The Exercise of Vital Powers: Rules of Military Cyber Operations in Outer Space

Roy Balleste

A thesis submitted to McGill University in partial fulfillment of the requirements of the degree of Master of Laws (LL.M. in Air and Space Law)

August 14, 2019

Dedication

This thesis is dedicated to three individuals…

To Enarda Çuni Balleste… *Nada… Sometimes we want to change the past and we dream about the future, but all we have is the present and an opportunity to make a difference. It is in this present time that I met You, the day my life began, and now we dream of the great expanse and the other side of the universe.*

To Arya Balleste… *The sun is coming up... You mother and I await for your arrival… When I began this thesis I had not realized that you were on the way… You will make the world brighter and reach for the stars.*

To the late Juan Senyed Deynes… *In his wise way he once observed that humanity can achieve greatness in peace.*

Acknowledgments

It is a pleasure to thank those who supported the work of this thesis, and my learning process in the field of air and space law. To them I owe a debt of gratitude.

First, my deepest and most sincere gratitude to Professor *Ram Jakhu*, my thesis advisor, for being more than a professor—a wise guide during the journey— for the most interesting discussions and invaluable support. I truly lack the appropriate words to express my appreciation for his encouragement, motivation, and class discussions. Professor Jakhu took the time to meet with me and guide me, and in this manner, my opportunity to attend the Institute of Air and Space Law was enriched significantly. Ram Jakhu is someone that I will always respect and admire for his kindness, his insights, and for his positive thoughts about the future. I am forever grateful.

I offer my deepest gratitude to my wife, *Enarda Çuni Balleste*, for her support, patience, and understanding while I worked on this project. Thank you for sharing my dreams of the stars and future exploration of the universe. I also offer my gratitude to *Ana M. Negron*, my mother, who always takes the time to listen to my stories about outer space.

I would like to thank the professors and staff of the Faculty of Law and the Institute of Air and Space Law, in particular, *Ludwig Weber*, *Tanveer Ahmad*, and *Maria D'Amico*. My deepest gratitude to the office of Graduate Studies: Associate Dean *Andrea Bjorklund*, Associate Dean *Richard Gold*, *Pasqualina Chiarelli*, *Bianca Bourgeois*, and *Nozomi Kanekatsu*, for all the work they do and outstanding support of all graduate students.

I am indebted to the following individuals at *St. Thomas University School of Law*, which left a positive mark in my journey: *Syvlia Ospina*, Professor and Advisor of the Space Law Moot Court team. I am grateful for her caring and showing me how important space law is to the world. *Alfredo Garcia*, Dean and Professor of Law, *Cecile Dykas*, Associate Dean for Academic Affairs, *Siegfried Wiessner*, Professor of Law and Director of the Graduate Program in Intercultural Human Rights, *Roza Pati*, Professor of Law & Executive Director of the Graduate Program in Intercultural Human Rights, and *Sonia Luna-Lamas*, Associate Director and Head of Technical Services.

I offer my appreciation to *Don Blumenthal*, former member of the Security and Stability Advisory Committee (*SSAC*) of the Internet Corporation for Assigned Names and Numbers (ICANN), for his time and wise discussions of internet governance. He will be forever missed.

I would also like to thank my fellow students at the Institute. Their encouragement was invaluable throughout the year. I would specifically like to thank my dear friends *Humaid Alshami* and *Michelle L.D. Hanlon* for their friendship and encouragement. It was truly a rewarding experience and I will never forget.

Lastly, I offer my deepest regards and gratitude to my dear friends from the outstanding McGill Law Graduate Class of 2016-2017, and those individuals not mentioned that supported me in any manner during the completion of the thesis.

Summary

The world has changed in many ways in modern times, and technology has been a key element in that change. The law applicable to military uses of cyberspace in outer space is in flux. The much simpler days of the ARPA Internet are over. The Internet, or cyberspace, as it now commonly designated by the US military, is a strategic vulnerability. Cyberspace is also defined as a domain analogous to a physical space. As States seek ways to protect their national critical infrastructure sectors, the international community wrestles with the legal challenges associated with innate vulnerabilities identified by malicious online attacks. Military activities in outer space, by default, will require some degree of cyberspace utilization. This thesis proposes a process to develop rules for cyberspace applicable to military uses in outer space. There cannot be peaceful activities in space without cybersecurity. The rule development process proposed considers the gaps in the law and the unwillingness of States to enforce the law as it exists. In addition, international space law has a rich array of treaties and principles that offer a foundation applicable to cyber operations in outer space. For present day scholars, thus, there is an opportunity to work at the intersection of cyberspace and outer space. This also means that some of the terrestrial ambiguities must be better clarified for purposes of outer space. This thesis is organized in five chapters. *Chapters 1* provides an introduction to the subjects and the methodological approach of the thesis. *Chapter 2* discusses the problem in need of resolution. The problem to be addressed begins with understanding cyberthreats. These cyberthreats illustrate weapons and case studies to demonstrate a problem of perceptions born out of real-life examples. As this chapter observes, the existence of cyberspace, the deployment of anti-satellite weapons, and the

challenges that follow delineate the landscape of threats, both technological and political. From these, the problem at hand and the drafting of new rules begins to emerge. *Chapter 3* sets the stage with the conflicting claims that delineate the *lex lata* of cyberspace as it is understood by the claimants. The conflicting claims in cyber law intersect the challenges illustrated as those space activities threatened by hidden dangers of global impact. *Chapter 4* delineates the applicable past trends of existing rules of engagement, suggesting future trends, and appraising existing rules. Manuals intended to clarify the applicability of international law to particular scenarios have a tall order given that cyberspace has become a factor. The dark side of innovation raises many questions, but only few answers are available. *Chapter 5* aims at seeking a solution to a problem that transcend politics, while devising new rules for cyber operations in outer space. The present domain of cyberspace is one of rising tensions. This specific ecosystem requires a new manual to guide future military activities and new rules that address cyber operations. Cyber operations exemplify a foreshadowing of what will be at the heart of the tensions anticipated at the intersection of space law and cyberspace law. This final chapter offers the *recommendations* or rules intended to address specific challenges associated with cyber operations in outer space. The thesis ends with some concluding thoughts.

Résumé

Le monde a change de nombreuses manières dans les temps modernes, et la technologie a été un élément clé dans ce changement. La loi applicable aux utilisations militarires du cyberespace dans l'espace est en pleine mutation. Les jours beaucoup plus simples de l'ARPA Internet sont révolus. L'Internet, ou cyberespace, tel qu'il est couramment

désigné par l'armée américaine, est une vulnérabilité stratégique. Le cyberespace est également défini comme un domaine analogue à un espace physique. Alors que les États cherchent des moyens de protéger leurs secteurs d'infrastructure nationaux, la communauté international se bat pour faire face aux défis juridiques aux associés aux faiblesses innées identifies par des attaques en ligne malveillantes. Les activités militaires dans l'espace extra-atmosphérique nécessiteront par défaut un certain degré d'utilisation du cyberespace. Cette thèse propose un processus permettant de définir les règles du cyberespace applicables aux utilisations militaires dans l'espace. Il ne peut y avoir d'activités pacifiques dans l'espace sans la cybersécurité Le règle de processus d'élaboration propose prend en compte les lacunes de la loi "et le refus des États d'appliquer la loi dans sa version actuelle. En outre, le droit international de l'espace contient un large éventail de traités et de principes qui constituent un fondement applicable aux cyber-opérations dans l'espace. Ainsi, pour les specialists d'aujoud'hui, il existe une opportunité de travailler à l'intersection du cyberespace et de l'espace extra-atmosphérique. Cela signifie également que certaines ambiguités terrestres devraient être mieux clarifies aux fins de l'espace extra-atmosphérique. Cette thèse est organisée en cinq chapitres.Chapitre 1 fournit une introduction aux sujets et à l'approche méthodologique de la thèse. Chapitre 2 traite du problème à résoudre. Le problème à résoudre commence par la comprehension des cybermenaces. Ces cybermenaces illustrent des armes à feu et des études de cas illustrant un problème de perceptions nées de la vie réelle. Comme le montre ce chapitre, l'existence du cyberespace, le déploiement d'armes anti-satellites et les changements qui nuisent à la creation de menaces pour la sécurité, tant du point de vue technologique que politique. A partir de là, le problème et la

redaction de nouvelles règles commencent à émerger. Chapitre 3 ouvre la voie aux revendications contradictoires qui déffinissent la lex lata du cyberespace telle qu'elle est comprise par les demandeurs. Les litiges en matière de cyber-loi recoupent les défis illustrés par les activités spatiales menaces par les dangers caches de l'impact mondial. Chapitre 4 définit les tendances antérieures applicables des règles d'engagement existantes, suggère les tendances futures et évalue les règles existantes Le droit international applicable à des scenarios particuliers est de taille, dans la mesure où le cyberespace est devenu un facteur primordial. Le côté obscure de l'innovation soulève de nombreuses questions, mais il n'existe que de rares réponses. Le domaine actuel du cyberespace est celui de tensions croissantes . Chapitre 5 a pour objectif de rechercher une solution à un problème qui transcende la politique, tout en élaborant de nouvelles règles pour les cyber operations dans l'espace. Cet écosystème spécifique nécessite un nouveau manuel pour guider les activités militaires futures et de nouvelles règles concernant les cyber-opérations. Les operations cybernétiques illustrent bien ce qui sera au coeur des tensions anticipées au croisement du droit de l'espace et du droit du cyberespace. Ce dernier chapitre propose des recommandationes ou des règles destinées à rèpondre des problems spécifiques liés aux cyber-operations dans l'espace. La thèse se termine par quelques réflexions finales.

Table of Contents

List of Abbreviations

ARPA – Advanced Research Projects Agency

ASATs – Anti-satellite weapons

CCDCOE – Cooperative Cyber Defence Centre of Excellence

CERT – Community Emergency Response Team

CoE – Council of Europe

COPUOS – United Nations Committee on the Peaceful Uses of Outer Space

CNA – computer network attack

CNE – computer network exploitation

EMP – Electromagnetic Pulse

EU – European Union

GA – United Nations General Assembly

GNSS – Global Navigation Satellite System

HPCR – The Program on Humanitarian Policy and Conflict Research

HRC – Human Rights Committee

IANA – Internet Assigned Numbers Authority

ICANN – Internet Corporation for Assigned Names and Numbers

ICJ – International Court of Justice

ICAO – International Civil Aviation Organization

ICS-CERT – Industrial Control Systems Cyber Emergency Response Team

ICTs – information and communications technologies

IGF – Internet Governance Forum

IHL – International Humanitarian Law

IO – Information Operations

ITU – International Telecommunication Union

ITRs – International Telecommunication Regulations

MRF– monitoring, reporting, and fact-finding mechanisms

NASA – National Aeronautics and Space Administration

NATO – North Atlantic Treaty Organization

NCI – NATO Communication and Information Agency

NSC – National Security Council

OST– Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (Outer Space Treaty)

SCADA – Supervisory Control and Data Acquisition

UN – United Nations

UN GGE – United Nations Governmental Group of Experts

UNIDIR – United Nations Institute for Disarmament Research

USA – United States of America (also, US)

USAF – United States Air Force

WGIG – Working Group on Internet Governance

1

In the Beginning

"Dream or nightmare, we have to live our experience as it is, and we have to live it awake. We live in a world which is penetrated through and through by science and which is both whole and real. We cannot turn it into a game simply by taking sides."
— Jacob Bronowski[1]

I. Introduction

The world has changed in many ways in modern times, and technology has been a key element in that change. The law applicable to military uses of cyberspace in outer space is in flux. In 1992, the potential for national power and prestige changed with the introduction of the commercial Internet and the ability to navigate it. In that year, the US Congress authorized the commercialization of cyberspace.[2] Two years later, Mark Andreessen and his team released the second color-graphical browser for the Web, known as Netscape.[3] By this time, the much simpler days of the ARPA Internet were over. The Internet, or cyberspace, as it now commonly designated by the US military, eventually became a strategic vulnerability.[4] *Cyberspace* was defined as a domain "analogous to a physical space where events occur separate from traditional

[1] Jacob Bronowski, *Science and Human Values* (New York: Harper Perennial, 1990) at 5.
[2] Memorandum from Robert P. Murphy, General Counsel (7 July 2000) Department of Commerce: Relationship with the Internet Corporation for Assigned Names and Numbers, B-284206, United States General Accounting Office. [Memorandum from Robert P. Murphy to Judd Gregg , Chairman, and Ernest F. Hollings Ranking Minority Member, Subcommittee on Commerce, Justice, State, and the Judiciary, Committee on Appropriations of the United States Senate, and to Harold Rogers, Chairman, and Jose Serrano, Ranking Minority Member, Subcommittee on Commerce, Justice, State, and the Judiciary, and Related Agencies, Committee on Appropriations of the House of Representatives.] *See also,* US, Bill HR 5344, *A Bill to Authorize the National Science Foundation to Foster and Support the Development and Use of Certain Computer Networks*, 102nd Cong, 1992. *See also, Scientific and Advanced-Technology Act of 1992*, 42 U.S.C. § 1862(g) (1991-1992).
[3] Janet Abbate, *Inventing the Internet* (Cambridge: MIT Press, 2000) at 216–18.
[4] Roger C. Molander, Peter A. Wilson, and Robert H. Anderson, "U.S. Strategic Vulnerabilities: Threats Against Society" in Tom LaTourrette, David R. Howell, et al., eds, *Strategic Appraisal: The Changing Role of Information in Warfare* (Washington D.C.: RAND Corporation, 1999) at 253.

geographic space."[5] The Internet (physical components, e.g. telecommunications networks and computer systems) would not be considered a synonym for *cyberspace*, but rather became that part of cyberspace that contains "the information environment consisting of interdependent networks of information technology infrastructures and resident data."[6] Cyberspace may also be defined as a domain "analogous to a physical space where events occur separate from traditional geographic space."[7] Thus, the Internet is not the same as cyberspace, but may be understood as part of cyberspace.[8] It is essential to remember that the Internet originated in the United States, and for that reason, the US Supreme Court had the first opportunity to define it within the American legal system. This definition has endured the test of time. The United States Supreme Court defined the Internet in *Reno v. ACLU* based on the purpose of "a wide variety of communication and information retrieval methods" comprising a "unique medium—known as cyberspace—located in no particular geographical location and available to anyone, anywhere in the world."[9] It is only a matter of time before this definition includes *anywhere in the solar system and beyond*. The cyberspace environment, inevitably, will eventually reach outer space. For spacefaring nations, the evolving challenge has begun to encompass cyberattacks, infrastructure threats, and much-needed mitigation practices.[10] The latest challenge for States is the need to focus on cybersecurity countermeasures on land and in outer space. An analysis of a constitutive process designed to standardize cyber operations in outer space may ultimately illustrate the difficult challenge. There cannot be peaceful activities in space without

[5] The Judge Advocate General's School, *Air Force Operations & the Law: A Guide for Air, Space, and Cyber Forces,* 3rd ed. (Alabama: Maxwell Air Force Base, 2014) at 104.
[6] *Ibid*. General Counsel of the Department of Defense, *Law of War Manual* (Washington, D.C.: Department of Defense) at § 16.1.1.
[7] The Judge Advocate General's School, *supra* note 5.
[8] *Ibid*. *See also*, General Counsel of the Department of Defense, *supra* note 6.
[9] *Reno v. ACLU*, 521 U.S. 844, 850-51; 117 S.Ct. 2329, 2334-2335; 138 L.Ed.2d 874, 851 (1997).
[10] *See*, for example, Council on Foreign Relations, "Cybersecurity and the New Era of Space Activities" (3 April 2018), online: <https://www.cfr.org/report/cybersecurity-and-new-era-space-activities>.

cybersecurity. The cyberspace ecosystem is now plagued by hidden cyberattacks with global impacts.[11] In each case, the attacks represent a complex set of events involving people, technology, facilities, and information. However, there was a time in the past when cyberspace was far safer.

A. Bygone Arpanet

In 1977, the Arpanet—which is considered the Internet's precursor—operated "in practical secrecy with a crude packet-switching system… and the first email system was five years old."[12] During this time, security vulnerabilities were not a matter of concern.[13] Yet, in 1988, "Robert Tappan Morris, a graduate student at Cornell, introduced a worm on the Internet that was designed to determine the Internet's size but that inadvertently shut down about 10 percent of the 60,000 computers then connected to it."[14] The worm released by the 23-year-old graduate student created chaos on the Internet, and the "exact damages were difficult to quantify, but estimates started at $100,000 and soared into the millions."[15] The worm spread "at remarkable speed and [ground] computers to a halt."[16] After it was over, two painful lessons were evident: the Internet was important, but vulnerable; and, "a new generation of hackers and a wave of Internet-driven assaults" had begun.[17] This became the reality that space lawyers now must understand and assimilate.

---

[11] Danny Palmer, "Cybercrime drains $600 billion a year from the global economy, says report" (21 February 2018), *ZDNet*, online: <https://www.zdnet.com/article/cybercrime-drains-600-billion-a-year-from-the-global-economy-says-report/>.
[12] Jack Goldsmith, "How Cyber Changes the Laws of War" (2013) 24:1 EJIL 129 at 129.
[13] *Ibid*.
[14] *Ibid*.
[15] U.S. Department of Justice, "The Morris Worm: 30 Years Since First Major Attack on the Internet" (2 November 2018), online: <https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218>.
[16] *Ibid*.
[17] *Ibid*.

As States seek ways to protect their national critical infrastructure sectors, the international community wrestles with the legal challenges associated with innate vulnerabilities identified by malicious online attacks. Military activities in outer space, by default, will require some degree of cyberspace utilization. The applicability of international cyber law to space activities intersects, for example, with Article III of the Outer Space Treaty (OST), highlighting States' military activities in outer space involving hacks of "the landlines that connect ground stations to terrestrial networks."[18] The applicability of the *lex generalis* international law originating with Article III of the Outer Space Treaty provides guidance by stating:

> "States Parties to the Treaty shall carry on activities in the exploration and use of outer space, including the Moon and other celestial bodies, in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international co-operation and understanding."[19]

As a result and by extension, Article III of the Outer Space Treaty provides part of the legal context for the application of international law to cyber operations in outer space. The concerns over cyber vulnerabilities have steadily become a matter of international priority and relevant to space activities. Michel Bourely explains that "[a]s soon as man began exercising certain activities in space, the international community became aware of the necessity of organizing these activates by adopting international regulations on the subject."[20] This was the first clue: new law would be needed to tackle future and emerging space activities. Indeed, he also notes that "by their very nature, space activities transgress national frontiers…"[21] Thus, this

[18] Center for Strategic and International Studies, "Space Threat Assessment 2018, Aerospace Security Project" (11 April 2018), online: <https://aerospace.csis.org/spacethreat2018/>.
[19] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, 27 January 1967, 610 UNTS 205, art III (entered into force 10 October 1967) [Outer Space Treaty].
[20] Michel Bourely, "Rules of International Law Governing the Commercialization of Space Activities" (1986) 29 Proceedings on the L of Outer Space 157 at 157.
[21] *Ibid*.

transgression, if considered from the opposite point of view, opens up new challenges and new opportunities. This has been the essence of space, and interestingly, also of cyberspace. Cyberspace was invented for a military purpose, and this purpose has evolved over time. Despite its promising future, the complexities of Internet communications have become tied to the emergent space activities of States and the commercial industry. Looking at the worldwide network of hardware parts, fiber optic cables, and antennas in a vacuum is not sufficient. The interconnection of cyberspace via ground stations and space via satellites operates within the context of the *lex lata*.

This thesis proposes a process to develop rules for cyberspace applicable to military uses in outer space. These rules offer a suggestion to fill a legal gap in the *Tallinn Manual* (Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations).[22] This manual is "the most comprehensive guide for policy advisors and legal experts on how existing international law applies to cyber operations."[23] The rule development process proposed here considers the gaps in the law and the unwillingness of States to enforce the law as it exists. In addition, international space law has a rich array of treaties and principles that offer a foundation that may be considered applicable to cyber operations in outer space. However, the treaty-founded base found in space law is unavailable within international cyberspace law. For present day scholars, thus, there is an opportunity to work at the intersection of cyberspace and outer space. This also means that some of the terrestrial ambiguities must be better clarified for purposes of outer space. This effort provides an avenue to consider the *lex lata* (as seen in Chapters 1 and 2 of this thesis) to project trends that will define the next five years, and seek a solution to problems that

[22] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).
[23] NATO Cooperative Cyber Defence Centre of Excellence, "Tallinn Manual 2.0", online: <https://ccdcoe.org/research/tallinn-manual/>.

transcend politics and devise new rules of engagement (Chapter 4 and 5). While the present cyberspace law offers political flexibility, it also represents a potential opportunity to engage in dangerous surreptitious behavior, and by extension, foreshadow political difficulties in outer space.[24] The use of cybernetworks in relation to space activities, at the onset, must be understood so as not to interfere with freedom of use. While this is discussed in greater detail in Chapter 2, it is relevant here to highlight one particular observation. Article I, paragraph 2 of the Outer Space Treaty, notes that:

> "Outer space, including the Moon and other celestial bodies, shall be free for exploration and use by all States, without discrimination of any kind, on a basis of equality and in accordance with international law, and there shall be free access to all areas of celestial bodies."[25]

The "use" of outer space, by extension, also includes cyber operations. As will be demonstrated through this thesis, the term "exploration and use"[26] can be applicable to States' cyber activities. There is no basis for excluding activities related to the use of cyberspace from the freedom and use of outer space. The members of the NATO (North Atlantic Treaty Organization) alliance noted the best and most urgent observation regarding cyber activities: "Cybersecurity threats pose challenges to individuals, corporations, states, and intergovernmental organizations."[27] This cyber-threat consideration is not surprising or novel. To acknowledge that NATO members have the ability to cooperate to face these threats is also nothing new.[28] What may be troublesome and perhaps even surprising is the inability of NATO to act. "Whether NATO can adapt its approach before a major cybersecurity crisis affects the Alliance's ability to

[24] Mette Eilstrup-Sangiovanni, "Why the World Needs an International Cyberwar Convention" (2018) 31:3 Philos. Technol. 379 at 379.
[25] Outer Space Treaty, *supra* note 19 at Article II.
[26] *Ibid* at Article I, paragraph 2.
[27] David P. Fidler, Richard Pregent & Alex Vandurme, "NATO, Cyber Defense, and International Law" (2013), 4:1 St. John's J of Intl & Comparative L 1 at 1.
[28] *Ibid*.

carry out its missions effectively remains, at the present time, in doubt."[29] These concerns about inadaptability and inability to act extend to cyber operations in outer space.

Of course, this raises the question "What should be the point of departure?" A suitable starting point could be how the historical freedom of use of outer space in conjunction with developing technological achievements have benefitted humanity. For example, the Apollo 11 mission illustrated a historic event with overall significance for humanity. On July 16, 1969 a Saturn V rocket lifted off transporting astronauts Neil A. Armstrong, Michael Collins, and Edwin E. Aldrin into the expanse of outer space.[30] Michael Collins had been selected as the member of the crew to stay orbiting "overhead in the Apollo command module."[31] Millions watched in awe as Armstrong walked on the surface of the moon, while hearing the words "One small step for man—one giant leap for mankind."[32] It was during this walk that Armstrong and Aldrin "planted an American flag but omitted claiming the land for the United States as had been routinely done during European exploration of the Americas…"[33] This historic moment opened the door to an evolution of emerging space activities and a masterful achievement of scientific standards that would become a remarkable example of the freedom of exploration of outer space. Indeed, Neil Armstrong observed that "if I wanted to get out of the atmospheric fringes and into deep space work, that was the way to go."[34] But the exploration of outer space, and probably most space activities, needed to be considered as serious business. Armstrong explained it best:

> "The unknowns were rampant. The systems in [the lunar] module had only been tested on Earth and never in the real environment. There just a thousand things to worry about in the final descent. It was hardest for the systems. And it was

[29] *Ibid*.
[30] Roger D. Launius, *APOLLO: A Retrospective Analysis* (Washington, DC: NASA History Office, NASA Headquarters, 1994) at 18.
[31] *Ibid*.
[32] *Ibid*. *See, also*, Andrew Chaikin & Victoria Kohl, *Mission Control, this is Apollo: The Story of the First Voyages to the Moon* (New York: Viking Books, 2009) at 46.
[33] *Ibid*.
[34] James R. Hansen, *First Man: The Life of Neil A. Armstrong* (New York: Simon and Shuster, Inc., 2018) at 85.

> hardest for the crew. It was the thing I most worried about, because it was so difficult."[35]

These very solemn and also insightful reflections continue to be at the center of the message contained in the 1958 *General Assembly Resolution on the Question of the Peaceful Use of Outer Space*.[36] The General Assembly, as noted in the resolution, decided to establish the United Nations Ad Hoc Committee on the Peaceful Uses of Outer Space, and is so doing, observed that it would be necessary to be mindful of "legal problems which might arise in the exploration of outer space."[37] Later, the members of the United Nations Ad Hoc Committee, Legal Committee observed that "it would be impossible to identify and define, exhaustively, all the juridical problems which might arise in the exploration of outer space."[38] In that light, our present understanding of *lex lata* seems to be challenged by the available understanding of the technology and legal tools for cyber operations. Thus, recent engineering developments inevitable lead to predictions based on projected legal trends related to those cyber operations.

II. Cyber Operations

Examining how cyber operations have evolved over time opens a window into the future state of affairs. *Cyber operations* have been defined as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."[39] These have also been defined as the "planning and synchronization of activities in and through cyberspace to enable freedom of maneuvering and to achieve military objectives."[40] These

---

[35] *Ibid* at 291.
[36] *Question of the Peaceful Use of Outer Space*, GA Res 1348(XIII), UNGAOR, 13th Sess, UN Doc A/RES/13/1348(XIII) (1958), at Preamble.
[37] *Ibid* at paragraph 1(d).
[38] *See*, Ad Hoc Committee on the Peaceful Uses of Outer Space, *Report of the Legal Committee*, UN Doc A/AC.98/2 (1959) at Paragraph A.1.
[39] U.S. Joint Chiefs of Staff, *Joint Publication 3-0, Join Operations* (17 January 2017) at GL-8.
[40] Ministry of Defence, *Joint Doctrine Publication 0-01.1, UK Terminology Supplement to NATOTerm* (January 2019, Edition A) at 11.

activities, for example, could involve "computers, software tools, or networks."[41] It is reasonable to assert that the world of cyberspace and cyber operations will evolve quickly within the next five years. Cyber operations are also defined by the purpose of two activities: *CNEs* or *CNAs*:

> An "activity encompassing reconnaissance, surveillance and the exfiltration of data and information, for example for espionage, often referred to as *computer network exploitation* (CNE), or "access operations;""[42]
>
> An "activity to generate effects on a targeted system or device, such as tampering with data integrity (deletion, modification), affecting availability (disabling, including for prolonged periods of time), or causing physical effects, such as damaging the system, often referred to as a *computer network attack* (CNA), or "effects operations.""[43]

The operations, whether exploitation or attack, need a medium or domain. C*yberspace* is "a world-wide virtual space, different from real space, with many sub-communities unevenly distributed using a technical environment – first of all the Internet – in which citizens and organizations utilize information and communication technology (ICT) for their social and commercial interactions."[44] It is also described as the "systems and services connected either directly to or indirectly to the Internet, telecommunications and computer networks."[45] The word *Internet*, in the other hand, has become a mere designation or label for what has become a much more complex arena of activities.

The word *cyberspace* has become a better designation. Indeed, the "word *cyber* is derived from an ancient Greek noun referring to a 'space' or a domain."[46] George R. Lucas noted the term *cyberspace* as redundant, yet he made it a point to explain that the "slightly redundant term

---

[41] US DoD, *Law of War Manual*, *supra* note 6 at § 16.1.2.
[42] Laurent Gisel & Lukasz Olejnik, "The Potential Human Cost of Cyber Operations" (2018) International Committee of the Red Cross at 7.
[43] *Ibid*.
[44] UNESCO, Internet Governance Glossary, online: <https://en.unesco.org/glossaries/igg>.
[45] Frederick Wamala, *The ITU National Cybersecurity Strategy* (Geneva: Switzerland, International Telecommunication Union, 2012) at 5.
[46] George R. Lucas, Jr., "Cyber Warfare" in James Turner Johnson & Eric D. Patterson, eds, *The Asgate Research Companion to Military Ethics* (Surrey: England, Asgate Publishing, 2015) at 246-47.

