An electric spark - Penetrating the void with the virtual

Tamara Blagojevic[1]

ABSTRACT

With the world entering the 'New Space' age, keeping up the pace with a fast developing technologically advanced and highly digitalized world is becoming harder due to numerous circumstances. Firstly, the internet is becoming more accessible to any average user with the help of satellite technologies. Secondly, the cyberspace and outer space domains are becoming more open and versatile in terms of actors and type of activities, and due to popularity and accessibility are becoming multi stakeholder spectrums. Lastly, both sectors are characterized by dual use, which implies the infiltration with malicious activities. On the other hand, the law, with its descriptive mechanisms, if not diligently considered and timely deployed might slowly lose its grip in these two important, and fast developing sectors. These are the Cybersecurity and Space sector, connected not only by their character, but also by mutual benefits and common threats.

To become situationally aware of the clash of these two domains, and to understand what is the electric spark bonding them, we will firstly examine the current trends and developments, and continue by explaining the concepts, phenomena and issues that appear relevant in such a situation. To bring the situation and the issue closer to reality, we will go on by enumerating and briefly showcasing numerous cases that shed light on the issues. We will finalize by examining whether and how such issues are approached in the legal world, by showcasing the development and relevant sources of law for the legal frameworks covering the issues at hand. Finally, we will briefly conclude and suggest hypothetical scenarios that might lead to a way forward.

The aim of this article is to inform, raise awareness and gather information currently scattered and unclear, due to the fragmentation of the legal frameworks and their current inability to entirely keep pace with the ever-changing and developing, digitized and commercialized world.

Keywords: Cyber, Cybersecurity, Law, IT, OT, Internet, Satellites, ITU, Space Law, Sustainability, Standard, Compliance, Prevention, Outer Space, Space, Hacker, Spoofing,

[1]L.L.M, Associate Director for Legal Research & Special Projects at the Space Court Foundation; Independent researcher and freelance legal writer specializing in International Law, Cyber Law and Space law. Speaker at a WSBA-World Peace through Law webinar and NALS webinar (USA), two Green Crimes Conferences held by the Jersey Law Commision, speaker at the International Environmental Forum (IEF) and a Jury member for EU Info Center and Open Communication in Serbia (Debate on the legitimacy of establishing space bases on the Moon). Author of the Chapter of the book on "Green Crimes and International Criminal Law", published by Vernon Press.

Jamming, Cyber Triad, Information, Mitigation, Congestion, Kessler, Space Debris, OST, Tallinn, McGill, MILAMOS, Manual, UN, Charter, International Law, Attack, Crime.

1. INTRODUCTION

The age of technological evolution, global digital transformation, and fast space sector development and commercialization, brings many questions regarding the complex relationships where these areas and domains intersect. Man's nature, mirrored in curiosity, competition, anthropocentrism and survival instincts brought us to the second space era, and created the "New Space", while the fast paced digital and technological evolution created the "cyberspace".

Although not so visible at a first glance, cyberspace and outer space do have various similarities and points of contact, either reflected in their character, importance, interdependence or the threats they both face. What is undisputed, is that they both represent global commons, outside national jurisdictions, beyond national appropriation, free for peaceful use by the entire humanity. Aside from this, the fact is that they are both fast developing, multi stakeholder sectors, providing various benefits for the entire humanity. The most obvious nexus between these spectrums is the fact that the space systems, infrastructure, supporting ground structure, and space objects, are all powered, controlled, monitored or supported thanks to the electronic and technological - cyber means.

However, this connection has two faces - one mutually beneficial, and the other, quite the opposite. The fact that space assets and infrastructure, as well as space objects, can be controlled remotely and digitally (through technology) and having in mind the current congestion of outer space traffic, increases the plausibility of malicious activities that could lead to various cyber incidents in a remote location, potentially not so easily and timely discovered, or even remediated or mitigated from a distance. This issue can be only aggravated when considering the fact that the technology and objects used in both of these spectrums have dual use, both military and peaceful, implying the potential for weaponization and militarisation of these spectrums, which then creates more risks and fertile ground for malicious actors.

In such a setting, and when regulation is lacking, late, inconsistent, underdeveloped or unharmonized, when interpretation in bad faith is utilized or when cyber and space activities are directed against each other rather than coordinated in mutual benefit, the possibility of breaches of human rights, perpetrating cybercrimes, international insecurity, or even serious effects on the Earth's and space environment, by intentional collisions which can lead to the generation and subsequent multiplication of space debris, becomes a viable scenario.

To raise awareness about the current issue connecting the two spectrums - outer space and cyberspace - a gradual, levelized approach will be taken, beginning firstly from

introducing the situation, the current trends and developments in these areas that should already imply their connection. This will lead to the necessity to understand the matter of our examination herein, which will be explained in the section on definitions and explanation of phenomena in question. When understanding the phenomena, to imagine them in the real world, we will need some examples or cases, only to finally see how they are tackled with, in the section on legal frameworks.

A deeper look into the similarities or trends in the development of the frameworks and regulations, should indicate for a positive and mutually beneficial relation between cybersecurity and sustainability in space - proper and timely implementation of cybersecurity practices and standards, in accordance with their legal frameworks, in the space sector should lead to greater security in space, while harmonized, synchronized development of the cybersecurity framework, taking into account the specifics of the space sector, should lead to enhanced sustainability on the long run.

2. RAISING (SITUATIONAL) AWARENESS
Current developments and trends, threats and their consequences

In 2022, while the global population reached the number of 8 billion,[2] with roughly 64.6% of that population (or about 5.18 billion people) using the internet in the second quarter of 2023,[3] humanity is paving its way through the 'NewSpace' age, known for the fast development of the space sector and its technological, legal, commercial, and social innovations.[4] While global space-related activities generated $447 billion in 2020,[5] supporting everything from vehicle navigation to efficient farm management,[6] space exploration by itself is projected to create $1.2 trillion[7] in retail revenues in 2020-2030.[8]

[2]"World Population to Reach 8 Billion on 15 November 2022" (*United Nations*) <https://www.un.org/en/desa/world-population-reach-8-billion-15-november-2022> accessed November 22, 2022

[3]"Digital around the World - Datareportal – Global Digital Insights" (*DataReportal*) <https://datareportal.com/global-digital-overview> accessed November 22, 2022

[4] Ms. Ruvimbo Samanga, "NewSpace" (*IISL Space Law Knowledge Constellation*July 2021) <https://constellation.iislweb.space/ruvimbo-samanga-newspace/> accessed November 20, 2022

[5]Lesley Conn, "Global Space Economy Nears $447B" (*The Space Report,* July 23, 2021) <https://www.thespacereport.org/uncategorized/global-space-economy-nears-447b/> accessed November 20, 2022.

[6]Tim Starks and Aaron Schaffer, "Analysis | Cyberattacks on Satellites May Only Be Getting More Worrisome" (*The Washington Post,* July 29, 2022) <https://www.washingtonpost.com/politics/2022/07/29/cyberattacks-satellites-may-only-be-getting-more-worrisome/> accessed November 20, 2022.

[7]"NSR Global Space Economy, 2nd Edition" (*NSR* October 19, 2022) <https://www.nsr.com/?research=nsr-global-space-economy-2nd-edition> accessed November 20, 2022.

[8]"Why We Need Increased Cybersecurity for Space-Based Services" (*World Economic Forum*May 25, 2022) <https://www.weforum.org/agenda/2022/05/increased-cybersecurity-for-space-based-services/> accessed November 20, 2022.

On the other hand, while the global security market is currently worth around $150 billion, with predictions it will rise up to about $400 billion in 2026,[9] the global financial losses due to cyber-attacks in 2021. were estimated at $6 trillion.[10]

As per the latest European Space Agency (ESA) Space Environment Report from 2023, the accelerated use of space over the last years continued unabated in 2022, leading to launch and re-entry traffic rates to see new records and challenges in keeping accurate track of the state of the environment.[11] The pace of satellite launches has also sped up considerably, going from 129 in 2011 to 1,809 in 2021, according to a United Nations Office for Outer Space Affairs (UNOOSA),[12] which estimates that there are currently about 9,254 objects in orbit.[13] According to the Union of Concerned Scientists, at the start of 2022. there were 4,852 satellites in orbit.[14] According to some analysts, the number of satellites in orbit is anticipated to expand tenfold in the next few years, with many of them delivering commercial services such as the internet, necessitating the development of systems to maintain space order.[15]

The growing participation of commercial actors makes space a more innovative environment, which in turn allows cheaper access to outer space for governmental and private actors alike, and at the same time, making space more crowded and congested.[16] From the time when only a few states were the main actors in the space race, up until today, companies such as SpaceX, Amazon, OneWeb, and others have already launched hundreds of satellites in order to sell internet access around the world, and are planning to send

[9] 'The NIS2 Directive: A high common level of cybersecurity in the EU - BRIEFING - EU Legislation in Progress;', (European Parliament, June 2022), page 2, available at <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf>.

[10] Di Freeze, "Cybercrime Damages $6 Trillion by 2021" (*Cybercrime Magazine*November 9, 2020) <https://cybersecurityventures.com/annual-cybercrime-report-2017/#:~:text=Cybersecurity%20Ventures%20predicts%20cybercrime%20damages,in%20size%2C%20sophistication%20and%20cost.> accessed December 21, 2022.

[11] See: The European Space Agency, *ESA'S ANNUAL SPACE ENVIRONMENT REPORT*, pg.15, June 12. 2023, <https://www.sdo.esoc.esa.int/environment_report/Space_Environment_Report_latest.pdf>, accessed: 9 july 2023.

[12]"See: UNOOSA Space Objects Index" <https://www.unoosa.org/oosa/osoindex/search-ng.jspx?lf_id=> accessed November 22, 2022.

[13]Supra n. 6, Starks and Aaron Schaffer, "Analysis | Cyberattacks" <https://www.washingtonpost.com/politics/2022/07/29/cyberattacks-satellites-may-only-be-getting-more-worrisome/>.

[14]Chuck Brooks, "The Urgency to Cyber-Secure Space Assets" (*Forbes*February 28, 2022) <https://www.forbes.com/sites/chuckbrooks/2022/02/27/the-urgency-to-cyber-secure-space-assets/?sh=45a439fc51b1> accessed November 20, 2022.

[15]Sakshi Tiwari, "China 'Decodes' an Orbiting US Satellite; Claims Expertise in Automatically Detecting & Fixing Security Flaws in Outer Space" (*Latest Asian, Middle-East, EurAsian, Indian News*April 10, 2022) <https://eurasiantimes.com/china-decodes-an-orbiting-us-satellite-claims-expertise-in-automatically-detecting-fixing-security-flaws-in-outer-space/> accessed November 22, 2022.

[16] Rajeswari Pillai Rajagopalan, "Electronic and Cyber Warfare in Outer Space "(*UNIDIR*,May 2019), page 1, <https://unidir.org/sites/default/files/publication/pdfs//electronic-and-cyber-warfare-in-outer-space-en-784.pdf> accessed November 22, 2022.

thousands more into orbit.[17] A good example of a significant environmental footprint is Starlink, a satellite network developed by SpaceX, with an aim to have 42,000 satellites in its mega constellation in order to provide low-cost internet to remote locations.[18] Starlink currently provides service to over 1 million active customers across 54 countries around the world, with about 4,368 low-earth-orbit (LEO) Starlink satellites,[19] including aiding Ukraine, during the ongoing Russian Ukrainian conflict.[20] However, underneath the veil of humanitarian aid, the Starlink project still raised numerous concerns among scientists and astronomers for various reasons. In September 2019, when ESA announced that it had directed its Aeolus satellite to undertake evasive maneuvers to avoid crashing into "Starlink 44," one of the first 60 satellites in the mega constellation.[21] According to computer models, at that time, Starlink satellites were involved every week in about 1,600 encounters between two spacecraft closer than 1 kilometer, making that about 50% of all such incidents, with this number rising with every new batch of satellites launched.[22] According to Astronomer Jonathan McDowell who tracks the constellation on his website, as of November 2022, there were 3,271 Starlink satellites in orbit, out of which 3,236 are operational.[23] In a report released in October 2022, the American Astronomical Society (AAS) likened the impact of mega constellations in astronomy to light pollution.[24] In another paper published in May 2021 in the journal Scientific Reports, Canadian researcher Aaron Boley said the aluminum the satellites are made of will produce aluminum oxide (a.k.a. alumina), during burn-up,[25] and the amount of metal that will be burning up in Earth's atmosphere as old satellites are deorbited could trigger unpredictable changes to the planet's climate.[26] It thus cannot be ruled out that over decades the pollution from burning mega constellation satellites could lead to changes on a scale akin to what we are currently experiencing with fossil-fuel-induced climate change.[27]

---

[17]Rebecca Heilweil, "For Hackers, Space Is the Final Frontier" (*Vox*July 29, 2021) <https://www.vox.com/recode/22598437/spacex-hackers-cyberattack-space-force> accessed November 22, 2022.

[18]Tereza Pultarova and Elizabeth Howell, "Starlink Satellites: Everything You Need to Know about the Controversial Internet Megaconstellation" (*Space.com*April 14, 2022) <https://www.space.com/spacex-starlink-satellites.html> accessed November 22, 2022.

[19] Tyler Cooper, Starlink Internet - Coverage and Availability Map, BoradBandNow, 07/02/2023, <https://broadbandnow.com/starlink#:~:text=In%20fact%2C%20Starlink%20provides%20service,internet%20service%20to%20many%20areas.> accessed July 2023.

[20] Eric Mack, "US Military Says SpaceX Handily Fought off Russian Starlink Jamming Attempts" (*CNET*April 22, 2022) <https://www.cnet.com/science/space/us-military-says-spacex-handily-fought-off-russian-starlink-jamming-attempts/> accessed November 27, 2022.

[21]Supra n. 18, Tereza Pultarova, Starlink Satellites

[22]Ibid. Supra n. 18.

[23]Ibid.

[24]Ibid.

[25]Ibid.

[26]Ibid.

[27]Ibid.

But, environmental impacts are sadly not the only concerns and potential consequences of the increasing space traffic congestion. Moreover, due to the fact that environmental damages are known for the inability to properly and fully assess and investigate all their causes, as they are often characterized with multiple causation, it is plausible that one of such causes can be a collision of spacecraft(s), the probability of which raises due to a phenomenon known as Kessler syndrome.[28] Since collisions can also be intentional, different actors with malicious intent can even trigger a collision by interfering with signals, hacking space objects and possibly even taking over controls and making them change their course. This is just one of the reasons why mega-constellations pose even greater challenges to protecting space assets from cyber threats.[29] Nowadays, as more spacecraft connect with ground-based assets and users, the attack surface is becoming exponentially larger, and the absence of a widespread and proper implementation of cybersecurity best practices by all companies operating in space poses a risk.[30] An aggravating circumstance is that the US Federal Communications Commission (FCC) didn't require public demonstration of means and methods to secure satellites or the Internet that commercial actors plan to provide, and SpaceX, like many other private space companies, has, up until recently, shared basically no information about its cybersecurity efforts or plans.[31] Only recently, in a series of overnight tweets, Musk, founder and chief executive of SpaceX, finally shared some basic information by stating that the company was shifting its resources in response to jamming of terminals, presumably in Ukraine.[32]

As we can see, the more people connected to the internet, and the more satellites in space, the greater the risk of cyber threats and potential accidents, especially at a time when space is believed to be heading towards militarization and while international rivalry is unfolding through space assets.[33] Within the past decade, more than 60 nations have been

[28] The effect whereby the generation of space debris via collisions and explosions in orbit could lead to an exponential increase in the amount of artificial objects in space, in a chain reaction which would render spaceflight too hazardous to conduct, was first postulated by Donald Kessler in 1978. See more in: D. J. Kessler and B. G. Cour-Palais. Collision frequency of artificial satellites: The creation of a debris belt. Journal of Geophysical Research, page 2637–2646, 1978.

