVINGSTONE, D., *The Cyber Threat in Outer Space*, in 'Bulletin of Atomic Scientists', 21 November 2016. Available at www.thebulletin.org

LIVINGSTONE, D. AND LEWIS, P., *Space, the Final Frontier for Cybersecurity*?, Chatham House, 2016, p. 21. Available at https://www.chathamhouse.org/

MALIK, T., *NASA Launches Astronaut Internet in Space*, 22 January 2010. Available at https://www.space.com/

MANSEL, T., *How Estonia became E-stonia*, 16 May 2013. Available at https://www.bbc.com/

MARCHISIO, S., *National Jurisdiction for Regulating Space Activities Of Governmental and Non-Governmental Entities*, United Nations/Thailand Workshop on Space Law, 16-19 November 2010, Bangkok, Thailand. Available at https://unoosa.org/

MARCHISIO, S., *Space Law and Governance*, 10th United Nations Workshop on Space Law 'Contribution of Space Law and Policy to Space Governance and Space Security in the 21th Century', 5-8 September 2016, Vienna. Available at https://unoosa.org/

MARCHISIO, S., *The Final Frontier: Prospects for Arms Control in Outer Space (Global Security Policy Brief)*, European Leadership Network, July 2019. Available at https://www.europeanleadershipnetwork.org/

MARKOFF, J., *Before the Gunfire, Cyber-attacks,* 12 August 2008. Available at https://www.nytimes.com/

MASSON-ZWAAN, T., *Legal Principles Governing the Exploration and Use of Outer Space in Times of Peace and War*, in 'ELSA magazine', Vol. 8, No. 2, 2008. Available at https://openaccess.leidenuniv.nl/

MCGUINNESS, D., *How a Cyber Attack Transformed Estonia,* 27 April 2017. Available at https://www.bbc.com/

MEDETSKY, A., *KGB Veteran Denies CIA Caused '82 Blast*, 18 March 2004. Available at http://oldtmt.vedomosti.ru/

METCALF, K., *A Legal View on Outer Space and Cyberspace: Similarities and Differences*, Tallinn, 2018. Available at https://ccdcoe.org/

MEYER, P., *The CD and PAROS. A Short History*, UNIDIR Resources, April 2011. Available at https://www.unidir.org/

MOON, M., *The Space Domain and Allied Defence*, NATO Parliamentary Assembly, 2017. Available at https://www.nato-pa.int/

MORRISON, R., *Broadband in Space*!, 13 February 2020. Available at https://www.dailymail.co.uk/

NASA Financial Report 2012. Available at www.nasa.gov

NATO, 'Assured access to the Common Globals, Findings and Recommendations', April 2011. Available at http://act.nato.int/

PAGANINI, P., *Satellite Infrastructures - Principal Cyber Threats*, Rome, 3 December 2013. Available at www.aofs.org

PANDA, A., *'No First Use' and Nuclear Weapons*, 17 July 2018. Available at https://www.cfr.org/

PARDINI, V. AND ANSELMO, L., *Evolution of the Debris Cloud Generated by the Fengyun-1c Fragmentation Event,* 2007. Available at https://ntrs.nasa.gov/

PAULAUSKAS, K., *Space: NATO's Latest Frontier*, 13 March 2020. Available at https://www.nato.int/

PELLEGRINO, M. AND STANG, G., *Space Security for Europe*, ISSUE Report No. 29, Paris, 2016. Available at https://espas.secure.europarl.europa.eu/

PELLEGRINO, M., PRUNARIU, D. AND STANG, G., *Security In Space: Challenges to International Cooperation and Options for Moving Forward*, 67th International Astronautical Congress (IAC), Guadalajara, 26-30 September 2016. Available at https://swfound.org/

POLLPETER, K., CHASE, M. AND HEGINBOTHAM, E., *The creation of the PLA Strategic Support Force and its implications for Chinese military space operations*, Santa Monica, 2017. Available at www.rand.org