'cyberspace' … was first coined by science fiction writer William Gibson in a short story written in 1982, and afterwards in his novel, *Neuromancer* (1984) to describe 'clusters and constellations' of data and their interconnections drawn from every computer in the universe."[47] While it may be tempting to simply agree with Lucas, individuals traveling into outer space, while aided by information found in cyberspace, will continue to interact within a world that now, to a degree, is beyond traditional State control.

While in outer space borders are imperceptible, closer to the ground, our legal challenges stress the threats to well-established legal notions that raise doubts within present realities. This is simply the case because technology is constantly evolving. Even Albert Einstein was challenged by a new discovery in cosmology that made him doubt his own definition of the dynamism of the universe. In the same manner, cyber scholars are challenged by the dynamism of cyberspace and its potential conflict with space activities. This recalls Einstein applying "history to [describe] the universe as a whole, [and it becoming] clear that the theory didn't describe the universe in which we apparently lived."[48] Later admitting his error, Einstein faced a new outer space environment that expanded with no special point of orientation and no particular spatial direction.[49] The distant and dynamic galaxies that formed our visible sky had dispersed into large-scale distances of approximately a billion light years.[50] In this galactic environment, space lawyers face a similar conceptual challenge of definition. It is not cosmological in nature but rather technological. The constant waves of cyberattacks also seem to lack any special point of orientation and no particular spatial direction. Considering how technology creates new

[47] *Ibid*.
[48] Øyvind Grøn & Sigbjørn Hervik, *Einstein's General Theory of Relativity* (New York: Springer-Verlag, 2007) at 261-62.
[49] *Ibid*.
[50] *Ibid*.

challenges opens a window into devising new rules for cyber operations involving space activities.

III. The Methodological Process

This thesis, supported by the New Haven School of Thought, or policy-oriented jurisprudence, analyzes cyber operations in search of new norms for outer space.[51] This is the definitional challenge associated with the utilization of cyberspace in outer space that now requires new norms, which in turn can be reflected in rules intended to address activities in outer space, and as these relate to cyberspace. The methodology employed delimits the problem of cyber operations, as illustrated by space activities involving the use of cyberspace. Policy-oriented jurisprudence provides a five-step process adapted for this analysis:[52]

> (1) The *problem* of cyberthreats in outer space,
> (2) Assessment of the *conflicting claims* associated with the sources of international law applicable to existing rules of engagement,
> (3) Analysis of the *past legal trend*s,
> (4) Prediction of *future trends*, and
> (5) *Appraisal of existing* rules and offering new rules as *recommendations*.[53]

The first step or *problem* to be addressed begins with understanding cyberthreats in Chapter 1, which is presented after the introduction and methodology sections. Chapter 2 follows with cyberthreats and anti-satellite weapons that offer case studies to demonstrate a problem of perceptions born out of real-life examples. Chapter 3 follows by setting the stage with the *conflicting claims* that delineate the *lex lata* of cyberspace as it is understood by the claimants, with the applicable *past trends* of existing rules of engagement, prediction of *future trends*, and *appraisal* of existing rules in Chapter 4. The final chapter, Chapter 5, proposes needed

[51] Siegfried Wiessner, "The New Haven School of Jurisprudence: A Universal Toolkit for Understanding and Shaping the Law" (2010) 81:1 Asia Pac L Rev 45 at 47.
[52] *Ibid*.
[53] *Ibid*.

recommendations as new rules intended to address cyber operations in outer space. Cyber operations exemplify a foreshadowing of what will be at the heart of the tensions anticipated at the intersection of space law and cyberspace law. For the last two decades, the world has experienced mounting threats to consumers, corporations, and nation-states concerning cyberattacks. These attacks in turn recall space weapons programs. For astronauts, activities in outer space involve the safety and integrity of their equipment. For space lawyers, outer space is becoming a domain that requires the guidance of treaty law and other sources, although that is only a beginning. Solutions are needed to resolve new questions arising out of scientific and technological challenges, as Lachs once noted.[54] More specifically, and affixed to the evolution of warfare, the path to the peaceful use of space, and one rooted in the Outer Space Treaty, requires a normative prescription for cooperation.[55] For this reason, this thesis envisions a recommendation comprised of relevant rules that hopefully will be beneficial to the global community, or to be more precise, helpful to scholars as they face challenges with the law applicable to cyber operations in outer space.

The problem at hand is one of uncertainty similar to the days of the attacks by the German V2 rockets that traveled at the edge of the atmosphere during World War II, when States became aware of the potential military use of outer space activities.[56] Could it be said that a new norm or custom has been forming? Satellite technology exists for use in space, where their military capability may be exploited for reconnaissance, guiding weapons, and supporting other warfare

[54] North Sea Continental Shelf Cases (Federal Republic of Germany v. Denmark; Federal Republic of Germany v. Netherlands), Dissenting Opinion of Judge Lachs, [1969] I.C.J. Rep 3, at 230, online: <http://www.icj-cij.org/docket/index.php?p1=3&p2=3&case=52&code=cs2&p3=4>.
[55] Outer Space Treaty, *supra* note 19 at Article I.
[56] Regina Hagen & Jürgen Scheffran, "International Space Law and Space Security: Expectations and Criteria for a Sustainable and Peaceful Use of Outer Space" in Marietta Benkö and Kai-Uwe Schrogl, eds, *Current Problems and Perspectives for Future Regulation* (AJ Utrecht: The Netherlands, Eleven International Publishing, 2005) at 273.

activities on the surface of the Earth.[57] The nature of the utilization of space is tied directly to the activities of States, as Bourely observed, as space activities have been developed within the realm of States, "be it either on an exclusive level as is the case in some countries, or on a partial level as is the case in other countries."[58] Without a doubt, States have kept the primary control over those space activities that belong to the military.[59] But then again, military activities are linked to State sovereignty, and thus, the defense of the nation.[60] Along this line of reasoning, the rapid expansion of space-based systems in support of military operations among the major powers has been observed.[61] These activities have translated into real events, with "significant resources now devoted by each of them to the development of ever-more effective (and potent) space-related weaponry."[62] Sadly, the "prospect of a celestial war can no longer be regarded as mere fantasy."[63] As a result, the main question that encapsulates the *problem* at hand, given the endemic nature of cyberattacks, should be as follows:

> When considering new rules, how should scholars and practitioners manage future cyberattacks, or more precisely, *what should be the rules intended to address the cyber operations in outer space?*

It would be appropriate to consider that given the need to achieve superiority or self-defense, the rules of engagement will likely be disobeyed. If we are to achieve peaceful cooperation and use of outer space, then the law applicable to cyber operations in outer space must be guided by best practices during the formulation of *opinio juris*. Cyber operations may seem innocuous at first glance, yet the potential use of cyberspace as a weapon evokes Carl von Clausewitz's warning:

---

[57] *Ibid*.
[58] Michel Bourely, "The Institutional Framework of Space Activities in Outer Space" (1998) 26:1 Journal Space Law 1 at 1.
[59] *Ibid*.
[60] *Ibid* at 5.
[61] *See*, Jackson Maogoto & Steven Freeland, "The Final Frontier: The Laws of Armed Conflict and Space Warfare" (2007) 23:1 Connecticut J of Intl L 165 at 169.
[62] *Ibid*.
[63] *Ibid*.

> "Kind-hearted people might of course think there was some ingenious way to disarm or defeat the enemy without too much bloodshed, and might imagine this is the true goal of the art of war. Pleasant as it sounds, it is a fallacy that must be exposed: War is such a dangerous business that mistakes that come from kindness are the very worst."[64]

If the story of outer space exploration is intrinsically connected to the tools that humans utilize in outer space, then mistakes could evolve from these cyber operations. Aggressive operations represent a danger to human life on land, in air space, at sea, and now in outer space. For this reason, above all, a rule-making process necessitates an understanding of cyber operations illustrated by current threat perceptions.

[64] Carl von Clausewitz, *On War* (Princeton: Michael Howard and Peter Paret, eds, Princeton University Press, 1976) at 75.

2

The World in Which We Fight

"Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding..."[65]
— *William Gibson*, Neuromancer

I. The Problem: Cyberthreat Perceptions

A new age of space activities promises historical heights. While new space stakeholders move forward into a new frontier, the global community watches with hopes for a better future. These hopes are based on the primary held belief that outer space is a realm of peaceful exploration and use. At the outset, it is non-controversial to assert that peaceful uses and the benefits to humanity can be harmonious with military and commercial activities in outer space.[66] Alternatively, cyberspace poses new challenges for space lawyers. If new rules are to address cyber operations in outer space, then these must be developed quickly or risk becoming out of date. The peaceful use of outer space is at risk. As Edith Hamilton notes, "'The exercise of vital powers, along lines of excellence, in a life affording them scope' is an old Greek definition of happiness."[67] Indeed, the rules of engagement applied to cyber operations in outer space should consider that cyberattacks and the risks attached to them are antithetical to the enjoyment of human activity in space. Future determinations tied to telecommunications will need to consider that cyber-risk has become an urgent priority. Wiessner notes that a major flaw of traditional

[65] William Gibson, *Neuromancer* (New York: Penguin Random House, 2016) at 52.
[66] *See for example*, US, Law Library of Congress, Marcia S. Smith, *U.S. Space Programs: Civilian, Military, and Commercial, Resources*, Science (IB92011) (Congressional Research Service, 2006).
[67] Edith Hamilton, *The Greek Way* (New York: W. W. Norton & Company, 1930; 2017) at 27.

legal theory has been tied to assumptions that expect one correct result for the authorized decision maker "on a point of law irrespective of the personality of the decision maker, irrespective of a particular factual scenario."[68] When we turn to considerations of the law governing activities in outer space, Wiessner agrees that the law "is needed predominantly if there is a conflict in society, and it helps to know the arena and the players in which this battle is being pursued."[69] This is precisely the problem that is emerging within the activities of governments and those influenced by them in cyberspace. It is indeed conceivable that the interconnectedness between ground networks and satellites—relying on the Internet—indicate a present and future threat with the potential to escalate into military aggression. The specter of the outbreak of war in outer space forces an examination of the participation of States and coordinated cyberattacks which may be directed towards space objects.[70] In this case, States have already become entangled in cyberattacks. Surely the most remarkable fact is the numerous and complex cyber threats involving State-sponsored activities. Recently, the European Union warned about precisely these increasing cyberattacks connected to particular States such as Russia and North Korea.[71] Possibly as a legacy of the attacks against Estonia and Georgia, in an unprecedented step, the EU warned that cyberattacks could rise to the level of war.[72] In other words, as stated by the General Secretariat of the Council:

> "The EU recognizes that cyberspace offers significant opportunities, but also poses continuously evolving challenges for EU external action. The EU is concerned by the increased ability and willingness of state and non-state actors to pursue their objectives through malicious cyber activities. Such activities may constitute wrongful acts under international law and could give rise to a joint EU response. The EU reiterates that states should not knowingly allow their territory

[68] Siegfried Wiessner, *supra* note 51 at 47.
[69] *Ibid* at 49.
[70] *See*, Deborah Housen-Couriel, "Cybersecurity and Anti-Satellite Capabilities (ASAT): New Threats and New Legal Responses" (2015) 4 J.L. & Cyber Warfare 116 at 119.
[71] James Crisp, "EU Governments to Warn Cyber Attacks can be an Act of War" *The Telegraph* (29 October 2017), online: <http://www.telegraph.co.uk/news/2017/10/29/eu-governments-warn-cyber-attacks-can-act-war/>.
[72] *Ibid*.

> to be used for internationally wrongful acts using Information and Communication Technologies (ICT)."[73]

These trends propelled the Council to develop a joint diplomatic response, designated as the *cyber diplomacy toolbox*.[74] The *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Activities* (or cyber diplomacy toolbox) recognized cyberspace as a stage for opportunities, but one also open to cyber threats and malicious cyber activities.[75] In this regard, it affirmed that "malicious cyber activities might constitute wrongful acts under international law and [emphasized] that States should not conduct or knowingly support ICT activities contrary to their obligations under international law."[76] If cyberattacks are to be considered an act of war, the EU was correct in noticing that managing the attribution regarding States or non-State actors had become more problematic, given that in the end, proving the origin of an attack had to be considered in light of international law and state responsibility y.[77] These recent cyberattack events represent opportunities for disruption and fear. H.G. Wells reminded us a long time ago that when we look at the stars with their unfathomable distance, suddenly these allow our own troubles to be dwarfed along with "all the gravities of terrestrial life."[78] By the same token, far in the future, humanity's access to space, despite its calls for peaceful uses, may carry into the heavens the gravities of terrestrial life.

---

[73] *Ibid*.
[74] Council of the European Union, Press Release, 357/17, "Cyber attacks: EU ready to respond with a range of measures, including sanctions" (19 June 2017), online: <http://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/>.
[75] Council of the European Union, Secretariat, *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Activities*, Doc 9916/17 (2017) at paragraph 1, online: <http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf.>.
[76] *Ibid* at paragraph 2.
[77] *Ibid* at paragraph 4.
[78] H.G. Wells, *The Time Machine* (Mineola: NY, Dover Publications, 1995).

II. Case Studies

As this chapter observes, the existence of cyberspace, the deployment of anti-satellite weapons, and the case studies that follow delineate the landscape of threats, both technological and political. From these, the problem at hand and the drafting of new rules emerge.

A. Anti-satellite Weapons

The landscape is clearly defined by the United Nations General Assembly resolution 69/32, "No first placement of weapons in outer space."[79] This resolution, was adopted on December 2, 2014:

> "with a vote of 126 in favor, 4 against and 46 abstentions… [indicated] the growing recognition of the positive role that transparency and confidence-building measures (TCBMs) play in preventing an arms race in space (PAROS), even from the perspective of those States that… suggested the adoption of a treaty on PAROS, namely China and Russia."[80]

Yet, this resolution, although well-intended, will not become part of the normative process that this thesis is attempting to achieve. There are two main observations to be made here. First, why did the resolution fail to gain better "traction" among many important space-faring nations? And second, why do weapons in space require new norms or rules of utilization? The answer to these two questions is based on three main criticisms that were noted at the time. First, the resolution did not include a definition of a "space weapon."[81] As it was explained, "[s]everal delegations have pointed out that this fact not only creates confusion on its scope but also compromises the significance and effectiveness of a similar commitment."[82] Indeed, the

[79] *No first placement of weapons in outer space*, GA Res, UNGAOR, 69th sess, Suppl. no. 49, UN Doc A/RES/69/32 (2014).
[80] Hao Liu & Fabio Tronchetti, *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?* (2016) 38 Space Policy 64 at 64.
[81] *Ibid* at 66.
[82] *Ibid*.

basis of a well-drafted manual of rules is the definitional section. For example, the Tallinn Manual includes a glossary section, and throughout the manual, several rules were designated as *general principles* when these were intended to be foundational in nature.[83] Second, it was noted that resolution 69/32 lacked "mechanisms to verify compliance with its provisions."[84] It was expected that TCBMs [transparency and confidence-building measures] "for space should be clear, practical, and be able to be effectively confirmed by other parties in their application."[85] The third criticism could be interpreted as the other side of the coin, or another way to note that utilizing cyberspace would raise the problem of attribution. It followed then, that "certain delegations… criticized the Resolution for being silent on terrestrial-based anti-satellite weapons, a choice that might contribute to, not reduce, mistrust and misunderstanding."[86] As the US representative Cynthia Plath noted, "in space any object with maneuvering capabilities [could] in theory be used for offensive purposes."[87] She explained that the resolution failed "to address the near-term threat from other types of anti-satellite weapons, for example, lasers or terrestrially-launched systems."[88] One of the consequences, as she observed, would be "large amounts of dangerous debris in valuable orbits."[89] As an example, Plath mentioned "the case of just one single ASAT test in 2007."[90] This choice of language to describe a particular ASAT (anti-satellite weapon) event was curious, although not surprising, since it is commonly known in

[83] Schmitt, *Tallinn Manual 2.0*, *supra* note 22 at 11, 563.
[84] Liu and Tronchetti, *supra* note 80 at 67.
[85] *Ibid*.
[86] *Ibid*. *See generally*, UNODA, Prevention of an arms race in outer space, Report of the First Committee, UNGAOR, 69th Sess, UN Doc A/69/438 (2014).
[87] US Department of State, Remarks and Release, Cynthia Plath, "Explanation of Vote in the First Committee on Resolution: L.50, "No First Placement of Weapons in Outer Space"" (5 November 2018), online: < https://www.state.gov/explanation-of-vote-in-the-first-committee-on-resolution-l-50-no-first-placement-of-weapons-in-outer-space/>.
[88] *Ibid*.
[89] *Ibid*.
[90] *Ibid*.

the "space law community" that China denies that this space activity ever occurred. Unfortunately, it did occur, and with grave consequences. According to the Secure World Foundation, "On January 11, 2007, China launched a ballistic missile… (kinetic kill vehicle [KKV]) that collided with a non-operational Chinese weather satellite… completely destroying the satellite."[91] The end result was "a cloud of more than 3,000 pieces of space debris, the largest ever tracked, and much of it will remain in orbit for decades, posing a significant collision threat to other space objects."[92] This example gives way to other progressively more complicated examples of more destructive means, although perhaps not as politically intricate as cyberspace itself.

Consider in light of the hopes associated with a peaceful use of outer space that one of the means in a State's arsenal includes kinetic anti-satellite operations.[93] This ASAT deployment may include "fixed or mobile direct ascent ASAT launchers, frequently rockets, to deliver an attack vehicle to the target satellite; the placement in orbit of an interceptor vehicle that subsequently attacks the target satellite...."[94] These traditional forms of deployed missiles are set to detonate in close proximity to a satellite.[95] It has been suggested that this kind of weapon could be deployed in a manner that would be similar to the effects of space mines.[96] This type of ASAT is more of an operation to detect, track, and target enemy missiles.[97] In this case, "space-based systems may be used for the detection and tracking elements in the process, but the engagement of the missiles seems likely to involve ground-based missile systems or ground-

[91] Brian Weeden, "2007 Chinese Anti-Satellite Test Fact Sheet", *Secure World Foundation* (23 November 2010), online: <https://swfound.org/media/9550/chinese_asat_fact_sheet_updated_2012.pdf>.
[92] *Ibid*.
[93] Bill Boothby, "Space Weapons and the Law" (2017) 93 Intl L Studies Series. US Naval War College 179 at 206.
[94] *Ibid*.
[95] Blair Stephenson Kuplic, "The Weaponization of Outer Space: Preventing an Extraterrestrial Arms Race" (2014) 39:4 North Carolina J of Intl L and Commercial Regulation 1123 at 1139.
[96] *Ibid*.
[97] Boothby, "Space Weapons and the Law", supra note 93 at 208.

based lasers."[98] The difference here is that while the initial step starts on land, the final interception and destruction occurs in space.[99] In this regard, a kinetic weapon could also be utilized to directly strike a ground station.[100] A station is defined as facilities that "directly support space activities terrestrially to accomplish a mission in or through space."[101]

The threat escalates further with ground-based lasers, which cause "power loss in satellites."[102] In this case, the loss of power would result in damage, given that the targeted satellite would require additional fuel to restart and probably would fail given its limited fuel capacity.[103] Similarly, electromagnetic weapons include nuclear bombs, lasers, and particle beams.[104] A nuclear detonation would discharge an electromagnetic pulse (EMP) while triggering a cascade of gamma rays.[105] The laser would be directed as a concentrated beam at the speed of light, while the particle beam would also be directed at the speed of light, but in this case transferring thermal energy similar to a lightning bolt.[106] However, "[w]hile a nuclear detonation would have immediate effects for satellites within range of the electromagnetic pulse it creates, the primary effect of a nuclear detonation in space is that it creates a high radiation environment that accelerates the degradation of satellite components."[107] The true nature of these ASATs begins to become clear if the Outer Space Treaty is used to shed light on the gravity of

[98] *Ibid*.
[99] *Ibid* at 209.
[100] Todd Harrison, Kaitlyn Johnson & Thomas G. Roberts, "Space Threat Assessment 2018: A Report of the CSIS Aerospace Security Project", Center for Strategic and International Studies (April 2018) 2, online: < https://aerospace.csis.org/wp-content/uploads/2018/04/Harrison_SpaceThreatAssessment_FULL_WEB.pdf>.
[101] Office of the Chairman of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms* (Washington DC: The Joint Staff, July 2019) at 200.
[102] Boothby, "Space Weapons and the Law", supra note 93 at 212.
[103] *Ibid*.
[104] Robert A. Ramey, "Armed Conflict on the Final Frontier: The Law of War in Space" (2000) 48 A.F. L. Rev. 1 at 19-20.
[105] *Ibid*.
[106] *Ibid* at 23-26.
[107] Harrison, Johnson & Roberts, *supra* note 100 at 3-4.

the situation. As noted earlier in Chapter 1 of this thesis, Article I (2) of the Outer Space Treaty noted the protection of freedom of use.[108]

In the case of jamming, the weaponization takes a systematic approach. As the US Department of Defense defines it, "… electromagnetic jamming is the deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, and with the intent of degrading or neutralizing the enemy's combat capability."[109] Therefore, there is no doubt of the aggressive capability behind its utilization, in this case, the actual jamming of the targeting and tracking capabilities.[110] The ultimate expected result would be to ensure that incoming missiles miss their final targets.[111] Plus, this would also include jamming the positioning of satellite communications.[112] These "electronic attacks target the means by which space systems transmit and receive data by jamming or spoofing radio frequency (RF) signals."[113] Yet, although related to data, "cyberattacks target… the antennas on satellites and ground stations, the landlines that connect ground stations to terrestrial networks and the user terminals that connect to satellites."[114] This mental picture of defined weapons and targets becomes blurred in the cyberspace arena of outer space. It is in that arena where politics, military objectives, and legal standards develop into a hazy amalgamation of surreptitious conduct that threatens to offset the balance found in the peaceful use of outer space. Since 1982, the almost forgotten words of

[108] Outer Space Treaty, Article II, *supra* note 25.
[109] Office of the Chairman of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, *supra* note 101 at 71.
[110] Boothby, *supra* note 93 at 210.
[111] *Ibid.*
[112] *Ibid.*
[113] Harrison, Johnson & Roberts, *supra* note 100 at 4.
[114] *Ibid.*

David Ritchie have provided an ominous warning for States contemplating space activities.[115] His warning was as follows:

> "Any future battles in outer space are unlikely to be jousts between knights in shining spacecraft… The militarization of space will not spare our world the devastation of nuclear blasts by carrying combat off the earth and into orbit. That halcyon view of the military buildup in space overlooks one important point about these space systems: they were built not to replace our armies and navies and air forces here on earth, but to supplement and assist them in any wars they carry out on the planet."[116]

ASAT technologies are known solely by their destructive purpose.[117] The list of anti-satellite weapons is short, yet they are extremely dangerous. The legal and military discussions around their legality and necessity seem superfluous and disappointing when one considers the amount of resources that equally could be utilized to explore and expand human presence across the solar system and beyond. As Ritchie stated, "It seems unrealistic, then, to expect that orbiting lasers and ASAT missiles are going to usher in a new era of post-nuclear warfare, and make the atomic and conventional arsenals of the world obsolete."[118]

B. Cyberattacks as Space Weapons

The mere thought of accepting aggressive cyber operations as a weapon is anathema, and the idea of aggressive military activities in outer space is beyond disappointing. Yet, when these two scenarios are put together, it presents as a challenge for international space law scholars. There must be a means by which scholars may define the path ahead. The global community is entering a historical phase in which information and communication technologies have a dual purpose. This dual purpose, unfortunately, may also be nefarious. This dichotomy includes the

[115] David Ritchie, *Space Wars* (New York: NY, Atheneum 1982) at 192.
[116] *Ibid.*
[117] Ramey, *supra* note 104.
[118] Ritchie, *supra* note 115 at 190.

utilization of cyberweapons based on malicious code that exploits, for example, vulnerabilities in the Microsoft code.[119] One particular example was the *WannaCry* ransomware attack.[120] It was reported that a group called the Shadow Brokers released cyberweapons stolen from the US National Security Agency."[121] If this is true, then States are facing a greater technological crisis that is bound to reach air space and outer space regimes. These circumstances may pose a challenge of interpretation of those legal standards found in the space law treaties. In particular, in the ambit of military operations, the utilization of these cyberweapons will be contingent on the standards delineated to govern them.[122] If States begin to lose control over their cyber-arsenal, it will be only a matter of time before a lack of governance materializes in the form of disabled national infrastructures.[123] But *WannaCry* was not a simple cyberattack, nor has it been the only one. It also had the makings of a true cyberweapon. Indeed, States are still facing the consequences associated with the "ongoing ransomware attack that hit institutions and businesses worldwide, including hospitals in the UK, the Russian interior ministry and universities in China… [that spread] quickly across the world, infecting around 200,000 computers in 150 countries."[124] The threat also exists in outer space. The Aerospace Security Project at the Center for Strategic and International Studies noted the following:

> "For example, if an adversary can seize control of a satellite through a cyberattack on the satellite's command and control system, the cyberattack could shut down all communications and permanently damage the satellite by expending its propellant supply or damaging its electronics and sensors."[125]

---

[119] Douglas Heaven, "US cyberweapons have been stolen and there's nothing we can do", *New Scientist*, (6 December 2017), online: <https://www.newscientist.com/article/mg23631550-100-us-cyberweapons-have-been-stolen-and-theres-nothing-we-can-do/?campaign_id=RSS%7CNSNS->.
[120] *Ibid.*
[121] *Ibid.*
[122] *Ibid.*
[123] *Ibid.*
[124] Matt Reynolds, "Ransomware attack hits 200,000 computers across the globe", *New Scientist* (15 May 2017), online: <https://www.newscientist.com/article/2130983-ransomware-attack-hits-200000-computers-across-the-globe/>.
[125] Harrison, Johnson & Roberts, *supra* note 100 at 5.

The problem has always been attribution, given that "attackers can use a variety of methods to conceal their identity, such as using hijacked servers to launch an attack."[126] We may wish to apply similar reasoning to the drafting of new rules that tackle the participation of States in outer space, including their responsibly, accountability, and liability along with related stakeholders authorized under their control.[127] The rule drafting may begin by recognizing that cyber operations will affect the evolution of the law of outer space.

C. The Sony Hack Case

The Sony hack case was an example of political pressure at its most basic level. It is a classic example of a corporation that failed to prepare for an attack and also failed to invest in the required security mechanisms.[128] The hack, attributed to North Korea, "began when screenwriter Evan Goldberg and actor Seth Rogen joked about making a comedy about assassinating the leader of North Korea, Kim Jong-un," which subsequently materialized "when Sony Pictures Entertainment announced that both Goldberg and Rogen would direct the comedy movie *The Interview*."[129] The event served to underscore the challenges associated with disabled computer systems "and the fallout from the wholesale distribution of internal documents."[130] In the end, the failures of Sony executives could have been significantly ameliorated by the availability of an effective mitigation strategy. The cost of the hack, estimated to be over $41 million, would

[126] *Ibid*.
[127] Ronal L. Spencer, Jr., "International Space Law: A Basis for National Regulation" in Ram S. Jakhu ed., *National Regulation of Space Activities* (New York, Springer, 2010) at 1.
[128] Peter Elkind, "Inside the Hack of the Century, Part 3", *Fortune* (25 June 25 2015), online: <http://fortune.com/sony-hack-final-part/>.
[129] Gabriel Sanchez, "Case Study: Critical Controls that Sony Should Have Implemented", *SANS* (1 June 2015) 2, online: <https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-sony-implemented-36022>.
[130] Andrea Peterson, "The Sony Pictures hack, explained", *The Washington Post* (18 December 2014), online: <https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?noredirect=on&utm_term=.a57072f4c5a7>.

not be the end of the problems for Sony.[131] There were also the "expenses for investigation of the attack, IT repairs… lost movie profits," along with litigation associated with "poor cybersecurity that exposed employees' private information."[132] Furthermore, there was the reputational damage that would need repair.[133] Future cyber operations may require the re-examination of Article VI of the Outer Space Treaty in light of state responsibility and cyberattacks that interfere with satellites.