[29]"Why Space Cyber?" (*Center for Space Cyber Strategy and CyberSecurity - University at Buffalo*March 4, 2021) <https://www.buffalo.edu/space-cybersecurity/center/why-space-cyber.html> accessed November 27, 2022.

[30] King M and Goguichvili S, "Cybersecurity Threats in Space: A Roadmap for Future Policy" (*Wilson Center*October 8, 2020) <https://www.wilsoncenter.org/blog-post/cybersecurity-threats-space-roadmap-future-policy>, accessed December 2022.

[31]Gregory Falco G, "Opinion | Our Satellites Are Prime Targets for a Cyberattack. and Things Could Get Worse." (*The Washington Post*May 7, 2019) <https://www.washingtonpost.com/opinions/our-satellites-are-prime-targets-for-a-cyberattack-and-things-could-get-worse/2019/05/07/31c85438-7041-11e9-8be0-ca575670e91c_story.html> accessed November 27, 2022.

[32]Jeff Foust, "SpaceX Shifts Resources to Cybersecurity to Address Starlink Jamming" (*SpaceNews*March 5, 2022) <https://spacenews.com/spacex-shifts-resources-to-cybersecurity-to-address-starlink-jamming/> accessed November 26, 2022.

[33]Supra n. 15, Sakshi Tiwari, "China 'Decodes' an Orbiting US Satellite"

developing cyber-offensive capabilities,[34] and more countries and private actors have acquired and employed counter-space capabilities in novel applications, which now pose a greater existential threat to critical space assets.[35] From a security perspective, the primary concern is safeguarding 'access' to these domains for commercial and military reasons.[36] Moreover, the activities of state actors in both space and cyberspace are heavily influenced by intelligence agencies and their culture of secrecy,[37] making such activities untransparent, and their monitoring and emergency preparedness a hard endeavor.

In December 2019, NATO foreign ministers formally declared space as an 'operational domain,' extending the alliance's range from land, sea, air and cyberspace to operations in space.[38] The Centre for Strategic and International Studies indicated in its study that there has been a dramatic increase of the number of sophisticated cyberattacks over the last decade.[39] On the other hand, China has developed a new cyber defense infrastructure that can automatically detect security flaws in orbiting satellites, calculate the most effective ways to attack it, and suggest countermeasures, according to military experts participating in that project.[40] The United States Space Force's Space Delta 6 (USF, DEL 6), in charge of providing secure access to space via the Air Force Satellite Control Network and defensive cyberspace capabilities for space mission systems, in support of US Space Command, plans, programs, integrates, runs, and maintains command and control and common-user systems.[41] As we can see, in recent decades, the states have been moving away from expensive ASAT-like options to developing more affordable and easily available electronic and cyber warfare methods that could affect space assets.[42]

Such a setting, with diverse actors, and multiple capabilities of creating chain events of incidents, potentially leading to an unsustainable space race, and global insecurity

[34]Microsoft, "Protecting People in Cyberspace - The Vital Role of the United Nations in 2020 "(*United Nations, 2020*) <https://www.un.org/disarmament/wp-content/uploads/2019/12/protecting-people-in-cyberspace-december-2019.pdf> accessed Novemeber 21, 2022

[35]Supra n. 30 King M "Cybersecurity Threats in Space".

[36] See: Gerald Stang, "Global Commons, between cooperation and competition", (European Union Institute for Security Studies, April 2013.,<https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_17.pdf> accessed: Novemeber 21, 2022

[37]Brett Biddington, T*he Regulation of Space and Cyberspace: One Coin, Two Sides , (Hereinafter: One Coin Two Sides),* 13th Australian Information Warfare and Security Conference, Australia, December 2012, <https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1046&context=isw> pg 40

[38]*Nato's approach to space*, Oct. 2022, NATO, <https://www.nato.int/cps/en/natohq/topics_175419.htm#:~:text=At%20the%20June%202019%20Defence,%2C%20land%2C%20maritime%20and%20cyberspace.>

[39]*Significant Cyber Incidents Since 2006*, CSIS. (Amazon News), <https://csis-prod.s3.amazonaws.com/s3fs-public/190904_Significant_Cyber_Events_List.pdf>

[40]Supra n. 15, Sakshi Tiwari, "China 'Decodes' an Orbiting US Satellite"

[41]See: Airman Ryan Prince, Peterson-Schriever Garrison, *Space Delta 6 protects space and cyberspace*, Public Affairs / (December 14, 2020), <https://www.spoc.spaceforce.mil/News/Article-Display/Article/2446117/space-delta-6-protects-space-and-cyberspace>, accessed. November 27. 2022.

[42]See: Supra n. 16, Rajagopalan, "Electronic and Cyber Warfare in Outer Space "

on a long run, implies the necessity to have a holistic view on the issues at hand, and for that to deploy multilateral cooperation and multidisciplinary coordinated approaches in emergency preparedness, risk and impact assessment, preventive mechanisms, and possibly even, preparedness for the timely application of mitigation and remediation mechanisms. To understand why it's all connected, we must first dissect the basic concepts and phenomena, and understand their meanings and scopes.

3. UNDERSTANDING THE VIRTUAL, THE VOID AND THEIR CONNECTION

3.1. Similarities, differences and the nexus

The security analysts generally identify four domains as global commons: high seas, airspace, outer space and, now, cyberspace.[43] The fact that both outer space and cyberspace are global commons, and that neither of them respect national borders,[44] implies the presumption of open accessibility and free use of both, for the entire humanity, on equal basis, and without discrimination, which enabled them to both become very diverse, multistakeholder spectrums. But, unlike outer space, which can be considered a sui generis ecosystem and a self-sustaining remote natural environment, cyberspace is an artificial, digital, virtual domain, physically untouchable by human hand. While space is remote and difficult to access, cyberspace is becoming more accessible, and considered as a system of systems, in which all parts are linked and the behavior of one influences, even ever so slightly, the behavior of every other.[45]

On the other hand, while outer space existed long before humans walked the Earth, and the outer space legal framework developed during the Cold War Era, when states were the predominant actors, the year of 1983. is considered the official birthday of the Internet[46], which is mainly a field dominated by private actors and companies, with the first cyber incidents truly connecting the two spectrums initiating about a decade after. In other words, while space is governed by a mix of international treaties, domestic laws and a number of international organizations, cyberspace is mainly self-regulated, and hosts the internet which has become a global utility, taken for granted by those who use it.[47]

Outer space, however, although being a remote natural environment, wasn't left completely untouched, but rather, our first encounter with it, implied the necessary use of

[43] Supra n. 36, Gerald Strang, "Global Commons", <https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_17.pdf>
[44] Supra n. 37, Brett Biddington, *One Coin, Two Sides,* pg 40
[45] Ibid., pg 39
[46] See: *A Brief History of the internet,* Online Library Learning Centre, <https://www.usg.edu/galileo/skills/unit07/internet07_02.phtml#:~:text=January%201%2C%201983%20is%20considered,Protocol%20(TCP%2FIP).>, accessed: Dec. 2022.
[47] Supra n. 37, Brett Biddington, *One Coin, Two Sides,* pg 39

technological means. In other words, human hands touched the void indirectly, by using spacecraft and satellites.[48] Moreover, much of the world's critical infrastructure and essential systems, such as communications, broadcasting, air transport, maritime trade, financial services, weather monitoring and defense, are heavily dependent on space-based assets and infrastructure, including satellites, ground stations and data links.[49] Most of the weather and communication satellites are located in geosynchronous (GEO) and geostationary (GSO) orbits.[50] Space navigation and positioning satellites, that fall under the Global Navigation Satellite Systems (GNSS), can provide precise positioning and timing information using radio messages.[51] Similarly to emitting signals, remote sensing is basically a means for obtaining information about distant objects without direct contact.[52]

Depicting and laying out the functions and benefits coming from satellites, brings us closer to the electrical tie binding the void with the virtual. Space objects, being our extended hand in space, need not only to be fueled to reach space, but need electronic, cyber means to be maneuvered, secured, monitored, to stay within our control and reach.

3.2. Understanding the phenomena and defining the concepts

Although from the perspective of governance both are considered global commons, due to either a lack of a formally and legally binding international definitions, or the nascent stage of development of their frameworks, there are various definitions of both cyberspace and outer space to be considered.

Outer space, as indicated above, is legally recognized as the Province of all Mankind,[53] and the Moon and its natural resources as the Common Heritage of Mankind.[54] However, when it comes to the physical boundary between Air and Space environments, the McGill Manual on International Law Applicable to Military Uses of Outer Space (McGill Manual or MILAMOS) confirms that the "*The definition and delimitation of outer*

48 See: *Sputnik and the Dawn of the Space Age*, NASA, History Division, <https://history.nasa.gov/sputnik.html#:~:text=History%20changed%20on%20October%204,Earth%20on%20its%20elliptical%20path.>

49 Supra n. 30, King M, "Cybersecurity Threats in Space"

50 See: Space Foundation Editorial Team, "Space Briefing Book - Types Of Orbits", <https://www.spacefoundation.org/space_brief/types-of-orbits/>

51 See: Global Navigation Satellite System (GNSS) Manual, Doc 9849 AN/457, First edition, (ICAO, 2005), <https://www.icao.int/Meetings/PBN-Symposium/Documents/9849_cons_en[1].pdf>

52 See:"*What is remote sensing?*", NOAA, <https://oceanservice.noaa.gov/facts/remotesensing.html>

53 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, T.I.A.S. No. 6347, 610 U.N.T.S. 205, Art 1, [hereinafter OST]. <https://www.unoosa.org/pdf/gares/ARES_21_2222E.pdf>

54 Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, Dec. 18, 1979, 1363 U.N.T.S. 3 [hereinafter Moon Agreement]. Article 11. <https://www.unoosa.org/pdf/gares/ARES_34_68E.pdf>

space have not been established in international law."[55] From the perspective of natural sciences, the closest we can come to precision and colloquially legitimate distinctions, outer space is also commonly geographically recognized as the spectrum above the Karman's line, about 110km (54 nautical miles; 62 miles; 330,000 feet) above Earth's sea level, stretching through the atmosphere's final layer, the exosphere.

However, on the other hand, when it comes to cyberspace, there are more definitions, due to the current lack of a holistic, harmonized, internationally acknowledged, developed and crystalized, formally accepted legal framework.

For example, 'Cyberspace' can be considered as *"a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."*[56]

But, it can also be seen as *"The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form."*[57]

Another definition of cyberspace is also provided by the Tallinn Manual on the International Law Applicable to Cyber Warfare (hereinafter Tallinn 1.0): *"The environment formed by physical and non-physical components, characterized by the use of computers and the electromagnetic spectrum, to store, modify and exchange data using computer networks."*[58]

Last, but not the least, the International Telecommunication Union (ITU) describes cyberspace as *"systems and services connected either directly to or indirectly to the internet, telecommunications and computer networks."*[59]

Even at a first glance at these definitions, components are visible that focus on the character, functionality and use of cyberspace and indicate a human made environment, clearly replicating the reality in a digital form and in a virtual forum, which has further implications on the scope of its regulation, as much as on objects of protection, to be further analyzed in the following sections. Upon dissecting given definitions of cyberspace, we can say that in its core, the cyber realm, aside from the objects (technological component)

[55]Ram S. Jakhu and Steven Freeland (eds), "McGill MANUAL on International Law Applicable to Military Uses of Outer Space" (hereinafter: MILAMOS) (*https://www.mcgill.ca*July 12, 2022), Rule 108, page 10, <https://www.mcgill.ca/iasl/files/iasl/mcgill_manual_volume_i_-_rules.pdf> accessed November 25, 2022.

[56]See: NIST Glossary, Term - Cyberspace Definition, csrc.nist.gov, <https://csrc.nist.gov/glossary/term/cyberspace#:~:text=Definition(s)%3A,and%20embedded%20processors%20and%20controllers.> Accessed: 23 November 2022.

[57] Ibid.

[58] Michael N. Schmitt, "International Cyber Security Law - States and Cyber Space," *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Hereinafter: Tallinn 1.0), Glossary of Technical terms, (Cambridge University Press 2017), page 211, available at: <http://csef.ru/media/articles/3990/3990.pdf>. Accessed: 23 November 2022.

[59]ITU National Cybersecurity Strategy Guide (September2011), <https://www.Itu.Int/Itu-D/Cyb/Cybersecurity/Docs/Itu-National-Cybersecurity-Guide.Pdf>, accessed: 23 November 2022.

and subject/actor (human element), consists also of units such as information and data (the content), which can is a valuable asset in today's society.

This brings us to something commonly used by tech experts and IT companies to subsume the components of cyberspace, or the objects of protection thereof, called - the 'Cyber Triad'. The Cyber Triad consists of three pillars which relate to people as the first, processes as the second and data and information as the third pillar.[60] In other words, these pillars presume the *confidentiality, integrity and availability of data*,[61] which preferably all have to be achieved simultaneously, in order to ensure non discriminatory access to all authorized users, of a common good consisting of presumably reliable, consistent, unbiased, and accurate information. The first pillar, confidentiality, relates to privacy (and secrecy) which implies protection and encryption.[62] The second pillar, integrity, relates to accuracy, quality, certainty and verifiability of data and information.[63] The third pillar relates to enabling equal opportunities for secure and justified usage, or in other words, allowing access to all authorized users.[64] This all implies not only the areas of cyberspace and its aspects, but also presumes the quality and the direction and scope of expected protection frameworks (as all of the above principles should be harmonized), but above else, also implies a balance made between privacy, security, transparency and access to all legitimate and authorized actors. This balanced protection of each of the elements of the cyber triad, can be said to belong to the umbrella of the term "Cybersecurity". The ITU defines Cybersecurity as: *"the collection of tools, policies, security concepts… risk management approaches… and technologies that can be used to protect the cyber environment and organization."*[65]

Space security can be understood similarly, but instead *towards the protection of outer space and assets there*.[66] But, space systems are specific, as they include not only the satellites themselves, but also the ground stations that operate and control them, and the links between them.[67] In other words, a critical aspect of the space systems is that they are a *hybrid of IT (information technology) and OT (operational technology)*, and therefore are

[60] "The Three-Pillar Approach to Cyber Security: Data and Information Protection" (*DNV*) <https://www.dnv.com/article/the-three-pillar-approach-to-cyber-security-data-and-information-protection-165683#:~:text=The%20third%20pillar%20is%20data%20and%20information%20protection&text=The%20first%20two%20pillars%20are,tangible%20of%20the%20three%20pillars.> accessed November 22, 2022.

[61] Ibid.

[62] Ibid.