PORTEOUS, H., *The Stuxnet Worm: just Another Computer Attack or a Game Changer?*, Publication No. 2010-81-E Ottawa, Canada, Library of Parliament (2010), Available at http://publications.gc.ca/

RAIN, O., *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective,* Tallinn, CCDCOE. Available at https://ccdcoe.org/

RAJESWARI PILLAI RAJAGOPALAN, *Assessing the British Proposal on Space Security*, 10 December 2020. Available at https://thediplomat.com/

RAJESWARI PILLAI RAJAGOPALAN, *Electronic and Cyber Warfare in Outer Space*, UNIDIR, May 2019. Available at https://www.unidir.org/

RID, T., *Cyberwar and Peace: Hacking Can Reduce Real-World Violence*, 2013, p. 79. Available at https://ridt.co/

RID, T., *Think Again: cyberwar*, 27 February 2012. Available at https://foreignpolicy.com/

RUSSELL, A., *CIA Plot led to Huge Blast in Siberian Gas Pipeline*, 28 February 2004. Available at https://www.telegraph.co.uk/

SANTAMARTA, R., *A Wake-up Call for SATCOM Security*, IOActive Research, 2014. Available at https://ioactive.com/

SCHMITT, M. AND VIHUL, L., *The Nature of International Cyber Norms*, CCDCOE, Tallinn Paper No. 5, Special Expanded Issue 2014. Available at https://ccdcoe.org/

SCHNEIER, B., *Cyberattacks against NASA*, 4 December 2008. Available at https://www.schneier.com

SCHULTE, G., *Protecting Global Security in Space*, Presentation at the S. Rajaratnam School of International Studies Nanyang Technological University, Singapore May 9, 2012. Available at https://archive.defense.gov/

SET, S., *India's Space Power: Revisiting the Anti-Satellite Test*, Carnegie Endowment for International Peace, September 2019. Available at https://carnegieendowment.org/

SETTER, K., *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*, 11 March 2014. Available at https://www.wired.com/

SHACKELFORD, S., *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, Conference on Cyber Conflict Proceedings 2010, CCD COE Publications Tallinn, (2010). Available at https://ccdcoe.org/

STANG, G., *Global Commons: Between Cooperation and Competition*, European Union Institute for Security Studies, April 2013. Available at https://www.iss.europa.eu/

STANLEY, M., *Space: Investing in the Final Frontier*, 2 July 2019. Available at www.morganstanley.com

STELMAKH, O., *Global Space Governance for Sustainable Development*, Presentation during the UNISPACE+50 HLF, Dubai, 2016. Available at www.oosa.org

STOUTLAND, P. AND PITTS-KIEFER, S., *Nuclear Weapons in the New Cyber Age*, Report of the Cyber-Nuclear Weapons Study Group, 2018. Available at www.nti.org

SVANTESSON, D., AZZOPARDI, R., BONYTHON, W., CROWE, J., FREELAND, S., HAATAJA, S., IRELAND-PIPER, D., MARK, N., *The Developing Concept of Sovereignty. Considerations for Defence Operations in Cyberspace and Outer Space*, June 2021. Available at https://research.bond.edu.au/

TAIATU, C., *Space Traffic Management: Top Priority for Safety Operations*, 60th IISL Colloquium on the Law of Outer Space, Adelaide, 26 September 2017. Available at https://iislweb.org

TANASE, S., *Satellite Turla: APT Command and Control in the Sky*, 9 September 2015. Available at https://securelist.com/

THÜRER, D., *Soft Law*, in 'Max Planck Encyclopedia of Public International Law', March 2009. Available at https://opil.ouplaw.com/

TIKK, E. AND KERTTUNEN, M., *The Alleged Demise of the UN GGE: An Autopsy and Eulog,* Cyber Policy Institute (2017). Available at https://cpi.ee/

TIKK, E., KASKA, K. AND VIHUL, L., *International Cyber Incidents: Legal Considerations*, Tallinn, 2010. Available at https://ccdcoe.org/