D. Estonia

The first major breakthrough in the exploration of outer space dates back to 1957 and the launch of the Soviet satellite Sputnik.[134] This technological milestone also propelled a legal milestone. Manfred Lachs notes that the "fundamental issue that arose on the day the first man-made instrument was launched into outer space concerned the law that should be applied to this domain and activities directed towards it: the identity, nature and framework of that law."[135] Lachs explained that once a new domain was accepted as an extension of these activities, international law would also be accessible in outer space.[136] Indeed, extending activities into outer space required the realization, as he notes, that this domain was not lawless or some kind of legal vacuum.[137] Cyberspace, in this manner, eventually became another milestone, but one with lacuna of identity, nature, and the framework of law. Over time, "there [have been] documented

[131] Peter Elkind, *supra* note 128.
[132] *Ibid.*
[133] *Ibid.*
[134] *See generally*, Paul Dickson, *Sputnik: The Shock of the Century* (Walker Publishing, 2001).
[135] Manfred Lachs, *The Law of Outer Space: An Experience in Contemporary Law-Making* (Leiden: The Netherlands, Martinus Nijhoff Publishers, 1972, 2010) at 125.
[136] *Ibid.*
[137] *Ibid.*

instances of state cyber practice, however, and these have begun to lay a pattern for establishing customary cyber law."[138]

The Estonian DDoS attack forced policymakers around the world to acknowledge that the utilization of cyberspace was evolving rapidly along with newly emerging customary rules, and for this reason, new methods would be needed to tackle these dangerous practices militarily. Yet, "with rare exceptions, no states or individuals come forward to take credit for these actions, so assessing the motivation of these unknown cyber actors [has been] difficult."[139] The attacks in Estonia were orchestrated via the utilization "of hundreds of thousands of ["zombie"] computers from around the world that had been hijacked previously by hackers."[140] In this manner, the computers flooded "designated Internet addresses with a variety of useless network-clogging data" and thus, created "the digital version of carpet bombing… referred to as a distributed denial of service, or DDoS attack."[141] The Estonian attack served as a wake-up call for States, stressing "the possibility that the Internet could one day suddenly disappear," even if this idea was considered "a mere speculation."[142] On April 26, 2007, the capital of Estonia, Tallinn, "fell victim to the first-ever real Internet war."[143] While the discontent between Russians and Estonians dates back to the Soviet occupation after World War II, the trigger incident was the removal of a "bronze statue of a Soviet soldier… erected in the capital as a memorial for the unknown soldier in WWII.[144] To the Estonians, however, the monument was a visual affirmation

[138] Gary Brown & Keira Poellet, "The Customary International Law of Cyberspace" (2012) 6:3 SSQ 126 at 129.
[139] *Ibid.*
[140] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe", *Wired* (21 August 2007), online: <https://www.wired.com/2007/08/ff-estonia/>.
[141] *Ibid.*
[142] Gadi Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War" (2008) 9:1 Geo. J. Int'l Aff. 121 at 121.
[143] *Ibid.*
[144] *Ibid.*

of Soviet oppression and occupation that deeply hurt their national pride."[145] The removal of the statue on April 27 "was met with outrage and retaliation from ethnic Russians, who rioted and looted downtown Tallinn."[146] Simultaneously, cyberattacks on "Estonia's network infrastructure [targeted] government offices, news agencies, and banks."[147]

In the end, the event was labeled as a "cyber riot."[148] While these cyber actions could not be attributed to the Russian government, "it is undisputed that Russians were responsible."[149] In the final analysis, questions arose regarding what should be "the proper response to this new kind of warfare," although the event imparted a lesson: "international legal mechanisms and law enforcement authorities [were now] hard-pressed to keep pace with the complexities of cyber-crime."[150] In the aftermath, on May 14, 2008, the previously proposed Estonian concept for a top-grade cyber defense center came into existence as the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) established with the participation of Estonia, Germany, Italy, Latvia, Lithuania, the Slovak Republic, and Spain.[151] More than ten years later, the CCDCOE has expanded to 21 member nations.[152]

E. Iran

A few years later, in 2010, cyberspace experienced the rise of a "cyber worm of unknown origin that was spreading across the world and embedding itself" in control systems that affected "[t]housands of computers in places like India and the United States."[153] Yet, "roughly 60

[145] *Ibid* at 122.
[146] *Ibid*.
[147] *Ibid*.
[148] *Ibid* at 123.
[149] *Ibid*.
[150] *Ibid* at 125.
[151] The NATO Cooperative Cyber Defence Centre of Excellence, "History", online: <https://ccdcoe.org/about-us/>.
[152] *Ibid*.
[153] P. W. Singer, "Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons" (2015) 47:1 Case W. Res. J. Int'l L. 79 (2015) at 80.

percent were in Iran."[154] While Iran seemed to be the obvious target, the worm, Stuxnet, subsequently behaved in a disastrous manner, "spreading uncontrollably to unintended targets all over the world, and thus demonstrating how indiscriminate and destructive cyber weapons were likely to be."[155] What made this weapon unique was its use of "four new zero days [that] utilized digital signatures with the private keys of two certificates stolen from separate well-known companies, and worked on all Windows operating systems down to the decade-old Windows 95 edition."[156] A *zero day* attack occurs when an adversary exploits "a vulnerability to gain access [via] software, hardware, or human vulnerability."[157] This is accomplished by exploiting "server-based vulnerabilities."[158] These vulnerabilities are common, such as "opening an attachment of malicious email or clicking a malicious link."[159] Stuxnet redefined the cyberspace landscape and became "one of the most complex threats" yet discovered.[160] Symantec described it as "a large, complex piece of malware with many different components and functionalities."[161] These particular traits made Stuxnet a matter of national defense and a potential source for kinetic deployment via cyber means. Indeed, this cyber weapon was designed to carry out sabotage "by reprogramming programmable logic controllers (PLCs) to operate as the attackers intend them to, most likely out of their specified boundaries."[162]

---

[154] *Ibid.*
[155] *Ibid.*
[156] *Ibid.*
[157] Lockheed Martin, "Gaining the Advantage, Applying Cyber Kill Chain Methodology to Network Defense" (2015) 4, online: <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf>.
[158] *Ibid.*
[159] *Ibid.*
[160] Nicolas Falliere, Liam O. Murchu & Eric Chien, "W32.Stuxnet DossierVersion 1.4, Symantec Security Response" (February 2011) 2, online: <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>.
[161] *Ibid.*
[162] *Ibid.*

A larger political problem is reflected by the fact that States, for the most part, chose "silence in reaction to the 2010 Stuxnet operation against Iranian nuclear enrichment centrifuges."[163] This is not to say that it was accepted as lawful.[164] On the other hand, it has been proposed that States may logically decide that this type of "operation was nevertheless a sensible means of avoiding a pre-emptive and destabilizing kinetic attack against the facilities by Israel."[165] This manner of thinking seems to be becoming a new norm. "If the damage caused by the Stuxnet malware had instead been caused by a traditional kinetic attack, such as a cruise missile, it is likely Iran would have vigorously responded."[166] Nevertheless, it remains unclear why Iran chose to remain silent, and "it remains true that no state has declared another to have violated international law by a cyber use of force or an armed attack through cyberspace."[167]

The same situation occurred in 2012, when the Shamoon virus targeted "Saudi Arabia's national oil company's computers," this time in a possible attack by Iran.[168] Despite these scenarios, there is reason to believe that these cyber activities are frowned upon by States, considering that it is "common for states to support or condemn a cyber activity in their international rhetoric."[169] States will need to work harder to enter successfully into the far reaches of space. From the point of view of cyber operations, the next theater of combat may be understood as military operations that require the transmission of data, and this in turn becomes a dark chess game dedicated to anticipating all threatening possibilities. While military challenges associated with cyber operations are guided by the *jus gentium* of cyberspace (and related

[163] Michael N. Schmitt & Liis Vihul, "The Nature of International Law Cyber Norms, Tallinn Paper No. 5" (NATO Cooperative Cyber Defence Centre of Excellence, 2014) at 26, online: < https://ccdcoe.org/uploads/2018/10/Tallinn-Paper-No-5-Schmitt-and-Vihul.pdf>.
[164] *Ibid.*
[165] *Ibid* at 27.
[166] Brown & Poellet, *supra* note 138 at 129.
[167] *Ibid* at 132
[168] Schmitt & Vihul *supra* note 163 at 27.
[169] *Ibid.*

considerations of the law of armed conflict), the resolution of these challenges in outer space—*ex definitione*—require a different approach and a different set of norms.

This chapter ends with one idea: the world in which we fight cyberattacks is filled with uncertainty. This uncertainty adds a layer of mystery to the future development of international space law. The 2016 Australian Cyber Security Threat Report noted that coercion, economic damage, and embarrassment are the goals behind cyberattacks on major industries, critical infrastructure, political entities, and other sectors.[170] The report observed that as a consequence of States developing the capability to conduct cyber operations and the lack of an effective method to deal with the repercussions of cyberattacks, the potential encouragement to continue this aggressive behavior "makes the threshold for response ambiguous, raising the risks of miscalculation."[171] Adding the layer of space activities to this conundrum enhances the need for a resolution. Maogoto and Freeland observe that space warfare has become the focus of military powers that now prepare for "high-tech combat."[172] The challenge this situation presents is one requiring a new approach and new thinking in regards to the rules of engagement, primarily focusing on outer space warfare.[173] Yet, scientific discoveries do not inevitably lead to conflict and related acts of war. For instance, the Moon landing was without a doubt a masterful achievement by many scientific standards. Above all, space has become strategic, with "more countries [deploying] their very own dedicated military satellites, and increasingly… blurring of satellites being used for commercial and military purposes."[174] The militaries of the world may be tempted to expand beyond merely blocking information by equating outer space outside the

[170] Government of Australia, Australian Cyber Security Centre, *ACSC 2016 Threat Report* (2016) at 7.
[171] *Ibid.*
[172] Jackson & Freeland, *supra* note 61 at 169.
[173] *Ibid* at 170.
[174] Ram S. Jakhu, "Sixty Years of Development of International Space Law" (Proceedings of the Symposium Celebrating the 90th Anniversary of the Cologne Institute of Air and Space Law, 2016) at 15.

atmosphere of the Earth to the treatment given the high seas.[175] But this scenario would quickly become unclear because "any projection of territorial sovereignty into space beyond the atmosphere would be inconsistent with the basic astronomical facts."[176] Professor John Cobb Copper observes that "the territory of a State may be defined as those regions in which the State is recognized by international law as having the right to exercise national sovereignty to the exclusion of all other States."[177] In particular, Oduntan added that "sovereignty appears not to rise above the bounds of the earth's airspace… [thus] it makes no sense in conventional terms to speak of sovereignty in outer space."[178] Conversely, it is "possible for a State to have jurisdiction over objects launched into space… but not jurisdiction over outer space itself."[179] Consequently, at this stage of technological development, cyberspace blurs the lines of legal analysis. Thus, it is now necessary to identify the legal claims within cyberspace and outer space. Furthermore, the problem is compounded by the existence of cyber weapons.

As will be discussed in Chapter 3, several criticisms have been made of the Tallinn Manual. Did the group of experts that drafted the Tallinn Manual anticipate what questions it would raise related to the realm of outer space? The efforts and accomplishments of the Tallinn Manual are no doubt highly commendable. Yet, it may also have been a missed opportunity to address several important considerations that will plague the second space age. Scholars continue to share the analysis of cyber law—one can almost hear the promises of international cyberspace law to the world, although they are slow to bring change to the non-committal actions of States.

---

[175] C. Wilfred Jenks, "International Law and Activities in Space" (1956) 5:1 The International and Comparative Law Quarterly 99 at 103.
[176] *Ibid* at 108.
[177] John C. Cooper, "High Altitude Flight and National Sovereignty" (1951) 4:3 The International Law Quarterly 411.
[178] Gbenga Oduntan, "The Never Ending Dispute: Legal Theories on the Spatial Demarcation Boundary Plane between Airspace and Outer Space" (2003) 1:2 Hertfordshire Law Journal 64 at 66-81.
[179] Alexandra Harris & Ray Harris, "Air and Space Demarcation" in Stanley D. Brunn, ed, *Engineering Earth: The Impacts of Megaengineering Projects* (Berlin: Germany, Springer, 2011) at 2161.

This is an ironic foreshadowing of what will be at the heart of the tensions anticipated at the intersection of space law and cyberspace law. Now that the problem is clearly defined, the next chapter considers difficult claims. The conflicting claims underscore the foundation for a proposed solution.

3

Setting the Stage

"As for me, the seven extraordinary days of Apollo 13 were my last in space. I watched other men walk on the Moon, and return safely, all from the confines of Mission Control and our house in Houston. I sometimes catch myself looking up at the Moon, remembering the changes of fortune in our long voyage, thinking of the thousands of people who worked to bring the three of us home. I look up at the Moon and wonder, when will we be going back, and who will that be?"[180]
— *James Lovell,* Apollo 13

I. Conflicting Claims in Cyber Law

In Chapter 1, it was noted that article I, paragraph 2 of the Outer Space Treaty states that "Outer space… shall be free for exploration and use by all States...."[181] The phrase "outer space should be used for peaceful purposes only" was recognized at the beginning of the preamble of the General Assembly Resolution on the Question of the Peaceful Use of Outer Space.[182] The resolution recognized the need for cooperation to promote mutual understanding and the strengthening of friendly relations to reach the goal of peaceful activities in outer space.[183] It is reasonable to infer that cyber operations are included in the "use" of outer space. The ultimate goal is to highlight the need for the development of rules of cyber operations related to space activities. Chapter 2 explores this question, setting the stage with the conflicting claims that delineate the law of cyber operations as it is understood by the claimants: the nation-states. The challenges that plague cyberspace are illustrated as the hidden dangers of global impact. In this cyberspace realm, these dangers embody a complex set of connections involving people,

[180] William Broyles Jr. & Al Reinert, "Apollo 13" (screenplay, 1995). [Adapted from the book by Jim Lovell & Jeffrey Kruger, *Lost Moon: The Perilous Voyage of Apollo 13* (Boston: Houghton Mifflin, 1994).]
[181] Outer Space Treaty, Article II, *supra* note 19.
[182] *Question of the Peaceful Use of Outer Space*, GA Res 1348(XIII), UNGAOR, 13th Sess, UN Doc A/RES/13/1348(XIII) (1958), at Preamble.
[183] *Ibid*.

networks, facilities, space objects, and information. The present-day world arena has become a theater of combat "with States armed with weapons to devastate the globe launched through the medium of outer space."[184] This environment must be understood from the numerous claimants or States with their respective claims.[185] These claimants represent a decision development process, in which, as noted before:

> "the factor of greatest significance affecting claims is the lack of a centralized political authority possessing sufficient control of force, military and other, to support, with whatever dispatch and comprehensiveness may be required, the general community efforts to minimize unauthorized coercion."[186]

This is the case given that these claimants are not homogeneous in their goals for deploying their activities in cyberspace. The process must recognize that cyber operations are an integral part of conducting space activities. The intersection of space activities and cyber operations raises a sense of nostalgia about the long-gone days of online innocence and safety. The challenge for those engaged in space activities is much more complex than in the early days of the Gemini and Apollo programs. It is in this emerging world of clandestine online maneuvers that scholars encounter the evolving law of cyberspace in outer space. The lessons of general international law predate the problems associated with the Internet and rules related to space activities. However, these earlier lessons do provide a useful frame of reference.

A. Concept of International Law

In 1895, Thomas J. Lawrence noted that in defining the concept of international law, "it is advisable to include as little controverted matter as is possible without sacrificing clearness to

[184] Myers S. McDougal, Harold D. Lasswell & Ivan A. Vlasic, *Law and Public Order in Space* (New Haven and London: Yale University Press, 1963) at 17.
[185] *Ibid* at 87.
[186] *Ibid* at 93.

a desire of avoiding difficulties."[187] This statement seems clear enough. The idea seems to allude to whether that characterization would be sufficiently useful to apply it to contemporary theological problems. Dr. Lawrence believed that rights and obligations were too controversial to be considered the necessary and final ingredients by which the law was to be defined.[188] Lawrence understood international law as a collection by which States needed to observe and manage coexistence.[189] Yet, even in those last years of the nineteenth century, he recognized that "international law proceeds first by the method of inquiry into the practices of states in their dealings with each other…"[190] Lawrence may have been thinking about the conflicting claims to be found in the future, as he considered that the rule of law needed in good measures both "the ideal with the real."[191] It is not inappropriate to seek out ideal rules applicable to real cyber operations. On the other hand, these rules must be practical. As if he were presented with the modern challenges associated with the use of technology by states, Lawrence noted that "international law, therefore, must cease to rely exclusively upon the method of observation and classification when [a drafter of international law] wishes to clear up a doubtful point or bring about a needful reform."[192] If a doubt needed resolution or a change was desired, Lawrence explained that a writer needed to ask "what the rules ought to be," and in essence become a legislator by *ipso facto* changing the law.[193] Lawrence's "rules concept" was not new at that time and it is definitely not new now. Yet, it matters now more in the present time than it did at the time he made his analysis.

[187] Thomas Joseph Lawrence, *The Principles of International Law* (Norwood: MA, Norwood Press, 1895) at 2.
[188] *Ibid* at 25.
[189] *Ibid.*
[190] *Ibid.*
[191] *Ibid* at 18, 25.
[192] *Ibid.*
[193] *Ibid.*

Lawrence lacked the tools provided by the International Court of Justice (ICJ) Statute, yet he seemed to be going in their general direction. Perhaps he was conceptualizing what would become *opinion juris*. If we were to apply his analysis to the last twenty years, two clear examples would emerge: the Tallinn Manual 2.0[194] and the upcoming Manual on International Law Applicable to Military Uses of Outer Space (MILAMOS Manual).[195] These manuals, and others mentioned later in this chapter, were drafted precisely because all States have claims. For Lawrence, the rules contained in those manuals would probably have the validity of persuasion and the power of legislation to eventually influence or even create international law.[196] What would have been important for Lawrence—we may reasonably speculate—includes the act of drafting these manuals and promoting them as a necessary evolution of the law of nations.[197] In 1916, possibly influenced by the events of World War I, Dr. Lawrence also observed that in the middle of a catastrophe, what was required would be "something more than a mere forensic discussion of particular cases," and by cases meant war atrocities.[198] Adopting the method of Hugo Grotius, he explained that Grotius observed the Thirty Years' War as someone "filled with holy indignation at the cruelty and licence around him, [which] he attacked with all the resources of his marvellous erudition the degrading and anarchic doctrine, *inter arma silent leges*."[199] Thus, if modern scholars are to assess the evolution of law in times of conflict, or in times when the *law falls silent*, Lawrence—just like Grotius—would describe "in general terms the terrible evils" that arise, and trace "them to the bad principles from" which they originate.[200] For

[194] Schmitt, *Tallinn Manual 2.0*, *supra* note 22.
[195] Manual on International Law Applicable to Military Uses of Outer Space [MILAMOS Manual], online: <https://www.mcgill.ca/milamos/>.
[196] Thomas Joseph Lawrence, *supra* note 187.
[197] *Ibid.*
[198] T. J. Lawrence, "The Effect of the War on International Law" (1916) 2 Probs. War. 105 at 105.
[199] *Ibid.*
[200] *Ibid* at 106.

Lawrence (and Grotius) it was better to fashion "wiser rules and more humane practices."[201] Lawrence noted:

> "And when we find in addition that all the resources of science are utilized for purposes of destruction, unrestrained by considerations of expense and unchecked by thoughts of mercy, we may well declare that the emergency we have to face is greater than that which fired the heart and sped the pen of the great Dutch jurist nearly three hundred years ago."[202]

This emergency now translates into cyberthreats. Indeed, Lawrence was in a position to make accurate predictions and "for many years held an important place in the ranks of International Lawyers."[203] Before he died, this scholar participated in the development of the law of nations simply by applying his own advice of writing rules in conjunction with the hopes of sharing them to a future world where these became recognized law.[204] One notable example involved his essays outlining "a scheme for the neutralization of the Suez Canal; and having the satisfaction four years later of seeing these principles adopted in the Suez Canal Convention, 1888."[205] If history serves as a good tutor, then it will demonstrate that the use of technologies and the knowledge they provide, including their misuse, warn of a troublesome future in which cyberspace may become a weapon of choice to threaten space objects.[206] As a result, it is now possible to direct a "cyberattack against some aspect of the vast space architecture" of a State that resides both in space and on the ground, rendering its military capabilities "effectively blind and deaf."[207] The future is ripe with opportunities to develop the rules for cyberspace in outer

---

[201] *Ibid* at 105-06.
[202] *Ibid* at 106.
[203] A. Pearce Higgins, "The Late Doctor T. J. Lawrence" (1920-1921) 1 Brit. Y.B. Int'l L. 231 at 231. [Dr. Lawrence was also known as Reverend Thomas Joseph Lawrence, LL.D. died after a short illness on August 16, 1919].
[204] *Ibid* 231-32.
[205] *Ibid* at 232.
[206] Aaron Bateman, "In Outer Space, the US is Vulnerable to China and Russia", *The Hill (blog)* (20 July 2017), online: <http://thehill.com/blogs/pundits-blog/defense/342992-in-outer-space-the-us-is-vulnerable-to-china-and-russia>.
[207] *Ibid.*

space, but that will primarily take place if States work together to redefine the legal landscape of cyberspace.

The borderless nature of cyberspace has turned it into the potential weapon of choice for surreptitious activities that now threaten to enter outer space. This is why future cyber operations involving space activities will demand that "the statesman and the jurist… know the extent to which a State [has] the acknowledged right to control all activity in the areas of space above its surface territory."[208] Jackson and Freeland observe how States have been approaching activities in outer space that increasingly consider these "as part of active engagement in the conduct of armed conflict."[209] If States eventually manage to adopt new rules for cyber operations in space, it may be because scientific discoveries will motivate new industries with the greater participation of the private sector. This participation will require further legal norms. In this context, one final observation of note about Lawrence is useful. Some years later and shortly before his death, the review of Lawrence's book, *The Principles of International Law* (fourth edition, 1910) included a memorable observation: "Dr. Lawrence calls this 'an age that is about to add warfare in the air to warfare on land and warfare at sea.'"[210] For him, the extension of warfare to cyberspace and outer space would have been foreseeable additions to the activities of States in the land and sea realms. He would have probably found without much surprise that the present treaty law lacked the mechanisms necessary to tackle present claims in cyberspace.

As noted earlier, the United Nations Ad Hoc Committee on the Peaceful Uses of Outer Space "recognized that it would be impossible at this stage to identify and define, exhaustively,

[208] John C. Cooper, "High Altitude Flight and National Sovereignty" (1951) 4:3 The International Law Quarterly 411 at 411.
[209] Jackson & Freeland, *supra* note 61 at 169.
[210] G.G. W., "Book Review" (1910-1911) 24 Harv. L. Rev. 413 at 414.

all the juridical problems which might arise in the exploration of outer space."[211] Cyber operations in outer space, in contrast to land, are particularly unique, including military activities. Just as the law of land warfare is characterized by particular threats, so are space activities tied to cyber operations. As Julian Gadzik writes, "The Committee considered the relevance to space activities of the provisions of the United Nations Charter and of the Statute of the International Court of Justice… [and] it observed that as a matter of principle those instruments were not limited in their operation to the confines of the earth."[212] The ICJ Statute has included the authoritative sources of *treaties*, *customary law*, and *general principles of law*.[213] In the ambit of *cyberspace*, the advantages of treaty law did not materialize, except with one limited exception (dealing with cybercrimes). After all these years, however, there has never been any "statutory authority" or international treaty of any kind for the overall management of the Internet.[214] While conflicting claims may be guided by the language of the five United Nations treaties on outer space, the distinctiveness of cyber operations narrows the options. This new war domain demonstrates a different legal history than the one present during the beginnings of space exploration. Although existing international space law, such as the Outer Space Treaty, applies to States' cyber operations in outer space, certain treaties do not apply to cyberspace. The space law treaties listed below may apply only in certain circumstances (such as with ground infrastructure facilities), and thus might not create obligations applicable to cyber operations in outer space.

[211] Julian GAZDIK, "International Review" (1959) 26:4 J. Air L. & Com. 359 at 386.
[212] *Ibid.*
[213] Antonio Cassese, *International Law* (New York: Oxford University Press, 2005) at 153, 170, 188. *See also,* Ian Brownlie, *Principles of Public International Law,* 8th ed. (New York: Oxford University Press, 2012) at 18-19.
[214] US, Law Library of Congress, Lennard G. Kruger, *Internet Domain Names: Background and Policy Issues*, (7-7070) (Congressional Research Service, 2009) at 1.

1. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (Outer Space Treaty or OST)[215] [*in particular, Articles I(2), III, VI, and IX*]

The other four below are *inapplicable to cyber operations in space*, unless tangentially related with matters that impose liability or State responsibility obligations under the Outer Space Treaty.

2. Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space (Rescue Agreement)[216]
3. Convention on International Liability for Damage Caused by Space Objects (resolution 2777 (1972 Liability Convention)[217]
4. Convention on Registration of Objects Launched into Outer Space (1975 Registration Convention)[218]
5. Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (the Moon Agreement)[219]

Regarding relevant instruments applicable to cyberspace, their applicability is noted below.

1. Convention on Cybercrime[220] [*inapplicable to cyber operations in space*]
2. 2006 Additional Protocol to the Convention on Cybercrime[221] [*inapplicable to cyber operations in space*]
3. Shanghai Cooperation Organization's International Information Security Agreement[222] [*inapplicable to most cyber operations in space*]

---

[215] Outer Space Treaty, *supra* note 19.
[216] *Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space*, 22 April 1968, 672 UNTS 119, 19. U.S.T. 7570, TIAS 6599 (entered into force on 3 December 1968) [Rescue Agreement].
[217] *Convention on International Liability for Damage Caused by Space Objects***,** 29 March 1972, 961 UNTS 187, 24 U.S.T 2389, TIAS 7762 (entered into force on 1 September 1972) [Liability Convention].
[218] *Convention on Registration of Objects Launched into Outer Space*,14 January 1975, 14:1 Intl Leg Materials 43 (entered into force on 15 September 1976) [Registration Convention].
[219] *Agreement Governing the Activities of States on the Moon and Other Celestial Bodies*,18 December 1979, 18:6 Intl Leg Materials 1434 (entered into force on 11 July 1984) [The Moon Agreement].
[220] *Convention on Cybercrime*, Council of Europe, 23 November 2001, 2296 UNTS 167, ETS 185 (entered into force 1 July 2004) [Budapest Convention on Cybercrime].
[221] *Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, Council of Europe, 28 January 2003, ETS 189 (entered into force 1 March 2006).
[222] *Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security*,16 June 2009, Shanghai Cooperation Organisation, online: < https://ccdcoe.org/organisations/sco/>.

4. ITU Constitution and Convention [223] [*applicable to specific space activities that involve cyberspace*]
5. International Telecommunication Regulations[224] [*useful provisions applicable to specific space activities that involve cyberspace*]

The template for general rules of application related to cyber operations noted above is found within Article 38 of the Statute of the International Court of Justice.[225] That is not to say that no suggestion was made for treaty-creation to be applied in cyberspace.[226] Yet, none of these suggestions offered all-encompassing guidance for the management of cyber operations in outer space. For example, the Cybercrime Convention, the only overarching treaty on cyber law, "perpetuates deference to state sovereignty by requiring parties to criminalize various forms of computer misuse by non-state actors. Its rules, however, do not apply to government activities, whether for law enforcement or national security purposes."[227] Article 2 of the Convention states that:

> "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system *without right*. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."[228]

For these reasons, it was noted in the Explanatory Report to the Convention on Cybercrime, regarding "unaffected conduct" the following:

[223] *Constitution and Convention of the International Telecommunication Union*, 22 December 1992, 1825 UNTS 330, ATS (1994) 28, BTS 24 (1996) (entered into force date 1 July 1994), as amended by the 2018 Plenipotentiary Conference [ITU Constitution].
[224] *International Telecommunication Regulations*, International Telegraph and Telephone Conference, 9 December 9, 1988, as revised and adopted by the 2015 World Radiocommunication Conference [ITU Radio Regulations].
[225] Statute of the International Court of Justice, Article 38, ¶ 1, TS No 993.
[226] *See*, Secretariat of the Working Group on Internet Governance, *Report of the UN Working Group on Internet Governance*, UNSG, Working Group on Internet Governance (June 2005).
[227] Duncan B. Hollis, "Why States Need an International Law for Information Operations" (2007) 11:4 Lewis & Clark L. Rev. 1023 at 1052.
[228] Council of Europe, *Convention on Cybercrime*, Explanatory Report, C.E.T.S. No. 185, ¶ 38 (Nov 8, 2001), https://rm.coe.int/16800cce5b.