[63] Ibid

[64] Ibid.

[65] See: Definition of cybersecurity, referring to ITU-T X.1205, ITU, <https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx>, Accessed: 23 November 2022.

[66] Nayef Al-Rodhan, "Cyber Security and Space Security" (*The Space Review: Cyber security and space security*May 26, 2020) <https://www.thespacereview.com/article/3950/1> accessed November 2, 2022

[67] Ibid.

a practical intersection of the cyber and physical worlds.[68]

In that regard, when it comes to understanding the meaning and scope of the term space object, MILAMOS restates the Convention on International Liability for Damage Caused by Space Objects (Liability Convention) and the Convention on Registration of Objects Launched into Outer Space (Registration Convention), by noting a somewhat of a circular and descriptive definition: *"a space object includes component parts of a space object as well as its launch vehicle and parts thereof."*[69]

The MILAMOS further confirms that *"Ground-based space infrastructure consists of terrestrial facilities that directly support space activities, including military space activities."*[70]

The Tallinn 1.0 provides that *"...In international airspace, outer space, cyber infrastructure will regularly be located on board such vessels, offshore installations…, and satellites".*[71]

These definitions reaffirm the connection and interdependency of the cyber, space and ground systems, all of which are controlled and communicate virtually and electronically by humans. Several data flows can be identified between the Earth and space-based assets, as information is sent from Earth to satellites and other space-based assets (Earth-space interactions), but information is also sent back to Earth from satellites and other space-based assets (space-Earth interactions), which data flows are both critical and vulnerable to threats.[72] The security of space-based infrastructure depends on the safety of Earth-space interactions, and the security of systems relying on data from space depends on the safety of space-Earth interactions.[73]

In other words, due to the interdependence between outer space and the cyber means, cyber vulnerabilities pose serious risks not just for space-based assets themselves but also for ground-based critical infrastructure, and if not contained, these threats could interfere with global economic development and international security.[74]

On that note, cyber threats and 'cyber attacks' are generally non-kynetic, non-physical, electronic threats which include actions damaging the transmission and reception of data (jamming, an OT attack) or enabling the transmission of false data (spoofing). Electronic threats, are regarded as 'harmful interference' in legal terminology and

[68]"Space Cyber Defense: An Adaptive, Proactive Approach" (*Booz Allen*) <https://www.boozallen.com/markets/space/space-cyber-defense-an-adaptive-proactive-approach.html> accessed November 22, 2022.

[69] Supra n. 55 MILAMOS, Rule 104, page 9

[70] Ibid, MILAMOS, Rule 107, page 10

[71] Supra n. 58. Tallinn 1.0, Rule 3, par 2. p.29

[72] Supra 66. Al-Rodhan, "Cyber Security and Space Security"

[73] Ibid.

[74] Supra 30.

accordingly defined by both the ITU Constitution[75] and the Radio Regulations[76] as:*"interference which endangers the functioning of a radionavigation service or of other safety services or seriously degrades, obstructs, or repeatedly interrupts a radiocommunication service operating in accordance with Radio Regulations*". The question is whether "degrading, obstructing and repeatedly interrupting" is sufficiently broad so as to cover and encompass the possible future high tech cyber attacks, which might be far less detectable, but create s far greater damage (for example, it might be sufficient to interrupt only once to initiate a grave but short-term cyber attack or to not so seriously degrade physically to finalize a digital disruption or damage).

The Tallinn Manual 1.0 applicable in times of war, accordingly defines a cyber attack as: '*A cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects'*.[77]

As mentioned earlier, due to the feasibility, states have recently been turning towards cyber defense strategies rather than to using traditional kinetic means, but may conduct both offensive and defensive counter-space operations to achieve certain desired objectives.[78] Additionally, counter-space capabilities can be used to create temporary, as well as permanent, destruction of space assets, and while kinetic systems create permanent and irreversible destruction, electronic and cyber means have created mostly temporary disruptions and damage to space systems thus far.[79] *Counter-space capabilities are military capabilities that seek to prevent "an adversary from exploiting space to their advantage", enabling a space power to maintain "a desired degree of space superiority by the destruction or neutralization of enemy forces"*.[80]

When it comes to cyber attacks in space specifically, they are mostly direct injection of false data or the unauthorized monitoring of traffic or activities in outer space, but can include jamming, spoofing and hacking attacks on communication networks, targeting control systems or mission packages, and attacks on the ground infrastructure such as satellite control centers.[81] Moreover, cyber-attacks on satellites in particular, are often related to accessing the satellite system via ground stations that control satellites and

[75] See: Constitution and Convention of the International Telecommunication Union as amended by the 1994 Plenipotentiary Conference (Kyoto, 1994), Annex, No. 1003, page 63. available at: <https://www.itu.int/en/council/Documents/basic-texts/Constitution-E.pdf,>, accessed: 25. November 2022.
[76]See: The Radio Regulations, 2016, (hereinafter: ITU RR), No. 1.169 of the RR. Available at: <https://www.itu.int/dms_pub/itu-s/opb/conf/S-CONF-PLEN-2019-PDF-E.pdf> and <https://www.itu.int/en/ITU-R/space/snl/Documents/ITU-Space_reg.pdf>, accessed: 25. November 2022.
[77]Ibid. Supra n.58, Tallinn 1.0, Rule 30, page 91-92
[78]Supra n. 16, Rajagopalan, "Electronic and Cyber Warfare in Outer Space " pg 2
[79]Ibid. pg 1.
[80]Ibid. pg 5
[81]Ibid.

are often run on computers with softwares vulnerable to potential attacks from hackers.[82] Therefore, malware could be used to infect systems on the ground (like satellite control centers) and for users, and links between the two and spacecraft could be spoofed (disguising communication from an untrusted source as a trusted one) or suffer from replay (interrupting or delaying communication by malicious actors).[83]

There are various attack pathways to inhibit the central point of failure of a space system, two of which are the manufacturer of the space asset equipment and the operator or management company of the space systems.[84] The ability to impact multiple systems by compromising a central point of failure makes space systems attractive targets.[85] Not only that electronic cyber attacks are much harder to detect because of the difficulty of distinguishing between unintentional failure or malfunction, but such capabilities can be developed and deployed or even used without detection.[86] As the Aerospace Corporation explains in a recent paper[87], there are four main segments of space infrastructure that need to be hardened against cyber attacks, which include vulnerabilities to command intrusions (giving bad instructions to destroy or manipulate basic controls), payload control and denial of service (sending too much traffic to overload systems).[88]

In plain words, the electronic threats that pertain to cyberspace can be subsumed under the ever growing plethora of cybersecurity issues produced by various cyber attacks of anonymous individuals known as hackers. Any of the elements of the aforementioned cyber triad can be threatened and tampered with through hacking. Hacking is a term used to describe *unauthorized access to systems, networks, and data as targets*.[89] Hacking may be perpetrated solely to gain access to a target or to gain and/or maintain such access beyond authorization.[90]

The negative contemporary connotation of the term 'hacker' is owed to the growing trend and fast developing methods of hacking with malicious intent, as well to the consequent rise in cyberattacks. However, hackers are actually very often highly skilled tech experts who can either be white hats, otherwise known as ethical hackers or

[82] Peeters W, "Cyberattacks on Satellites" (*London School of Economics and Political Science* 2022), <https://www.lse.ac.uk/ideas/projects/space-policy/publications/Cyberattacks-on-Satellites> accessed November 21, 2022.

[83] Supra n. 30. King M "Cybersecurity Threats in Space: A Roadmap for Future Policy"

[84]Ibid.

[85] Gregory Falco, *Job for One Space Force: Space Asset Cyber Security*, <https://www.gregoryfalco.com/_files/ugd/e741d3_b8f6b65b8f4046a785066c9e0bf8c1ad.pdf >

[86]Supra n. 16, Rajagopalan, "Electronic and Cyber Warfare in Outer Space " pg 3.

[87] Brandon Bailey, Ryan J. Speelman and Prachant A. Doshi, "Defending Space Craft in the Cyber Domain" (*Home | The Aerospace Corporation*November 2019) <https://aerospace.org/sites/default/files/2019-11/Bailey_DefendingSpacecraft_11052019.pdf> accessed November 25, 2022

[88]Supra n. 30, King M "Cybersecurity Threats in Space".

[89] Cyber Crime Module 2: Key Issues, UNODC <https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/offences-against-the-confidentiality--integrity-and-availability-of-computer-data-and-systems.html>

[90]Ibid.

penetration testers, who protect their companies systems by testing their cybersecurity, or black hats, differentiated by the existence of malicious intent, who enter systems without authorization and often for personal gain.

However, it has been said that the traditional hacking schemes do not work well with space control systems, as in such classic schemes hackers purchase a publicly available controller, download the firmware from the manufacturer, examine it on their own test bed and then attack the actual system by exploiting the vulnerabilities they find.[91] But space technology is rather unique, which would presume years of working on a given system to penetrate it, and a comparable test version just isn't accessible.[92] On the other hand, many space systems are old, created before cybersecurity became a top policy priority, and vulnerabilities like hardcoded credentials used by ships, planes and the military, make access by sophisticated actors feasible.[93] But, in contrast to military satellites which are commonly designed so that the security aspect is duly considered, commercial satellites are more vulnerable to attacks because of a lack of awareness and implementation of security.[94] Often, manufacturers of satellites use off-the-shelf technology to make the costs more reasonable, while some of these components can be screened by hackers for vulnerabilities in open-source technology and software.[95]

A not-really that new, but currently trending, developing in the increasingly accelerated pace, and potentially dual use tool is Artificial Intelligence (AI) technology, associated with both IT and OT, algorithms and robotics, and thus relevant and worth to mention, when talking about in-space security.[96] As per the Council of Europe Artificial Intelligence Glossary, AI is: "*A set of sciences, theories, and techniques whose purpose is to reproduce by a machine the cognitive abilities of a human being.*"[97] As the AI framework is only just emerging, having in mind numerous in-space and space related AI applications, ranging from satellite remote sensing, to even space debris mitigation, cybersecurity is just

[91] Andreev A, "What's Going on with Cybersecurity in Space" (*Daily English Global blogkasperskycom*, February 3, 2022) <https://www.kaspersky.com/blog/cybersecurity-in-outer-space/43531/> accessed November 22, 2022.

[92] Ibid.

[93] Supra n. 30. King M "Cybersecurity Threats in Space"

[94] Supra n. 82, W, Peeters "Cyberattacks on Satellites"

[95] Ibid.

[96] Due to the complexity of this subject, along with the fact that it is not the direct matter of this article, and that this author had already covered the subject, we will not examine it further herein. To read more on in-space and space-related AI and its emerging framework, read: - Tamara Blagojevic, *"A brave new world: In-space AI and space-related AI and its soon-to-be fitting legal robe"*, Bulletin No11, Observatorio Juridico Aerospatial, AEDAE, June 2023.

[97] Glossary - Artificial Intelligence - www.coe.int. (n.d.). Artificial Intelligence. <https://www.coe.int/en/web/artificial-intelligence/glossary>, Accessed: July 2023.

as important in that domain, and much of its rules and principles can extend so as to cover AI cybersecurity.[98]

Many experts, in various disciplines (such as law, economy, management and engineering), advise IT and OT companies and private entrepreneurs to deploy cyber security techniques and standards in early stages of development in their supply chains, such as 'security by design',[99] and monitor and adapt them throughout the entire product lifecycle, and to ensure this approach by creating strategies which would allow for a secure and sustainable growth in this industry, by making policies inlined with cybersecurity standards, as well as an overall culture of cybersecurity.

Another very important mechanism, implied subtly when mentioning means and methods to enhance cybersecurity in space in general, is Space Situational Awareness (SSA). As per the SatCen, SSA refers to the knowledge of the space environment, including location and function of space objects and space weather phenomena. SSA is generally understood as covering three main areas:

Space Surveillance and Tracking (SST) of man-made objects.
Space WEather (SWE) monitoring and forecast.
Near-Earth Objects (NEO) monitoring (only natural space objects).[100]

As we can see, the interconnection of the cyber spectrum and space spectrum is visible across a wide range of different areas, implying the necessity for a harmonized development of their legal frameworks. Additionally, the necessity for a cooperative and collaborative holistic and multidisciplinary approach in cybersecurity is practically implied by the variety of the elements it subsumes beneath its umbrella.

Conclusively, we can begin to grasp the nexus between cyberspace and outer space - benefits, but also cyber threats and cyber attacks to space assets, satellites, spacecraft, other space infrastructure, as space objects in need for secure and sustainable use and regulation, which can be achieved through the means of the electromagnetic or cyber spectrum, necessary for their proper controlling and monitoring. However, to highlight the contemporary relevance of the issues related to this cyber-space relation, we need to take a look at some examples in practice, to better understand how to assess the current development of their frameworks.

4. EXAMPLES OF CYBER ATTACKS ON SPACE ASSETS

[98]See: Tamara Blagojevic, *"A brave new world: In-space AI and space-related AI and its soon-to-be fitting legal robe"*, Bulletin No11, Observatorio Juridico Aerospatial, AEDAE, June 2023.
[99] See: Data Privacy by Design: Legal meets Technology, KPMG, (Summary of webinar,January 17, 2022), <https://assets.kpmg/content/dam/kpmg/tt/pdf/data-privacy-by-design-legal-meets-technology.pdf>
[100]Space Situational Awareness, SatCan.Europa.EU, < https://www.satcen.europa.eu/page/ssa>

A recent survey[101] informs that experts nowadays are concerned about a possibility of massive cyber-attacks on satellites.[102] In such a hypothetical scenario it is not so unlikely that it could even initiate a global shutdown.[103] In that case, it is predicted that all flights would be grounded, trains stopped, and due to loss of GNSS signals, massive traffic jams would appear, the communications would be congested, while the intervention of police, ambulances or fire brigades would be delayed, the stock markets would considerably drop, and the power blackouts would start, while the ISS crew would need to be evacuated, which would all lead to the overall gradual economic collapse.[104] However, to move such a scenario from a sci-fi sounding hypothesis, into a real possibility realm, we need to enumerated some real-life incidents.

In that regard, several attempts, often considered by cyber-experts as experimental and preparatory tests, are known but not widely reported by satellite operators for obvious commercial reasons.[105] Similarly, cyberattacks on commercial satellite systems providing services to the economy are equally important as attacks on military satellites, although this impact is not as widely considered and reported.[106]

To highlight the gravity and scope of such issues, some examples of cyberattacks on satellites and space companies will be listed and briefly explained, starting from newer examples, towards the older ones, in hopes to show how long it took us to initiate an appropriate regulatory (re)action.