TÜLLMANN, T. et. al., *On the Implementation of a European Space Traffic Management System*, STM Tuellman, DLR GfR, June 2017. Available at https://elib.dlr.de/

VÄLJATAGA, A., *Tracing Opinio Juris in National Cyber Security Strategy Documents*, Tallinn, 2018. Available at https://ccdcoe.org/

VALO, J., *Cyber Attacks and the Use of Force in International Law*, Master Thesis, University of Helsinki, January 2014. Available at https://helda.helsinki.fi/

VILLORESI, P., *Quantum Communications in Space*, 19 February 2019. Presentation available at www.unoosa.org

VIVERO, J. AND DEL MONTE, L., *Space Missions Cybersecurity*, SpaceOps 2014 Conference, Pasadena, 2014. Available at https://arc.aiaa.org/

VON DER DUNK, F., *Contradictio in terminis or Realpolitik? A Qualified Plea for a Role of 'Soft Law' in the Context of Space Activities*, University of Nebraska Faculty Publications, 2012. Available at https://digitalcommons.unl.edu/

VON DER DUNK, F., *The 1972 Liability Convention. Enhancing Adherence and Effective Application,* in Proceedings of the Forty-First Colloquium on the Law of Outer Space, Vienna, 23 March 1998. Available at https://digitalcommons.unl.edu/

WALDRON, K., *Space: the Last Frontier for Cybersecurity*, 28 July 2018. Available at https://thehill.com/

WALL, M., *China Launches Pioneering 'Hack-Proof' Quantum-Communications Satellite,* 16 August 2016. Available at www.space.com

WATERMAN, S., *Space Industry Seeks Designation as Critical Infrastructure*, 14 October 2019. Available at https://www.airforcemag.com/

WEEDEN, B. AND SAMSON, V. (eds), *Global Counterspace Capabilities: an Open Source Assessment*, Colorado-Washington, 2019. Available at https://swfound.org/

WEEDEN, B., *Iridium-Cosmos Collision*, Fact Sheet, Updated November 10, 2010. Available at https://swfound.org/

WEEDEN, B., *Space Security Index 2019. Featuring a Global Assessment of Space Security*, Ontario, 2019. Available at https://spacesecurityindex.org/

WEISS, G., *The Farewell Dossier*, 1996. Available at https://www.cia.gov/

WILLIAMS, M., *Safeguarding Outer Space: on the Road to Debris Mitigation, in Security in Space: The Next Generation*—Conference Report, 31 March–1 April 2008, UNIDIR, 2008. Available at https://unidir.org/

WILSON, T., *Threats to United States Space Capabilities*. Available at http://www.fas.org/

WINGFIELD, T., *Legal Aspects of Offensive Information Operations in Space*, Department of Defense Washington DC, 2005. Available at https://apps.dtic.mil/

WOLFRUM, R., *Cooperation,* in Max Planck Encyclopedia of Public International Law, updated April 2010 (online version). Available at https://opil.ouplaw.com/

WOLFRUM, R., *The Principle of the Common Heritage of Mankind*, in 'Zeitschrift für Ausländisches Öffentliches Recht und Völkerrecht', 1983. Available at https://www.zaoerv.de/

YATSU, M., *Not Only China: Quantum Satellite Communication on the Rise in the Indo-Pacific*, 26 September 2018. Available at www.thediplomat.com

ZEMANEK, K., *Armed attack*, in Max Planck Encyclopedia of Public International Law, updated April 2010 (online version). Available at https://opil.ouplaw.com/

ZORN, E., *Israel's Quest for Satellite Intelligence*, 8 May 2007. Available at https://www.cia.gov/

***

A Basic Guide to Nanosatellites. Available at https://alen.space/

African Space Policy towards Social, Political and Economic Integration. Available at https://au.int/

Allied Joint Doctrine for Air and Space Operations, NATO Standard AJP-3.3, Edition B Version 1, April 2016. Available at https://www.japcc.org/

Assessment of International Legal Issues in Information Operations, Department of Defense, Office of General Counsel. Available at https://fas.org/