> "Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised… It is left to the Parties to determine how such exemptions are implemented within their domestic legal systems (under criminal law or otherwise)."[229]

Thus, it has been inferred that the "reference suggests the negotiators were well aware of states' developing [information operations] doctrines and sought to draft around them in this Convention."[230] This is particularly problematic. Carl Christol may have anticipated a quarrelsome future when he noted that the hybrid capabilities of satellites via remote sensing provided valuable data that contributed "to commercial profitability and military efficiency."[231] To be sure, it was noted recently that the United States has become "completely reliant on space-based systems," and because of this, its status represented "a strategic vulnerability."[232] It would be possible for another state with the know-how seeking to enhance its geopolitical sphere of influence to interfere with "critical space-based resources" belonging to the United States.[233]

B. The Stationary Treaty Law

The *jus gentium* of cyberspace now extends to the great expanse of the spiral galaxy.[234] The search for new solutions now requires a realization of the status of international law. The

[229] Hollis, *supra* note 227; Council of Europe, Committee of Experts on Crime in Cyber-Space, 50th plenary Sess, Explanatory report of the Convention on Cybercrime, CM (2001)144 addendum (2001) at ¶ 38, online: <https://rm.coe.int/16804d873c>.
[230] *Ibid*.
[231] Carl Q. Christol, "Remote Sensing and National Security" (2003) 46 Proc. on L. Outer Space at 224.
[232] Aaron Bateman, *supra* note 206.
[233] *Ibid*.
[234] "The Milky Way Galaxy", National Aeronautics and Space Administration, Goddard Space Flight Center (December 2015), online: <https://imagine.gsfc.nasa.gov/science/objects/milkyway1.html>. *See also*,

rules to be proposed later in the thesis have more meaning when this status is understood vis-à-vis existing treaty law. These rules will address a perceived gap in the Tallinn Manual and will be intended to create awareness at what may be new subjects to be addressed in a potential Tallinn Manual 3 or MILAMOS Manual 2. These rules will illustrate new technological developments that will be associated with space activities involving the use of cyberspace. These rules will also stress the anathema of aggressive military cyber operations that represent a serious challenge for the future outer space exploration. A much-needed normative prescription of guidance is needed in these changing times.

Neil Armstrong probably understood the need for guidance and he was sure about one particular aspect of traveling to the Moon, despite its inherent engineering risks and hazards. To him it was plain and simple—it would be "to take man to the Moon, make a landing there, and return".[235] He noted, "I think we are going to the Moon... because it's in the nature of the human being to face challenges. It's by the nature of his deep inner soul."[236] These very simple and also profound words are at the center of the guidance contained in the preamble of the Outer Space Treaty.[237] The OST's preamble recognizes "the exploration and use of outer space for peaceful purposes."[238] But then, what good is international law? This is an odd question to ask at this point. Nevertheless, it is a necessary exercise of analysis if the rules presented in Chapter 4 and 5 are to have meaning in the future.

"Supermassive Black Hole Sagittarius A", *NASA* (10 May 2016), online: <https://www.nasa.gov/mission_pages/chandra/multimedia/black-hole-SagittariusA.html>.
[235] Hansen, supra note 34 at 199.
[236] *Ibid* at 202.
[237] Outer Space Treaty, *supra* note 19.
[238] *Ibid*.

Michael Handel observes that since the Industrial Revolution, wars have evolved due to the accelerating development of technology.[239] "As a result, no major wars since the mid-nineteenth century have been fought with the same weapons or doctrines."[240] While new technologies have changed the war landscape over time, the ambit of international law and the cooperation it generates cannot be ignored, given that "modern warfare appears to be dominated by weapons technology, other factors such as human nature, the political essence of war, the quality of leadership, national commitment, coalitions and diplomacy [that] have remained the same."[241] Although there has been a strong foundation of treaty law in space law, this has not been the case with cyberspace law, a *sui generis* area of governance. In 2001, the US-China Economic and Security Review Commission reported that "hackers had achieved 'all steps required to command' a NASA satellite and had interfered with other satellites too."[242] Once a State interferes with a satellite via cyberspace means, the other State (or States) is propelled into a legal inquiry about the next steps. At first glance, treaty law offers a very useful tool to begin resolving the problem. Article 45(1) of the ITU Constitution constitutes a partial legal basis for the establishment and operation of all [ground-based] stations, which, "whatever their purpose, must be established and operated in a manner as not to cause harmful interference to the radio services of communications…"[243] Ground-based infrastructure consists of terrestrial facilities that directly support space activities "effecting terrestrial radiocommunication."[244] It would be reasonable to continue the analysis by stating that hacking of a satellite would constitute a breach

[239] Michael I. Handel, *Sun Tzu and Clausewitz: The Art of War and On War Compared* (Carlisle Barracks, PA, Strategic Studies Institute, U.S. Army War College, 1991) at iii.
[240] *Ibid*.
[241] *Ibid*.
[242] Joan Johnson-Freese, "The United States' Space Security Policy: Cyber Security Vulnerabilities", *in Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives* (Chatham House, December 2014) at 38.
[243] ITU Constitution, *supra* note 223.
[244] ITU Radio Regulations, *supra* note 224 at art 1.61.

of a State's international obligations. In case of a conflict, the "law of war treaties and the customary law of war are understood to regulate the conduct of hostilities, regardless of where they are conducted, which would include the conduct of hostilities in outer space."[245] Wiessner observes that …"[f]or us, law, like life, is moving, and so we see the decision making body and its environment change."[246] The positive values of science trigger an evolution of that life, or more precisely, the life of international space law, but this law is also realistically permeated by the shadow of potential cyberattacks directed at space objects along with the expansion of human conflict into outer space. In the absence of rules applicable to cyberspace operations in outer space, uncertainty will remain.

II. The Case of Kosovo

What good is international space law? To consider this question, the discussion forces a candid evaluation of *lex lata*, or more precisely, those provisions available to scholars and practitioners alike. The ambiguities that surround cyberspace operations, even if related to space activities, can be illuminated by applying space law principles to cyber conflicts. It seems that applying space law to cyber operations would still be the best initial course of action. Thus, the point of departure is to evaluate States' claims in light of cyber operations as part of the cyberspace domain, and anywhere where these take place: on land, in the air, at sea, in cyberspace, and in outer space. Understanding this paradigm in outer space illustrates challenges to the application of present norms and the development of future rules. A manual intended to clarify the applicability of international law to particular scenarios of cyberspace in outer space in times of peace has not been fully developed to date. This is the ultimate goal to be addressed

[245] US DoD, Law of War Manual, supra note 6 at §14.10.2.2.
[246] Siegfried Wiessner, *supra* note 51 at 50.

in subsequent chapters of this thesis. One valuable lesson that serves as a backdrop to the present analysis is found within Jed Rubenfeld's story about Kosovo. He notes:

> "So Roosevelt called for a new system of international law and multilateral governance that would be designed to stop future wars before they began. Hence, the irony of America's current position: More than any other country, the United States is responsible for the creation of the international law system it now resists."[247]

Perhaps, this claim could be made of other nations too. The claims of America, of course, are not an isolated case. But it is a useful case study. In 2003, several scholars asked the question "What good is international law?" At the time of the inquiry, the scholars intended a reexamination of the role of United States, its allies, and international law.[248] To begin the formulation of a solution prosed by this thesis, it is important to clarify the reason for the 2003 inquiry. While most of that analysis honed in on the foreign policy of the United States, given the nature of cyber operations, the same analysis could be extrapolated and by extension be applicable to space activities. The status of cyber operations as they relate to military activities in outer space needs clarification. The evolution of activities in outer space involving cyber operations forces all stakeholders to revisit this question. The evolution of cyber operations requires a reanalysis of the applicability of international law. To begin devising an answer, Rubenfeld shares his observations about Kosovo.[249] He recounted the following regarding the applicability of international law in the new nation:

> "We met in Paris and Venice, and the proceedings were professional and expert in every respect. But though the committee had visited Kosovo for three days, it had no Kosovar members. Uncertain as to whether their absence was deliberate, I made inquiries among the committee members. It was indeed intentional. The framing of a constitution was a delicate business, I was told, and to have involved

[247] Jed Rubenfeld, "The Two World Orders" (2003) XXVII: 4 The Wilson Quarterly 22 at 22.
[248] The Autumn 2003 issue of the The Wilson Quarterly (Volume XXVII, Number 4) was titled: "What good is International Law."
[249] Rubenfeld, *supra* note 247 at 25.

> Kosovars in the process would have impeded the committee's work and mired it in political infighting."[250]

Rubenfeld is referring to one of his experiences as an observer in the United Nations Vienna Commission.[251] Perhaps he perceived that under *lex lata* standards the resolution to the situation on the ground was impractical.

> "Might it therefore be desirable, I asked, to draft an explicitly transitional document… one that created institutions through which local drafting and ratification of a permanent charter could later take place? No, was the committee's answer. We were drafting a *constitution*, and constitutions are not meant to be transitional documents."[252]

In the end, Rubenfeld explains that the committee members did not consider it "particularly important for a constitution to be the product of a national participatory political process."[253] The members were satisfied that "a committee of expert foreign jurists [would] draw up a constitution… [and] the occupying power was recognized as valid under international law…."[254] This gray area of legal application illustrated problems now perceived in the claims associated with cyber operations, and Rubenfeld seemed to deal in similar notions, although for different reasons.

> "Because the UN Security Council never approved the use of force in Kosovo, international lawyers regarded the U.S.-led bombing as plainly illegal… [But], it has reinforced the view that events in the former Yugoslavia represented an appalling failure on the part of the international law system, the United Nations, and, in particular, the nations of Europe.… The United States… intervention sought rather, at least in the American account, to prevent manifest, grotesque, genocidal crimes. And if the United Nations did not respond to the most blatant, wanton, and massive of human rights violations in Kosovo, how could it be trusted to respond to less demonstrable but perhaps more dangerous threats elsewhere?"[255]

---

[250] *Ibid* at 26.
[251] *Ibid.*
[252] *Ibid.*
[253] *Ibid.*
[254] *Ibid* at 27.
[255] *Ibid* at 31-32.

Just as in 2003, the emerging cyberthreats now force States to consider a second look at international space law. Following Rubenfeld's reasoning, uncertainty could partly arise due to the lack of legal standards applicable to cyber operations in outer space, just as those "human rights… that are systematically violated by many of the states subscribing to them."[256] The solution could begin to take shape simply by predicting what rules will be successful in view of events that define State behavior in outer space. The conflictive claims are surprisingly helpful, given that similar questions exist in the ambit of cyberspace law and may extend into the fragile realm of space law. If a lesson is to be learned, it is that international law "does not descend from on high. Rather, it's created by states to serve their collective interests."[257] The behavior of States "almost always flows from a tangled web of motives… [and] it's often impossible to separate self-interested behavior from behavior caused by legal requirements."[258] According to Michael J. Glennon:

> "So while it's important to know that most states observe most rules most of the time, it's equally important to realize that when some states violate some rules some of the time, those states are likely to be among the most powerful states, the rules are likely to be extraordinarily significant rules, and violations are likely to be highly visible and historically significant. Hence, the recent burst of skepticism about international law."[259]

Oona Hathaway summarizes this skepticism by highlighting two main factors. First, she notes that reputation carries significant weight for States, especially if "violations [were] likely to be discovered."[260] Unfortunately, the result would be completely the opposite if violations were "difficult to detect"—such as in cyberspace—

[256] *Ibid* at 32.
[257] Anne-Marie Slaughter, "Leading Through Law" (2003) XXVII: 4 The Wilson Quarterly 37 at 37.
[258] Michael J. Glennon, "Sometimes a Great Notion" (2003) XXVII: 4 The Wilson Quarterly 45 at 48.
[259] *Ibid* at 49.
[260] Oona A. Hathaway, "Two Cheers for International Law" (2003) XXVII: 4 The Wilson Quarterly 50 at 54.

with violations likely becoming common.[261] With respect to cyber operations, while there has been little guidance available within treaty law, or to be more exact, international cyberspace law, a glimmer of customary law can be identified. It is this hazy and still in formation legal standards that begin to show direction in matters of cyber operations in outer space. This law-in-formation or international cyberspace law can be culled within emerging norms acknowledged by the UN Governmental Group of Experts (UN GGE).[262] The UN GGE was "established under the UN General Assembly, to identify fundamental first steps and behaviors to protect critical national and international infrastructures from cyber harm…"[263] In this regard, customary law, as potentially fast-forming, provides the best course of action. Fortunately, fast-forming norms began to take shape with the 2013 Report of the UN Group of Governmental Experts (GGE).[264] The 2015 subsequent report observed that "international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment."[265] Above all, very relevant to potential rules of cyberspace in space, the GGE note that:

> "States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts."[266]

---

[261] *Ibid* at 54.
[262] United Nations Office for Disarmament Affairs, Group of Governmental Experts, online: https://www.un.org/disarmament/group-of-governmental-experts/.
[263] Melissa Hathaway, *Getting Beyond Norms: When Violating the Agreement Becomes Customary Practice*, *Center for International Governance Innovation*, Papers No. 127 (Waterloo: ON, Canada, 2017) at 2.
[264] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UNGAOR, 60th Sess, UN Doc A/68/98 (2013).
[265] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UNGAOR, 70th Sess, UN Doc A/70/174 (2015) at ¶24.
[266] *Ibid* at ¶28 (e).

As a consequence, a State has "original responsibility for its own acts or the acts it authorized."[267] This authority must be examined when cyberspace is involved during peace time and in periods of rising tension, given that States often deny their own cyberattacks or might disguise them as the actions of non-state actors. The US Department of Defense has observed:

> "But the challenge is not whether existing international law applies to State behavior in cyberspace. As the 2012-13 GGE affirmed, international law does apply, and such law is essential to regulating State conduct in this domain. The challenge is providing decision-makers with considerations that may be taken into account when determining how existing international law applies to cyber activities. Despite this challenge, history has shown that States, through consultation and cooperation, have repeatedly and successfully applied existing bodies of law to new technologies."[268]

The GGE later agreed in consensus, once again, as noted by their report of June 2015, "on norms, rules or principles of the responsible behavior of States in the cyber-sphere" and the applicability of international law to ICTs.[269] If definition of international cyberspace law where to be codified in future treaty law, the consensus of the Group of Experts would provide the point of departure:[270]

- "States must observe, among other principles of international law, State sovereignty, the settlement of disputes by peaceful means, and non-intervention in the internal affairs of other States."[271]
- "Existing obligations under international law are applicable to State use of ICTs. States must comply with their obligations under international law to respect and protect human rights and fundamental freedoms."[272]
- "The inherent right of States to take measures consistent with international law and as recognized in the Charter."[273]

---

[267] Ronal L. Spencer, Jr., "International Space Law: A Basis for National Regulation" in Ram S. Jakhu ed., *National Regulation of Space Activities* (New York, Springer, 2010) at 2.
[268] US DoD, *Law of War Manual*, *supra* note 6 at 1011. [The quote is from footnote 1, noting the United States Submission to the U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2014–15) at 1.]
[269] Group of Governmental Experts, *supra* note 265 at ¶19.
[270] *Ibid* at ¶ 28.
[271] *Ibid* at ¶ 28(b).
[272] *Ibid*.
[273] *Ibid* at ¶ 28(c).

- "States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts."[274]
- "The indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State. The Group noted that the accusations of organizing and implementing wrongful acts brought against States should be substantiated."[275]

The condition that the *implementation of wrongful acts brought against states* must be substantiated is a clear loophole, considering that attribution of cyberattacks continues to be a challenge. As noted in Chapter 4 of this thesis, this source of a claim offers new potential avenues for resolution within the rules applicable to space activities. These rules are key to the development of peace and security, both in cyberspace and outer space. The GGE Report conclusion offered, among others, this recommendation: "Further development by States collectively and individually of concepts for international peace and security in the use of ICTs at the legal, technical and policy levels."[276] As the Estonia case illustrated, this lack of agreeable concepts would become highly problematic.

III. In Search of Norms: Estonia Revisited

The existing legal standards for cyber operations—in outer space—are inadequate, and this may become more troublesome in times of rising tension. The analysis must include potential cyberattacks, and just as on land, space activities are bound to be "understood in relation to a broader concept of 'information warfare'—as its offensive aspect, i.e. 'activities aimed at destruction, take-over, harmful modification or use of informational resources of

[274] *Ibid* at ¶ 28(e).
[275] *Ibid* at ¶ 28(f).
[276] *Ibid* at ¶30(a).

attacked entity or the means of their storage, transfer and processing.'"[277] This was the case in Estonia. There is no doubt that the utilization of cyberspace in outer space will require a prescription of legal norms, which in turn can be reflected in *rules intended to address the activities in outer space, and as these activities relate to cyber operations*. Much can be learned from the 2007 Estonian incident. For purposes of rule creation, some factors are particularly relevant. The more a nation becomes engaged with cyberspace services, the more vulnerable it becomes. For this reason, "to understand the role of IT networks in Estonia, it should be emphasized that this country is one of European leaders in terms of the intensity of use of Internet in everyday life."[278] While States are bound by the emerging principles of international space law, the Distributed Denial of Service (DDOS) attacks in Estonia served as a wake-up call. These "DDoS attacks were carried out on a large scale, affecting government sites and the "servers of the second-largest bank in Estonia."[279]

The utilization of cyber operations in conjunction with space activities could be managed with rules intended to address this particular scenario. Looking at the rule making process at its most basic level, Gerald Postema explains that such practices offer "participants normative guidance, providing them standards for their performances and reasons for their actions."[280] The norms associated with normative practice "must take into account the background aims of the practice (and other moral values or principles)."[281] It must also be based on "those who

[277] Marcin Terlikowski, "Cyberattacks on Estonia: Implications for International and Polish Security" (2007) 16:3 Polish Q of Intl Affairs 68 at 69.
[278] *Ibid* at 71.
[279] *Ibid* at 72.
[280] Gerald J. Postema, "Custom, Normative Practice, and the Law" (2012) 62:3 Duke U 707 at 723.
[281] *Ibid*.

participate in it, and the social and material context in which the practice is located."[282] Postema presents a background formula for those who participate in the practice of a custom:[283]

> "(a) to judge certain performances as appropriate or correct and others as mistaken;
> (b) to act when the occasion arises in accord with these judgments;
> (c) to challenge conduct that falls short of these judgments; and,
> (d) to recognize appeals to the judgments as vindications of their actions or valid criticisms of them."[284]

While these elements are helpful to illustrate a process of rule creation, customary law as a source for both space law and cyber law must be understood along with developed standards tied to the environment of space activities and the associated claimants. For Estonia and its political conflict with Russia, this translated into efforts "to avoid discontinuation of Internet operations in the entire country, [with] connections with the world… interrupted and access to network in rural areas … limited." Russell Hardin explained that "[c]onsistency of individual motivations is central to the task of general explanation of behavior."[285] As Hardin noted, behavior is explicable if self-interest is an included element.[286] Citing Adam Smith, he quoted that it is "not from the benevolence of the butcher, the brewer, or the baker, that we expect our dinner, but from their regard to their own interest."[287] In other words, by seeking individual contentment, a collective may achieve a greater result for the benefit of its members.[288] This reasoning resonates with a process that seeks to identify rules for States and their peaceful use of outer space. These rules, by the nature of these space activities, also guarantee a collective peaceful utilization. This is

[282] *Ibid.*
[283] *Ibid.*
[284] *Ibid* at 724.
[285] Russell Hardin, "Normative Methodology" in Janet M. Box-Steffensmeier, Henry E. Brady & David Collier, eds., *The Oxford Handbook of Political Methodology* (Oxford: UK, Oxford University Press, 2010) at 36.
[286] *Ibid.*
[287] *Ibid* at 37
[288] *Ibid.*

compatible with the guiding light—international custom—defined in the ICJ North Sea Continental Shelf Cases.

The Court's process of analysis began by noting that it was necessary that "all events potentially be of a fundamentally norm-creating character such as could be regarded as forming the basis of a general rule of law."[289] The Court offered a normative approach constituted by the following factors:

(a) "a very *widespread and representative participation* in the convention [of States] might suffice of itself, provided it included that of States whose interests were specially affected;"[290]
(b) "the *passage of* only a short period of *time* is not necessarily, or of itself, a bar to the formation of a new rule of customary international law on the basis of what was originally a purely conventional rule;"[291]
(c) "an indispensable requirement would be that within the period in question, short though it might be, *State practice*, including that of States whose interests are specially affected;"[292]
(d) "should have been both extensive and virtually uniform in the sense of the provision invoked;"[293]
(e) "and should moreover have occurred in such a way as to show a general recognition that a rule of law or *legal obligation* is involved."[294]

Thus, the interests of States that are specially affected along with the other elements raises their "individual contentment" and a collective enjoyment of outer space.[295] When considering cyber operations in outer space, this process of rule drafting would be in need of one more element. In other words, there is no need to consider *in abstracto* the process of norm creation or *rules* relative to the present state of cyber operations by States. Ironically, it is in the dissenting opinion of Judge Lachs where the final factor is revealed:

[289] North Sea Continental Shelf Cases, Dissenting Opinion of Judge Lachs, *supra* note 54 at 230.
[290] *Ibid* at paragraph 73.
[291] *Ibid.*
[292] *Ibid.*
[293] *Ibid.*
[294] *Ibid.*
[295] Russell Hardin, *supra* note 285 at 37.

(f) "However, the great acceleration of social and economic change, combined with that of science and *technology*, have confronted law with a serious challenge: *one it must meet, lest it lag even farther behind events than it has been wont to do*."[296]

Lachs further explains:

> "To give a concrete example: 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 a remarkably *short period of time*. *Similar developments* are affecting, or may affect, other branches of international law."[297]

It has been noted that the length of time needed to develop a custom may vary depending of the situation.[298] For example, while *jus ad bellum* "developed over thousands of years," the protection of noncombatants associated with *jus in bello* "evolved primarily in the last 150 years."[299]

This evolution continued and "the Greeks began developing the concept of *jus ad bellum*, or just war, in the fourth century BC."[300] In the other hand, *jus in bello* "did not begin to assume [the] current form until the 1860s during the Franco-Prussian War and the American Civil War."[301] On the other hand, the customary law of outer space developed quickly:[302]

> "An example of customary law that developed quickly is space law. In 1958, just one year after the launch of Sputnik, the UN General Assembly created a committee to settle on the peaceful uses of outer space. By 1963, the United Nations had put forth the Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space, formally recognizing what had become customary law applicable to space activities."[303]

[296] North Sea Continental Shelf Cases, Dissenting Opinion of Judge Lachs, *supra* note 54 at 230.
[297] *Ibid.*
[298] Gary Brown & Keira Poellet, *supra* note 138 at 128.
[299] *Ibid.*
[300] *Ibid.*
[301] *Ibid.*
[302] *Ibid.*
[303] *Ibid.*

Nirmala Chandrahasan highlights the North Sea Continental Shelf cases, noting the court's explanation that a rule of treaty law could become binding customary law for non-parties to the treaty "if it could be shown that there was a general practice of states and the presence of opinion juris."[304] To clarify this custom, Chandrahasan pointed to the Tadić case of the International Criminal Tribunal for the former Yugoslavia, which explained that the common Article 3 of the 1949 Geneva Conventions shape "the minimum protections available to civilians in non-international armed conflicts… [thus becoming] a rule of customary international law."[305] Vereshchetin and Danilenko explain that "the emergence of a constant and uniform State practice in a new field of international relations" would set the stage for the establishment of a new rule of custom, as long as certain requirements were met, including generality, consistency, uniformity, and *opinio juris*.[306] When these considerations are analyzed in the context of State practice before the Outer Space Treaty, it demonstrates fundamental principles and rules which were recognized at the time:

> "outer space is open and free for exploration and use by all states;
> the sovereignty of states does not extend to outer space;
> outer space is not subject to national appropriation; and states retain jurisdiction
> and control over space objects launched into outer space."[307]

Vereshchetin and Danilenko also agree that "the passage of only a short period of time after the beginning of the exploration and use of outer space did not prevent the customary norms of the international law of outer space from coming into existence."[308] Jakhu and Freeland note the "emergence of customary international law in the context of outer space," echoing the words of

[304] Nirmala Chandrahasan, "The Continuing Relevance of Customary International Law in the Development of International Humanitarian Law" (2009) 21:2 Sri Lanka J of Intl L 55 at 62.
[305] *Ibid*.
[306] Vladlen S. Vereshchetin & Gennady M Danilenko, "Custom as a Source of International Law of Outer Space" (1985) 13:1 J of Space L 22 at 24.
[307] *Ibid* at 25.
[308] *Ibid*.