- In February, the Russian government hackers allegedly launched an attack on U.S. satellite company Viasat, disabling communications in Ukraine just before the invasion.[107] In the wake of this cyberattack which disrupted internet services in Europe provided by Viasat's KA-SAT, the U.S. government advised satellite operators to put their guard up,[108] while the Cybersecurity and Infrastructure Security Agency (CISA) requested that all organizations significantly lower their threshold for reporting and sharing indications of malicious cyber activity.[109] Following CISA's advisory, the Satellite Industry Association (SIA) issued a

[101] Supra n. 16, Rajagopalan, R., "Electronic and Cyber Warfare in Outer Space "
[102] Ibid. Supra 82, W. Peeters, Cyberattacks on Satellites.
[103] Ibid.
[104] Ibid.
[105] Ibid.Supra 82, W. Peeters, Cyberattacks on Satellites
[106] Ibid.
[107] Starks T and Schaffer A, "Analysis | Cyberattacks on Satellites May Only Be Getting More Worrisome" (*The Washington Post*July 29, 2022) <https://www.washingtonpost.com/politics/2022/07/29/cyberattacks-satellites-may-only-be-getting-more-worrisome/> accessed November 21, 2022.
[108] "Strengthening Cybersecurity of SATCOM Network Providers and Customers - Alert (AA22-076A)" (*CISA*March 2022) <https://www.cisa.gov/uscert/ncas/alerts/aa22-076a> accessed November 24, 2022
[109] Erwin S, "Cyber Warfare Gets Real for Satellite Operators" (*SpaceNews*March 21, 2022) <https://spacenews.com/cyber-warfare-gets-real-for-satellite-operators/> accessed November 17, 2022

statement of "commitment to cybersecurity best practices"[110] and expressed concern about "evolving attacks by criminals, terrorists, and nation states."[111] This cyberattack has been investigated by French, U.S. and Ukrainian intelligence services as a potential act by Russian hackers.[112] Viasat stated that the company believes that this attack was "a deliberate, isolated and external cyber event" and that customer data was not compromised.[113]

Similarly, according to CEO Elon Musk, SpaceX's Starlink internet system in low Earth orbit also very recently experienced "signal jamming" in user terminals in Ukraine.[114]

- Although not as recent as the attacks above, of a broader scope and longer duration certainly was the alleged campaign of identity theft and hacking on behalf of Iran's Islamic Revolutionary Guard Corps (IRGC), in order to steal critical information related to U.S. aerospace and satellite technology and resources.[115] As alleged in the indictment, the defendants' hacking campaign, which targeted numerous companies and organizations in the United States and abroad, began in approximately July 2015 and continued until 2019.[116] Apparently, the defendants possessed a target list of over 1,800 online accounts, including accounts belonging to organizations and companies involved in aerospace or satellite technology and international government organizations in Australia, Israel, Singapore, the U.S, and the United Kingdom.[117] Charged[118] in the indictment were defendants Said Pourkarim Arabi, Mohammad Reza Espargham, and Mohammad Bayati, with some sentences ranging even up to 20 years in prison.[119] This case, although not directed at outer space objects, as important space related information was stolen, can be used as a typical example of a breach of the right to privacy, showcasing relevance of the protection of the basic human rights in the cyber realm, and

[110] Satellite Industry Association, "Cybersecurity – Satellite Industry Association, Washington, D.C." (*Satellite Industry Association*February 17, 2020) <https://sia.org/policy/cybersecurity/> accessed November 21, 2022.
[111]Supra 109
[112]Ibid.
[113]Ibid.
[114]Ibid.
[115]U.S. Department of Justice Office of Public Affairs, "State-Sponsored Iranian Hackers Indicted for Computer Intrusions at U.S. Satellite Companies" (*The United States Department of Justice*July 13, 2022) <https://www.justice.gov/opa/pr/state-sponsored-iranian-hackers-indicted-computer-intrusions-us-satellite-companies> accessed November 24, 2022.
[116]Ibid.
[117]Ibid.
[118]*United States Of America V Said Pourkarim Arabi, Mohammad Reza Espargham, Mohammad Bayati* (2020) Indictment 22 <https://wwwjusticegov/opa/press-release/file/1317521/download>
[119]Ibid. Supra 134.

reaffirming that the cyber triad's pillars also imply the application and protection of human rights on the internet.

Another attack by Iranian hackers also took place in 2019. where computers of the American satellite technology industry were breached with help from a fake website and an unsuspecting college professor.[120] Court documents show that the U.S. Federal Bureau of Investigation (FBI) believed Iranian hackers going by the nicknames MRSCO and N3O, members of a long-running Iranian hacker collective known as the "Iranian Dark Coders Team, may have been involved in the attempted breaches, but the Department of Justice declined to comment publicly on the investigation.[121]

- In 2018. a group of Chinese state-backed hackers reportedly launched a sophisticated hacking campaign aimed at satellite operators and defense contractors.[122] This hack was discovered by Symantec, which provides the most widely used paid higher-end security software and services for consumers, companies and public agencies, who detected the misuse of common software tools at client sites, leading to the campaign's discovery at unnamed targets.[123] Symantec then shared technical information on the hack with the FBI and Department of Homeland Security,[124] but no further information was provided publicly by the FBI. However, this case definitely sheds light on how important the appropriate implementation of cyber security mechanisms and standards is throughout the entire supply chain life-cycle, all the way from the development and design stages.

- In September 2017, Norwegian authorities reported jammed GPS signals affecting civil flights in the north of the country during Russia's large "Zapad" military exercise.[125]

- In another case in 2017. an indictment was unsealed in US against Wu Yingzhuo, Dong Hao and Xia Lei, all of whom are Chinese nationals, for computer hacking,

[120]Hughes S and Rawnsley A, "Iranian Hacking Group Targeted Satellite Industry Nerds" (*The Daily Beast*October 22, 2019) <https://www.thedailybeast.com/iranian-hacking-group-targeted-us-satellite-companies?ref=scroll> accessed November 21, 2022

[121]Ibid.

[122]CNBC, "China-Based Hacking Campaign Is Said to Have Breached Satellite, Defense Companies" (*CNBC*, June 20, 2018) <https://www.cnbc.com/2018/06/19/china-based-hacking-breached-satellite-defense-companies-symantec.html> accessed November 19, 2022.

[123]Ibid.

[124]Ibid.

[125]Luke Harding, "Russia Denies Disrupting GPS Signals during NATO Arctic Exercises" (*The Guardian*, November 12, 2018) <https://www.theguardian.com/world/2018/nov/12/russia-denies-blame-for-arctic-gps-interference> accessed November 21, 2022

theft of trade secrets, conspiracy and identity theft[126] directed at U.S. and foreign employees, computers and firms working on satellite, energy, technology, transportation, and economic analysis to steal credentials and access sensitive data.[127]

- In 2014. the U.S. officials blamed China for a cyberattack that forced the National Oceanic and Atmospheric Administration (NOAA) to cut off public access to imagery data from a satellite network used for weather forecasting.[128] However, as University of Washington meteorologist Cliff Mass said that "there isn't any visible gain for the Chinese, as they have their own weather satellites, but also use U.S. data in their forecasting, they could have just been testing U.S. defenses".[129]

- In 2011. Tehran brought down a US RQ-170 UAV drone, "by jamming its satellite communications links and spoofing the GPS signals it received".[130] This case shows that attackers can interfere with satellite signals through a process called "meaconing" in which a legitimate GPS signal is spoofed and rebroadcast at a higher power level with a slight time delay, without the need to crack the encryption used in the military GPS signal because the data in the signal is not modified.[131]

- In 2010 and 2012. the Democratic People's Republic of Korea was accused of jamming the Republic of Korea's GPS signals for days, affecting many planes, ships and personal devices.[132]

- In 2009. Iran jammed Eutelsat's transmissions, upon which the European Union foreign ministers have urged Iran to stop jamming satellite signals that have affected transmissions by several Western broadcasters, including Deutsche Welle

[126]*United States Of America V Wu Yingzhuo, Dong Hao, Xia Lei* (2017) Indictment 16 <https://wwwjusticegov/opa/press-release/file/1013866/download> accessed November 21, 2022

[127]U.S. Department of Justice Office of Public Affairs, "U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage" (*The United States Department of Justice*November 27, 2017), <https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations> accessed November 21, 2022 .

[128]Doyle Rice, "China Hacks into U.S. Weather Satellite Network" (*USA Today,* November 13, 2014) <https://www.usatoday.com/story/weather/2014/11/12/china-weather-satellite-attack/18915137/> accessed November 21, 2022.

[129]Ibid.

[130]"Space Threat 2018: Iran Assessment" (*Aerospace Security,* June 22, 2022) <https://aerospace.csis.org/space-threat-2018-iran/> accessed November 19, 2022.

[131]Ibid.

[132] Rajeswari Pillari Rajagopalan R, "Changing Space Security Dynamics and Governance Debates" in Melissa de Zwart, Stacey Henderson (ed), *Commercial and Military Uses of Outer Space* (Springer 2021) , p159, < https://doi.org/10.1007/978-981-15-8924-9> , accessed November 19, 2022.

and the BBC.[133]

- In 2007, Sri Lanka's Tamil Tigers rebel group hijacked an Intelsat satellite to broadcast ethno-nationalist propaganda to Europe and Asia.[134] The Tamil Tigers fought a devastating civil war with the Sri Lankan military that led to extensive war crimes and crimes against humanity.[135] This type of hackers are commonly known as 'hacktivists', due to their intent being tied with a political agenda, and this case is therefore, yet another example of how human rights can be threatened by cyber attacks aimed at satellites.

- In 2007. and again in 2008. two U.S. environment-monitoring satellites, the Landsat-7 and a NASA-managed Terra AM-1 earth observation satellite were interfered with four or more times via a ground station in Norway.[136] In this case, although China's military was once again a prime suspect, the U.S.-China Economic and Security Review Commission, which reported the interference, said the events had not actually been traced to China.[137]

- In 1999, a 15 year old J. Jonathan hacked and shutdown NASA's computers for 21 days, in which circumstance about 1.7m software downloaded cost NASA $41,000.[138] This case, although not as relevant as previous ones, might serve to show just how easily even the supposedly most secure and advanced systems could be hacked more than 20 years ago, by a kid.

- In 1998. hackers took control of the U.S.-German ROSAT X-Ray satellite, by hacking into computers at the Goddard Space Flight Center in Maryland, and instructing the satellite to aim its solar panels directly at the sun, which effectively fried its batteries and rendered it useless.[139] Defunct satellite re-entered the Earth's

[133]Andreas Illmer, "Iran Censorship" (*dw.com*, March 22, 2010) <https://www.dw.com/en/eu-slams-irans-jamming-of-satellite-signals-as-unacceptable/a-5377813> accessed November 25, 2022

[134]SpaceNews Staff, "Intelsat Vows to Stop Piracy by Sri Lanka Separatist Group" (*SpaceNews,* December 6, 2014) <https://spacenews.com/intelsat-vows-stop-piracy-sri-lanka-separatist-group/> accessed November 19, 2022.

[135]Wenzel Michalski, "Sri Lanka: High Ranking Officials Involved in War Crimes" (*Human Rights Watch,* February 26, 2021) <https://www.hrw.org/news/2021/02/26/sri-lanka-high-ranking-officials-involved-war-crimes> accessed November 19, 2022.

[136]Jim Wolf, "China Key Suspect in U.S. Satellite Hacks: Commission" (*Reuters,* October 28, 2011) <https://www.reuters.com/article/us-china-usa-satellite-idUSTRE79R4O320111028> accessed November 21, 2022 .

[137]Ibid.

[138]Catherine Wilson, "15-Year-Old Admits Hacking NASA Computers" (*ABC News*) <https://abcnews.go.com/Technology/story?id=119423&page=1#:~:text=M%20I%20A%20M%20I%2C%20Sept.,cruise%20around%20like%20an%20employee> accessed November 21, 2022.

[139] Jsamuel (Staff Writer), "NASA Computers Hacked by Intruders - via Satellite -" (*Via Satellite,* August 21, 2013),<https://www.satellitetoday.com/government-military/2008/12/01/nasa-computers-hacked-by-intruders/> accessed November 19, 2022.

atmosphere over the Bay of Bengal, and eventually crashed back to Earth in 2011, which was confirmed by the German space agency (DLR).[140] According to Astronomer Jonathan McDowell, although the surviving fiery plunge would have probably splashed into the ocean, avoiding populated areas, two Chinese cities with millions of residents each, Chongqing and Chengdu, layed further north-east along the satellite's projected path.[141]

As we can see, many of the cases of cyber attacks showcased in the media appear to be mainly against the US or at least in between the main space powers, Russia and China. But, as the situation develops, and as cyber means are much cheaper than traditional kinetic and ASAT weapons, this just might intensify over the following years, especially due to the fact that private actors and other states are surely and steadily joining the game. Former Director of National Intelligence Dan Coats testified in 2018 that Iranian hackers ranked alongside hacking groups from China, Russia, and North Korea as among the greatest cyberthreats to the U.S.[142] However, the US military has also disclosed that it self-jams its own systems 23 times per month on average due to accidental interference,[143] and cyber attacks cannot be traced so easily and surely to their true perpetrator, as the geolocation of the attack can possibly be hidden or pinned to a different state or even region, for which reasons we shouldn't be too quick to judge on one state's general intention.

To better understand the severeness and the plausibility of the cyber attacks on space infrastructure turning into an everyday reality, we must consider the development and the status of the frameworks enabling the prevention of such (not-so) hypothetical scenarios.

5. THE DEVELOPMENT, STATUS AND MAIN ELEMENTS OF THE APPLICABLE LEGAL FRAMEWORK(S)

5.1. Applicability of International Law, International Human Rights and International Humanitarian Law

[140]--, "German ROSAT Spacecraft Re-Entered over Bay of Bengal" (*BBC News,* October 26, 2011) <https://www.bbc.com/news/science-environment-15466361> accessed November 19, 2022.

[141]Ibid.

[142]Adam Rawnsley, *Iranian Hacking Group Targeted Satellite Industry Nerds*, (TheDailyBeast, Oct. 22, 2019),<https://www.thedailybeast.com/iranian-hacking-group-targeted-us-satellite-companies>

[143]Juliana Suess, "Jamming and Cyber Attacks: How Space Is Being Targeted in Ukraine" (*Royal United Services Institute*April 5, 2022) <https://www.rusi.org/explore-our-research/publications/commentary/jamming-and-cyber-attacks-how-space-being-targeted-ukraine> accessed November 24, 2022.

Due to the fact that Cyber Law is a new concept covering the activities in a fast changing and developing environment, but having in mind that the Internet is merely a mirror to all the subjects, objects and their interactions from the physical world, in a virtual reality, to understand the scope of the Cyber law framework, we would thus have to carefully consider all the rules that are already applicable to the cyber realm, before looking into the specific rules, regulating it more directly and explicitly.[144]

On that note, the 2013 UN Group of Governmental Experts (GGE) report found that "*International law, and in particular the Charter of the United Nations, is applicable to cyberspace and essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment*".[145] The latter 2015 GGE report reiterated these conclusions and went a step further, offering a non-exhaustive list of how international law applies, including by (i) granting states jurisdiction over ICT infrastructure in their territory; (ii) directing states to observe principles of sovereignty, sovereign equality, peaceful settlement of disputes, non-intervention, and human rights; (iii) referencing International Humanitarian Law (IHL) principles (without endorsing IHL's application explicitly); and (iv) prohibiting states from using proxies to violate international law via ICTs.[146]

Today, most states and several international organizations, including the UN General Assembly's First Committee on Disarmament and International Security, the G20, the EU, ASEAN, and the OAS have affirmed that existing international law applies to the use of information and communication technologies (ICTs) by states.[147]

Similarly to the question of applicability of International Law in general, and having in mind the cyber triad's pillars (confidentiality, integrity and accessibility), imply the application of certain, if not all, basic Human Rights, it is also important to note that the United Nations Human Rights Council has repeatedly affirmed that the "same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice".[148] The freedom of expression is recognised by the United Nations General Assembly[149] as a kind

[144] In this section, for the purpose of finding the similarities and points of contact between cyber law and space law, if any, and assessing whether their development is synchronized, the main focus will be on such areas of international law relevant for both fields, or applicable to joint cyber-space activities.