*Assured Access to the Global Commons*, NATO Allied Command Transformation, April 2011. Available at https://www.act.nato.int/

*Bold Orion Weapons System 199 (WS-199B)*. Available at https://www.globalsecurity.org/

Brussels Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021. Available at https://www.nato.int/

Cabinet Office of the United Kingdom, Public Summary of Sector Security and Resilience Plans, December 2017. Available at www.gov.uk/

China's National Cyberspace Security Strategy, an English version is available at https://chinacopyrightandmedia.wordpress.com/

Club of Rome Official Website. Available at https://www.clubofrome.org/

Commission on Global Governance, *Our Global Neighbourhood*, 1995. Available at https://www.gdrc.org/

Convention on International Information Security (Russian Federation). Available at http://www.mid.ru/

Cyber Security Strategy of New Zealand (2015). Available at the ITU Repository: https://www.itu.int/

Cybersecurity and Infrastructure Security Agency of the United States. Available at https://www.cisa.gov/communications-sector

Decision by the Information Security Council of Japan, Action Plan on Information Security Measures for Critical Infrastructure, 13 December 2005. Available at https://www.nisc.go.jp/

*Defence Space Research Agency: Modi govt approves new body to develop space warfare weapon systems*, in 'India Today', 11 June 2019. Available at https://www.indiatoday.in/

Director of Central Intelligence, *The Soviet Gas Pipeline in Perspective*, 21 September 1982. Available at https://www.cia.gov/

Doctrine of Information Security of the Russian Federation, 5 December 2016. Available at https://www.mid.ru/

DOD Dictionary of Military and Associated Terms, as of May 2019. Available at https://www.jcs.mil/

Draft CoC version of 31 March 2014. Available at https://eeas.europa.eu/

Emmanuel Macron's Speech at the Hotel de Brienne, 13 July 2019. Available at https://www.elysee.fr/

ENISA Strategy 1016-2020, January 2016. Available at https://www.enisa.europa.eu/

*Estonia's reaction to cyber attacks influenced global security policy',* 25 April 2017. Available at https://news.err.ee/

EU Explanation of Vote – UNGA First Committee: No First Placement of Weapons in Outer Space, New York, 2 November 2018. Available at https://eeas.europa.eu/

European Code of Conduct for Space Debris Mitigation, 28 June 2008. Available at https://www.unoosa.org/

European External Action Service official website. Available at https://eeas.europa.eu/

European Space Agency official website. Available at https://www.esa.int/

Executive Order on Encouraging International Support for the Recovery and Use of Space Resources, 6 April 2020. Available at https://www.whitehouse.gov/

Final Report of the World Telecommunication Development Conference (WTDC-17), Buenos Aires, Argentina, 9-20 October 2017. Available at https://www.itu.int/

Government of Japan, The Cybersecurity Policy for Critical Infrastructure Protection, April 18, 2017. Available at https://www.nisc.go.jp/

Government of the Netherlands, 'Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW', 4 October 2010. Available at https://www.government.nl/

Government of the United Kingdom official website. Available at https://www.gov.uk/

Government of United Kingdom, *UK and Allies Reveal Global Scale of Chinese Cyber Campaign*, 20 December 2018. Available at https://www.gov.uk/

*Hackers Could Shut Down Satellites – or Turn Them into Weapons*, 12 February 2020. Available at https://theconversation.com/

*How the Dutch foiled Russian 'cyber-attack' on OPCW*, 4 October 2018. Available at https://www.bbc.com/

IASL-IAASS Webinar Series IV, 'Constraints on Military Uses of Outer Space: What Might International Law Offer?', Panel by Paul Meyer. Available at https://www.mcgill.ca/

ICRC Commentary on Protocol Additional to the Geneva Conventions of 12 August 1949, 1987. Available at https://www.icrc.org/

IISL Working Group on Cyber Law, Report by Stephan Hobe, Cologne, 2018. Available at https://iislweb.org/

Information Security Doctrine of the Russian Federation (2008). English text available at the ITU Repository https://www.itu.int/