Manfred Lachs.[309] They explain that "many of the principles contained in the Outer Space Treaty also reflect customary international law and thus bind State parties and non-Parties to the Treaty alike."[310] Jakhu and Freeland noted the binding characteristic of the principles that are validated by the language in Article III of the Outer Space Treaty.[311] Indeed, the experiences that humanity has faced and will face in outer space will be unique and influenced by the passage of time—a reminder that principles of international humanitarian law should be refashioned to better reflect future military activities in outer space.[312] Freeland further explains:

> "Even though every effort should be made to apply the existing [international humanitarian law] principles as directly as possible, the largely unprecedented nature of such circumstances means that more specific rules will almost certainly be required, if they are to provide a comprehensive framework to properly protect humanity from the otherwise disastrous consequences of outer space (potentially) becoming another theatre of warfare."[313]

The same is the case for the existing international cyberspace law. If Estonia serves as a precursor for what would follow, then it is critical to accept that DDoS attacks will include zombie computers characterized by "IT networks from all over the world were used... [Participating] without any knowledge on the part of their users, as their PCs were infected on purpose with special software… [becoming]… the so-called 'botnets'—computer networks serving illegal purposes from different countries."[314] If botnets target space objects, legislators and scholars will arrive at a crossroads of interactions between *technology* and a *time-sensitive decision-making process*, in which new rules formulated will offer a new dimension. It would be reasonable to affirm that technology speeds up

[309] Ram S. Jakhu & Steven Freeland, "The Sources of International Space Law" (2013) 56 Proceedings of the Intl Institute of Space L 461 at 466.
[310] *Ibid*.
[311] *Ibid* at 467.
[312] Steven Freeland, "In Heaven as on Earth - The International Legal Regulation of the Military Use of Outer Space" (2011) 8:3 US-China L Rev 272 at 285.
[313] *Ibid*.
[314] Marcin Terlikowski, *supra* note 277 at 74.

the process of customary law formation. There also seems to be concurrence from the *Max Planck Encyclopedia of Public International Law*. It notes that "[r]ecent developments show… that customary rules may come into existence rapidly. This can be due to the urgency of coping with new developments of technology, for instance… space technology as regards the rule on the freedom of extra-atmospheric space."[315] The claims that arise from the expectations of States may need to be contrasted with similar ethics utilized in the battlefield.[316] For example, Martin Cook observes that with any State deliberately harboring terrorists, "no great stretch is required to extend the Westphalian paradigm to cover such cases."[317] The legal challenge behind this paradigm may become the acceptance of threats within the borders of States refusing to handle cyberattacks and the consequences of a declaration of a just cause of war.[318] Cook presents the following example:

> "One way of construing the conflict in Afghanistan is precisely this: that the Taliban government wished to shelter and protect al Qaeda on its territory and, after sufficient warning, placed its own continued existence in jeopardy."[319]

This example clarifies a basis for a rule in outer space. Cook would probably agree that similar activities involving cyberattacks could warrant the abandonment of "the just cause restriction to aggression… in favor of a "preemptive" or "preventative" action.[320] This is in contrast with Wilfred Jenks' 1968 analysis in relation to the governance formula of the OST, noting that the

---

[315] *See*, Siegfried Wiessner, "The Public Order of the Geostationary Orbit: Blueprints for the Future" (1983) 9:2 Yale J of World Public Order 217 at 235. [Professor Wiessner notes the global process of claims by States.] Tullio Treves, Customary International Law, Max Planck Encyclopedia of Public International Law November 2006 at §24.
[316] Martin L. Cook, "Ethical Issues in War: An Overview" in J. Boone Bartholomees, Jr., ed, *U.S. Army War College: Guide to National Security Policy and Strategy* (Carlisle: PA, 2004) at 21.
[317] *Ibid* at 29.
[318] *Ibid.*
[319] *Ibid.*
[320] *Ibid.*

treaty included the demilitarization provisions, and second, the provisions of jurisdiction and control over objects launched into outer space and their ownership.[321] With the development of cyber technology, militarization or the need for demilitarization becomes highly relevant. It is true, as Jenks observed, that the OST demilitarization provisions converge on the placing in orbit of objects carrying nuclear or other weapons of mass destruction.[322] Yet, fearing perhaps what the future would eventually reveal, Jenks suggested the potential negotiation of a Space Treaty "analogous in general character to the Antarctic Treaty."[323] He hoped for an outer space that would be used peacefully for all time.[324] He was content that the OST provisions provided "the arrangements necessary to ensure that space shall continue forever to be used exclusively for peaceful purposes."[325] However, the eventual incident in Estonia and the techniques utilized there began to cast a shadow over those noble principles: "the use of such a technique required know-how, funding and some coordination, and cooperation of groups of 'professional' hackers."[326] For this reason, the potential exists "that the primary incentive to commence the attacks came from Russian authorities."[327] In this stage of conflict, new rules can motivate better harmony between States. Jakhu observes that "the formulation of international space law has logically been based on the fact that outer space and outer space activities have been and are fundamentally transnational in nature, for there is invariably some connection to more than one State."[328] This is the case of not just the present status of space activities, but a necessary precondition for the future exploration and exploitation of outer space. For this reason, "purely

[321] C. Wilfred Jenks, "The Evolution of Space Law Continues" in *Essays in International Law in Honour of Juraj Andrassy* (The Hague: Netherlands, Martinus Nijhoff, 1968) at 135, 137.
[322] *Ibid.*
[323] *Ibid.*
[324] *Ibid.*
[325] *Ibid.*
[326] *Ibid* at 74.
[327] *Ibid* at 75.
[328] Ram S. Jakhu, "Sixty Years of Development of International Space Law", *supra* note 174 at 2.

national space activities cannot be effectively carried out without some form of international link or cooperation."[329] While cyber operations in outer space must be conducted with the understanding that consent within the customary law perspective may not be absolute, due to its connection to sovereignty, in the other hand, oppressive governments may lose the ability to object to a custom, simply by actions that annul their claim to sovereignty.[330] Above all, and as noted earlier, rules may come into existence rapidly, especially when these involve technology.[331]

Now rules are needed to address emerging cyber operations. Again, future practitioners and legislators must pierce the veil of gray areas in search of answers. "Cyber *opinio juris* is a rare phenomenon since, for understandable reasons, states often shy away from strong verbal commitments and their consequences."[332] A *Law of War Manual*, for example, is very helpful and useful as it incorporates the essence of "national cyber security strategies… [that] communicate a state's general position as to the rules and principles in cyber state practice and scholarly opinion."[333] The key is to find that "prevalent state legal opinion" or strategy that contains "declarations and aims that a state evaluates to be realistic and achievable."[334] For example, "the general statement by Harold Koh that the US had made a firm commitment to applying existing [international humanitarian law] IHL to situations of armed conflict involving cyber activities" or the "response to the Sony attack, [by] President Barack Obama," in which it

[329] *Ibid.*
[330] John Tasioulas, "Customary International Law and the Quest for Global Justice" in Amanda Perreau-Saussine & James Bernard Murphy, eds, *The Nature of Customary Law: Legal, Historical and Philosophical Perspectives* (Cambridge: UK, Cambridge University Press, 2007) at 314.
[331] Treves, *supra* note 314 at paragraphs 24, 91.
[332] Ann Väljataga, "Tracing Opinio Juris in National Cyber Security Strategy Documents" (NATO Cooperative Cyber Defence Centre of Excellence, 2018) at 4, online: <https://ccdcoe.org/uploads/2019/01/Tracing-opinio-juris-in-NCSS-2.docx.pdf>.
[333] *Ibid.*
[334] *Ibid.*

was hinted that a response "could include a coercive element and publicly attributing the attacks to North Korea."[335] These statements raise questions about Article 2(4) of the UN Charter, which provides a red line against cyber operations that interfere with the peaceful uses of outer space. Two other recent comments help delineate the emerging norms of cyberspace. Russian Foreign Minister Andrei Krutskikh noted as followes:

> "in response to the failure of the UN GGE in 2017. He argued that a permissive system of countermeasures and self-defense should not come before reliable technical and legal means of attribution, and consequently did not affirm the applicability of IHL in the cyber domain."[336]

Even more relevant, the UK Attorney General "shed some light on what would constitute an armed attack according to the UK's approach." He observed that a cyberattack would equate an armed attacked, as follows:

> "If a hostile state interferes with the operation of one of our nuclear reactors, resulting in widespread loss of life, the fact that the act is carried out by way of a cyber operation does not prevent it from being viewed as an unlawful use of force or an armed attack against us. If it would be a breach of international law to bomb an air traffic control tower with the effect of downing civilian aircraft, then it will be a breach of international law to use a hostile cyber operation to disable air traffic control systems which results in the same, ultimately lethal, effects."[337]

For now, the greatest cyber threat may not be technological in nature, but instead political, and cyber operations exist within the legal gray area in between, where new rules may become the shining guide posts in outer space. To achieve this goal, a manual intended to clarify the applicability of international law to particular scenarios involving space activities has become a necessity.

---

[335] *Ibid* at 5.
[336] *Ibid*.
[337] Jeremy Wright, "Cyber and International Law in the 21st Century", *Attorney General's Office* (23 May 2018), online: <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>.

4

Inter Mundos: Manuals of Past Trends

"If we could first know where we are, and whither we are tending,
we could then better judge what to do, and how to do it."
—Abraham Lincoln[338]

I. Threats, Risks and Trends

This chapter delineates, following the policy-oriented process, the applicable past trends of existing rules of engagement, appraising them, while suggesting future trends. These past trends represent important considerations that acknowledge that the greatest cyber threat is not technological in nature, but as noted earlier, political. This political threat may not be apparent at first. While a manual intended to clarify the applicability of international law to particular scenarios involving space activities has become a necessity, two considerations are paramount. It is within those considerations that scholars may find the legal gray area between technology and politics. One consideration relates to the importance of the military manuals themselves, while the other one relates to the rules individually. The subjects addressed by the rules are critical. Yet, the drafting process has a higher value. It is the value of that process that this thesis seeks to emphasize. With the understanding provided by the previous chapters, Chapter 4 proceeds with the first consideration.

As noted earlier in this thesis, manuals intended to clarify the applicability of international law to particular situations were drafted precisely because all States have claims.

[338] Abraham Lincoln, "A House Divided: Speech at Springfield, Illinois" in Roy P. Basler, ed, *The Collected Works of Abraham Lincoln, Volume 2* (New Brunswick, Rutgers University Press, 1953) at 461.

If a manual is going to address the domain of cyberspace as it relates to outer space, then prior manuals require a closer assessment of past trends in rule drafting processes. Thus, it is necessary to be mindful of the value of the rules to practitioners within the context of international law. Chapter 5 will introduce two suggested rules as examples of gaps in the legal analysis of the Tallinn Manual. These gaps in turn are intended to demonstrate the importance of the rules as tools for the future development of State practice.

The Estonia incident demonstrated that the inherent vulnerability of a global network is exacerbated by potential political motivations. This is further complicated in cyberspace, given that geography is unimportant due to the lack of applicability of regular border controls, or even enforceability of a delimitation of space. In 2006, the United Nations Institute for Disarmament Research reported its concerns that interference may be experienced by satellite systems and that the military space capability now supports traditional war-making in outer space.[339] At present, the reliability of a system is directly related to its defined likelihood of proper operation.[340] In other words, the "reliability of a complete satellite communications system depends on the reliability of its principal constituents — the satellite and the ground stations."[341] Manuals intended to clarify the applicability of international law to particular scenarios involving satellite systems face a difficult task if cyberspace becomes a factor in their activities of space.

The dark side of innovation raises many questions, but few answers are available. As Henriksen states, "The overall agreement that international law (also) applies in cyberspace is

[339] Laura Grego, "Technologies and Behaviors of Concern: What Threatens Long-Term Space Security and How Can These Threats be Monitored?" in UN Institute for Disarmament Research, *Building the Architecture for Sustainable Space Security: Conference Report 30-31 March 2006* (UN Publications, Geneva, 2006) at 68.
[340] Gérard Maral & Michel Bosquet, *Satellite Communications Systems* (West Sussex: UK, 2 Wiley, 2009) at 679.
[341] *Ibid.*

not, however, yet matched by universal consensus on how, exact, that law must be applied."[342] A preliminary observation can be gleaned from the Tallinn Manual 2.0, the most significant source of rules available regarding how international law may apply in cyberspace.[343] In particular, this observation relates to Rule 58 – Peaceful purposes and uses of force.[344] However, the combination of both of these subjects in a single rule is problematic. To understand why this is the case, it is best to begin by briefly examining the relevant rule-making process of the past one hundred years. In this manner, the policy-oriented rule-making process requires us to consider past trends found in previously drafted manuals in order to appraise prior considerations. This is necessary to achieve the goal of recommending an appropriate alternative to current rules.

The key to identifying a solution begins on April of 1915. Imagine an observer standing in an open field with a horizon that has become hazy. As he continues to look forward toward the horizon, a cloudy image emerges from within a greenish cloud of rising smoke. The observer sees soldiers choking and suffering, victims of a new technology. This was the case of the horrors of trench warfare of April 22, 1915, which became a painful lesson in military history.[345] "German forces shock Allied soldiers along the western front by firing more than 150 tons of lethal chlorine gas against two French colonial divisions at Ypres, Belgium."[346] Unfortunately, "chlorine gas represented an escalation in chemical warfare, still very new at the time."[347] This example underscores the need to identify *past trends* of existing rules of engagement, to *appraise* them, and to allow predictions of *future trends*. It is relevant to note that the rules of permissible

[342] Andres Henriksen, "Politics and the development of legal norms in Cyber Space" in Karstn Friis & Jens Ringsmose, *Conflict in Cyber Space* (NY: NY, Routledge, 2016) at 152.
[343] Schmitt, *Tallinn Manual 2.0*, *supra* note 22.
[344] *Ibid* at 273.
[345] "Germans introduce poison gas", *History* (21 August 2018), online: <https://www.history.com/this-day-in-history/germans-introduce-poison-gas>.
[346] *Ibid.*
[347] Tony Long, "April 22, 1915: A Fearful Word in the Trenches: 'Gas!'", *Wired* (22 April 22 2008), online: <https://www.wired.com/2008/04/dayintech-0422/>.

actions of warfare before World War I were not far from present day standards. Throughout history, "war consumed science and scientists, technology and technologists. But military institutions in preparation for war were among the principal patrons of these activities."[348]

The use of chlorine gas in trench warfare was a difficult lesson to understand and to apply to higher standards of relations among States. As the twentieth century opened, the *Convention for the Amelioration of the Condition of the Wounded and Sick in Armies in the Field* (Geneva Convention of 1906) represented a new opportunity. The Convention's preamble noted that the Contracting States were "animated by the desire to lessen the inherent evils of warfare" that existed within their power to control.[349] Along with this Convention, States were also guided by the *Convention (IV) respecting the Laws and Customs of War on Land* (Hague Convention of 1907), and particularly its annex, *Regulations concerning the Laws and Customs of War on Land*.[350] These regulations could be considered an embodiment of a 'rules manual' and several of the rules could be considered precursors of the modern international law applicable to military activities. The legal principles and military limitations of these rules may be applicable to cyber operations intended to disable a satellite or injure an astronaut:

> *Article 22* stated that "the right of belligerents to adopt means of injuring the enemy is not unlimited."[351]
>
> *Article 23* stated in part that:
> "it is especially forbidden (a) to employ poison or poisoned weapons;
> (b) to kill or wound treacherously individuals belonging to the hostile nation or army;
> (c) to kill or wound an enemy who, having laid down his arms, or having no longer means of defense, has surrendered at discretion;

[348] Alex Roland, "Science, Technology, and War" (1995) 36:2 Technology and Culture 83 at 95.
[349] *Convention for the Amelioration of the Condition of the Wounded and Sick in Armies in the Field,* 6 July 1906, 11 L.N.T.S. 440 at Preamble, online: <https://ihl-databases.icrc.org/ihl/INTRO/180?OpenDocument>.
[350] *Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land*, 18 October 1907, 36 Stat. 2277, TS 539, online: < https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?action=openDocument&documentId=4D47F92DF3966A7EC12563CD002D6788>.
[351] *Ibid* at Article 22.

> (d) to declare that no quarter will be given;
> (e) to employ arms, projectiles, or material calculated to cause unnecessary suffering…"[352]
>
> *Article 25* prohibited "the attack… by whatever means, of towns, villages, dwellings, or buildings which are undefended."[353]

The International Committee of the Red Cross further noted that "the provisions of the Hague Convention [were] considered as embodying rules of customary international law [and] as such they [were] also binding on States… not formally parties to them."[354] Legal experts have had at their disposal "a large body of ethical and legal thought" that has been intended to restrain actions related to the use of violence on behalf of the State.[355] One of these restraints exists in the form of the US Army's *Law of Land Warfare*, which clarifies and contrasts 'just war' "from other types of killing of human beings."[356] It is useful to assess past trends in warfare manuals. Military activities in space—just as on land—are in need of formulation to address moral terms in the midst of combat.[357] The historical process of rule drafting to clarify military operations offers some understanding that may illuminate political motivations behind cyber operations. Cyber operations need not be in conflict with that force that obliges "the conscientious person to obey the laws of his country."[358] This element raises another, because if the unconscientious person is expected to obey the law, they will do so simply because of constraints enforced by "the existence of the policeman."[359] Yet, for multiple reasons, there are many law-breakers.[360]

---

[352] *Ibid* at Article 23.
[353] *Ibid* at Article 25.
[354] International Committee of the Red Cross, "Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907", online: <https://ihl-databases.icrc.org/ihl/INTRO/195>.
[355] Martin L. Cook, "Ethical Issues in War: An Overview" in J. Boone Bartholomees, Jr., ed, *U.S. Army War College: Guide to National Security Policy and Strategy* (Carlisle: PA, 2004) at 21.
[356] *Ibid*.
[357] *Ibid*.
[358] J. A. Hall, *The Law of Naval Warfare* (London: Chapman & Hall, LTD., 1914) at 4.
[359] *Ibid*.
[360] *Ibid*.

Furthermore, so long "as we have wrong-doing by individuals, so long shall we have international wrong-doing by states. And for the latter there is no international policeman to deter or judge to punish."[361] As a matter of illustration, regarding the law of naval warfare, it was noted in 1914 that it would be reasonable to believe that any State willing to embark in the course of war to achieve a goal could not expect international law to have anything "to do with the origin or purpose of that war or the rights or wrongs of the parties."[362] This reasoning highlighted the importance of future manuals to address and clarify rules of behavior during peace time, rising tensions, and conflicts.

This thesis has emphasized more than once the privileged legal status of "freedom of use" that space explorers are expected to enjoy. From the cyberspace point of view, this also includes a warning to mitigate cyberattacks. Another way to view this mitigation process in outer space is to equate it with an element of national defense.

> "Up until [the early 1960s], Field Manual 100-5, Operations, the U.S. Army's main warfighting manual, drew its understanding of the relationship between attack and defense from the Principles of War. Ideally, a commander would seize the initiative with the attack. Thereby, the attacking force would dictate the tempo of operations and undermine the adversary's plans by forcing it to react to the initiator's actions."[363]

A. Manuals for Existing Norms

The earlier 1960s version of the Army manual "did not appreciate the advantages of defensive operations," yet, the 1962 and 1968 versions of this manual "argued that the defender could actually enjoy the initiative. A commander could possess the initiative in the defense by

[361] *Ibid* at 5.
[362] *Ibid.*
[363] Peter Campbell, "Generals in Cyberspace: Military Insights for Defending Cyberspace" (2018) 62:2 Orbis 262 at 269.

compelling the attacker to respond to the defender's plan."[364] In other words, proper defensive planning could produce better-than-expected results.

> "For instance, the attacker must traverse ground prepared by the defender. The defender can exploit the terrain to canalize the attacker into areas where the defender enjoys advantages."[365]

It was likewise observed that "Clausewitz's unremitting promotion of the attack in *On War* helped fuel the mindless offensives and slaughter of World War I."[366] However, a counterpoint noted "Clausewitz's deep appreciation for the power of the defense at the tactical, strategic, and political level."[367] Thus, past and present commanders in the field have had a useful reference source, with rules that could be seen as *teachings of the most highly qualified publicists* providing "a broader and important function" giving "shape and order to the disparate strands that make up international law."[368] In other words, whether a forming customary law or delineation via the teachings of publicists, the ultimate goal continues to be the shaping of existing norms in the form of *manuals* with precise rules that fundamentally clarify the international legal system.[369] In light of the wisdom of the International Law Commission (ILC), the value of a rules manual resides in the clarification of existing law.[370] However, while a manual may take note of a law in development, it is not helpful to persuade practitioners to accept or accelerate that development. The ILC noted that "assessing the authority of a given

[364] *Ibid.*
[365] *Ibid.*
[366] *Ibid* at 272.
[367] *Ibid.*
[368] Michael Wood, "Teachings of the Most Highly Qualified Publicists", *Max Planck Encyclopedia of Public International Law* (March 2017) at paragraph 3, online: <http://opil.ouplaw.com/home/epil>.
[369] *Ibid.*
[370] International Law Commission, *Report of the International Law Commission*, UNGAOR, 68th Sess, Supp No 10, UN Doc A/71/10 (2016) at 111.

work is thus essential."[371] The ILC referred to the following observation of the United States Supreme Court in the *Paquete Habana Case*:[372]

> "International law is part of our law, and must be ascertained and administered by the courts of justice of appropriate jurisdiction, as often as questions of right depending upon it are duly presented for their determination. For this purpose, where there is no treaty, and no controlling executive or legislative act or judicial decision, resort must be had to the customs and usages of civilized nations; and, as evidence of these, to the works of jurists and commentators, who by years of labor, research and experience, have made themselves peculiarly well acquainted with the subjects of which they treat. Such works are resorted to by judicial tribunals, not for the speculations of their authors concerning what the law ought to be, but for trustworthy evidence of what the law really is."[373]

To be sure, the collective wisdom found in each manual discussed below is a testament to the work of each the groups of experts.

II. Manual of Land Warfare

The present domain of cyberspace is one of rising tensions. This specific environment of past trends and future trends includes cyber-warriors, or more specifically their actions as "cyber-based effects" interfering with networks of computers and their "electronic information processing systems across *land*, *air*, *sea*, *space*, and *cyberspace* domains."[374] A land-generated attack could interfere with the "freedom of maneuver in all war-fighting domains" that may threaten "non-Internet-connected networks such as tactical data links, satellite-control networks, launch-control networks, and other networks not traditionally based on Internet data-transfer protocols and technologies."[375] Thus, a land-generated attack could interfere with the freedom of use of space. "Beginning with *General Orders 100* in 1863 the obvious intention of the [US

[371] *Ibid*
[372] *Ibid*. *See also*, *The Paquete Habana and the Lola*, 175 U.S. 677 (1900).
[373] *Ibid* at 700.
[374] William J. Poirier & James Lotspeich, "Air Force Cyber Warfare: Now and the Future" (2013) 27:5 ASPJ 73 at 86.
[375] *Ibid* at 86-87.

Army] manuals was to provide information to soldiers concerning the laws or rules of war so that those who gave orders knew that such orders were in compliance with the laws of war."[376] The past and present rules of land warfare present trends that serve as templates for the formulation of future manuals applicable to other domains. "While winning wars was the task of armies, there were rules which set limits to what actions were permitted to accomplish this task."[377] The legal principles found in these rules offer an initial foundation applicable to cyber operations in space:

> *Article 15* stated that "Men who take up arms against one another in public war do not cease on this account to be moral beings, responsible to one another and to God."[378]
>
> *Article 68* stated in part that "the destruction of the enemy in modern war, and, indeed, modern war itself, are means to obtain that object of the belligerent which lies beyond war. Unnecessary or revengeful destruction of life is not lawful."[379]

The latest iteration of this manual, the 21st Century US Army *Law of the Land Warfare Manual*, reminds soldiers of their legal limitations.[380]

> *Article 33* states that "the right of belligerents to adopt means of injuring the enemy is not unlimited."[381]

Yet, this new manual offers no direct advice regarding cyber operations. What appeared to be a mysterious oversight turned out to be a surprising development. Given the unique nature of cyberspace, the US Army drafted a separate manual to address cyber operations. The manual

[376] Donald A. Wells, *The Laws of Land Warfare: A Guide to the U.S. Army Manuals* (Westport: Connecticut, Greenwood Press, 1992) at 21.
[377] *Ibid.*
[378] *Ibid* at 22.
[379] *Ibid.*
[380] US Army Training and Doctrine Command, *21st Century U.S. Army Law of the Land Warfare Manual (FM 27-10)* (Washington, D.C.: Department of Defense, 2017) at 18.
[381] *Ibid* at 18.

for *Cyberspace and Electronic Warfare Operations* includes a structured definition for cyberspace, describing it as:

> "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."[382]

This definition is relevant to clarify the use of cyberspace that crosses into the realm of outer space. The manual further notes that *"cyberspace operations* are the employment of *cyberspace capabilities* where the primary purpose is to achieve objectives in or through cyberspace."[383] This implies that the utilization of cyberspace may violate space law, in particular Article III of the Outer Space Treaty, if the outcome of a cyber operation is equal to the results of kinetic means. This is further clarified by the manual, since it defines a cyberspace capability as "a device, computer program, or technique, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace."[384] In fact, Freeland noted with foresight how most States depended significantly on technology developed for space activities for the betterment of their livelihood and standard of living.[385] The problem has been, as Freeland observed, that satellites are now regarded as dual-use, which means that they are also designed with military and strategic purposes.[386] "This raises difficult questions about the 'status' of such assets under the rules of war—particularly as to whether they may be regarded as legitimate military objectives."[387] The contemporary legal community also recognizes that in cyberspace there are no clearly defined combatants, and none have been sent

[382] US Army, *FM 3-12 Cyberspace and Electronic Warfare Operations* (Washington, D.C.: Department of the Army, 2017) at 1-2.
[383] *Ibid.*
[384] *Ibid.*
[385] Steven Freeland, *supra* note 312 at 272-73.
[386] *Ibid* at 284.
[387] *Ibid* at 286.

to outer space. Similarly, in both environments, there are no defined non-combatants. Unfortunately, the reassuring quality of these 'rules' of law manuals cannot alone guarantee peace during a tense military operation. Indeed, there are many historical examples of the violation of existing rules. Yet, in the new age of cyberwarfare, the evolving rules of military cyber operations in outer space continue to hold meaning. This meaning helps to clarify the drafting process for the formulation of future manuals as we search for answers not in outer space, but within the domains of air and sea.

III. Manual of Air and Missile Warfare

The next domain that will be addressed is that of air space. This domain may also include the functionality of a missile that is intercepted via cyber means by a premeditated act of a State. "In 2013, more than 75 US airports reported phishing—e-mails that attempt to defraud users into revealing financial information. The same year, Miami International Airport experienced more than 20,000 hack attempts per day, and Los Angeles World airports blocked almost 60,000 cases of Internet misuse and 2.9 million hacking attempts."[388] These attacks are escalating in intensity, and concern for military activities is real. This threat remains unresolved, with States denying their cyber operations. "For example, a White Sands Missile Range test exercise demonstrated that the GPS signals used for navigating an unmanned aircraft, or drone, can be accessed remotely to divert the flight onto erroneous paths."[389] Charles Dunlap, former Deputy Judge Advocate General of the US Air Force, noted the challenges associated with the development of any manual on the law of war.[390] In particular, he noted that a key challenge in this process is

[388] Jon Haass, Radhakrishna Sampigethaya & Vincent Capezzuto, "Aviation and Cybersecurity: Opportunities for Applied Research" (2016) Tr News (304): 39 at 40.
[389] *Ibid.*
[390] Charles J. Dunlap, "Law of War Manuals and Warfighting: A Perspective" (2012) 47:2 Texas Intl LJ 265.

turning the focus toward an area involving "new technology that is the subject of few international treaties and does not always easily fit within the legal traditions that emerge from many centuries of conflicts on the land and sea domains."[391] While discussing air and missile warfare, Dunlap observed that "when it involves a means and method of warfare that largely is dominated by a few countries, the challenge is even more daunting to reconcile the legitimate concerns of the leading aviation powers with those of the rest of the family of nations."[392] This reasoning may also be applicable to launching States.

The *Manual on International Law Applicable to Air and Missile Warfare* offers several useful rules that further solidify the understanding of cyber operations in outer space. Rule 1(e) defines the term *attack*.[393] In relevant part, it states in the commentary that:

> "The definition of 'attacks' also covers 'non-kinetic attacks… such as CNAs (*certain computer network attacks*)…that result in death, injury, damage or destruction of persons or objects… There was agreement among the Group of Experts that the term 'attack' does not encompass CNAs that result in an inconvenience (such as temporary denial of internet access)."[394]

The proliferation of cyber incidents interfering with aviation operations highlights some of the future trends that by extension will threaten space activities. Rule 1(m) defines *computer network attack* as:

> "operations to manipulate, disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computer network itself, or to gain control over the computer or computer network."[395]

An actual attack could pose further problems, however, when a State seeks to minimize liability by availing itself of deception, as noted in Rule 167(b). It states in relevant part:

---

[391] *Ibid.*
[392] *Ibid.*
[393] *Manual on International Law Applicable to Air and Missile Warfare*, Rule 1(e) (Cambridge: UK, Cambridge University Press, 2013) at 11-13.
[394] *Ibid* at 12-13.
[395] *Ibid* at 20.

> "(b) However, when Belligerent Parties use for military purposes a public, internationally and openly accessible network such as the Internet, the fact that part of this infrastructure is situated within the jurisdiction of a Neutral does not constitute a violation of neutrality."[396]

Thus, in this case, the question related to cyberspace is not whether the utilization of the network violates the rule. Instead, if it were to be applied to space operations, the rule establishes that regardless of neutrality, the utilization of the network constitutes an attack only if it violates international space law—for example, by displaying characteristics or outcomes that physically harm astronauts.

VI. Manual of Armed Conflicts at Sea

The utilization of technology to carry out cyber operations could have serious consequences for space activities. This notion can be gleaned from the *San Remo Manual on International Law Applicable to Armed Conflicts at Sea*.[397] The lesson extrapolated by the manual is that States are responsible not only for their cyber operations conducted in outer space, but also by their methods chosen, which are not unlimited. These lessons or rules from the sea domain do not address electronic means directly—a notable oversight, although the manual was drafted in 1995. These rules are significant nonetheless, as evidenced by Rules 38, 39, 41, and 42. These rules note in relevant part that:

> Rule 38: "In any armed conflict the right of the parties to the conflict to choose methods or means of warfare is not unlimited."[398]

> Rule 39: "Parties to the conflict shall at all times distinguish between civilians or other protected persons and combatants and between civilian or exempt objects and military objectives."[399]

---

[396] *Manual on International Law Applicable to Air and Missile Warfare*, *supra* note 393 at 386.
[397] Louise Doswald-Beck, ed, *San Remo Manual on International Law Applicable to Armed Conflicts at Sea* (Cambridge: UK, Cambridge University Press, 1995) at pp. 1-4 [San Remo Manual].
[398] *Ibid* at Rule 38.
[399] *Ibid* at Rule 39.

> Rule 41. "Attacks shall be limited strictly to military objectives…"[400]
>
> Rule 42: "In addition to any specific prohibitions binding upon the parties to a conflict, it is forbidden to employ methods or means of warfare which:
>
> (a) are of a nature to cause superfluous injury or unnecessary suffering; or
>
> (b) are indiscriminate, in that:
>
> > (i) they are not, or cannot be, directed against a specific military objective; or
> > (ii) their effects cannot be limited as required by international law as reflected in this document."[401]

Rules 42 in particular would be a useful example for applicability in cyber operations. An attack against the infrastructure associated with a network of satellites, for example, would likely meet the definition of this rule, especially in relation to systems needed for the safety of space activities. Of course, this rule opens the door to potential considerations regarding acts of aggression. Regarding the challenge at hand, Davis Brown, a former US Air Force Judge Advocate, observed that Article 2(4) of the UN Charter is in reality "a complex minefield of nuances, disputable exceptions, and unresolved problems."[402] This is the same challenge presented by the published manuals. The MILAMOS Manual could be viewed as having a focus on decisions made for the protection of the peaceful enjoyment of outer space—activities that are now in danger of suffering the effects of diminished necessary legal mechanisms. Brown was concerned with the contemporary *jus ad bellum* burdened with disagreements entrenched "in the methodologies—and sometimes ideologies—of the law's interpreters."[403] Brown was emphasizing that current positive international law was failing in the provision of needed clarity

[400] *Ibid* at Rule 41.
[401] *Ibid* at Rule 42.
[402] Davis Brown, "Contemporary International Law on the Decision to Use Armed Force", in James Turner Johnson & Eric D. Patterson, eds, *The Ashgate Research Companion to Military Ethics* (New York: NY, Routledge, 2015) at 46.
[403] *Ibid*.

and precision, lacking in natural law, and with a contemporary *jus ad bellum* seemingly moving in the opposite.[404] To turn this in the opposite direction, the MILAMOS Manual must remind its readers that *rules for times of peace* have greater value than those that seek to remedy actions in times of war.