[145] Ibid. Supra n.37, pg 2.

[146] Ibid. Supra n. 37, Brett Biddington, *One Coin, Two Sides,* pg. 3

[147] Duncan Hollis, "A Brief Primer on International Law and Cyberspace" (*Carnegie Endowment for International Peace,* June 14, 2021) <https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763> accessed November 19, 2022.

[148] See for example: A/HRC/RES/20/8; A/HRC/RES/38/7; GA resolution A/RES/68/167 - for the same affirmation for the right to privacy. Available at: <https://undocs.org/A/HRC/RES/20/8> ; <https://undocs.org/A/HRC/RES/38/7> ; <https://undocs.org/A/RES/68/167> ; accessed November 19, 2022

[149] See: UN GA resolution A/RES/68/167: "that the exercise of the right to privacy is [also] important for the realization of the right to freedom of expression and to hold opinions without interference, and is one of

of a precondition, enabling and facilitating the enjoyment of other essential human rights, including the right to freedom of peaceful assembly and association, the right to education, and right to participate in cultural life.[150] Moreover, in 2016, the United Nations Human Rights Council passed a resolution condemning the practice of preventing and/or disrupting individuals' access to the Internet.[151] Although the universal access to the Internet is not recognized as a human right in international human rights law, State obligations to promote Internet connectivity can be derived from a number of human rights,[152] such as freedom of expression.[153] Such obligations include "*adopt[ing] effective and concrete policies and strategies - developed in consultation with individuals from all segments of society, including the private sector as well as relevant Government ministries - to make the Internet widely available, accessible and affordable to all*".[154]

In addition (especially having in mind the before mentioned attack by the hacktivists Tamil Tigers) in the opinion of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, certain "forms of expression" should be "prohibited by international law," among them are the "advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence," and "direct and public incitement to commit genocide".[155] The same prohibition is also included in the International Covenant on Civil and Political Rights of 1966,[156] and Article III(c) of the Convention on the Prevention and Punishment of the Crime of Genocide of 1948.[157]

As visible from above, the Human Rights law approach focuses mainly on the need for a balanced protection of both the first pillar of the cyber triad, relating to confidentiality, as it is mirrored in the right to privacy, and the third pillar relating to availability and

---

the foundations of a democratic society", available at: https://undocs.org/A/RES/68/167 ; accessed November 19, 2022.

[150] Ibid, Supra note 147. D. Hollis

[151] See: United Nations General Assembly Human Rights Council, "Resolution Adopted by the Human Rights Council A/HRC/RES/32/13" (*UN.org*July 18, 2016), Available at: <https://www.undocs.org/A/HRC/RES/32/13> ; accessed November 19, 2022.

[152] Ibid, Supra note 147. D. Hollis

[153] See: United Nations General Assembly Human Rights Council, Resolution A/HRC/17/27, Available at: <https://undocs.org/A/HRC/17/27>; accessed November 19, 2022.

[154]Ibid. para.66

[155] Ibid, Supra note 147. D.Hollis 2013, p. 111.

[156]General Assembly of the United Nations, "International Covenant on Civil and Political Rights, and the Optional Protocol to the above-Mentioned Covenant" (*treaties.un.org*December 19, 1966), Article 20(2), <https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf>,accessed November 25, 2022.

[157]General Assembly of the United Nations , "Convention on the Prevention and Punishment of the Crime of Genocide - No. 1021 "(*treaties.un.org*December 9, 1948) <https://treaties.un.org/doc/Publication/UNTS/Volume%2078/volume-78-I-1021-English.pdf> accessed November 23, 2022.

implying equal access to all authorised users, mirrored in the freedom of expression and prohibition of discrimination.

However, in jurisprudence, there were several legal manuals created for clarification of what of the existing International law is applicable to the cyber realm. For example, the two Tallinn Manuals,[158] confirmed the application of International Law, International Humanitarian Law principles and even Space Law to cyberspace[159] (the last of which to be further discussed in the following subtitle).

For example, the Tallinn 1.0, applicable only during armed conflict, confirms the application of the UN Charter[160] and the International Humanitarian law principles, both by indicating that the exercise of the right to Self Defense, which the state is entitled to in cases when a cyber operation constitutes an armed attack (depending on its scale and effects), is subject to requirements of *necessity, proportionality, imminence, immediacy, and the determination ex ante and reasonable determination that the attack has occured, or is about to occur, as well as the identity of the attacker.*[161] This manual also reaffirms the geographical limitation for conducting cyber operations, which include, the "*place from which relevant cyber operations are launched, the location of any necessary instrumentalities and the location of target cyber systems."*[162] Moreover, it states that the cyber operations might be conducted from "...on, or with effect in the entire territory of the parties to the conflict, international waters, *airspace and subject to certain limitations outer space*, and are generally prohibited elsewhere."[163] Furthermore, the Tallinn 1.0 also confirms that the neutral cyber infrastructure, *both in airspace and in outer space is protected by the national sovereignty of a State.*[164] Additionally, *interference* is referred to as a *violation of a state's sovereignty*, if it's directed at a state's *cyber infrastructure that envoys sovereign immunity, aboard a platform, or wherever located.*"[165] This provision, although not explicitly mentioning outer space, the use of the wording 'wherever located', implies outer space as well. On the other hand, going on with the prohibition of states knowingly allowing the use of their cyber infrastructure, located in their territory or under

[158] As mentioned in appropriate sections earlier, these manuals are: The Tallinn Manual On International Law Applicable To Cyber Warfare - only applicable strictly during armed conflict, tying both space law provisions and cyber means to *Ius in bello*; and the Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter Tallinn 2.0]. Both manuals are just restatements of the existing law, and not their interpretation. They are funded by the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE)

[159] Ibid, Supra note 147. Duncan Hollis 2013

[160]'Statute of The United Nations and the Statute of the International Court of Justice', (hereinafter: UN Charter) 1945, San Francisco, Article 51, <https://treaties.un.org/doc/publication/ctc/uncharter.pdf>, accessed: November 2022.

[161]Supra n. 58, Tallinn 1.0, Rule 13, p 53.

[162] Supra n. 58, Tallinn 1.0, Rule 21. Par.1 page71

[163] Ibid. Supra n. 58, Tallinn 1.0, Rule 21. Par.1 page71

[164] Supra n. 58, Tallinn 1.0, Rule 9, page 203

[165] Supra n. 58, Tallinn 1.0, Rule 4

their exclusive government control, for acts that adversely or unlawfully affect other states, *including satellites in outer space over which is exercises exclusive control*[166], explicitly reaffirms the applicability of non-interference and the due diligence principle to space.

The principle of non-intervention with cyber means explicitly, is also referred to in Tallinn 2.0 applicable in times of peace, without limiting it to outer space, but more generally, in either internal or external affairs of another state,[167] which can provide a good point for avoiding any legal lacunae or bad faith interpretations in the future. The same manual also provides the reaffirmation of the explicit prohibition of the "*United Nations to intervene, including by cyber means,* in matters that are within the domestic jurisdiction of a certain State, without prejudice to the enforcement measures potentially decided by the UN Security Council under Chapter VII of the United Nations Charter."[168]

As we can see in the takeouts from the Tallinn Manuals, the mere applicability of the general principles of International law and International Humanitarian Law are not questioned by law experts. However, keeping in mind the difficulties of detecting the perpetrator of a cyber attack, the question is more, to which extent can these principles really be enacted, and how can it be proven whether the state in question exercised effective control over its forces or proxies, in order to apply the due diligence principle, in such a vast, virtual, or an untransparent, remote area.

5.2. Space Law

When thinking about electronic and cyber threats, in relation to outer space, we would need to utilize a kind of an evolutive approach to interpretation, in consideration of the fact that some of the well established outer space principles, could have not explicitly enumerate the cyber activities, attacks, weapons, objects and infrastructure *stricto sensu*, as such means were only beginning to be utilized at the time that the outer space framework was developed.

[166] Ibid. Supra n. 58, Tallinn 1.0, Point 5. Rule 4
[167] *Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations* (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter Tallinn 2.0], Rule 66
[168]Ibid, Tallinn 2.0, Rule 67

Although neither of the five main UNOOSA Space Treaties,[169] nor the soft law instruments such as the Space Debris Mitigation guidelines,[170] or the Guidelines for the Long-term Sustainability of Outer Space Activities,[171] contain any express reference to cybersecurity whatsoever or any direct cybersecurity obligations, similar to the International Law in general, there are provisions the compliance of which may require the implementation of security measures within satellite systems.[172] Similar goes for all the existing Transparency and confidence building measures (TCBM),[173] where the only applicable principles might be related to exchanges of information on forecasted natural hazards in outer space, or notification in the case of emergency situations.[174]

However, similarly to the reaffirmation of International law, the Tallinn Manuals can serve as guides to what is applicable. As per the Tallinn 2.0 which reaffirms the rules applicable in times of peace or the prevention of an armed conflict, "*cyber operations on the Moon and other celestial bodies may be conducted only for peaceful purposes*,"[175] and "*the offensive cyber capabilities cannot be placed on the Moon"*,[176] (while no similar prohibition is repeated for outer space in general), and whereas "*only those Cyber operations in outer space (as a whole) are subject to international law limitations on the use of force"*.[177] This rule is a clear affirmation of the UN Charter's prohibition of threats

[169] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, T.I.A.S. No. 6347, 610 U.N.T.S. 205, [hereinafter OST]. <https://www.unoosa.org/pdf/gares/ARES_21_2222E.pdf>; 'Agreement on the Rescue of Astronauts and the Return of Objects Launched in Outer Space', Apr. 22, 1968, 19 U.S.T. 7570, 672 U.N.T.S. 119 [hereinafter Rescue Agreement]; 'Convention on International Liability for Damage Caused by Space Objects', Mar. 29, 1972, 24 U.S.T. 2389, 961 U.N.T.S. 187 [hereinafter Liability Convention]; 'Convention on Registration of Objects Launched into Outer Space', June 6 1975, 28 U.S.T. 695, 1023 U.N.T.S. 15 [hereinafter Registration Convention]; Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, Dec. 18, 1979, 1363 U.N.T.S. 3 [hereinafter Moon Agreement]. <https://www.unoosa.org/pdf/gares/ARES_34_68E.pdf>;

[170] *Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space,* UN COPUOS, UNOOSA, (Vienna, 2010) Preamble, pg. iii, iv, <http://www.unoosa.org/pdf/publications/st_space_49E.pdf>

[171] *Guidelines for the Long-term Sustainability of Outer Space Activities, A/AC.105/2018/CRP.20,* Conference room paper by the Chair of the Working Group on the Long-term Sustainability of Outer Space Activities (27 June 2018 , Vienna), Available at: <https://www.unoosa.org/res/oosadoc/data/documents/2018/aac_1052018crp/aac_1052018crp_20_0_html/AC105_2018_CRP20E.pdf> accessed: 20. November 2022.

[172] M, Cocco, "Data Policy, Regulatory Framework, and Cybersecurity", Dec. 2020,UNOOSA, presentation, page 14, <https://www.unoosa.org/documents/pdf/spacelaw/activities/2020/SLC2020Presentations/SLC2020PDFPresentations/I._Cocco_-_9_Dec_2020_Apresentacao_-_UN_Africa_Presentation_08.12.2020_CC8982136.1_0028985173.1.pdf>

[173] Transparency and confidence-building measures in outer space activities, February 2017, UN General Assembly,<https://www.unoosa.org/res/oosadoc/data/documents/2017/a/a7265_0_html/A_72_065E.pdf>

[174] Ibid. Supra 172. M. Cocco

[175] Ibid. Supra n. 167. Tallinn 2.0, Rule 58 point a)

[176] Ibid. Supra n. 167. Tallinn 2.0, Rule 58 point b)

[177] Ibid. Supra n. 167. Tallinn 2.0, Rule 58 point

or use of force,[178] but also of the OST provision that activities in outer space should be conducted "*... in accordance with International law ....and in the interest of promoting international peace, security and promoting international cooperation*…",[179] and the Moon Treaty provision that the Moon and other celestial bodies are to be used for "*exclusively peaceful purposes"*.[180] Therefore, military cyber operations may not be launched from the Moon or other celestial bodies, despite the fact that the treaty predates the technical capability to do so.[181]

The Tallinn 2.0 also confirms the applicability of the principles of due diligence, retaining jurisdiction and international responsibility (originally envisioned by the OST and the Liability convention) in regards to registered space objects.[182] In that regard, the manual further reaffirms that the "*Cyber operations involving space objects are subject to the responsibility and liability regime of space law*,"[183] and confirms the need for the *"authorization and supervision of the cyber activities in outer space of the state's non-governmental entities."*[184] These rules in conjunction, with the explicit reference to cyber operations, and with having in mind that cyber infrastructure can be located on satellites, should reaffirm that the state using cyber infrastructure on/in a satellite or a space object under its registration, will retain jurisdiction, and can be taken as the liable state, in case of an outer space related cyber attack. However, the manual further states that: "The mere fact that a Cyber Operation is *launched* from Governmental Cyber Infrastructure or otherwise originates from Governmental Cyber Infrastructure is not sufficient evidence for attributing an operation to that state but is an *indication* that such a State is *associated* with the cyber operation," indicating a slight difference from Space Law, where the launching state is the liable state as per the Liability convention.[185] This provision has a legal ratio in the difficulty to trace the exact origin of a cyber attack, and/or prove the nexus, or in other words - that the supposedly liable (launching) state hired an agent, as hackers can act from any territory, due to the characteristics of cyber attacks.