International Court of Justice Official Website. Available at https://www.icj-cij.org/en/declarations

*International Space Station attacked by 'virus epidemics'*, 12 November 2013. Available at https://www.theguardian.com/

International Strategy for Cyberspace of the United States (2011). Available at https://obamawhitehouse.archives.gov/

International Strategy of Cooperation on Cyberspace of China (2017). Available at https://www.fmprc.gov.cn/mfa_eng/

Intervention by the Alternate Representative and Charge d'Affaires of Italy to the United Nations, Ambassador Inigo Lambertini in multilateral negotiations on an 'international code of conduct on space activities', 27 July 2015. Available at http://www.italyun.esteri.it/

Introductory remarks by the Director of OOSA, 22 October 2019. Available at http://www.unoosa.org/

ITU Cybersecurity National Strategy Guide, September 2011. Available at https://www.itu.int/

Joint Chiefs of State, *The Joint Force in a Contested and Disordered World,* 2016. Available at https://www.jcs.mil/

Joint Panel Discussion of the First and Fourth Committees on possible Challenges to Space Security and Sustainability. Available at https://www.unoosa.org/

London Declaration issued by the Heads of State and Government participating in the Meeting of the North Atlantic Council in London 3-4 December 2019. Available at https://www.nato.int/

*Making the Connection: The Future of Cyber and Space*, International Security Workshop Summary-Chatham House Royal Institute, 24 January 2013. Available at www.chathamhouse.org

Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems, 4 September 2020. Available at https://www.whitehouse.gov/

Ministry of Defence of the Russian Federation, Aerospace Forces. Available at https://eng.mil.ru/

Ministry of Defense and Self-Defense Forces of Japan, Launch of the Space Operations Squadron, Japan Defense Focus No. 125, July 2020. Available at https://www.mod.go.jp/

Ministry of External Affairs of India official website. Available at https://mea.gov.in/

Munich Security Conference 2020 (Westlessness). Available at https://securityconference.org/

National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD23), 8 January 2008. Available at https://irp.fas.org/

NASA Report, *Cybersecurity Management and Oversight at the Jet Propulsion Laboratory*, June 2019. Available at https://oig.nasa.gov/

National Oceanic and Atmospheric Administration Final Report, *Significant Security Deficiencies in NOAA's Information Systems Create Risks in Its National Critical Mission*, 15 July 2014. Available at https://www.oig.doc.gov/

National Security Decision Directive No. 42, "National Space Policy", July 4, 1982, available at https://www.hq.nasa.gov/

National Strategic Framework for Cyberspace Security, December 2013 (Italy). Available at the ITU Repository: https://www.itu.int/

Order of the State Council of the People's Republic of China no. 745, published on 16 August 2021. Available at http://www.gov.cn/

Our Common Agenda, Report of the Secretary-General, United Nations, New York, 2021. Available at https://www.un.org/

Outer Space Act 1986 of the UK, available at https://www.legislation.gov.uk/

Position Paper on Space Debris Mitigation, Implementing Zero Debris Creation Zones, International Academy of Astronautics, ESA, Noordwijk, 15 October 2005. Available at http://www.esa.int/

Presidential Decision Directive/NSC-49/NSTC-8, National Space Policy, September 14, 1996. Available at https://irp.fas.org/

Presidential Directive on National Space Policy, 11 February 1988. Available at https://www.hq.nasa.gov/

Presidential Directive NSC-37, "National Space Policy", May 11, 1978. Available at https://www.hq.nasa.gov/

Presidential Policy Directive -- Critical Infrastructure Security and Resilience, The White House, Office of the Press Secretary, 12 February 2013. Available at https://obamawhitehouse.archives.gov/

Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City, 11 October 2012. Available at https://archive.defense.gov/

Report by the Chair of the Group of governmental experts on further practical measures for the prevention of an arms race in outer space, New York, 31 January 2019. Available at https://www.un.org/

Report to Congress - Kosovo Operation Allied Force. Available at https://archive.org/