V. Manual of Cyber Operations

Military use of cyberspace in outer space should take note of the lessons learned in the domains of land, sea, and air, while conforming to international space law. The consideration to be made should be one of peace; as Ram Jakhu explained, "an action contrary to this spirit would result in the repudiation of this constitution of outer space."[405] Jakhu noted that "the legal principles of current international space law, especially the Outer Space Treaty, recognize…the global public interest in outer space by assuring all States the right of free access to outer space without discrimination of any kind."[406] While some may be tempted to rationalize that the crossroads of outer space and cyberspace fall in a legal *lacunae*, Jakhu also noted that the drafters of the Outer Space Treaty intentionally left its meaning broad in scope to anticipate future developments in space activities.[407] The guiding principle for the future development of space activities highlighted by Jakhu should be a requisite of any future development of rules applicable to cyber operations conducted in outer space.[408]

Article III of the Outer Space Treaty serves as an important legal basis for cyber operations.[409] Article III also addresses military space activities that rely on cyber operations.[410]

---

[404] *Ibid.*
[405] Ram Jakhu, "Legal Issues Relating to the Global Public Interest in Outer Space" (2006) 32:1 J of Space L 31 at 37. [Referring to the Outer Space Treaty].
[406] *Ibid* at 32.
[407] *Ibid.*
[408] *Ibid.*
[409] Outer Space Treaty, *supra* note 19 at Article 1.
[410] *Ibid.*

Yet, this is strengthened by a prior provision of the treaty: Article I (2) of the Outer Space Treaty declares that "Outer space… shall be free for exploration and use by all States without discrimination of any kind, on a basis of equality and in accordance with international law…"[411] The challenge lies in fitting new cyber-technologies to new realities. "One of the major problems of international law is to determine when and how to incorporate new standards of behavior and new realities of life into the already existing framework, so that, on the one hand, the law remains relevant and, on the other hand, the system itself is not too vigorously disrupted."[412] The central challenge of future rules involves determining the actions to be taken to minimize potential challenges such as attribution. To use an example cited earlier, States, for the most part, chose "silence in reaction to the 2010 Stuxnet operation against Iranian nuclear enrichment centrifuges."[413]

A. Tallinn Manual: Chapter 10

The *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* is the most comprehensive manual on cyber law and addresses some space activities. However, even in its new expanded edition, this manual suffers from a lack of precision. Chapter 10 of the manual contains the rules for space law and cyber activities. The manual should be praised for its focus on the Outer Space Treaty, as noted in Rule 58 (peaceful purposes and uses of force), Rule 59 (respect for space activities), and Rule 60 (supervision, responsibility, and liability).[414] Each rule offers its own specific view and contribution to the clarification of future cyber operations in

[411] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, Article III, January 1967, 18 UST 2410, 610 UNTS 205, 6 ILM 386 at Article I (para 2)1 (entered into force October 1967) [*Outer Space Treaty*].
[412] Malcolm N. Shaw, *International Law* (7th Edition, Cambridge University Press, 2014) at 31
[413] Michael N. Schmitt and Liis Vihul, *supra* note 167.
[414] Tallinn Manual 2.0, *supra* note 22 at 270.

space. Unfortunately, these rules are limited in scope. This limitation is likely attributable to the scope of the manual overall. While a cyberwar *per se* has never been recognized by any nation and while the likelihood of a cyberwar in outer space is remote, the Tallinn Manual focuses on two main phases: *jus ad bellum* and *jus in bello*.[415] This is problematic because the point of departure should have been rules associated with cyber operations in peacetime. Unfortunately, the manual states: "The remainder of Tallinn Manual 2.0 examines key aspects of the public international law governing 'cyber operations' during peacetime. It is not comprehensive in this regard."[416] While the intention was to cover those activities that States' legal advisors would encounter, that process was not comprehensive.[417] The Tallinn Manual, Chapter 10 – Space Law offers three rules applicable to cyber operations in outer space, and Chapter 11, to a lesser degree, offers three rules specific to cyber and international telecommunication law. This thesis will not address the rules in Chapter 11, as these do not offer significant clarification beyond the information found in international space law, specifically the ITU Constitution and Convention and ITU Regulations. These rules could be summarized as Rule 61 (ground infrastructure facilities),[418] Rule 62 (cyber operations subject to national law),[419] and Rule 63 (harmful interference).[420] Returning to Chapter 10, the chapeau states in relevant part that:

> "The International Group of Experts took note of the importance of outer space with regard to cyber activities ranging from civilian communications and navigation to military operations."[421]

[415] *Ibid* at 3.
[416] *Ibid*.
[417] *Ibid*.
[418] Tallinn Manual 2.0, *supra* note 22 at 288.
[419] *Ibid* at 291.
[420] *Ibid* at 295.
[421] *Ibid* at Chapter 10, paragraph 1.

However, the Tallinn Manual makes a neat but unnecessary distinction that appears to originate with US Air Force practices.[422] It states that:

> "Conceptually, when considering the relationship between cyber operations and outer space, it can be useful to distinguish between space-enabled cyber operations and cyber-enabled space operations."[423]

> "As an example, space law per se, as distinguished from other regimes of international law that are applicable to space activities, plays only a small role in assessing the lawfulness of the transmission of malicious code via a satellite communications link."[424]

Space-enabled cyber operations are presented as a different concept from cyber-enabled space operations; however, there is no reference available in the manual (or anywhere) that clearly defines space-enabled cyber operations other than by the two examples that are provided in the manual (which are not referenced). It notes that *space-enabled cyber operations* or "satellite-to-earth and satellite-to-satellite cyber communications have little to do with outer space beyond being enabled by cyber infrastructure based on space assets."[425] The US Department of Defense notes that some satellite communications "preclude the need for long terrestrial communications links", enabling communication "without the need for physical connectivity."[426] While this capability may offer greater cybersecurity to a satellite, nothing precludes an adversary from attempting to interfere with satellite-to-satellite cyber communications from the ground, or in outer space via other means. Even if the technology is sufficiently advanced to avoid interference, there is no indication or source in international law that would exempt space-enabled cyber operations from international space law, as claimed by the Tallinn Manual. It

[422] The only reference to space-enabled cyber operations (other than the Tallinn Manual) is found in a speech by General William Shelton, Commander, Air Force Space Command, titled "Integrating Air, Space & Cyberspace Capabilities" given at the Air and Space Technology Exposition on 17 September 2013. The particular reference is found in page 2.
[423] Tallinn Manual 2.0, Chapter 10, paragraph 2, *supra* note 22 at 270.
[424] *Ibid.*
[425] *Ibid.*
[426] U.S. Department of Defense, Joint Publication 3-14 *Space Operations*, Chapter I (10 April 2018) at II-5.

would be unfounded to base the applicability of space law on the likelihood of vulnerability to cyberattack of a space object. Article III of the Outer Space Treaty requires that space activities shall be conducted "in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international co-operation and understanding."[427] Based on the fundamental principles enshrined in Article III and in the absence of an expressed and clear statement excepting a particular cyber activity in space, there is no reason to assume that Article III does not apply to *space-enabled cyber operations.*

On the other hand, the Tallinn Manual only briefly references Article III, and only within the concept of *cyber-enabled space operations*, which may include "telemetry, tracking, and command systems for communications between ground stations and spacecraft."[428] The Manual further notes that the "legal regime of space law regulates space activities (as well as space objects), a concept that is generally understood to include the 'use', 'exploration', and 'scientific investigation' of outer space."[429] The Manual correctly references Article I of the Outer Space Treaty. Thus, if Article I applies to the use of space objects, then whether these objects are connected to a ground station is immaterial, and space law applies. An equal discord exists within the drafting of the first space rule in the manual: Rule 58 – Peaceful purposes and uses of force. The rule states:

Rule 58 – Peaceful purposes and uses of force

> "(a) Cyber operations on the moon and other celestial bodies may be conducted only for peaceful purposes.
> (b) Cyber operations in outer space are subject to international law limitations on the use of force."[430]

[427] Outer Space Treaty, *supra* note 19 at Article III.
[428] Tallinn Manual 2.0, Chapter 10, paragraph 3, *supra* note 22 at 273.
[429] *Ibid* at paragraph 7.
[430] *Ibid at 273.*

The combination of "peaceful purposes" and "uses of force" in one rule appears to be problematic, simply because it begins the outer space analysis from the point of view of a conflict involving the use of force. In particular, while the commentary of Rule 58 references Article III of the Outer Space Treaty, the use of force would require reliance on the UN Charter Article 2(4), which has already been noted to be a victim of ambiguities.[431] It is these ambiguities that become heightened within the newness of cyberspace. It is possible that Rule 58 would have been better served by drafting two separate rules rather than combining the concepts. Because the two subjects are combined, the rule's commentary suffers from lack of clarity. In addition, the drafters of the manual, on occasion, referred to particular actions by States that would be considered a violation of Rule 58, but did not also refer those violations to the relevant provisions of international space law. While the manual is an important reference, it is not a source of international law. While this manual could become evidence of customary law, now in its second iteration, it cannot reach the level of precision promised by the MILAMOS Project.

Chapter 10 of the Tallinn Manual continues with Rule 59 – Respect for space activities. It states that:

Rule 59 – Respect for space activities

> "(a) A State must respect the right of States of registry to exercise jurisdiction and control over space objects appearing on their registries.
> (b) A State must conduct its cyber operations involving outer space with due regard for the need to avoid interference with the peaceful space activities of other States."[432]

Rule 59 would suffice with section (b) above, while section (a) could have been included in the commentary. That is the case because the action noted in (b) must occur before triggering (a).

[431] Brown, *supra* note 392.
[432] *Tallinn Manual 2.0*, Chapter 10, *supra* note 22 at 277.

The rule extends the reasoning of Rule 58 to registry and jurisdiction. The commentary of Rule 59 addresses a crucial and additional subject that requires its own rule. "The International Group of Experts agreed, therefore, that when cyber activities are conducted in or through outer space, States must consider the impact of their cyber activities on astronauts and, relatedly, the equipment on which astronauts depend for their survival."[433]

The chapter concludes with Rule 60 – Supervision, responsibility, and liability. This rule is likely the most relevant as it addresses the consequences between States associated with cyber operations. It notes that:

Rule 60 – Supervision, responsibility, and liability

> "(a) A State must authorise and supervise the cyber 'activities in outer space' of its non-governmental entities.
> (b) Cyber operations involving space objects are subject to the responsibility and liability regime of space law."[434]

Again, in this case, the drafters appear to have combined what could have been two different rules: one for the activities of non-governmental entities and one needed to address responsibility and liability. Still, this rule is of high relevance given the observations regarding liability found in paragraphs 7 and 8 of the commentary. The scenarios offered within differentiate between cyber operations that have an impact on the surface of the earth versus those that are exclusive to outer space.

Scenario 1:

> "State A is the sole launching State and is operating its satellite… State B's cyber operation causes… the satellite to deorbit, thereby resulting in damage on the territory of State C. State C would be entitled to bring a claim against State A under the Liability Convention or the Outer Space Treaty…[and] State A separately would have recourse against State B under Article VI of the Outer Space Treaty."[435]

[433] *Ibid*, paragraph 7 at 279.
[434] *Ibid* at 279-80.
[435] *Ibid* at 281.

Scenario 2 is similar and liability depends on the State conducting cyber operations. It refers to Article III of the Liability Convention:

> "State A is conducting cyber operations against State B's communications satellite's control system's ground station. The operations alter the satellite's orbit and it collides with State C's satellite. State B is not liable because it was not at fault for the incident."[436]

Although determining exactly what constitutes an illegal cyber operation is not always simple, the final chapter of this thesis aims to provide further clarification. However, one additional matter requires attention within the current chapter: namely, steps to address monitoring, reporting, and fact-finding, which become relevant given the surreptitious nature of cyber operations as they relate to military activities.

VI. Monitoring, Reporting, and Fact-Finding

The results of an investigation or the facts gathered after a cyberattack may provide the grounds for a claim on violations of international law, or specifically international space law. There is no doubt that cyberattacks will continue to be prevalent, or that cyberattacks will continue to be denied by States and by non-State actors alike. However, the next lesson to benefit future rules of engagement requires that mitigation be included in the process of attributing responsibility. Although many attacks have been blamed on specific governments, the required threshold to trigger the relevant international law mechanisms for war has not been met to date. One way to strengthen attribution efforts could be the utilization of monitoring, reporting, and fact-finding practices in cases that involve cyberattacks.[437] The peaceful utilization of outer space will most likely benefit from fact-finding practices aided by a mechanism of prevention.

[436] *Ibid* at 282.
[437] Rob Grace & Claude Bruderlein, "HPCR Draft Working Paper: Building Effective Monitoring, Reporting, and Fact-finding Mechanisms" (2012) Program on Humanitarian Policy and Conflict Research.

The mechanisms of monitoring, reporting, and fact-finding "are the eyes and ears of the international community, allowing international actors to…investigate potential violations of international law."[438] The goal is to seek out evidence that will lead to the establishment of responsibility.[439] After the acquisition of the evidence, the information would be presented to the international community and sanctions would apply accordingly.[440] For example, the *HPCR Practitioner's Handbook on Monitoring, Reporting, and Fact-Finding* discusses the method for determining the sufficiency of international law to be applied domestically.[441] It notes that to "analyze information systematically," the process must include a "standard of proof" that includes "reasonable suspicion, reasonable grounds to believe, and balance of probabilities."[442] One recommendation by the author of this thesis to legal scholars and practitioners is to consider that there could be no accountability without a *standard of proof* becoming part of the process. The driving force should be one of finding solutions that work for the better enjoyment of cyberspace in outer space.

This chapter ends with a note on rules for cyber operations in outer space. The Tallinn Manual and, to a greater extent, the MILAMOS Manual are multi-stakeholder projects. The matter that remains is whether this multi-stakeholder rule-making process will prove advantageous. There is sufficient reason to assert that this is the case. "Having a system in which the relevant actors themselves actively participate in the rule-making and enforcement can be helpful, [which] explains the popularity of such phenomena as… multi-stakeholderism – which

[438] *Ibid* at 1.
[439] *Ibid* at 13.
[440] *Ibid*.
[441] Rob Grace & Claude Bruderlein, eds, *HPCR Practitioner's Handbook on Monitoring, Reporting, and Fact-finding: Investigating International Law Violations* (Cambridge: UK, Cambridge University Press, 2017) at 27.
[442] *Ibid* at 29.

moves us into the area of what cyberspace can teach outer space."[443] Indeed, the actors of space activities appear to be evolving as those already in existence in cyberspace.[444] In a way, cyberspace is better understood as a *sui generis* area of governance. This means that cyberspace exists in a *multi-stakeholder* environment.[445] For these reasons, we may consider the following:

> "The solution is not so hard to identify but extremely hard to implement: it takes political will from states to say that it is acceptable that rules for… cyberspace or for certain activities in outer space can be decided by the relevant parties in a setting of multi-stakeholder participation, including public and private bodies, academia and civil society, on equal terms and with equal rights."[446]

This process may prove easier to implement if the MILAMOS Project is a reflection of the future. As previously noted, military challenges associated with cyber operations are guided by the *jus gentium* of cyberspace; thus, the resolution of these challenges in outer space requires practical rules born out of a multi-stakeholder approach. In this light, Chapter 5 turns toward the *Alternative Rules of Cyberspace.*

[443] Katrin Nyman Metcalf, "A Legal View on Outer Space and Cyberspace: Similarities and Differences", Tallinn Paper No. 10 (NATO Cooperative Cyber Defence Centre of Excellence, 2018) at 9.
[444] *Ibid.*
[445] *See generally*, Internet Corporation for Assigned Names and Numbers, online: < https://www.icann.org/>.
[446] Katrin Nyman Metcalf, *supra* note 443 at 10.

5

Ad Astra: Alternative Rules for Cyberspace

"Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur."
—Air Marshal Giulio Douhet[447]

I. Rules for Post-attack Consequences

The future development of technologies applicable to cyberspace in outer space offers exciting new opportunities for humanity. The stakeholder involved in space activities has new opportunities to participate in the foundation of international space law, and each stakeholder may contribute to the legitimacy of the process simply by conducting cyber operations consistent with international law. Chapter 5 arrives at the final element of consideration: recommendations. The final step in the policy-oriented process is to recommend new rules that aim at an appropriate framework of legal principles of space law for the betterment of humanity. This chapter offers the *recommendations* or rules intended to address specific challenges associated with cyber operations in outer space. One notable gap in the Tallinn Manual is its focus on *jus ad bellum* and *jus in bello*, with no major consideration for activities in times of peace or the ramifications associated with *jus post bellum*.

As noted in Chapter 4, the utilization of cyberspace may violate space law, in particular Article III of the Outer Space Treaty, if the outcome of a cyber operation is equal to the results of kinetic means. For this reason, the rules presented in this chapter are envisioned as potential templates in the formulation of a future manual applicable to the outer space domain. Military

[447] Giulio Douhet, *The Command of the Air*, Joseph Patrick Harahan, and Richard H. Kohn, eds (Tuscaloosa: AL; University of Alabama Press, 1921; 2009) at 30.

manuals provide an avenue to illustrate emerging norms in the form of rules that clarify international law. This is the essence of their drafting process. The process referenced here is not only an emphasis of the rules. Indeed, these rules are the final outcome of a process cemented on international law principles. In this case, two rules or recommendations are proposed in this chapter to manage cyber operations based on gaps observed in the Tallinn Manual and guided by considerations of artificial intelligence and the applicability of the manual's examples found in aviation law and space law. These rules offer a process of analysis that demonstrates how in the absence of treaty law—or at the very least—in the absence of clear answers regarding the applicability of international law to particular scenarios of cyberspace in outer space, these represent a road map to the commanders and practitioners in the field.

The 2015 events faced by Ukrainians with their power grid are illustrative. For example, should civilians' lives be put at risk due to the loss of heat during a cyberattack to a power grid in the middle of the winter? Such a cyberattack may not be an easy feat, but would have terrible consequences. Hackers or "skilled and stealthy strategists" may spend "many months… [conducting] extensive reconnaissance, exploring and mapping the networks and getting access to the Windows Domain Controllers, where user accounts for networks are managed."[448] Once that is accomplished, the reward for the attacker is the access to log in credentials to the SCADA network, which allows the attack.[449] The SCADA acronym stands "for supervisory control and data acquisition, or system control and data acquisition. An application or system utilized for the real-time collection of data from one or more remote locations, with the obtained information

[448] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", *WIRED* (3 March 2016), online: <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>.
[449] *Ibid.*

being utilized to monitor and manage ongoing processes."[450] This monitoring can be utilized as a reverse cyberweapon, given that SCADA systems are utilized "to supervise and control a factory, a transportation system, or a power grid."[451]

Again, nothing is more illustrative to aid in considering future cyber operations in outer space than the events of December 23, 2015, when in the late afternoon hours, the "residents of the Ivano-Frankivsk region of Western Ukraine" experienced an extensive power outage.[452] This is what an operator at the Prykarpattyaoblenergo control center discovered when, to his amazement, "the cursor on his computer suddenly skittered across the screen of its own accord."[453] The SCADA "collection of equipment", which are normally useful for remote operators to access "sufficient information to determine the status of particular equipment or a process", were the source of the vulnerability.[454] Experts observed how hackers were able to incapacitate the power grid, setting the troublesome precedent of becoming "the first confirmed hack to take down a power grid."[455] The problem lies in the way these cyberattacks are conducted: following lawless operations that endanger human life. These types of attacks are also difficult to define; for example, "labeling a *cyberattack* as *cybercrime* or *cyberterrorism* is problematic because of the difficulty determining with certainty the identity, intent, or the political motivations of an attacker."[456] Whether they involve the use of malicious code or additional techniques, these acts expand into the day-to-day life of citizens.[457]

---

[450] Steven M. Kaplan, *Wiley Electrical and Electronics Engineering Dictionary* (Piscataway: NJ, IEEE Press, 2004) at 680.
[451] *Ibid.*
[452] *Kim Zetter, supra* note 448.
[453] *Ibid.*
[454] Mini S. Thomas & John D McDonald, *Power System Scada and Smart Grids* (Boca Raton: FL, CRC Press, 2015) at 4.
[455] *Kim Zetter, supra* note 448.
[456] US, Law Library of Congress, Clay Wilson, *Botnets* (RL32114) (Congressional Research Service, 2008) at 3.
[457] *Ibid.*

While the goal for cyber operations must be one that facilitates global communication, prevention is of high importance to prepare for the dangers associated with military objectives threatening the critical infrastructure of a nation. It is here that the lines between the cyberspace and outer space domains blur. Unfortunately, an attack interfering with air navigation could begin in outer space. For example, "the German military's aviation safety chief [recently] launched a new initiative against cyber threats, citing research that he said shows hackers can commandeer military airplanes with the help of equipment that costs about 5,000 euros."[458] A tool designed to share information may now be utilized as a weapon in the air or outer space. States must also engage and develop countermeasures to ensure that airborne airplanes cannot be hacked from the ground or even by one of the passengers.[459] Imagine another attack that interferes with the Global Navigation Satellite System. Given the nature of cyberspace, difficulties remain about what should be the limit and consequences of State-sponsored activities that may threaten the peaceful utilization of outer space. Article VI of the Outer Space Treaty specifies that:

> "States Parties to the Treaty shall bear international responsibility for national activities in outer space, including the Moon and other celestial bodies, whether such activities are carried on by governmental agencies or by non-governmental entities, and for assuring that national activities are carried out in conformity with the provisions set forth in the present Treaty."[460]

State responsibility arises when cyber operations are conducted in outer space. One alternative offered here is a recommendation by the author of this thesis to include within the space law section of the next draft of the Tallinn Manual an analogous provisions to those found in Rules

[458] Andrea Shalal, "German military aviation command launches cyber threat initiative", *Reuters* (12 July 2017), online: <https://www.reuters.com/article/us-germany-military-cyber-aviation/german-military-aviation-command-launches-cyber-threat-initiative-idUSKBN19X2J6>.
[459] *Ibid.*
[460] Outer Space Treaty, *supra* note 19 at Article VI.

40 and 57 of the same manual. The author of this thesis highlights the importance of these rules and recommends their inclusion in future manuals that address space activities. Rule 40 exemplify future trends in decision by addressing the duty to protect cyber infrastructures, but from the limited point of view of diplomatic and consular missions.[461] A better approach would be to address interference with cyber infrastructures from the point of view of space law. In this manner, ground-based infrastructure facilities are linked to Article VI of the Outer Space Treaty, which provides the legal context within which space activities are assessed to determine whether cyber operations are carried out in conformity with the Outer Space Treaty and the ITU Constitution.[462] Article 45(1) of the ITU Constitution constitutes further context for the establishment and operation of all radiocommunication stations in "a manner as not to cause harmful interference…."[463] Cyber operations conducted by a State in contravention of these principles would be in breach of its international obligations.[464] For the purposes of drafting a new rule, it is necessary to note that the ITU Radio Regulations define *station* as "one or more transmitters or receivers or a combination of transmitters and receivers, including the accessory equipment, necessary at one location for carrying on a radiocommunication service, or the radio astronomy service."[465]

The duty to protect cyber infrastructures should also note that "US Army researchers are surveying the defense industry to find companies able to develop autonomous cyber defenses for tactical networks and communications that capitalize on artificial intelligence and machine learning."[466] For the drafters of future manuals of rules, the main point of analysis should not be

[461] *Tallinn Manual 2.0*, *supra* note 22 at 217.
[462] ITU Constitution, *supra* note 223 at Article 45 (1).
[463] *Ibid*.
[464] *Tallinn Manual 2.0*, *supra* note 22 at 294.
[465] ITU Radio Regulations, *supra* note 224 at art 1.61.
[466] John Keller, "Army eyes autonomous cyber defenses, artificial intelligence, and machine learning for tactical networks, Military & Aerospace Electronics" (January 16, 2019), online:

the technological capabilities of the State, but rather, and in light of space activities, to foresee the consequences of the use of this new technology.[467] Autonomous systems are usually considered from the context of being an 'active' or 'passive' cyber defense.[468] A passive cyber defense usually focuses "on preventing intrusions by making one's network and systems more resilient… [and including for example,] cryptography and steganography (analogous to the use of camouflage and stealth aircraft), security engineering and verification, configuration monitoring and management."[469] For the purposes of a new rule, another example illustrates the potential impact of this technology for space activities:

> "Another example of such an internally functioning autonomous agent would be a program that detects instances of unauthorized access and deletes the data contained in a database on detecting a suspicious access pattern. Given the sheer amount of network traffic flowing through even a regular office network, human intervention or even supervision rarely happens."[470]

Collectively, all factors demonstrate that an effective cyber operation needs to be assessed carefully to guarantee the peaceful utilization of outer space. According to WaterISAC, which collaborates with the US Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), there are 10 basic cybersecurity recommendations that should be top priorities "to reduce exploitable weaknesses and defend against avoidable data breaches and cyber attacks."[471] While the report addressed concerns about

<https://www.militaryaerospace.com/computers/article/16722030/army-eyes-autonomous-cyber-defenses-artificial-intelligence-and-machine-learning-for-tactical-networks>.

[467] Rain Liivoja, Maarja Naagel & Ann Väljataga, "Autonomous Cyber Capabilities under International Law" (NATO Cooperative Cyber Defence Centre of Excellence, 2019) at 11.

[468] *Ibid.*

[469] *Ibid.*

[470] *Ibid.*

[471] "10 Basic Cybersecurity Measures, Best Practices to Reduce Exploitable Weaknesses and Attacks", *WaterISAC* (June 2015) at ii, <online: https://ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_S508C.pdf>. [Developed in partnership with the U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the FBI, and the Information Technology ISAC].

water utilities, the concept can be extrapolated to cyber operations in outer space. From the 10 items proposed, one is included here to illustrate how cybersecurity measures may be integrated into the law applicable to cyber uses of outer space.[472]

> "**Maintain an Accurate Inventory of Control System Devices and Eliminate Any Exposure of this Equipment to External Networks**
>
> Never allow any machine on the control network to talk directly to a machine on the business network or on the Internet. Although some organizations' industrial control systems may not directly face the Internet, a connection still exists if those systems are connected to a part of the network – such as the corporate side – that has a communications channel to external (non-trusted) resources (i.e., to the Internet).
>
> Organizations may not realize this connection exists, but a persistent cyber threat actor can find such pathways and use them to access and exploit industrial control systems to attempt to create a physical consequence. Therefore, organizations are encouraged to conduct thorough assessments of their systems, including the corporate enterprise segments, to determine where pathways exist. Any channels between devices on the control system and equipment on other networks should be eliminated to reduce network vulnerabilities."