However, aside from the aforementioned, other principles such as the principle of due diligence and avoiding harmful interference with peaceful state activities, are also reaffirmed (in Tallinn 2.0) regarding peaceful cyber operations involving outer space. For example, an association to the due diligence principle is visible in requiring the State's to

[178] Supra n. 179. UN Charter, Article 1, paragraph 4, <https://treaties.un.org/doc/publication/ctc/uncharter.pdf>
[179] Supra n.53, OST, Article III, <https://www.unoosa.org/pdf/gares/ARES_21_2222E.pdf>
[180] Supra 54. Moon Treaty, Article III, par 1, <https://www.unoosa.org/pdf/gares/ARES_34_68E.pdf>
[181] Schmitt , M.N. and Vihul, L. (2016) *Chapter 2 the nature of International Law Cyber Norms*. NATO CCD COE, pg 33, Available at: https://195.222.11.251/uploads/2018/10/InternationalCyberNorms_Ch2.pdf (Accessed: November 14, 2022)
[182] Ibid. Supra n. 167. Tallinn 2.0, Rule 59 point a)
[183] Ibid. Supra n. 167. Tallinn 2.0, Rule 60 point a and b
[184] Supra 55,Milamos 142
[185] Liability Convention, Articles II and VII

take measures to *ensure* the establishment of international telecommunication infrastructure required for *rapid and uninterrupted* international telecommunications, and to *maintain and safeguard it*.[186] Additionally, the manual reaffirms that a "*State's use of radio stations may not harmfully interfere with other States' protected use of radio frequencies for wireless cyber communications or services.*"[187] In that regard, it also reaffirms that the State has a possibility to *suspend* (partially or fully) *international cyber communication services* within its territory and if so, immediately notify other States.[188] Similarly, as per the same manual, a State may *stop the transmission of private cyber communication that appears contrary to its national laws, public order, or decency, or that is dangerous to national security*.[189]

Similarly to the Tallinn Manuals, the McGill Manual, restates International law of critical importance to space activities conducted during peacetime and in times of tension that pose challenges to peace.[190] MILAMOS embodies multiple principles by reaffirming that the "*States shall, to the extent required by international law, refrain from intentionally causing either physical or non-physical harmful interference with space activities of another State in its peaceful exploration and use of outer space, including the Moon and other celestial bodies*."[191] Another reference to due diligence, avoiding harmful interference, including an explicit reference to satellite regulations, is then made by providing that the "*States shall ensure that stations within their jurisdiction which use radio frequencies are established and operated in such a manner as not to cause harmful interference to the radio services or communications of other States or of recognised operating agencies, or of other duly authorized operating agencies which carry on a radio service, and which operate in accordance with the provisions of the Radio Regulations of the International Telecommunication Union*."[192] The MILAMOS also mentions the *prohibition of interference with Telemetry, Tracking and Command (TT&C) operations of space objects under the jurisdiction and/or control of another State, including those used in military space activities*.[193]

Therefore, by frequent referencing of the relevant framework regulating satellites, as well as the telecommunication and radio spectrum, both the Tallinn and the MILAMOS manuals imply the applicability of the ITU Radio Regulations (ITU RR) and ITU Constitution.[194] Moreover, further references to the same regulatory framework are made

[186]Supra n. 167. Tallinn 2.0, Rule 61
[187]Ibid., Rule 63
[188]Ibid, Rule 62 point a)
[189]Ibid, Rule point b)
[190] Supra n. 55, MILAMOS
[191]Ibid, Rule 139.
[192]Ibid. Rule 141
[193]Ibid. Rule 144
[194] Supra n. 75, ITU Constitution, Article 45. Par.No. 197-199.Page 50., available at: <https://www.itu.int/en/council/Documents/basic-texts/Constitution-E.pdf , accessed: 25. November 2022.

in Tallinn 2.0 by stating that the State *retains its entire freedom under international telecommunication law with regard to military radio installations*,[195] while the MILAMOS manual goes into a more direct reference, by adding that this retention of freedoms should be "*in accordance with the Constitution of the ITU and subject to other applicable rules of international law, including international space law.*"[196] But, it also adds references to prevention, as well as international cooperation and emergency assistance by stating that "*States shall ensure that such (military) installations within their jurisdiction must, as far as possible, observe statutory provisions relative to giving assistance in case of distress, measures to be taken to prevent harmful interference, and the types of emission and the frequencies to be used, according to the nature of the service performed by such installations*."[197] It then goes on to mention that "*When such installations take part in the service of public correspondence or other services governed by the Administrative Regulations of the ITU, they must, in general, comply with the regulatory provisions for the conduct of such services.*"[198]

Milamos also goes further in the aspect of prohibitions of certain cyber attacks, such as "*Jamming and Spoofing of Communications",* and reiterates that *"In accordance with general international law, but without prejudice to provisions regarding military radio installations under the Constitution of ITU, States must refrain from intentionally causing harmful interference to communications within the jurisdiction and/or control of another State by means of jamming and/or spoofing of radio services.*"[199] This concise reference to particular types of cyber attacks, stems from the ITU RR original and more detailed prohibition of jamming, which provides, among else, that *"all stations are forbidden to carry out unnecessary transmissions, or the transmission of superfluous signals, or the transmission of false or misleading signals(…)"*.[200] It is further pertinent to mention that *safety services* (aeronautical, maritime and radionavigation), require *absolute international protection and imperative elimination of harmful interference*.[201] This broadens the protection from cyber attacks, but leaves the question open regarding the exact interpretation and scope of the terms used, such as 'unnecessary', in light of the fast paced technological developments.

The MILAMOS contains clear and exact reaffirmation of the the ITU RR and ITU Constitution's[202] main principles of efficient use of and equitable access of the spectrum/orbit resources, which and stipulate that:

[195] Supra n. 167, Tallinn 2.0 rule 64
[196] Supra n. 55, MILAMOS, Rule 142
[197] Ibid. Supra n. 55, MILAMOS
[198] Ibid.
[199] Ibid, Rule 143
[200] Supra n. 76, ITU RR, No. 15.1.
[201] Ibid, No. 15.28.
[202] Supra n. 75 and 76, ITU Constitution (Article 44), No. 196. And ITU RR

"In using frequency bands for radio services, including in the conduct of military space activities, States shall take into account that radio frequencies and any associated orbits, including the geostationary orbit, are limited natural resources. Such resources must be used rationally, efficiently and economically, in conformity with the provisions of the RR and other applicable instruments of the ITU, so that countries or groups of countries may have equitable access to those orbits and frequencies, taking into account the special needs of the developing countries and the geographical situation of particular countries.".[203]

To ensure such efficient and equitable use, and avoid harmful interference, the ITU RR set out the procedure as a direct approach between the administrations concerned, as well as the conditions for resolving the harmful interference issue.[204] However, in cases when action on a bilateral is unsuccessful, ITU can also be informed of the harmful interference issues or a specific request for assistance can be launched.[205] When contacted, ITU investigates the causes of the potential harmful interference and forwards its findings and recommendations to the administrations involved.[206] If this approach proves unsuccessful, a report is prepared for the ITU RR Board and the conclusions with invitations to apply ITU's recommendations and eliminate harmful interference, are transmitted to the administrations concerned.[207] But, the ITU also organizes international monitoring programs to identify sources where signal emissions are not compliant with the ITU RR and to take necessary actions for eliminating unauthorized emissions[208]. Once a source is located, ITU then contacts the administration believed to be responsible for the source of harmful interference to request prompt action to eliminate it.[209]

The Dispute Resolution Mechanism provided is based on diplomatic channels,[210] but there is an Optional Protocol for Compulsory Arbitration, which also provides an opportunity for an additional legal instrument, if signed and accepted.[211] Similar peaceful means to ones envisioned in ITU Constitution, RR and other main space treaties are implied in the Tallinn 2.0, but in a different wording: *"(a) States must attempt to settle their international disputes involving cyber activities that endanger international peace and security by peaceful means; (b) If States attempt to settle international disputes involving*

[203] Supra n. 55, MILAMOS, 140
[204] Supra n.76 ITU RR, Section VI, Article 15; See also: ITU, "Regulation of Satellite Systems" (*ITU.int*) <https://www.itu.int/en/mediacentre/backgrounders/Pages/Regulation-of-Satellite-Systems.aspx> accessed November 25, 2022
[205] Ibid.
[206] Ibid
[207] Ibid
[208] Ibid
[209] Ibid
[210] Supra n. 75, ITU Constitution, Article 56, par no. 233-235, page 61
[211] ITU, "Regulation of Satellite Systems" (*ITU.int*), <https://www.itu.int/en/mediacentre/backgrounders/Pages/Regulation-of-Satellite-Systems.aspx>, accessed November 25, 2022

cyber activities that do not endanger international peace and security, they must do so by peaceful means."[212]

As we were able to see, some issues such as harmful interference and jamming were covered very early on, and the principles provided by the Space Law and the ITU frameworks, are quite aligned with the stipulations provided by the umbrella of the cyber triad. But, as new technology develops daily, it is a question of how much of the new cyber attacks could be subsumed under the existing principles and provisions provided by the unchanged framework of the ITU, RR and general Space Law. This is why a look into newly developed efforts, with a more direct focus on potential cyber attacks is needed.

5.3. Cyber law framework development and status

As evidenced in the previous section, in cyberspace in general, to some extent, a legal framework existed from the very beginning, at least for a certain type of activities and rules related to telecommunications, as well as content rules, primarily for broadcasting.[213] The main instruments were licensing by regulatory agencies, international coordination of frequencies and numbers, mainly under the auspices of the International Telecommunications Union (ITU).[214] Additionally, a partial framework was already provided by the International Law in general, as well as by International Human Rights Law, International Humanitarian law, and Space law.

Therefore, the big cyberspace challenge from the legal viewpoint was not the total absence of rules or regulatory bodies but the question to which amount and limit are the traditional rules really applicable, due to the borderless nature of cyberspace.[215] As a response to the question of applicability, as well as in order to ensure some responsibility so as not to provoke states into having to take restrictive action, various multi-stakeholder fora and self-regulatory systems developed.[216] Consequently, the development of the cybersecurity and cyber crime framework on the international level wasn't really coordinated and harmonized, but on the contrary, polarized between states seeking a new UN convention, on one end, with another group in favor of sticking with existing instruments, focusing on capacity building and improved technical assistance.[217]

---

[212] Supra n. 167, Tallinn 2.0, Rule 65

[213] Katrin Nyman Metcalf, "A Legal View on Outer Space and Cyberspace: Similarities and Differences" (*CCDCOE*2018), page 9. Available at: <https://ccdcoe.org/uploads/2018/10/Tallinn-Paper_10_2018.pdf> accessed November 24, 2022

[214] Ibid.

[215] Ibid.

[216] Ibid.

[217] Summer Walker and Ian Tennant, "Control, Alt or Delete? - The UN Cybercrime Debate Enters a New Phase" (*globalinitiative*, December 2021) <https://globalinitiative.net/wp-content/uploads/2021/12/UN-Cybercrime-PB-22Dec-web.pdf>, accessed November 25, 2022

The result, given that cyber activities are relatively new, aside from the ITU regulation, the older Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108),[218] and the Council of Europe Convention on Cybercrime (Budapest Convention) adopted in 2001,[219] was that very few international treaties deal with them explicitly and directly.

While the primary focus of the Convention 108 is mainly the protection of personal data, it also contains certain provisions relevant for cybersecurity, such as: Prescribing measures and duties of parties; Prescribing the Quality and Security of Data, as well as distinguishing Special categories of Data; Additional safeguards for the data subject - data subject rights (e.g. to be informed of the processing of their personal data, to have access to that data, to rectify inaccuracies, and request the erasure of unlawfully processed data); International Cooperation between the parties and Safeguards concerning assistance rendered by designated authorities.[220] This convention provides the definition of personal data and data subjects as follows: " *... means any information relating to an identified or identifiable individual ("data subject")*".[221] Furthermore, as per the Convention 108, the *"automated data file" means any set of data undergoing automatic processing,* which processing is then enumerated as the following activities: "*storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination" if carried out in whole or in part by automated means.*[222] The "*controller of the file is the natural or legal person, public authority, agency or any other body … competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them".*[223] Finally, this convention addresses the requirements regarding the quality of the data which needs to be: *Obtained and processed fairly and lawfully*; *Stored for specified and legitimate purposes and not used in a way incompatible with those purposes*; *Adequate, relevant and not excessive in relation to the purposes for which they are stored*; *Accurate and, where necessary, kept up to date*; *Preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.*[224]

[218] *Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (CETS 108, Strasbourg, 1981), (hereinafter: Convention 108), <https://rm.coe.int/1680078b37>, Accessed: Dec. 2022.
[219] *Council of Europe Convention on Cybercrime*, ETS No.185, (Hereinafter: Budapest Convention), (Council of Europe,Budapest, 23.XI.2001), available at: <https://rm.coe.int/1680081561>, accessed: 27. November 2022.
[220] Ibid.
[221] Ibid, Article 2 – Definitions, point a)
[222] Ibid, Article 2 – Definitions , point b) and c)
[223] Ibid, Article 2 – Definitions , point d)
[224] Ibid, Article 5 – Quality of data, Points a) to e).

The Budapest Convention is focused only on the criminal aspect, and mainly addressed child pornography under content related offenses.[225] Some main provisions in its Chapter II were mainly measures to be taken at the national level related to substantive and procedural Criminal law, as well as expedited preservation of stored computer data, production order, and rules on the search and seizure of stored computer data.[226] Chapter III relates to the General principles for International cooperation, Mutual Assistance, and Extradition, as well as the establishment of a 24/7 Network for immediate assistance.[227] Chapter IV final provisions provided for the European Committee on Crime Problems (CDPC) as a mechanism for settlement of disputes and consultations.[228] The cyber triad is in fact respected by providing main offenses against the confidentiality, integrity and availability of computer data and systems (such as Illegal access; Illegal interception; Data interference; System interference; Misuse of devices;).[229] Other offenses are mainly computer-related (forgery and fraud), content-related offenses (child pornography),[230] and offenses related to infringements of copyright and related rights.[231] The Budapest Convention also provides certain definitions, such as: a) Computer system: "*...Any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data*"; b) Computer data: "*...Any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function*"; c) Service provider is: "*Any public or private entity that provides to users of its service the ability to communicate by means of a computer system; And any other entity that processes or stores computer data on behalf of such communication service or users of such service";* and d) Traffic data means: "*Any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service"*.[232]

The 2003. Protocol on 'criminalisation of acts of a racist and xenophobic nature committed through computer systems'[233] to Budapest Convention, called for states to criminalize dissemination of racist and xenophobic material through computer systems as

[225] Supra n. 217. Summer Walker and Ian Tennant, "Control, Alt or Delete? page 9.
[226] Supra n. 219. Budapest Convention, Chapter II Sections 1, 2, points 1, 3, 3, 4.
[227] Ibid, Supra n. 219. Budapest Convention,Chapter III
[228] Ibid,Chapter IV
[229] Ibid, Articles 2-6.
[230] Ibid, Art 7-9.
[231] Ibid, Article 10
[232]Ibid, See: Article 1 – Definitions, point a) to d).
[233] *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, CETS-No.189, (Strasbourg, 28.I.2003), available at: <https://rm.coe.int/168008160f>,accessed: 27. November 2022.

well as motivated threats or insults through computer systems.[234] Finally, in 2021, the Budapest parties adopted the additional protocol on electronic evidence,[235] which has already entered into force. Although the latter protocol includes data protection, its aim is not to create an international data protection instrument, but rather a practical criminal justice cooperation framework.[236] The provided direct cooperation between states and service providers in the territory of other states, should speed up the procedure of inquiries into cybercrime proceedings, and the fact that implies the application of the multi-stakeholder approach, should indicate strengthening the fight against cybercrimes.[237]

Meanwhile, when it comes to other regional efforts, the situation developed as follows:

- The Draft UNODC cybercrime study[238] recommended a new convention based on inputs from the intergovernmental expert group (EGM) meetings, but it was rejected by Western countries.[239]
- The African Union Convention on Cyber Security and Personal Data Protection,[240] was finally adopted in 2014, although many opposed it at the beginning, claiming it included vague provisions that could endanger privacy or limit the freedom of speech.[241] The AU Convention shares similar parameters to the Budapest Convention, and establishes similar content-related offenses.[242]

[234] Supra n. 217, Summer Walker and Ian Tennant, "Control, Alt or Delete? Page 8.

[235]*Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, CETS No. 224, (Strasbourg 12/05/2022), available at <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224>, accessed: 27. November 2022.