Report to the Commission to Assess United States National Security Space Management and Organization, 11 January 2001. Available at https://spp.fas.org/

*Russia Committed to Full Demilitarization of Outer Space*, 24 July 2020. Available at https://tass.com/

Second Manfred Lachs International Conference on Global Space Governance, held at McGill University, Montreal, 29-31 May 2014. Available at https://www.mcgill.ca/

Selected Examples of National Laws Governing Space Activities. Available at https://www.unoosa.org/

*Sochi 2014 Olympic Torch Makes Historic Space Walk*, 9 November 2013. Available at https://www.olympic.org/

Sources: CIA gets go-ahead to destabilize Yugoslavia, 24 May 1999. Available at www.edition.cnn.com/

Space Command Public Affairs Office, *Russia Conducts Space-Based Anti-Satellite Weapons Test*, 23 July 2020. Available at https://www.spacecom.mil/

Space Security 2010 from Foundations to Negotiations, UNIDIR Conference Report, Geneva, 29-30 March 2010. Available at https://www.unidir.org/

Speech by Judge Rosalyn Higgins, President of the International Court of Justice to the Sixth Committee of the General Assembly, 2 November 2007. Available at https://www.icj-cij.org/

*Sri Lankan Terrorist Attacks*, 13 April 2017. Available at http://www.impactlab.net

Statement by Representative of the Russian Federation Andrei Belousov in the First Committee of the 74th Session of the UNGA on cluster 3 Outer Space (disarmament aspects). Available at https://russiaun.ru

Statement by the Head of the Chinese delegation, H. E. Ambassador Shi Zhongjun at the UNISPACE+50 high-level segment 20 June 2018, Vienna, Austria. Available at https://www.unoosa.org/

Supporting Diplomacy: Clearing the Path for Dialogue, UNIDIR Space Security Conference 2019, 28-29 May, Geneva, 2019. Available at https://www.unidir.org/

Telegram 443 from the Department of State to the Mission at the United Nations, Washington, August 18, 1958. Available at https://history.state.gov/

The Critical Infrastructure Protection in France, January 2017. Available at http://www.sgdsn.gouv.fr/

The European Space Policy, presentation made on 13 June 2008, Vienna. Available at https://www.unoosa.org/

The French Ministry for the Armed Forces, Space Defence Strategy, Report of the 'Space' working group, 2019. Available at https://www.defense.gouv.fr

*The International Space Station Struggles with Computer Virus Infections Contracted by Astronauts*, 13 November 2013. Available at https://www.news.com.au/

The National Medium- and Long-Term Program for Science and Technology Development (2006-2020). English text available at the ITU Repository https://www.itu.int/

*Transcript: Tech expert Ben Buchanan talks with Michael Morell on 'Intelligence Matters'*, 19 February 2020. Available at https://www.cbsnews.com/

U.S.-China Economic and Security Review Commission, 2011 Report to Congress of the U.S.-China Economic and Security Review Commission, Washington, 2011. Available at https://www.uscc.gov/

U.S.-China Economic and Security Review Commission, 2015 Report to Congress of the U.S.-China Economic and Security Review Commission, Washington, 2015. Available at https://www.uscc.gov/

U.S.-China Economic and Security Review Commission, 2019 Report to Congress of the U.S.-China Economic and Security Review Commission, Washington, 2019. Available at https://www.uscc.gov/

UK Space Command, published on 1 April 2021. Available at https://www.gov.uk/

United States Department of Justice, *Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information*, 20 December 2018, available at https://www.justice.gov/

United States Department of Justice, *U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations*, 4 October 2018. Available at https://www.justice.gov/.