Another alternative in the ambit of outer space is to extend or add a similar commentary to that found in Rule 6 of the Tallinn 2.0 Manual (due diligence). Accordingly, a similar rule would have to be rewritten and redirected to applicable cyber operations related to space activities.[473]

Rule 6 – Due diligence

> "A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States."[474]

This rule could also be applied to instances that extend cyber operations into outer space and the new vulnerability: artificial intelligence or AI. As it will be explained in the first proposed rule

[472] *Ibid* at 1.
[473] Tallinn Manual 2.0, *supra* note 22 at 30.
[474] *Tallinn Manual 2.0*, Chapter 2, *supra* note 22 at 30.

below, States must anticipate the challenges associated with artificial intelligence as a step to be addressed in any mitigation strategy. Cyber operations that support space activities may include those related to autonomous systems. This, in turn, remind us that these systems could aid or disrupt the freedom of exploration in the outer space domain. Liu noted:

> "[t]he lack of directly applicable regulation does not absolve legal considerations surrounding the intrinsic characteristics of the weapons themselves, or their use in 'some or all circumstances', because all new means and methods of warfare must be subjected to legal review… recently expressed in Article 36 of Additional Protocol I of 1977 to the Geneva Conventions."[475]

He explained "[t]hat 'the use of means and methods of warfare' may be subject to legal consideration is considered to be customary IHL."[476] Indeed, he reminds of the criteria "elaborated upon by the International Court of Justice in its 1996 Advisory Opinion:"[477]

> "…States do not have unlimited freedom of choice of means in the weapons they use."[478]

These words very much echo what other military manuals have highlighted as noted in Chapter 4. Surprisingly, the commentary of the Tallinn Manual admits that its Group of Experts identified the general due diligence principle as one not achieving *lex lata* status.[479] Yet, the experts saw the need to observe that their comments did not "definitely refute the existence of such a principle."[480] This observation seemed to push the *lex lata* boundary to its limit. Could it be assumed that under *lex lata* standards the resolution to this situation was impractical? However, as noted earlier, the changing nature of technology requires a flexible and rapid approach to problems in existence and for others that are emerging in the horizon.

---

[475] Hin-Yan Liu, "Categorization and Legality of Autonomous and Remote Weapons Systems" (2012) 94:886 Intl Rev Red Cross 627 at 638.
[476] *Ibid*.
[477] *Ibid*. *See also, Legality of the Threat or Use of Nuclear Weapons*, "Advisory Opinion" [1996] ICJ Rep 226, 1996 at 257.
[478] Ibid.
[479] *Tallinn Manual 2.0*, *supra* note 22 at 31.
[480] *Ibid*.

Another approach is to consider Rule 57 of the same manual as an avenue to identify an alternative approach: those that are considered permissible cyber operations. The beauty of this rule is that its approach is drafted from the point of view of international air law, in particular the Chicago Convention.[481] In other words, rather than stating when cyber operations are permissible (and given that international cyber law is still vague), the approach should be to identify when cyber operations are not applicable. Rule 57 deals with "cyber operations jeopardizing the safety of international civil aviation."[482] This rule is intended to tackle air law challenges, and its commentary addresses safety, object functionality, and the term 'weapon,' while referencing back to the Chicago Convention, Article 3*bis*.[483] A similar rule should be applicable to space activities, especially now that the private sector is developing sub-orbital flights and planning deep-space mining missions. In particular, the rule should address those networks that connect to the launching processes, navigation, and overall functioning of satellites. The best available example, although it is not completely applicable, is the above-mentioned Rule 57.

II. Autonomous Cyber Operations

Creating effective cyber policy requires considering the post-attack consequences. This implies that there is value in addressing a cyberattack by giving equal attention to both the first day of an aggressive cyber operation and the consequences of that aggression after the attack. For example, the infrastructure of a nation provides supports for its society's survival and ability to thrive.[484] This critical infrastructure includes government facilities, power plants, water, and

[481] *Convention on Civil Aviation*, 7 December 1944, 15 U.N.T.S. 295 (entered into force 4 April 1947) [Chicago Convention].
[482] Tallinn Manual 2.0, supra note 22 at 268.
[483] *Ibid*.
[484] Georg Kerschischnig, *Cyberthreats and International Law* (The Hague: The Netherlands, Eleven International Publishing, 2012) at 41.

telecommunications.[485] The root of present and future challenges lie with cyber operations that do not easily fit definitions in international law; this is further exacerbated by challenges related to evolving or emerging technologies.

For example, cyberattacks are controlled activities, while autonomous cyber operations, by their designation, imply a degree of autonomy. While this developing concept originates in computer engineering activities, it also affects matters of space activities. "The key benefit realized from autonomy technology is the ability of an autonomous system to explore the possibilities for action and decide 'what to do next' with little or no human involvement."[486] This technology requires an assessment applicable to cyber operations as an integral part of conducting space activities. Indeed, "the most important strength of the technology [is the ability to] perform in ways we cannot *a priori* anticipate."[487]

This chapter discusses "alternative structures and strategies designed to achieve a public order of freedom and human dignity."[488] While cyber operations in support of space activities are permitted in accordance with international law, these must be compatible with established space law principles. For the purposes of this chapter and in order to set the stage for the next set of recommendations, it is important to return to the definition of cyber operations, and in particular, *computer network attacks* as follows:

> An "activity to generate effects on a targeted system or device, such as tampering with data integrity (deletion, modification), affecting availability (disabling, including for prolonged periods of time), or causing physical effects, such as damaging the system, often referred to as a *computer network attack* (CNA), or "effects operations."[489]

[485] *Ibid.*
[486] David J. Atkinson, "Emerging Cyber-Security Issues of Autonomy and the Psychopathology of Intelligent Machines" (Papers delivered at the 2015 AAAI Spring Symposium) at 7.
[487] *Ibid.*
[488] Arthur Jay Silverstein, "Emigration: A Policy Oriented Inquiry" (1974) 2:2 Syracuse J Intl L & Com 149 at 150.
[489] Laurent Gisel & Lukasz Olejnik, *supra* note 42.

The alternatives noted here are further enhanced by the recommendations that follow. These should be understood as "a challenge to the imagination since it makes the creation of alternative-desired futures a factor that the inquirer might commend to the policy process. The task of inventing and evaluating policy alternatives may enable us to realistically approximate the preferred future which we have postulated as a public order of… human dignity."[490] As noted earlier, Article I (2) of the Outer Space Treaty states that "Outer space… shall be free for exploration and use by all States without discrimination of any kind, on a basis of equality and in accordance with international law…"[491] The process referenced here is permeated by the spirit of the treaty and it is beyond proposed new rules for a manual. These rules and its addressed subjects are examples of a potential final outcome found in a legitimate drafting process. In light of these concepts, the first proposed rule is noted below.

A. Proposed Rule 1

Proposed Rule 1 – Autonomous cyber operations

States shall bear international responsibility for national autonomous cyber operations that utilize the medium of outer space as an attack vector against space objects, including those carried out by non-governmental entities, if the State knowingly allows its territory to be used for those activities.

This rule offer four main considerations. First, this rule is inspired by Rule 44 of *the Manual on International Law Applicable to Air and Missile Warfare,* which, in turn, is motivated by Article 58(c) of the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts of June 8, 1977.[492] This

[490] Winston P. Nagan, "African Human Rights Process: A Contextual Policy-Oriented Approach" (1992) 21:1 Southwestern U L Rev 63 at 103.
[491] Outer Space Treaty, *supra* note 19 at Article I (para 2).
[492] International Committee of the Red Cross (ICRC), *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts* (Protocol I), 8 June 1977, 1125 UNTS 3 (entered into force 7 December 1978).

rule is also consistent with Article III of the Outer Space Treaty, since military space activities would involve cyber operations. Chapter 10 of the Tallinn Manual 2.0 clearly notes that:

> "Most of the cyber activities involving outer space contemplated in [the] Manual fall within the ambit of 'use'. The International Group of Experts agreed that the term encompasses both economic and non-economic activities, whether public or private in nature, in outer space and on celestial bodies."[493]

Second, Article VI of the Outer Space Treaty would address States' responsibility for cyber operations in outer space and those carried out by non-governmental entities, while States' responsibility involved in the launch of a space object and as noted in Article VII would also have to be considered in relation to autonomous systems. Proposed Rule 1 is further inspired by Tallinn Manual Rule 58 – Peaceful purposes and uses of force.[494] The rule's commentary makes several references to the '*use-of-force threshold*,' which is problematic by nature. Thus, it is unclear how this term of art that originates in the UN Charter can be applied to cyber operations in outer space. Rule 58 is too limited if its only application involves the precise moment when a State crosses the *use-of-force threshold*. However, it is worth noting that according to Rule 58, the Charter of the United Nations applies to the use of cyberspace during times of peace and rising tensions.[495] Article 2(4) of the Charter states:

> "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[496]

Third, an attack vector on satellites or other space objects would not be conducted "in accordance with international law, including the Charter of the United Nations, in the interest of

[493] Tallinn Manual 2.0, *supra* note 22 at 272.
[494] *Ibid* at 273.
[495] *Ibid* at 274.
[496] United Nations, *Charter of the United Nations*, 24 October 1945, 1 UNTS XVI at Article 2(4).

maintaining international peace and security and promoting international co-operation and understanding."[497] An attack vector should be understood as a method or "[t]he approach used to assault a computer system or network."[498] For this reason, "[c]ybersecurity can be loosely defined as the security measures taken to protect computer information assets and computer controlled assets from attack, where the attack vector has an electronic or "cyber" component."[499] If we are to consider a cyberattack that may tragically end in the destruction of a satellite, or worse, the destruction of a constellation of satellites, then we should also consider this scenario in accordance with the principles of space law and *jus post bellum*. "The goals of cyber warfare—inflicting painful asymmetric damage on an adversary from a distance—are similar to those of aerial bombardment, submarine warfare, special operations forces, and assassins."[500] In reality, "convenience has come at a price" in a world where national critical infrastructures are connected to the Internet and managed remotely and easily.[501] Ironically, back in 1994, the idea that true damage could be done via the Internet would have been considered hypothetical. However, the Estonia attacks changed that perspective.[502]

We were also reminded in Chapter 3 that State activities designated as cyber operations are supported by the norms found in the General Assembly Resolution 70/237. This resolution emphasizes emerging principles formed by consensus in the UN GGE on Developments in the Field of Information and Telecommunications in the Context of International Security.[503] The

[497] *Ibid* at Article 1(1).
[498] "Definition of Attack Vector", *PC Magazine*, Encyclopedia (2019), online: <https://www.pcmag.com/encyclopedia/term/57711/attack-vector>.
[499] Ben Meroney, "Cybersecurity for Critical Infrastructure Operators in the Oil and Gas Industry" (2018) 64 Annual Institute on Mineral L 2 at 2.
[500] Kenneth Geers, "The Cyber Threat to National Critical Infrastructures: Beyond Theory" (2009) 18:1 Information Security Journal: A Global Perspective 1 at 4.
[501] *Ibid* at 5.
[502] Gadi Evron, *supra* note 142.
[503] United Nations Office for Disarmament Affairs, Group of Governmental Experts, *supra* note 262. *See also*, Resolution adopted by the General Assembly 70/237, Developments in the field of information and

2015 UN GGE report delineated an emerging consensus "on norms, rules or principles of the responsible behavior of States," and in particular it noted:[504]

- "States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts."[505]

The collective wisdom found in this UN GGE report points toward the observation of States that may knowingly allow their territory to be utilized for cyber operations contrary to the rights of other States. For example, "sometimes persons or entities who are not state organs are permitted by the domestic law of a state to exercise elements of governmental authority. So long as they are acting in that capacity, their actions will be considered an act of that state."[506]

Fourth, one important realization is that the issue of autonomous systems was not addressed in the Tallinn Manual. One way to enhance the understanding and clarification of *lex lata* would be to consider autonomous systems along with the ethical implications associated with cybersecurity law and its impact on cyber operations conducted in outer space. For example, the Montréal Declaration for Responsible Development of Artificial Intelligence offers a set of ethical guidelines for the development of artificial intelligence.[507] In particular, Principle 9(2) states that:

---

telecommunications in the context of international security (23 December 2015) [report of the First Committee (A/70/455)] at ¶2 (a).

[504] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UNGAOR, 70th Sess, UN Doc A/70/174 (2015) at ¶24. [List of members of the Group of Government Experts (2015): Belarus, Brazil, China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, Republic of Korea, Russian Federation, Spain, United Kingdom of Great Britain and Northern Ireland, and the United States of America].

[505] *Ibid* at ¶ 28(e).

[506] Michael N. Schmitt and Liis Vihul, "Proxy Wars in Cyberspace: The Evolving International Law of Attribution" (2014) 1 FLETCHER SEC. REV. 53 at 60.

[507] "Montréal Declaration for Responsible Development of Artificial Intelligence", *Université de Montréal* (2017), online: < https://www.montrealdeclaration-responsibleai.com/>.

> "[i]n all areas where a decision that affects a person's life, quality of life, or reputation must be made, where time and circumstance permit, the final decision must be taken by a human being and that decision should be free and informed."[508]

The principles of the Montreal Declaration could easily be understood as an extension of a cybersecurity mitigation plan. Indeed, military space activities could involve the use of autonomous systems to interfere with the quality of life of astronauts. Calo observed that "[i]nternational consensus holds that people should never give up "meaningful human control" over a kill decision. Yet debate lingers as to the meaning and scope of meaningful human control. Is monitoring enough? Target selection?"[509] He also noted that "[t]here is also the question of who bears responsibility for the choices of machines."[510] The international space law applicable to military activities needs to consider ethical principles that fundamentally changes the future outlook of space activities. Schmitt & Thurnher also noted that "[t]he crux of full autonomy, therefore, is the capability to identify, target, and attack a person or object without human interface. Although a human operator may retain the ability to take control of the system, it is capable of operating on its own."[511] The past and present rules of warfare have presented trends that serve as templates for a future manual applicable to outer space. In the ambit of cyber or cyber and space, autonomous systems could be seen as an avenue to potential escalation in cyber warfare. Schmitt & Thurnher also observed that "[t]here is universal consensus that the law of armed conflict applies to autonomous weapon systems… What is contentious is *how* particular norms apply to new systems, such as… cyber weapons, and autonomous weapon

[508] *Ibid* at Principle 9(2).
[509] Ryan Calo, "Artificial Intelligence Policy: A Primer and Roadmap" (2017) 51:2 UC Davis L Rev 399 at 416.
[510] *Ibid.*
[511] Michael N Schmitt & Jeffrey S Thurnher, "Out of the Loop: Autonomous Weapon Systems and the Law of Armed Conflict" (2013) 4:2 Harvard National Security J 231 at 235.

systems."[512] Would the use of autonomous weapon systems be considered an attack or an inconvenience as noted in Rule 1(e) of the Manual on International Law Applicable to Air and Missile Warfare?[513] Would it be considered an action that causes superfluous injury as noted by Rule 42 of the San Remo Manual?[514] As noted earlier, Rule 42 in particular would be a useful example for its applicability in relation to systems needed for the safety of space activities. It is safety that provides the foundation for the second proposed rule.

III. Safety of Space Activities

The intention of the next proposed rule below is one of cooperation and, as such, is intended for cyberthreat prevention. It also addresses the actions to be taken to minimize attribution challenges.

A. Proposed Rule 2

Proposed Rule 2 – Cyber operations concerning the safety of space activities

A State may not conduct cyber operations that adversely affect the safe use of outer space.

The elements necessary to consider what constitutes an act that adversely affect the safe use of outer space could be culled from the 1972 Liability Convention,[515] San Remo Manual Rule 39 and Tallinn Manual Rule 57. As noted earlier, these rules state the following:

> San Remo Rule 39: "Parties to the conflict shall at all times distinguish between civilians or other protected persons and combatants and between civilian or exempt objects and military objectives."[516]

[512] *Ibid* at 243.
[513] *Manual on International Law Applicable to Air and Missile Warfare*, Rule 1(e), *supra* note 393.
[514] Doswald-Beck, ed, *San Remo Manual on International Law Applicable to Armed Conflicts at Sea*, *supra* note 397 at Rule 42.
[515] *Convention on International Liability for Damage Caused by Space Objects*, *supra* note 217.
[516] San Remo Manual, *supra* note 397 at Rule 39.

> Tallinn Rule 57 – Cyber operations jeopardizing the safety of international civil aviation: "A State may not conduct cyber operations that jeopardize the safety of international civil aviation."[517]

The rule also highlights the principles of the Liability Convention and Article VI of the Outer Space Treaty, which, in its first sentence, notes that "*States Parties to the Treaty shall bear international responsibility for national activities in outer space….*"[518] Legal issues related to cyber operations arise from the article's words "national activities in outer space."[519] As noted by consensus, the principles of the responsible behavior of States in cyberspace requires refraining "from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations…"[520] A violation could occurs when a State utilizes "proxies to commit internationally wrongful acts using ICTs," and when non-State actors utilize their territory to violate those principles.[521] The safety of activities or personnel in outer space would be an expected outcome. Yet, "[i]n the realm of cyberspace, an internationally wrongful act can consist of a breach of either the rules governing peacetime or those applicable in an armed conflict."[522] The safety associated with cyber operations in outer space should consider not only those by the State but also those carried out by non-governmental entities, when the State has knowledge of those activities. "Since non-state actors such as hacktivists often launch harmful cyber operations, and, in light of the likelihood of the use of cyberspace by terrorists, a State's obligation to take measures to control cyber activities taking place on its territory looms especially large."[523]

[517] Tallinn Manual 2.0, *supra* note 22 at 268.
[518] Outer Space Treaty, *supra* note 19 at Article VI.
[519] *Ibid*.
[520] Group of Governmental Experts, *supra* note 265 at ¶26.
[521] *Ibid* at ¶28(e).
[522] *Tallinn Manual 2.0*, Chapter 4, ¶4, *supra* note 22 at 85.
[523] *Ibid* at ¶5.

However, a malicious cyber operation could pose further problems if a State seeks to minimize liability by availing itself of deception—for example, as noted in Air and Missile Warfare Manual Rule 167(b). It states in relevant part:

> "(b) However, when Belligerent Parties use for military purposes a public, internationally and openly accessible network such as the Internet, the fact that part of this infrastructure is situated within the jurisdiction of a Neutral does not constitute a violation of neutrality."[524]

Thus, in this case, the question related to cyberspace is not whether the utilization of the network violates the rule. Rather, if it were to be applied to space activities, the rule establishes that regardless of neutrality, the utilization of the network constitutes an attack posing challenges of attribution associated with liability for damage caused to a hacked space object. "Given the complexity and interdependence of an openly accessible network such as the Internet, it is impossible for any State to effectively control or interfere with communications over such a network."[525] For the victim State, without knowing who initiated an attack, it would be difficult to determine responsibility, and much less liability.[526] The victim State would also have to deal with the post-attack consequences. For this reason, the related after-effects and consequences of an attack should also be understood within the alternative lessons of *jus post bellum*. Following the line of progression begun by *jus ad bellum* and *jus in bellow*, *jus post bellum* reminds "about the ethical and moral actions that States face after a war has concluded."[527] For the purposes of cyber operations, the consequences would be noticed within hours. It is reasonable to predict that space lawyers may have to "anticipate the changes in the character of war."[528] This anticipatory step takes into consideration that "*jus ad pacem* has recently gained currency in just war theory

[524] *Manual on International Law Applicable to Air and Missile Warfare*, *supra* note 393 at 386.
[525] *Ibid* at 387.
[526] Kerschischnig, *Cyberthreats and International Law*, *supra* note 477 at 128-29.
[527] Maribel Cisneros, *Cyber-warfare: Jus Post Bellum* (Master of Science Thesis, Cyber Systems and Operations, Naval Postgraduate School, 2015) at 10, online: < https://calhoun.nps.edu/handle/10945/45169>.
[528] Douhet, *supra* note 447.

as a blanket term for ethical responsibilities at the end of war and in peacekeeping operations. Literally 'justice in achieving peace,' *jus ad pacem* is also commonly referred to as '*jus post bellum*,' justice after war."[529] In the realm of cyberspace, it would be difficult to dismiss the consequences of a successful cyberattack against the sophisticated systems of a power grid [or satellite]; for this reason, such cyberattacks would require significant resources available only to the aggressor States.[530] There is a high probability of a potential disaster residing within global "critical infrastructures, including electric power, telecommunications, and the Internet."[531] This is why attribution must be part of the discussion associated with space activities. Following the guidance of the ICJ, cyber-attribution could be identified as an operation under the control of an agent or representative of the State.[532] The ICJ decision on the *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* noted the:

> "well-established rule, one of the cornerstones of the law of State responsibility, that the conduct of any State organ is to be considered an act of the State under international law, and therefore gives rise to the responsibility of the State if it constitutes a breach of an international obligation of the State."[533]

This rule, which the Court noted as "one of customary international law" is reflected in Article 4 and 5 of the International Law Commission Articles on State Responsibility as follows:

"Article 4: Conduct of organs of a State"[534]

> "1. The conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State,

[529] Jordy Rocheleau, "Jus ad Pacem" in Deen K Chatterjee, ed, *Encyclopedia of Global Justice* (Dordrecht: Netherlands, Springer, 2011) at 582.
[530] Robert K. Knake, "Contingency Planning Memorandum No. 31: A Cyberattack on the U.S. Power Grid" (Council on Foreign Relations, 2017), online: <https://cfrd8files.cfr.org/sites/default/files/pdf/2017/03/ContingencyPlanningMemo31_Knake.pdf>.
[531] *Ibid*.
[532] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)*, "Merits Judgement" [2007] ICJ Rep 43 at 202.
[533] *Ibid*.
[534] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, Supplement No. 10, UN Doc A/56/10, chp.IV.E.1 (2001) at Article 4.

> and whatever its character as an organ of the central Government or of a territorial unit of the State.
> 2. An organ includes any person or entity which has that status in accordance with the internal law of the State."[535]
>
> "Article 5. Conduct of persons or entities exercising elements of governmental authority"[536]
> "The conduct of a person or entity which is not an organ of the State under article 4 but which is empowered by the law of that State to exercise elements of the governmental authority shall be considered an act of the State under international law, provided the person or entity is acting in that capacity in the particular instance."[537]

The commentary of Article 4 notes in relevant part that this article "states the first principle of attribution for the purposes of State responsibility in international law—that the conduct of an organ of the State is attributable to that State. The reference to a 'State organ' covers all the individual or collective entities…"[538] The question arises when a State knowingly allows its territory to be used for cyber operations of non-State actors. Thus, a cyberattack on a space object, "because of its scale and effects," could be classified as violation of space law rather than as a "mere" cyber operation with little consequence.[539] Furthermore, following the reasoning of the ICJ, this violation of state responsibility would likely apply to a non-government group of hackers under the supervision of the State.[540] The commentary of Article 5 appears to support this assessment. Uncertainty remains regarding whether the group of hackers that were involved in the Estonia attack had Russian supervision.[541]

[535] *Ibid.*
[536] *Ibid.*
[537] *Ibid.*
[538] *Ibid.*
[539] *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America);* "Merits, Judgement" [1986] ICJ Rep 4, at 93.
[540] International Law Commission, *Draft Articles on Responsibility of States*, supra note at Article 5 Commentary.
[541] Gadi Evron, *supra* note 142 at 124.

Conclusion

"*Here men from the planet Earth/First set foot upon the Moon/July 1969 A.D./ We came in peace for all mankind*."[542]

Two main factors take the conclusion of this thesis to its final comments. First, the cyberspace environment now interacts with space activities. And second, there cannot be peaceful activities in outer space without cybersecurity. There is a new motivation to expand the valuable resources afforded by cyberspace into the expanse of outer space. There is also enough proposals for exploration to be optimistic about the future. Yet, there are also enough threats to foresee a worrisome future of challenges and political perceptions. As noted in Chapter 1, this is the ironic foreshadowing of what will be at the heart of the tensions anticipated at the intersection of space law and cyberspace law. To resolve the overall challenge, the analysis concentrated in the wisdom provided by the shaping of emerging norms in the form of *manuals* with precise rules that fundamentally clarify the international legal system. With respect to cyber operations, there has been little guidance found within international cyberspace law. However, there are signs that an emerging customary law is in formation. This law-in-formation, as noted in Chapter 3, can begin to be culled from emerging norms acknowledged by the UN Governmental Group of Experts.[543]

As States seek ways to protect their space infrastructure sectors, scholars and practitioners will need to evaluate the emerging cyberthreats. Due to this evolution, active military personnel in the field of operations should anticipate that the law applicable to military uses of cyberspace in outer space will be in flux. A manual intended to clarify the applicability of international law to particular scenarios of cyberspace in outer space in times of peace is

[542] NASA, News Release, No 69-83F, "Apollo 11 Goodwill Messages" (13 July 1969) at 2.
[543] Group of Governmental Experts, *supra* note 264.

necessary and vital. Both, a future edition of the Tallinn Manual and the new MILAMOs Manual must address cyber operations as these relate to space activities. This thesis proposed new trends and rules for cyberspace applicable to military uses in outer space (as noted in Chapters 4 and 5). These suggestions offer a step forward to fill a legal gap in the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.[544] Following the Rubenfeld's reasoning previously noted, vagueness and ambiguity may arise due to the lack of legal standards applicable to cyber operations in outer space.[545] The solution begins to take shape simply by predicting what rules will be successful in view of events that define State behavior in outer space. Also, following the reasoning from Judge Lachs previously noted in Chapter 3, regarding the serious challenge associated with law and technology, he noted "one it must meet, lest it lag even farther behind events than it has been wont to do."[546]

To meet this challenge directly, rules intended to clarify the applicability of international law to particular scenarios involving space activities is a necessity. If a manual is going to address the domain of outer space as it relates to cyberspace, then the wisdom contained in prior military manuals has been very useful to predict and identify trends for rule drafting processes. If scholars intend to aid the commanders in the field, as seen in Chapter 5, the aim should be to find a solution that transcend politics, while devising new rules for cyber operations and space activities. The utilization of cyberspace will require new rules of engagement, which in turn will reflect the *lex lata* intended to address space activities. Looking at the rule making process at it most basic level, Gerald Postema explained the importance of practices and participants to identify "normative guidance… and reasons for their actions."[547] This process may prove easier

[544] Schmitt, *Tallinn Manual 2.0*, *supra* note 22.
[545] Rubenfeld, *supra* note 247 at 32.
[546] North Sea Continental Shelf Cases, Dissenting Opinion of Judge Lachs, *supra* note 54 at 230.
[547] Gerald J. Postema, *supra* note 723.

to implement if the MILAMOS Project reveals the accepted military standards associated with cyber operations. The *Rules of Cyberspace*, noted in the last chapter of this thesis, offers an alternative to protect the future legacy of space activities in accordance with international law and established space law principles.

Bibliography

Legislation

US, Bill HR 5344, *A Bill to Authorize the National Science Foundation to Foster and Support the Development and Use of Certain Computer Networks*, 102nd Cong, 1992. *See also*, *Scientific and Advanced-Technology Act of 1992*, 42 U.S.C. § 1862(g) (1991-1992).

Jurisprudence: ICJ

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro), "Merits Judgement" [2007] ICJ Rep 43.

Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America); "Merits, Judgement" [1986] ICJ Rep 4.

Legality of the Threat or Use of Nuclear Weapons, "Advisory Opinion" [1996] ICJ Rep 226, 1996 at 257.

North Sea Continental Shelf Cases (Federal Republic of Germany v. Denmark; Federal Republic of Germany v. Netherlands), "Dissenting Opinion of Judge Lachs" [1969] I.C.J. Rep 3.

Jurisprudence: US

Reno v. ACLU, 521 U.S. 844, 850-51; 117 S.Ct. 2329, 2334-2335; 138 L.Ed.2d 874, 851 (1997).

The Paquete Habana and the Lola, 175 U.S. 677 (1900).

UN Treaties, Agreements and Conventions

Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Council of Europe, 28 January 2003, ETS 189 (entered into force 1 March 2006).

Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security,16 June 2009, Shanghai Cooperation Organisation, online: < https://ccdcoe.org/organisations/sco/>.

Agreement Governing the Activities of States on the Moon and Other Celestial Bodies,18 December 1979, 18:6 Intl Leg Materials 1434 (entered into force on 11 July 1984).

Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space, 22 April 1968, 672 UNTS 119, 19. U.S.T. 7570, TIAS 6599 (entered into force on 3 December 1968).
Convention on Civil Aviation, 7 December 1944, 15 U.N.T.S. 295 (entered into force 4 April 1947).

Convention on Cybercrime, Council of Europe, 23 November 2001, 2296 UNTS 167, ETS 185 (entered into force 1 July 2004).

Convention for the Amelioration of the Condition of the Wounded and Sick in Armies in the Field, 6 July 1906, 11 L.N.T.S. 440, online: <https://ihl-databases.icrc.org/ihl/INTRO/180?OpenDocument>.

*Convention on International Liability for Damage Caused by Space Objects***,** 29 March 1972, 961 UNTS 187, 24 U.S.T 2389, TIAS 7762 (entered into force on 1 September 1972).

Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, 18 October 1907, 36 Stat. 2277, TS 539, online: < https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?action=openDocument&documentId=4D47F92DF3966A7EC12563CD002D6788>.