[236] Dominick Zachar, Battling Cybercrime Through the New Additional Protocol to the Budapest Convention <https://ccdcoe.org/library/publications/battling-cybercrime-through-the-new-additional-protocol-to-the-budapest-convention/>, accessed: 27. November 2022.

[237] Ibid.

[238]Steven Malby, Anika Holterhof and Robyn Mace, "United Nations Office on Drugs and Crime Comprehensive Study on Cybercrime Draft" (*www.unodc.org/documents*February 2013) <https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> accessed November 20, 2022

[239] Supra n. 217, Summer Walker and Ian Tennant, "Control, Alt or Delete? page 15

[240]The African Union Convention on Cyber Security and Personal Data Protection (2011/2014, 23rd Ordinary Session of Assembly, Malabo, Equatorial Guinea), (Hereinafter "AU Convention")<https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf>,accessed November 20, 2022

[241]See: --, "Mixed Feedback on the 'African Union Convention on Cyber Security and Personal Data Protection'" (*CCDCOE*) <https://ccdcoe.org/incyder-articles/mixed-feedback-on-the-african-union-convention-on-cyber-security-and-personal-data-protection/> accessed November 25, 2022.

[242] Supra n. 217, Summer Walker and Ian Tennant, "Control, Alt or Delete?" page 8.

- The League of Arab States' Arab Convention on Combating Information Technology Offences,[243] also provides for content-related offenses.[244]
- The Shanghai Agreement on Cooperation in Ensuring International Information Security[245] from 2009, includes cybercrime as a key risk to information security but is not considered solely a cybercrime treaty. The agreement does not list content-related offences or delineate cybercrimes, but it does list cybercrime alongside risks such as 'information terrorism' and 'use of a dominant position in the information space to the detriment of the interests and security of other States'. It defines cybercrime as 'using information resources and/or influencing them in the information space for illegal purposes'.[246]
- Russia also submitted a draft convention to the UN General Assembly, although at first facing no support for its proposal, with some slight progress later on.[247] It included provisions on child pornography, racial or ethnicity-based incitement and crimes against humanity, similar to what is included in the Budapest and AU treaties.[248] Under its extremism-related offenses (article 21), the draft treaty includes a 'Pandora's box' clause: "*Each State party shall adopt such legislative and other measures as are necessary to establish as an offense or other unlawful act under its domestic law distribution by means of ICT of materials that call for unlawful acts motivated by political, ideological, social, racial, ethnic, or religious hatred or enmity, advocacy and justification of such actions or the provision of access to them.*"[249]

On the other hand, unlike the polarized and fragmented efforts to create an international agreement, the European Union (EU) efforts seem to be progressing, at least in comparesance.

In 2016, the EU adopted the Directive On Security Of Network And Information Systems (NIS Directive).[250] Although Micro and small entities were excluded from the

[243] See: The Arab Convention on Combating Information Technology Offences, (League of Arab States Geeral Secretariat 21/12/2010, Cairo, the Arab Republic of Egypt), (Arab Convention), <https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf>

[244] Supra n. 217, Summer Walker and Ian Tennant, "Control, Alt or Delete?, page 8.

[245] See: The Shanghai Agreement on Cooperation in Ensuring International Information Security, (2008/9), (Hereinafter: Shanghai Convention), <https://ccdcoe.org/uploads/2018/10/SCO-090616-IISAgreement.pdf>

[246] Supra n. 217, page 8.

[247] Ibid. Supra n. 217, page 8.

[248] Ibid, page 8.

[249] Ibid, page 8.

[250] DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (hereinafter: NIS Directive), Official Journal of the European Union, 2016, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC>

scope, and that its implementation proved difficult and apparently resulted in fragmentation of the single market, leading to insufficient security levels,[251] it provided legal measures to strengthen the overall level of cybersecurity in the EU. Some of such measures are related to ensuring the preparedness of member states with appropriate equipping, setting up a support cooperation group and facilitate strategic cooperation and the information exchange, ensuring the cross-sectorial culture of security, undertaking of appropriate security measures from the side of businesses in the critical sectors, and of digital service providers,[252] and so on.

In 2019, the EU Cybersecurity Act was adopted,[253] granting a permanent mandate, and a key role in setting up and maintaining the European cybersecurity certification framework, to the EU cybersecurity Agency (ENISA).[254]

In November 2022, the European Parliament adopted the Directive on measures for a high common level of cybersecurity across the Union ("NIS2 Directive"),[255] supposed to repeal and replace the EU's existing cybersecurity NIS Directive.[256] The new NIS2 Directive expanded the scope of the NIS Directive by adding new sectors based on their criticality for the economy and society, and by introducing a clear size cap and including all medium and large companies in selected sectors, while leaving some flexibility for Member States to identify smaller entities with a high security risk profile.[257] The NIS2 Directive eliminated the previous distinction between operators of essential services and digital service providers, with entities now classified based on their importance, and divided in essential[258] and important[259] categories subjected to different supervisory regimes.[260] It also strengthened security requirements for companies, by imposing a risk management approach providing a minimum list of basic security elements that have to be

[251] Supra n. 9, The NIS2 Directive BRIEFING

[252] See: "The NIS 2 Directive", available at: <https://www.nis-2-directive.com>

[253] See: REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), (European Commission, Brussels, 13.9.2017), available at:<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0477&rid=3>

[254] Supra n. 9, The NIS2 Directive BRIEFING

[255] DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (hereinafter NIS2 Directive), (Adopted 10th November 2022.), available at: <https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF> and <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf>

[256] Supra n. 9.The NIS2 Directive BRIEFING

[257] Supra n. 245, "The NIS 2 Directive"

[258] Annex I: 'Essential sectors' covered by the new security provisions include: health, energy, transport, banking, digital infrastructure, public administration and space sectors.

[259] Annex II: 'Important sectors' include: entities manufacturing medical devices, postal services, waste management, food production and processing and digital providers.

[260] Supra n. 245, See: "The NIS 2 Directive".

applied.[261] Provisions are more precise when it comes to incident reporting, report contents and timelines.[262] It also requires individual companies to address cybersecurity risks in supply chains and supplier relationships, carrying out coordinated risk assessments of critical supply chains in cooperation with the Commission and ENISA, all while strengthening the supply chain cybersecurity for key information and communication technologies.[263] Additionally, more stringent supervisory measures for national authorities, as well as stricter enforcement requirements and aims at harmonizing sanctions regimes across Member States are introduced.[264] The role of the Cooperation Group in shaping strategic policy decisions on emerging technologies and new trends is also enhanced.[265] The information sharing and cooperation between Member States is increased, especially in regards to cyber crisis management.[266] Finally, the NIS2 established a basic framework with responsible key actors on coordinated vulnerability disclosure for newly discovered vulnerabilities across the EU and created an EU registry for it, to be operated by ENISA.[267]

Additionally, there is currently an ongoing initiative for a new EU Cyber Resilience Act (CRA),[268] which went through consultations in 2022. This CRA is supposed to complement the existing EU legislative framework, and encompass regulation on cybersecurity requirements for products with digital elements, to strengthen cybersecurity rules and ensure more secure hardware and software products, throughout their entire life cycle, all the way from designing and development stages.[269] The issues that it is supposed to address are the low level of cybersecurity, widespread vulnerabilities, and insufficient transparency and understanding and access to information by users.[270]

However, aside from the more formal approaches, undertaken at the regional and international levels, there have been other cross-sectorial initiatives and developments, falling more under the scope of non-binding, soft-law. Such efforts are related to the existing cybersecurity principle, promulgated by many standardization bodies, international organizations and even tech companies.[271] However, out of a wide diapazon

[261]Ibid. Supra n. 245
[262]Ibid.
[263]Ibid.
[264]Ibid.
[265]Ibid.
[266]Ibid.
[267]Ibid. Supra n. 245, "The NIS 2 Directive"
[268]The European Cyber Resilience Act, (September 2022), available at: <https://www.european-cyber-resilience-act.com/Cyber_Resilience_Act_Articles_(Proposal_15.9.2022).html>
[269]Cyber Resilience Act, (15 September 2022), available at: <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act>
[270]Ibid.
[271] AAT Team, Complete List of Cybersecurity Standards (Updated 2023), January 2023, AllSAboutTesting, <https://allabouttesting.org/complete-list-of-cyber-security-standards/>, accessed: February 2023.

of such emerging trends, two are most distinguished. The first effort is one of the International Organization for Standardization (ISO), which issued its Information security management systems standards (ISO/IEC 27001).[272] The ISO/IEC 27001 standards provide companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system. promotes a holistic approach to information security: vetting people, policies and technology.[273] An information security management system implemented according to this standard is a tool for risk management, cyber-resilience and operational excellence.[274] Ofcourse, aside from the aforementioned wellknown standards, ISO created many more privacy, cybersecurity and information security related guidance and standards, providing for a framework for companies to implement throughout the entirety of their IoT and related product lifecycle and supply chain, as much as for the management and security of internal and external organizational relations.[275]

Similarly to ISO Standards, a U.S. based Agency, National Information Security Agrency (NIST),[276] has created its own sets of cybersecurity, information security and privacy related standards, guidelines, best practices, and other resources,[277] which actually served as basis for many other similar frameworks.

In summary of the current developments in the field of cybersecurity, based on all initiatives and regulation listed, it can be said that:

- Cyber Law hasn't yet been internationally and officially acknowledged as a separate branch of law, rather it stays fragmented in numerous different branches of law, and the rules regulating cyber activities, protecting cyber infrastructure, as well as relevant subjects and objects from the variety of cyber threats, are scattered throughout the framework of both international and regional law. In other words, Cyber Law is still an emerging and developing legal framework, for which reason, bot direct and indirect sources of law should be duly considered, and the Cyber Triad should guide us towards all applicable frameworks, rules and areas of law.[278]

[272] See: International Organization for Standardization (ISO), *Information security management systems standards (ISO/IEC 27001,)* 2022, <https://www.iso.org/standard/27001>, January 2023.
[273] Ibid.
[274] Ibid
[275] See more at: ISO.org, search for: Cybersecurity, Standards, <https://www.iso.org/search.html?q=cybersecurity&hPP=10&idx=all_en&p=0&hFR%5Bcategory%5D%5B0%5D=standard> , accessed July 2023.
[276]See more at: Search I CSRC, csrc.nist.gov, <https://csrc.nist.gov/publications/sp800> , accessed: July 2023.
[277] See more at: NIST.gov, Cybersecurity, <https://www.nist.gov/cybersecurity>, and <https://www.nist.gov/system/files/documents/2022/07/21/Extended%20Cybersecurity%20Vitals%20Fact%20Sheet.pdf>, accessed: June, 2023.
[278] See more: Tamara Blagojevic, *Defining and Evaluating the concept of Cyber Justice,* AContrario International Criminal Law - Blog, (March 2023, AcontrarioICL.com), :<https://acontrarioicl.com/2023/03/28/defining-evaluating-and-utilizing-the-concept-of-cyber-justice/>, accessed: July 2023.

- Cybercrimes have in fact been regulated at the international level, but the international law still fails to gather and codify relevant primary cyber norms in one comprehensive document, due to the polarization and different views of various key state actors. Therefore, the development and progress of the emergence of a unified and harmonized international cyber security legal framework appears to be slow on the international level. Aside from criminalization, main efforts have been apparently made in the legal jurisprudence and through soft law approaches, by reaffirmation of the already existing rules, and confirming their applicability to cyberspace and outer space.
- EU law, on the other hand, fairly answers the needs of the fast developing IT sector for the time being, which is apparent based on frequent updates and adaptation of the framework. Moreover, the EU cybersecurity framework, unlike the international cyber rules, has a more direct approach towards cybersecurity, as it focuses mainly on preparedness, preventive measures, and primary norms. By doing so, this framework appears to be mirroring the needs of the IT sector, by acknowledging the technical measures and standards that are pertinent for creating a culture of cybersecurity throughout the entire life cycle of a business working with digital products. In other words, this regional framework, similar to the soft-law frameworks mentioned, is more geared towards tech and IoT companies, or companies selling digital products and services, or doing business in that area, in other ways. Finally, the EU Digital Strategy, not only allows more transparency regarding the current status of this framework, but also dictates the future plans and developments, implying more positive changes soon to come.
- When it comes to the outer space - cyberspace relation, their legal nexus, for the time being, stays within the scope of the frameworks provided by International Law, Space Law and the ITU Constitution and ITU RR. However, the adaptability of those frameworks to the current needs of the technology sector, having in mind how long it takes to revise such frameworks, and how long they haven't been revised, remains questionable. In such situations, usually the soft law approach can help patch up the possible gaps and ambiguities, but since the field of technology changes trends very fast, it remains to be seen whether this approach can be applied in this area.

6. **CONCLUSION**

Knowing the characteristics of the world we live in, and knowing they could adversely affect our "tomorrow", is a scary thought, by itself. Knowing the trend towards which we are leaning to as humanity, is not so comforting as well. The fear that we have, is what pushes us to fight it. The knowledge of facts is what gives us an opportunity to

overcome every difficulty. The awareness allows for activism. But we have to keep our eyes and minds open, and think outside the box. These general thoughts are applicable to the legal field as well. Therefore, if we strive to the skies, we should keep our eyes wide open.

Having in mind that the general trend in the cyber field is to constantly change and develop, and considering the fact that slow-paced legal discipline wasn't sufficient to tackle the difficulties encountered in the modern society, it is only logical to conclude that the natural order of things, the one that we are so used to, might just have to change.

A good example of a multi-disciplinary approach, mirroring the needs of the technology field, at least in comparesance and for the time being, is - the EU cybersecurity framework. Collaborative approaches, not just across areas of law or disciplines, but across different sectors and sciences, should be of great focus and utmost importance in the near future. Science and technology, as evidenced in this article, as well as human nature, won't wait for the law to tell them what to do. Therefore, law, in general, has to be more subtle, precautious, and "soft". Gently overshadowing the developments of technology should start at the beginning of its life cycle, before it's on the market and put to use. In such endeavors, all the stakeholders should be included, and mostly, the ones that truly count - the IT private companies and businesses working with digital products.

The Soft Law approaches, such as standards, principles, manuals and guides, enshrining the soul of the "future law", are generally easier to accept, even by the riskiest of investors and innovation driven individuals. We should maybe start from there, and allow for an easier development or adaptation of the legal framework, to the future's ever-changing world.

This is how 'legal' has to consider the 'economic' segment, which has to consider the 'engineering, technical and technological segment', and which multidisciplinary back-and-forth relation should be the natural order of things when two spectrums collide and are interdependent, like the space and cybersecurity sectors are. Otherwise, the risk of world-effecting, wide cyber attacks can turn into an every-day reality.