United States Space Force Official Website. Available at https://www.spaceforce.mil/

United States, Department of State press release, Hillary Rodham Clinton, Secretary of State, International Code of Conduct for Space Activities, 17 January 2012. Available at https://www.state.gov/

United States, National Military Strategy for Cyberspace Operations (NMS-CO), December 2006. Available at https://www.hsdl.org/

University of Adelaide Official Website. Available at https://law.adelaide.edu.au/

Unofficial translation of France's 'LOI no 2008- 518 du 3 juin 2008 relative aux opérations spatiales'. Available at https://aerospace.org/

Updated inventory chart of General Assembly resolutions on the revitalization of the work of the General Assembly, issued pursuant to resolution 74/303, draft as of 3 February 2021. Available at https://www.un.org/

US Explanation of Vote in the First Committee on Resolution: L.50, 'No First Placement of Weapons in Outer Space', New York, 5 November 2018. Available at https://geneva.usmission.gov/

US Joint Chiefs of Staff, Joint Publication 3-14, Space Operations, 10 April 2018. Available at https://fas.org/

US National Security Space Strategy, January 2011. Unclassified summary available at https://www.dni.gov/

US National Security Strategy, May 2010. Available at https://obamawhitehouse.archives.gov/

US National Space Policy, 31 August 2006. Available at https://history.nasa.gov/

US Strategic Defense Initiative, 1983. Available at https://2001-2009.state.gov/

View of the Ministry of Foreign Affairs and Trade of Australia on the Space Sustainability Conference, Beijing, 2012. Available at https://swfound.org/

Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 5 September 2014. Available at https://www.nato.int/

*War in the fifth domain. Are the mouse and keyboard the new weapons of conflict?*, 1 July 2010. Available at https://www.economist.com/

Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016. Available at https://www.nato.int/

White House Fact sheet, 23 March 2018. Available at https://www.whitehouse.gov/

Working Together to Forge a New Partnership of Win-win Cooperation and Create a Community of Shared Future for Mankind, Statement by H.E. Xi Jinping President of the People's Republic of China At the General Debate of the 70th Session of the UN General Assembly, New York, 28 September 2015. Available at https://www.fmprc.gov.cn/mfa_eng/

**MISCELLANEOUS**:

Additional Protocol to the 1967 'Outer Space Treaty, formally the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies', CD/9, 26 March 1979.

Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity, OAS General Assembly Res AG/RES. 2004 (XXXIV-O/04), 8 June 2004.

Commission Communication (EC), Critical Infrastructure Protection in the fight against terrorism, COM (2004) 702 final, 20 October 2004.

Commission Communication (EC), European Programme for Critical Infrastructure Protection, COM (2006) 786 final, 12 December 2006.

Commission Communication (EC), European Space Policy, COM (2007) 212, 26 April 2007.

Commission Communication (EC), Green Paper on a European Programme for Critical Infrastructure Protection, COM (2005) 576, 17 November 2005.

Commission Communication (EC), Space: a new European Frontier for an Expanding Union – An Action Plan for implementing the European Space Policy (White Paper), COM (2003) 673 final, 11 November 2003.

Commission Communication (EC), The Community and Space: a Coherent Approach, COM (88) 417 final, 26 July 1988.

Commission Communication (EC), Towards a European Space Policy, COM (2001) 718, 7 December 2001.

Commission Communication (EU), The EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final, 16 December 2020.

Commission Communication (EU), Towards a Space Strategy for the European Union that Benefits its Citizens, COM (2011) 152 final, 4 April 2011.

Commission Staff Working Document (EU), Executive Summary of the Evaluation of Council Directive 2008/114 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection, SWD (2019) 308 final, 23 July 2019.

Commission Staff Working Document (EU), New approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure, SWD (2013) 318 final, 28 August 2013.

Commission Working Document (EC), Towards a coherent European approach for space, SEC (1999) 789 final, 7 June 1999.

Council (EU) Draft Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Toolbox'), 9916/17, 7 June 2017.

Council (EU) Implementing Regulation 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 246/4.

Council (EU), Conclusions and Draft Code of Conduct on Space Activities, 17175/08, 17 December 2008.

Council (EU), Conclusions of 27 September 2010 on a Revised Draft Code of Conduct on space activities, 14455/10, 11 October 2010.

Council (EU), EU Statements in Multilateral Organizations: General Arrangements, 15901/11, 24 October 2011.

Council (EC), Presidency Conclusions, 11177/1/07 REV 1, 20 July 2007.