Constitution and Convention of the International Telecommunication Union, 22 December 1992, 1825 UNTS 330, ATS (1994) 28, BTS 24 (1996) (entered into force date 1 July 1994), as amended by the 2018 Plenipotentiary Conference.

Convention on Registration of Objects Launched into Outer Space,14 January 1975, 14:1 Intl Leg Materials 43 (entered into force on 15 September 1976).

International Committee of the Red Cross, *Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land*, The Hague, 18 October 1907", online: <https://ihl-databases.icrc.org/ihl/INTRO/195>.

International Telecommunication Regulations, International Telegraph and Telephone Conference, 9 December 9, 1988, as revised and adopted by the 2015 World Radiocommunication Conference.

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, 27 January 1967, 610 UNTS 205, 6 ILM 386 (entered into force 10 October 1967).

United Nations, *Charter of the United Nations*, 24 October 1945, 1 UNTS XVI.

U.N. Resolutions and Other International Documents

Ad Hoc Committee on the Peaceful Uses of Outer Space, *Report of the Legal Committee*, UN Doc A/AC.98/2 (1959).

Council of Europe, Committee of Experts on Crime in Cyber-Space, 50th plenary Sess, Explanatory report of the Convention on Cybercrime, CM (2001)144 addendum (2001), online: <https://rm.coe.int/16804d873c>.

Council of Europe, *Convention on Cybercrime*, Explanatory Report, C.E.T.S. No. 185, ¶ 38 (Nov 8, 2001), https://rm.coe.int/16800cce5b.

Council of the European Union, Press Release, 357/17, "Cyber attacks: EU ready to respond with a range of measures, including sanctions" (19 June 2017), online: <http://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/>.

Council of the European Union, Secretariat, *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Activities*, Doc 9916/17 (2017) at paragraph 1, online: <http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf.>.

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UNGAOR, 60th Sess, UN Doc A/68/98 (2013).

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UNGAOR, 70th Sess, UN Doc A/70/174 (2015) at ¶24.

International Committee of the Red Cross (ICRC), *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts* (Protocol I), 8 June 1977, 1125 UNTS 3 (entered into force 7 December 1978).

International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, Supplement No. 10, UN Doc A/56/10, chp.IV.E.1 (2001).

International Law Commission, *Report of the International Law Commission*, UNGAOR, 68th Sess, Supp No 10, UN Doc A/71/10 (2016).

Question of the Peaceful Use of Outer Space, GA Res 1348(XIII), UNGAOR, 13th Sess, UN Doc A/RES/13/1348(XIII) (1958).

No first placement of weapons in outer space, GA Res, UNGAOR, 69th sess, Suppl. no. 49, UN Doc A/RES/69/32 (2014).

Secretariat of the Working Group on Internet Governance, *Report of the UN Working Group on Internet Governance*, UNSG, Working Group on Internet Governance (June 2005).

Statute of the International Court of Justice, Article 38, ¶ 1, TS No 993.

UNODA, *Prevention of an arms race in outer space, Report of the First Committee*, UNGAOR, 69th Sess, UN Doc A/69/438 (2014).

Secondary Material: Books

Abbate, Janet. *Inventing the Internet* (Cambridge: MIT Press, 2000).

Bronowski, Jacob. *Science and Human Values* (New York: Harper Perennial, 1990).

Brown, Davis. "Contemporary International Law on the Decision to Use Armed Force", in James Turner Johnson & Eric D. Patterson, eds, *The Ashgate Research Companion to Military Ethics* (New York: NY, Routledge, 2015).

Brownlie, Ian. *Principles of Public International Law*, 8th ed. (New York: Oxford University Press, 2012).

Cassese, Antonio. *International Law* (New York: Oxford University Press, 2005).

Chaikin, Andrew & Victoria Kohl, *Mission Control, this is Apollo: The Story of the First Voyages to the Moon* (New York: Viking Books, 2009).

Cook, Martin L. "Ethical Issues in War: An Overview" in J. Boone Bartholomees, Jr., ed, *U.S. Army War College: Guide to National Security Policy and Strategy* (Carlisle: PA, 2004).

Dickson, Paul. *Sputnik: The Shock of the Century* (Walker Publishing, 2001).

Douhet, Giulio. *The Command of the Air*, Joseph Patrick Harahan, and Richard H. Kohn, eds (Tuscaloosa: AL; University of Alabama Press, 1921; 2009) at 30.

Grace, Rob & Claude Bruderlein, eds, *HPCR Practitioner's Handbook on Monitoring, Reporting, and Fact-finding: Investigating International Law Violations* (Cambridge: UK, Cambridge University Press, 2017).

Grøn, Øyvind & Sigbjørn Hervik, *Einstein's General Theory of Relativity* (New York: Springer-Verlag, 2007).

Gibson, William. *Neuromancer* (New York: Penguin Random House, 2016).

Hagen, Regina & Jürgen Scheffran, "International Space Law and Space Security: Expectations and Criteria for a Sustainable and Peaceful Use of Outer Space" in Marietta Benkö and Kai-Uwe

Schrogl, eds, *Current Problems and Perspectives for Future Regulation* (AJ Utrecht: The Netherlands, Eleven International Publishing, 2005).

Hall, J. A. *The Law of Naval Warfare* (London: Chapman & Hall, LTD., 1914).

Hamilton, Edith, *The Greek Way* (New York: W. W. Norton & Company, 1930; 2017).

Handel, Michael I. *Sun Tzu and Clausewitz: The Art of War and On War Compared* (Carlisle Barracks, PA, Strategic Studies Institute, U.S. Army War College, 1991).

Hansen, James R. *First Man: The Life of Neil A. Armstrong* (New York: Simon and Shuster, Inc., 2018).

Hardin, Russell. "Normative Methodology" in Janet M. Box-Steffensmeier, Henry E. Brady & David Collier, eds., *The Oxford Handbook of Political Methodology* (Oxford: UK, Oxford University Press, 2010).

Harris, Alexandra & Ray Harris, "Air and Space Demarcation" in Stanley D. Brunn, ed, *Engineering Earth: The Impacts of Megaengineering Projects* (Berlin: Germany, Springer, 2011).

Henriksen, Andres "Politics and the development of legal norms in Cyber Space" in Karstn Friis & Jens Ringsmose, *Conflict in Cyber Space* (NY: NY, Routledge, 2016).

Jenks, C. Wilfred. "The Evolution of Space Law Continues" in *Essays in International Law in Honour of Juraj Andrassy* (The Hague: Netherlands, Martinus Nijhoff, 1968).

Kaplan, Steven M. *Wiley Electrical and Electronics Engineering Dictionary* (Piscataway: NJ, IEEE Press, 2004).

Kerschischnig, Georg. *Cyberthreats and International Law* (The Hague: The Netherlands, Eleven International Publishing, 2012).

Lachs, Manfred. *The Law of Outer Space: An Experience in Contemporary Law-Making* (Leiden: The Netherlands, Martinus Nijhoff Publishers, 1972, 2010).

Launius, Roger D. *APOLLO: A Retrospective Analysis* (Washington, DC: NASA History Office, NASA Headquarters, 1994).

Lawrence, Thomas Joseph. *The Principles of International Law* (Norwood: MA, Norwood Press, 1895).

Lincoln, Abraham. "A House Divided: Speech at Springfield, Illinois" in Roy P. Basler, ed, *The Collected Works of Abraham Lincoln, Volume 2* (New Brunswick, Rutgers University Press, 1953).

Lucas Jr, George R. "Cyber Warfare" in James Turner Johnson & Eric D. Patterson, eds, *The Asgate Research Companion to Military Ethics* (Surrey: England, Asgate Publishing, 2015).

Maral, Gérard & Michel Bosquet, *Satellite Communications Systems* (West Sussex: UK, 2 Wiley, 2009).

McDougal, Myers S., Harold D. Lasswell & Ivan A. Vlasic, *Law and Public Order in Space* (New Haven and London: Yale University Press, 1963) at 17.

Molander, Roger C. Peter A. Wilson, and Robert H. Anderson, "U.S. Strategic Vulnerabilities: Threats Against Society" in Tom LaTourrette, David R. Howell, et al., eds, *Strategic Appraisal: The Changing Role of Information in Warfare* (Washington D.C.: RAND Corporation, 1999).

Rocheleau, Jordy. "Jus ad Pacem" in Deen K Chatterjee, ed, *Encyclopedia of Global Justice* (Dordrecht: Netherlands, Springer, 2011).

Schmitt, Michael N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).

Shaw, Malcolm N. *International Law* (7th Edition, Cambridge University Press, 2014).

Spencer, Jr., Ronal L. "International Space Law: A Basis for National Regulation" in Ram S. Jakhu ed., *National Regulation of Space Activities* (New York, Springer, 2010).

Tasioulas, John. "Customary International Law and the Quest for Global Justice" in Amanda Perreau-Saussine & James Bernard Murphy, eds, *The Nature of Customary Law: Legal, Historical and Philosophical Perspectives* (Cambridge: UK, Cambridge University Press, 2007).

Thomas, Mini S. & John D McDonald, *Power System Scada and Smart Grids* (Boca Raton: FL, CRC Press, 2015).

Von Clausewitz, Carl, *On War* (Princeton: Michael Howard and Peter Paret, eds, Princeton University Press, 1976).

Wells, Donald A. *The Laws of Land Warfare: A Guide to the U.S. Army Manuals* (Westport: Connecticut, Greenwood Press, 1992).

Wells, H.G. *The Time Machine* (Mineola: NY, Dover Publications, 1995).

Secondary Material: Military Manuals

Doswald-Beck, Louise, ed, *San Remo Manual on International Law Applicable to Armed Conflicts at Sea* (Cambridge: UK, Cambridge University Press, 1995).

General Counsel of the Department of Defense, *Law of War Manual* (Washington, D.C.: Department of Defense).

Manual on International Law Applicable to Air and Missile Warfare (Cambridge: UK, Cambridge University Press, 2013).

Manual on International Law Applicable to Military Uses of Outer Space, online: <https://www.mcgill.ca/milamos/>.

Ministry of Defence, *Joint Doctrine Publication 0-01.1, UK Terminology Supplement to NATOTerm* (January 2019, Edition A).

The Judge Advocate General's School, *Air Force Operations & the Law: A Guide for Air, Space, and Cyber Forces,* 3rd ed. (Alabama: Maxwell Air Force Base, 2014).

U.S. Department of Defense, Joint Publication 3-14 *Space Operations*, Chapter I (10 April 2018).

U.S. Joint Chiefs of Staff, *Joint Publication 3-0, Joint Operations* (17 January 2017).

Office of the Chairman of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms* (Washington DC: The Joint Staff, July 2019).

US Army, *FM 3-12 Cyberspace and Electronic Warfare Operations* (Washington, D.C.: Department of the Army, 2017).

US Army Training and Doctrine Command, *21st Century U.S. Army Law of the Land Warfare Manual (FM 27-10)* (Washington, D.C.: Department of Defense, 2017).

Secondary Material: Law Journals

Boothby, Bill, "Space Weapons and the Law" (2017) 93 Intl L Studies Series. US Naval War College 179.

Bourely, Michel. "The Institutional Framework of Space Activities in Outer Space" (1998) 26:1 Journal Space Law 1.

Brown, Gray & Keira Poellet, "The Customary International Law of Cyberspace" (2012) 6:3 SSQ 126.

Calo, Ryan. "Artificial Intelligence Policy: A Primer and Roadmap" (2017) 51:2 UC Davis L Rev 399 at 416.

Campbell, Peter. "Generals in Cyberspace: Military Insights for Defending Cyberspace" (2018) 62:2 Orbis 262.

Chandrahasan, Nirmala. "The Continuing Relevance of Customary International Law in the Development of International Humanitarian Law" (2009) 21:2 Sri Lanka J of Intl L 55 at 62.

Cooper, John C. "High Altitude Flight and National Sovereignty" (1951) 4:3 The International Law Quarterly 411.

Dunlap, Charles J. "Law of War Manuals and Warfighting: A Perspective" (2012) 47:2 Texas Intl LJ 265.

Eilstrup-Sangiovanni, Mette. "Why the World Needs an International Cyberwar Convention" (2018) 31:3 Philos. Technol. 379.

Evron, Gadi. "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War" (2008) 9:1 Geo. J. Int'l Aff. 121.

Fidler, David P., Richard Pregent & Alex Vandurme, "NATO, Cyber Defense, and International Law" (2013), 4:1 St. John's J of Intl & Comparative L 1.

Freeland, Steven. "In Heaven as on Earth - The International Legal Regulation of the Military Use of Outer Space" (2011) 8:3 US-China L Rev 272.

Geers, Kenneth. "The Cyber Threat to National Critical Infrastructures: Beyond Theory" (2009) 18:1 Information Security Journal: A Global Perspective 1.

GAZDIK, Julian "International Review" (1959) 26:4 J. Air L. & Com. 359.

Goldsmith, Jack. "How Cyber Changes the Laws of War" (2013) 24:1 EJIL 129.

G.G. W., "Book Review" (1910-1911) 24 Harv. L. Rev. 413.

Higgins, A. Pearce. "The Late Doctor T. J. Lawrence" (1920-1921) 1 Brit. Y.B. Int'l L. 231.

Hollis, Duncan B. "Why States Need an International Law for Information Operations" (2007) 11:4 Lewis & Clark L. Rev. 1023.

Housen-Couriel, Deborah, "Cybersecurity and Anti-Satellite Capabilities (ASAT): New Threats and New Legal Responses" (2015) 4 J.L. & Cyber Warfare 116.

Jakhu, Ram. "Legal Issues Relating to the Global Public Interest in Outer Space" (2006) 32:1 J of Space L 31.

Jenks, C. Wilfred. "International Law and Activities in Space" (1956) 5:1 The International and Comparative Law Quarterly 99.

Kuplic, Blair Stephenson. "The Weaponization of Outer Space: Preventing an Extraterrestrial Arms Race" (2014) 39:4 North Carolina J of Intl L and Commercial Regulation 1123.

Lawrence, T. J. "The Effect of the War on International Law" (1916) 2 Probs. War. 105.

Maogoto, Jackson & Steven Freeland, "The Final Frontier: The Laws of Armed Conflict and Space Warfare" (2007) 23:1 Connecticut J of Intl L 165.

Nagan, Winston P. "African Human Rights Process: A Contextual Policy-Oriented Approach" (1992) 21:1 Southwestern U L Rev 63.

Oduntan, Gbenga. "The Never Ending Dispute: Legal Theories on the Spatial Demarcation Boundary Plane between Airspace and Outer Space" (2003) 1:2 Hertfordshire Law Journal 64.

Poirier, William J. & James Lotspeich, "Air Force Cyber Warfare: Now and the Future" (2013) 27:5 ASPJ 73.

Postema, Gerald J. "Custom, Normative Practice, and the Law" (2012) 62:3 Duke U 707.

Ramey, Robert A. "Armed Conflict on the Final Frontier: The Law of War in Space" (2000) 48 A.F. L. Rev. 1.

Silverstein, Arthur Jay. "Emigration: A Policy Oriented Inquiry" (1974) 2:2 Syracuse J Intl L & Com 149.

Singer, P. W. "Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons" (2015) 47:1 Case W. Res. J. Int'l L. 79.

Schmitt, Michael N. & Jeffrey S Thurnher, "Out of the Loop: Autonomous Weapon Systems and the Law of Armed Conflict" (2013) 4:2 Harvard National Security J 231 at 235.

Schmitt, Michael N. & Liis Vihul, "Proxy Wars in Cyberspace: The Evolving International Law of Attribution" (2014) 1 FLETCHER SEC. REV. 53 at 60.

Terlikowski, Marcin. "Cyberattacks on Estonia: Implications for International and Polish Security" (2007) 16:3 Polish Q of Intl Affairs 68.

Vereshchetin, Vladlen S. & Gennady M Danilenko, "Custom as a Source of International Law of Outer Space" (1985) 13:1 J of Space L 22.

Wiessner, Siegfried. "The New Haven School of Jurisprudence: A Universal Toolkit for Understanding and Shaping the Law" (2010) 81:1 Asia Pac L Rev 45.

Wiessner, Siegfried. "The Public Order of the Geostationary Orbit: Blueprints for the Future" (1983) 9:2 Yale J of World Public Order 217.

Secondary Material: Other Scholarly Articles & Reports

Gisel, Laurent & Lukasz Olejnik, "The Potential Human Cost of Cyber Operations" (2018) International Committee of the Red Cross.

Glennon, Michael J. "Sometimes a Great Notion" (2003) XXVII: 4 The Wilson Quarterly 45 at 48.

Grace, Rob & Claude Bruderlein, "HPCR Draft Working Paper: Building Effective Monitoring, Reporting, and Fact-finding Mechanisms" (2012) Program on Humanitarian Policy and Conflict Research.

Haass, Jon, Radhakrishna Sampigethaya & Vincent Capezzuto, "Aviation and Cybersecurity: Opportunities for Applied Research" (2016) Tr News (304): 39.

Hathaway, Melissa. *Getting Beyond Norms: When Violating the Agreement Becomes Customary Practice, Center for International Governance Innovation*, Papers No. 127 (Waterloo: ON, Canada, 2017).

Hathaway, Oona A. "Two Cheers for International Law" (2003) XXVII: 4 The Wilson Quarterly 50.

Johnson-Freese, Joan. "The United States' Space Security Policy: Cyber Security Vulnerabilities", in *Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives* (Chatham House, December 2014).

Liivoja, Rain, Maarja Naagel & Ann Väljataga, "Autonomous Cyber Capabilities under International Law" (NATO Cooperative Cyber Defence Centre of Excellence, 2019).

Liu, Hao & Fabio Tronchetti, *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?* (2016) 38 Space Policy 64.

Liu, Hin-Yan. "Categorization and Legality of Autonomous and Remote Weapons Systems" (2012) 94:886 Intl Rev Red Cross 627 at 638.

Metcalf, Katrin Nyman. "A Legal View on Outer Space and Cyberspace: Similarities and Differences", Tallinn Paper No. 10 (NATO Cooperative Cyber Defence Centre of Excellence, 2018).

Meroney, Ben. "Cybersecurity for Critical Infrastructure Operators in the Oil and Gas Industry" (2018) 64 Annual Institute on Mineral L 2 at 2.

Roland, Alex. "Science, Technology, and War" (1995) 36:2 Technology and Culture 83.

Rubenfeld, Jed. "The Two World Orders" (2003) XXVII: 4 The Wilson Quarterly 22

Schmitt, Michael N. & Liis Vihul, "The Nature of International Law Cyber Norms, Tallinn Paper No. 5" (NATO Cooperative Cyber Defence Centre of Excellence, 2014) at 26, online: < https://ccdcoe.org/uploads/2018/10/Tallinn-Paper-No-5-Schmitt-and-Vihul.pdf>.

Slaughter, Anne-Marie. "Leading Through Law" (2003) XXVII: 4 The Wilson Quarterly 37 at 37.

Treves, Tullio. "Customary International Law", Max Planck Encyclopedia of Public International Law, November 2006.

Wamala, Frederick *The ITU National Cybersecurity Strategy* (Geneva: Switzerland, International Telecommunication Union, 2012).

Wood, Michael. "Teachings of the Most Highly Qualified Publicists", (March 2017) *Max Planck Encyclopedia of Public International Law*, online: <http://opil.ouplaw.com/home/epil>.

US, Law Library of Congress, Clay Wilson, *Botnets* (RL32114) (Congressional Research Service, 2008).

US, Law Library of Congress, Lennard G. Kruger, *Internet Domain Names: Background and Policy Issues* (7-7070) (Congressional Research Service, 2009).

US, Law Library of Congress, Marcia S. Smith, *U.S. Space Programs: Civilian, Military, and Commercial,* Resources, Science (IB92011) (Congressional Research Service, 2006).

Articles from Proceedings

Atkinson, David J. "Emerging Cyber-Security Issues of Autonomy and the Psychopathology of Intelligent Machines" (Papers delivered at the 2015 AAAI Spring Symposium).

Bourely, Michel. "Rules of International Law Governing the Commercialization of Space Activities" (1986) 29 Proceedings on the L of Outer Space 157.

Christol, Carl Q. "Remote Sensing and National Security" (2003) 46 Proc. on L. Outer Space at 224.

Grego, Laura. "Technologies and Behaviors of Concern: What Threatens Long-Term Space Security and How Can These Threats be Monitored?" in UN Institute for Disarmament Research, *Building the Architecture for Sustainable Space Security: Conference Report 30-31 March 2006* (UN Publications, Geneva, 2006).

Jakhu, Ram S. & Steven Freeland, "The Sources of International Space Law" (2013) 56 Proceedings of the Intl Institute of Space L 461.

Jakhu, Ram S. "Sixty Years of Development of International Space Law" (Proceedings of the Symposium Celebrating the 90th Anniversary of the Cologne Institute of Air and Space Law, 2016).

Online and Internet Sources

"10 Basic Cybersecurity Measures, Best Practices to Reduce Exploitable Weaknesses and Attacks", *WaterISAC* (June 2015) at ii, <online: https://ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_S508C.pdf>.

Bateman, Aaron. "In Outer Space, the US is Vulnerable to China and Russia", *The Hill (blog)* (20 July 2017), online: <http://thehill.com/blogs/pundits-blog/defense/342992-in-outer-space-the-us-is-vulnerable-to-china-and-russia>.

Center for Strategic and International Studies, "Space Threat Assessment 2018, Aerospace Security Project" (11 April 2018), online: <https://aerospace.csis.org/spacethreat2018/>.

Cisneros, Maribel. *Cyber-warfare: Jus Post Bellum* (Master of Science Thesis, Cyber Systems and Operations, Naval Postgraduate School, 2015) at 10, online: < https://calhoun.nps.edu/handle/10945/45169>.

Council on Foreign Relations, "Cybersecurity and the New Era of Space Activities" (3 April 2018), online: <https://www.cfr.org/report/cybersecurity-and-new-era-space-activities>.

Crisp, James "EU Governments to Warn Cyber Attacks can be an Act of War" *The Telegraph* (29 October 2017), online: <http://www.telegraph.co.uk/news/2017/10/29/eu-governments-warn-cyber-attacks-can-act-war/>.

Davis, Joshua. "Hackers Take Down the Most Wired Country in Europe", *Wired* (21 August 2007), online: <https://www.wired.com/2007/08/ff-estonia/>.

"Definition of Attack Vector", *PC Magazine*, Encyclopedia (2019), online: <https://www.pcmag.com/encyclopedia/term/57711/attack-vector>.

Elkind, Peter. "Inside the Hack of the Century, Part 3", *Fortune* (25 June 25 2015), online: <http://fortune.com/sony-hack-final-part/>.

Falliere, Nicolas, Liam O. Murchu & Eric Chien, "W32.Stuxnet DossierVersion 1.4, Symantec Security Response" (February 2011) 2, online: <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>.

"Germans introduce poison gas", *History* (21 August 2018), online: <https://www.history.com/this-day-in-history/germans-introduce-poison-gas>.

Harrison, Todd, Kaitlyn Johnson & Thomas G. Roberts, "Space Threat Assessment 2018: A Report of the CSIS Aerospace Security Project", Center for Strategic and International Studies (April 2018) 2, online: < https://aerospace.csis.org/wp-content/uploads/2018/04/Harrison_SpaceThreatAssessment_FULL_WEB.pdf>.

Heaven, Douglas. "US cyberweapons have been stolen and there's nothing we can do", *New Scientist,* (6 December 2017), online: <https://www.newscientist.com/article/mg23631550-100-us-cyberweapons-have-been-stolen-and-theres-nothing-we-can-do/?campaign_id=RSS%7CNSNS->.

Internet Corporation for Assigned Names and Numbers, online: < https://www.icann.org/>.

Keller, John. "Army eyes autonomous cyber defenses, artificial intelligence, and machine learning for tactical networks, Military & Aerospace Electronics" (January 16, 2019), online: <https://www.militaryaerospace.com/computers/article/16722030/army-eyes-autonomous-cyber-defenses-artificial-intelligence-and-machine-learning-for-tactical-networks>.

Knake, Robert K. "Contingency Planning Memorandum No. 31: A Cyberattack on the U.S. Power Grid" (Council on Foreign Relations, 2017), online: <https://cfrd8files.cfr.org/sites/default/files/pdf/2017/03/ContingencyPlanningMemo31_Knake.pdf>.

Long, Tony. "April 22, 1915: A Fearful Word in the Trenches: 'Gas!'", *Wired* (22 April 22 2008), online: <https://www.wired.com/2008/04/dayintech-0422/>.
Martin, Lockheed. "Gaining the Advantage, Applying Cyber Kill Chain Methodology to Network Defense" (2015) 4, online: <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf>.

NATO Cooperative Cyber Defence Centre of Excellence, "Tallinn Manual 2.0", online: <https://ccdcoe.org/research/tallinn-manual/>.

Palmer, Danny. "Cybercrime drains $600 billion a year from the global economy, says report" (21 February 2018), *ZDNet,* online: <https://www.zdnet.com/article/cybercrime-drains-600-billion-a-year-from-the-global-economy-says-report/>.

Peterson, Andrea. "The Sony Pictures hack, explained", *The Washington Post* (18 December 2014), online: <https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?noredirect=on&utm_term=.a57072f4c5a7>.

Reynolds, Matt. "Ransomware attack hits 200,000 computers across the globe", *New Scientist* (15 May 2017), online: <https://www.newscientist.com/article/2130983-ransomware-attack-hits-200000-computers-across-the-globe/>.

Sanchez, Gabriel. "Case Study: Critical Controls that Sony Should Have Implemented",

SANS (1 June 2015) 2, online: <https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-sony-implemented-36022>.

Shalal, Andrea. "German military aviation command launches cyber threat initiative", *Reuters* (12 July 2017), online: <https://www.reuters.com/article/us-germany-military-cyber-aviation/german-military-aviation-command-launches-cyber-threat-initiative-idUSKBN19X2J6>.

"Supermassive Black Hole Sagittarius A", *NASA* (10 May 2016), online: <https://www.nasa.gov/mission_pages/chandra/multimedia/black-hole-SagittariusA.html>.

"The Milky Way Galaxy", National Aeronautics and Space Administration, Goddard Space Flight Center (December 2015), online: <https://imagine.gsfc.nasa.gov/science/objects/milkyway1.html>.

The NATO Cooperative Cyber Defence Centre of Excellence, "History", online: <https://ccdcoe.org/about-us/>.

UNESCO, Internet Governance Glossary, online: <https://en.unesco.org/glossaries/igg>.

United Nations Office for Disarmament Affairs, Group of Governmental Experts, online: https://www.un.org/disarmament/group-of-governmental-experts/.

U.S. Department of Justice, "The Morris Worm: 30 Years Since First Major Attack on the Internet" (2 November 2018), online: <https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218>.

US Department of State, Remarks and Release, Cynthia Plath, "Explanation of Vote in the First Committee on Resolution: L.50, "No First Placement of Weapons in Outer Space"" (5 November 2018), online: < https://www.state.gov/explanation-of-vote-in-the-first-committee-on-resolution-l-50-no-first-placement-of-weapons-in-outer-space/>.

Weeden, Brian "2007 Chinese Anti-Satellite Test Fact Sheet", *Secure World Foundation* (23 November 2010), online: <https://swfound.org/media/9550/chinese_asat_fact_sheet_updated_2012.pdf>.

Wright, Jeremy. "Cyber and International Law in the 21st Century", *Attorney General's Office* (23 May 2018), online: <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>.

Väljataga, Ann. "Tracing Opinio Juris in National Cyber Security Strategy Documents" (NATO Cooperative Cyber Defence Centre of Excellence, 2018) at 4, online: <https://ccdcoe.org/uploads/2019/01/Tracing-opinio-juris-in-NCSS-2.docx.pdf>.

Zetter, Kim. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", *WIRED* (3 March 2016), online: <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>.

Other Miscellaneous Documents

Broyles Jr., William & Al Reinert, "Apollo 13" (screenplay, 1995). [Adapted from the book by Jim Lovell & Jeffrey Kruger, *Lost Moon: The Perilous Voyage of Apollo 13* (Boston: Houghton Mifflin, 1994).]

Government of Australia, Australian Cyber Security Centre, *ACSC 2016 Threat Report* (2016).

Memorandum from Robert P. Murphy, General Counsel (7 July 2000) Department of Commerce: Relationship with the Internet Corporation for Assigned Names and Numbers, B-284206, United States General Accounting Office.

NASA, News Release, No 69-83F, "Apollo 11 Goodwill Messages" (13 July 1969).