7. BIBLIOGRAPHY

- --, "German ROSAT Spacecraft Re-Entered over Bay of Bengal" (*BBC News*October 26, 2011) <https://www.bbc.com/news/science-environment-15466361>

- --, "Mixed Feedback on the 'African Union Convention on Cyber Security and Personal Data Protection'" (*CCDCOE*) <https://ccdcoe.org/incyder-articles/mixed-feedback-on-the-african-union-convention-on-cyber-security-and-personal-data-protection/>
- AAT Team, Complete List of Cybersecurity Standards (Updated 2023), January 2023, AllSAboutTesting, <https://allabouttesting.org/complete-list-of-cyber-security-standards/>
- Adam Rawnsley, *Iranian Hacking Group Targeted Satellite Industry Nerds*, (TheDailyBeast, Oct. 22, 2019), <https://www.thedailybeast.com/iranian-hacking-group-targeted-us-satellite-companies>
- Andreev A, "What's Going on with Cybersecurity in Space" (*Daily English Global blogkasperskycom*, February 3, 2022) <https://www.kaspersky.com/blog/cybersecurity-in-outer-space/43531/>
- Andreas Illmer, "Iran Censorship" (*dw.com*March 22, 2010), <https://www.dw.com/en/eu-slams-irans-jamming-of-satellite-signals-as-unacceptable/a-5377813>
- Blagojevic, T.*"A brave new world: In-space AI and space-related AI and its soon-to-be fitting legal robe"*, Bulletin No11, Observatorio Juridico Aerospatial, AEDAE, June 2023.
- Blagojevic T., *Defining and Evaluating the concept of Cyber Justice,* AContrario International Criminal Law - Blog, (March 2023, AcontrarioICL.com), :<https://acontrarioicl.com/2023/03/28/defining-evaluating-and-utilizing-the-concept-of-cyber-justice/>
- Brandon Bailey, Ryan J. Speelman and Prachant A. Doshi, "Defending Space Craft in the Cyber Domain" (*Home | The Aerospace Corporation*, November 2019) <https://aerospace.org/sites/default/files/2019-11/Bailey_DefendingSpacecraft_11052019.pdf>
- Chuck Brooks, "The Urgency to Cyber-Secure Space Assets" (*Forbes,* February 28, 2022) <https://www.forbes.com/sites/chuckbrooks/2022/02/27/the-urgency-to-cyber-secure-space-assets/?sh=45a439fc51b1>
- Catherine Wilson, "15-Year-Old Admits Hacking NASA Computers" (*ABC News*) <https://abcnews.go.com/Technology/story?id=119423&page=1#:~:text=M%20I%20A%20M%20I%2C%20Sept.,cruise%20around%20like%20an%20employee>
- CNBC, "China-Based Hacking Campaign Is Said to Have Breached Satellite, Defense Companies" (*CNBC*, June 20, 2018) <https://www.cnbc.com/2018/06/19/china-based-hacking-breached-satellite-defense-companies-symantec.html> - Cocco M, "Data Policy, Regulatory Framework, and Cybersecurity"
- Di Freeze, "Cybercrime Damages $6 Trillion by 2021" (*Cybercrime Magazine*, November 9, 2020) <https://cybersecurityventures.com/annual-cybercrime-report-2017/#:~:text=Cybersecurity%20Ventures%20predicts%20cybercrime%20damages,in%20size%2C%20sophistication%20and%20cost.>
- "Digital around the World - Datareportal – Global Digital Insights" (*DataReportal*) <https://datareportal.com/global-digital-overview>

- Doyle Rice, "China Hacks into U.S. Weather Satellite Network" (*USA Today,* November 13, 2014) <https://www.usatoday.com/story/weather/2014/11/12/china-weather-satellite-attack/18915137/>
- Duncan Hollis D, "A Brief Primer on International Law and Cyberspace" (*Carnegie Endowment for International Peace,* June 14, 2021) <https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763>
- Eric Mack, "US Military Says SpaceX Handily Fought off Russian Starlink Jamming Attempts" (*CNET,* April 22, 2022) <https://www.cnet.com/science/space/us-military-says-spacex-handily-fought-off-russian-starlink-jamming-attempts/>
- Erwin S, "Cyber Warfare Gets Real for Satellite Operators" (*SpaceNews*March 21, 2022) <https://spacenews.com/cyber-warfare-gets-real-for-satellite-operators/>
- General Assembly of the United Nations , "Convention on the Prevention and Punishment of the Crime of Genocide - No. 1021 "(*treaties.un.org*December 9, 1948) <https://treaties.un.org/doc/Publication/UNTS/Volume%2078/volume-78-I-1021-English.pdf>
- General Assembly of the United Nations, "International Covenant on Civil and Political Rights, and the Optional Protocol to the above-Mentioned Covenant" (*treaties.un.org,* December 19, 1966) <https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf>
- Gregory Falco, *Job for One Space Force: Space Asset Cyber Security,* <https://www.gregoryfalco.com/_files/ugd/e741d3_b8f6b65b8f4046a785066c9e0bf8c1ad.pdf >
- Gregory Falco G, "Opinion | Our Satellites Are Prime Targets for a Cyberattack. and Things Could Get Worse." (*The Washington Post,* May 7, 2019) <https://www.washingtonpost.com/opinions/our-satellites-are-prime-targets-for-a-cyberattack-and-things-could-get-worse/2019/05/07/31c85438-7041-11e9-8be0-ca575670e91c_story.html> accessed November 27, 2022
- Harding L, "Russia Denies Disrupting GPS Signals during NATO Arctic Exercises" (*The Guardian,* November 12, 2018) <https://www.theguardian.com/world/2018/nov/12/russia-denies-blame-for-arctic-gps-interference>
- Hughes S and Rawnsley A, "Iranian Hacking Group Targeted Satellite Industry Nerds" (*The Daily Beast*October 22, 2019) <https://www.thedailybeast.com/iranian-hacking-group-targeted-us-satellite-companies?ref=scroll>
- International Organization for Standardization (ISO), *Information security management systems standards (ISO/IEC 27001,)* 2022, <https://www.iso.org/standard/27001>
- ISO.org, search for: Cybersecurity, Standards, <https://www.iso.org/search.html?q=cybersecurity&hPP=10&idx=all_en&p=0&hFR%5Bcategory%5D%5B0%5D=standard>

- ITU, "Regulation of Satellite Systems" (*ITU.int*) <https://www.itu.int/en/mediacentre/backgrounders/Pages/Regulation-of-Satellite-Systems.aspx>
- Jeff Foust, "SpaceX Shifts Resources to Cybersecurity to Address Starlink Jamming" (*SpaceNews*March 5, 2022) <https://spacenews.com/spacex-shifts-resources-to-cybersecurity-to-address-starlink-jamming/>
- Jsamuel (Staff Writer), "NASA Computers Hacked by Intruders - via Satellite -" (*Via Satellite*, August 21, 2013) <https://www.satellitetoday.com/government-military/2008/12/01/nasa-computers-hacked-by-intruders/>
- Juliana Suess, "Jamming and Cyber Attacks: How Space Is Being Targeted in Ukraine" (*Royal United Services Institute*April 5, 2022) <https://www.rusi.org/explore-our-research/publications/commentary/jamming-and-cyber-attacks-how-space-being-targeted-ukraine>
- KATRIN NYMAN METCALF, "A Legal View on Outer Space and Cyberspace: Similarities and Differences" (*CCDCOE*2018) <https://ccdcoe.org/uploads/2018/10/Tallinn-Paper_10_2018.pdf>
King M and Goguichvili S, "Cybersecurity Threats in Space: A Roadmap for Future Policy" (*Wilson Center*October 8, 2020) <https://www.wilsoncenter.org/blog-post/cybersecurity-threats-space-roadmap-future-policy>

- Lesley Conn, "Global Space Economy Nears $447B" (*The Space Report*July 23, 2021) <https://www.thespacereport.org/uncategorized/global-space-economy-nears-447b/>
- Michael N. Schmitt, "International Cyber Security Law - States and Cyber Space," *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2017)
- Microsoft, "Protecting People in Cyberspace - The Vital Role of the United Nations in 2020 "(*United Nations*) <https://www.un.org/disarmament/wp-content/uploads/2019/12/protecting-people-in-cyberspace-december-2019.pdf>
- Ms. Ruvimbo Samanga, "NewSpace" (*IISL Space Law Knowledge Constellation*July 2021) <https://constellation.iislweb.space/ruvimbo-samanga-newspace/>
- Nayef Al-Rodhan, "Cyber Security and Space Security" (*The Space Review: Cyber security and space security*May 26, 2020) <https://www.thespacereview.com/article/3950/1>
- NIST.gov, Cybersecurity, <https://www.nist.gov/cybersecurity>, and <https://www.nist.gov/system/files/documents/2022/07/21/Extended%20Cybersecurity%20Vitals%20Fact%20Sheet.pdf>,
- NIST, Search I CSRC, csrc.nist.gov, <https://csrc.nist.gov/publications/sp800>
- "NSR Global Space Economy, 2nd Edition" (*NSR*October 19, 2022) <https://www.nsr.com/?research=nsr-global-space-economy-2nd-edition>

- Peeters W, "Cyberattacks on Satellites" (*London School of Economics and Political Science*2022) <https://www.lse.ac.uk/ideas/projects/space-policy/publications/Cyberattacks-on-Satellites>
- Rajeswari Pillai Rajagopalan, "Electronic and Cyber Warfare in Outer Space "(*UNIDIR*May 2019) <https://www.unidir.org/publications>
- Rajeswari Pillari Rajagopalan R, "Changing Space Security Dynamics and Governance Debates" in Melissa de Zwart, Stacey Henderson (ed), *Commercial and Military Uses of Outer Space* (Springer 2021)
- Ram S. Jakhu and Steven Freeland (eds), "McGill MANUAL on International Law Applicable to Military Uses of Outer Space" (*https://www.mcgill.ca*July 12, 2022) <https://www.mcgill.ca/iasl/files/iasl/mcgill_manual_volume_i_-_rules.pdf> accessed
- Rebecca Heilweil, "For Hackers, Space Is the Final Frontier" (*Vox*July 29, 2021) <https://www.vox.com/recode/22598437/spacex-hackers-cyberattack-space-force>
- Satellite Industry Association, "Cybersecurity – Satellite Industry Association, Washington, D.C." (*Satellite Industry Association*February 17, 2020) <https://sia.org/policy/cybersecurity/>
- Schmitt M and Vihul L, "Chapter 2 the Nature of International Law Cyber Norms" (2016) <https://195.222.11.251/uploads/2018/10/InternationalCyberNorms_Ch2.pdf>
- SpaceNews Staff, "Intelsat Vows to Stop Piracy by Sri Lanka Separatist Group" (*SpaceNews*December 6, 2014) <https://spacenews.com/intelsat-vows-stop-piracy-sri-lanka-separatist-group/> accessed November 19, 2022
- Starks T and Schaffer A, "Analysis | Cyberattacks on Satellites May Only Be Getting More Worrisome" (*The Washington Post*July 29, 2022) <https://www.washingtonpost.com/politics/2022/07/29/cyberattacks-satellites-may-only-be-getting-more-worrisome/>
- "Strengthening Cybersecurity of SATCOM Network Providers and Customers - Alert (AA22-076A)" (*CISA*March 2022) <https://www.cisa.gov/uscert/ncas/alerts/aa22-076a>
- Sakshi Tiwari, "China 'Decodes' an Orbiting US Satellite; Claims Expertise in Automatically Detecting & Fixing Security Flaws in Outer Space" (*Latest Asian, Middle-East, EurAsian, Indian News,* April 10, 2022) <https://eurasiantimes.com/china-decodes-an-orbiting-us-satellite-claims-expertise-in-automatically-detecting-fixing-security-flaws-in-outer-space/>
- "Space Cyber Defense: An Adaptive, Proactive Approach" (*Booz Allen*) <https://www.boozallen.com/markets/space/space-cyber-defense-an-adaptive-proactive-approach.html>
- "Space Threat 2018: Iran Assessment" (*Aerospace Security*June 22, 2022) <https://aerospace.csis.org/space-threat-2018-iran/>
- Steven Malby, Anika Holterhof and Robyn Mace, "United Nations Office on Drugs and Crime Comprehensive Study on Cybercrime Draft" (*www.unodc.org/documents*February

2013) <https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>

- Summer Walker and Ian Tennant, "Control, Alt or Delete? - The UN Cybercrime Debate Enters a New Phase" (*globalinitiative*December 2021) <https://globalinitiative.net/wp-content/uploads/2021/12/UN-Cybercrime-PB-22Dec-web.pdf>
- Tereza Pultarova and Elizabeth Howell, "Starlink Satellites: Everything You Need to Know about the Controversial Internet Megaconstellation" (*Space.com,* April 14, 2022) <https://www.space.com/spacex-starlink-satellites.html>
- "The Three-Pillar Approach to Cyber Security: Data and Information Protection" (*DNV*) <https://www.dnv.com/article/the-three-pillar-approach-to-cyber-security-data-and-information-protection-165683#:~:text=The%20third%20pillar%20is%20data%20and%20information%20protection&text=The%20first%20two%20pillars%20are,tangible%20of%20the%20three%20pillars.>
- Tim Starks and Aaron Schaffer, "Analysis | Cyberattacks on Satellites May Only Be Getting More Worrisome" (*The Washington Post,* July 29, 2022) <https://www.washingtonpost.com/politics/2022/07/29/cyberattacks-satellites-may-only-be-getting-more-worrisome/>
- U.S. Department of Justice Office of Public Affairs, "State-Sponsored Iranian Hackers Indicted for Computer Intrusions at U.S. Satellite Companies" (*The United States Department of Justice,* July 13, 2022) <https://www.justice.gov/opa/pr/state-sponsored-iranian-hackers-indicted-computer-intrusions-us-satellite-companies>
- U.S. Department of Justice Office of Public Affairs, "U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage" (*The United States Department of Justice*November 27, 2017) <https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations>
- United Nations General Assembly Human Rights Council, "Resolution Adopted by the Human Rights Council A/HRC/RES/32/13" (*UN.org*July 18, 2016)
- *UNITED STATES OF AMERICA v WUYINGZHUO, Dong Hao, Xia Lei* (2017) Indictment 16 (https://wwwjusticegov/opa/press-release/file/1013866/download)
- "UNOOSA Space Objects Index" <https://www.unoosa.org/oosa/osoindex/search-ng.jspx?lf_id=>
- "Why Space Cyber?" (*Center for Space Cyber Strategy and CyberSecurity - University at Buffalo,* March 4, 2021) <https://www.buffalo.edu/space-cybersecurity/center/why-space-cyber.html>
- "Why We Need Increased Cybersecurity for Space-Based Services" (*World Economic Forum*May 25, 2022) <https://www.weforum.org/agenda/2022/05/increased-cybersecurity-for-space-based-services/>

- "World Population to Reach 8 Billion on 15 November 2022" (*United Nations*) <https://www.un.org/en/desa/world-population-reach-8-billion-15-november-2022>
- *United States OF AMERICA V SAID POURKARIM ARABI, MOHAMMAD REZA ESPARGHAM, MOHAMMAD BAYati* (2020) Indictment 22 (https://wwwjusticegov/opa/press-release/file/1317521/download)
- Wolf, Jim "China Key Suspect in U.S. Satellite Hacks: Commission" (*Reuters*October 28, 2011) <https://www.reuters.com/article/us-china-usa-satellite-idUSTRE79R4O320111028>
- Wenzel Michalski, "Sri Lanka: High Ranking Officials Involved in War Crimes" (*Human Rights Watch*February 26, 2021) <https://www.hrw.org/news/2021/02/26/sri-lanka-high-ranking-officials-involved-war-crimes>