Council (EU), Proposal for a Regulation of The European Parliament and of the Council establishing the space programme of the Union and the European Union Agency for the Space Programme, 15490/18, 14 December 2008.

Council (EC), Resolution on the European Space Policy, 10037/07, 25 May 2007.

Council Decision (CFSP) 2015/203 of 9 February 2015 in support of the Union Proposal for an International Code of Conduct for Outer-Space Activities as a Contribution to Transparency and Confidence-Building Measures in Outer-Space, OJ L 33/38.

Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 129 I/13.

Council Directive (EU) 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, OJ L 345/75.

Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 129 I/1.

Draft Articles on the Law of the Treaties with commentaries, *Yearbook of the International Law Commission, 1966*, vol. II, pp. 187-274.

European Economic and Social Committee, Opinion on the Communication from the Commission to the Council and the European Parliament: European Space Policy, COM (2007) 212 final, INT/360, 13 February 2008.

European Parliament (EC), Resolution on Community Participation in Space Research, OJ C 127/42, 21 May 1979.

European Parliament (EC), Resolution on European Space Policy, OJ C 190/78, 20 July 1987.

Parliament and Council Directive (EU) 2016/1148 of 6 July 2016 concerning Measures for a High Common Level of Security of Network and Information Systems across the Union, OJ L 194/1.

Parliament and Council Regulation (EU) 2021/696 of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU, OJ L 170/69.

Cyber Space Strategy of the Argentine Republic (2019), Government Secretary of Modernization, Resolution 829/2019 (free translation).

Declaration of Principles of the World Summit on Information Society, 12 December 2003, WSIS-03/GENEVA/DOC/4-E.

ILA Resolution 3/2002: New Delhi Declaration of Principles of International Law Relating to Sustainable Development, in ILA Report of the Seventieth Conference in New Delhi, 2-6 April 2002.

International Atomic Energy Agency Report, GOV/2010/62, 23 November 2010.

LEE, J., *Counterspace Operations for Information* (Thesis presented to the Faculty of the School of Advanced Airpower Studies), Alabama, 1994.

ITU Resolution 130 (Rev. Dubai, 2018).

Letter dated 10 June 2014 addressed to the Acting Secretary-General of the Conference on Disarmament from the Permanent Representative of the Russian Federation and the

Permanent Representative of China, for which the Date in Chinese texts and Russian Draft Treaty are transmitted for the Prevention of Weaponisation of Outer Space and the Threat or Use of Force against Objects in Outer Space, presented by the Russian Federation and China, CD 1985, 12 June 2014.

Plan of Action of the World Summit on Information Society, 12 December 2003, WSIS-03/GENEVA/DOC/5-E.

Possible Elements for a Future International Legal Agreement on the Prevention of the Deployment of Weapons in Outer Space, the Threat or Use of Force Against Outer Space Objects (China, The Russian Federation, Vietnam, Indonesia, Belarus, Zimbabwe and Syrian Arab Republic), CD/1679, 28 June 2002.

Public Law 114 - 90 - U.S. Commercial Space Launch Competitiveness Act of 2015.

Public Law 107–296 US Homeland Security Act of 2002.

Public Law 107- 56 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.

Recommendation ITU–T X.1205, Approved on 18 August 2008.

Report of the Conference on Disarmament (1984), General Assembly 39th Session, UN Doc. A/39/27.

Report of the Ad Hoc Committee on Prevention of an Arms Race in Outer Space, CD/641, 6 August 1985.

Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, 28 May 2021(only draft available at this stage).

Rules of Procedure of the Conference on Disarmament, CD/8/Rev. 9, 19 December 2003.

Strategy for Homeland Defense and Civil Support of the United States (2005), Department of Defense.

Treaty on Outer Space: Hearings before the Committee on Foreign Relations, United States Senate, Ninetieth Congress, first session, on Executive D, 90th Congress, First Session, 7, 13 March and April 12, 1967.

(*) Materials marked with an asterisk were not cited but consulted.