https://doi.org/10.18778/8331-719-9.06

Low Orbit Blues: The Noir in Cybersecurity

Roy Balleste[1]

You are one thousand miles above the surface of Delmak-O...
— Philip K. Dick[2]

A Prelude to Exploration

Human life is valuable. Whether short or long, it leaves an imprint on humanity's story. The implications of entering the vastness of space and the fabric of time stir profound reflections on existence and the essence of survival. The outcome of space exploration and long-duration missions underscores the notion that traveling through space and time could grant astronauts an expansive panorama of the cosmos, compelling them to grapple with the realization that confronting the future is far more complex than it initially appears. The challenge ahead reminds humanity of valuable lives against the rising horizon of technology expanding from our cislunar space into interstellar space. The future compels legal experts to consider the meaning of space exploration. This exploration means embarking on a journey that, in essence, shifts one's place within the continuum of time.[3] Entering the great expense of outer space focuses our immediate attention on the Low Earth Orbit (LEO). The LEO orbit encompasses Earth-centered orbits with an altitude of 1,200 miles (2,000 km) or less.[4] This orbit is considered near enough to Earth for convenient

1 Stetson University College of Law, Gulfport, Florida, United States.
2 P.K. Dick, *A Maze of Death,* First Mariner Books edition 2013, New York 1970, p. 22.
3 W. Grey, Troubles with Time Travel, *Philosophy,* 1999, 74(287), p. 57.
4 A. Bowman, *Commercial Space Frequently Asked Questions*, NASA, 7 April 2024. Available at: https://www.nasa.gov/humans-in-space/leo-economy-frequently-asked-questions/#:~:text=What%20is%20the%20LEO%20Economy,services%20this%20region%20of%20space (accessed: 31/12/2024).

transportation, communication, observation, and resupply. It also is the area where the International Space Station currently orbits and where many proposed future platforms will be located.[5] A more precise measure of this orbit involves examining the range of elevations beneath which satellites are unable to sustain their trajectory (80–100 km) and the altitude beyond which the level of the entrapped radiation belts complicates satellite operations (up to approximately 2,000 km).[6] The LEO space is a symbol of present and future economic growth, where national interests in research evolve in parallel with plans of deep space exploration led by the Artemis program.[7]

This fascinating orbital space is not without challenges. A sort of low orbit blues menaces the future success of commerce and peaceful use of outer space. The International Telecommunication Union (ITU) noted in 2021 that about 2.9 billion people around the world lack access to the Internet.[8] This scenario offers the private sector commercial opportunities to work on the construction of small satellite constellations to provide Internet access from LEO.[9] One great advantage of this LEO orbit is its close proximity to the Earth's surface, with almost no delay in data transmission.[10] While this is a sign of hope and human development, additional geopolitical factors foreshadow this expected progress. Objects in Low Earth Orbit have become integrated into the vast web of the internet, resulting in an expanded attack surface for potential hackers.[11] The hack or destruction of LEO satellites could represent a disruption of a vital communication network, foreshadowing unexpected legal dilemmas. This is profoundly important in various situations, from regular Internet users relying on LEO data to astronauts exploring deep space, where the availability of services is vital for commerce or even survival.

LEO satellites serve as vital conduits, facilitating data transmission from earth-based stations to spacecraft, venturing into the vastness of deep space. The effect arises from a vast array of antennas strategically positioned across the globe, spanning all seven continents, complemented by satellites orbiting in space, which collectively facilitate the transmission of radio waves.[12] "Astronauts and mission

5 *Ibidem*.

6 J.C. McDowell, The Low Earth Orbit Satellite Population and Impacts of the SpaceX Starlink Constellation, *The Astrophysical Journal Letters*, 2020, 892(2), p. 1.

7 A. Guzman, *What is the Commercial Low Earth Orbit Economy?*, NASA, 26 July 2023. Available at: https://www.nasa.gov/humans-in-space/commercial-space/what-is-the-commercial-low-earth-orbit-economy/ (accessed: 31/12/2024).

8 Ch. Suwijak, S. Li, Global Internet Access from the Low Earth Orbit: Legal Issues regarding Cybersecurity in Outer Space, *Journal of East Asia and International Law*, 2022, 15(1), p. 93.

9 *Ibidem*.

10 *Ibidem*.

11 M. Holmes, 10 Defining Moments in Cybersecurity and Satellite in 2023, *Via Satellite*, 22 January 2024. Available at: https://interactive.satellitetoday.com/via/january-february-2024/10-defining-moments-in-cybersecurity-and-satellite-in-2023 (accessed: 31/12/2024).

12 *How Do We Communicate with Spacecraft? We Asked a NASA Technologist: Episode 37*, NASA. Available at: https://www.nasa.gov/general/how-do-we-communicate-with-spacecraft-we-asked-a-nasa-technologist-episode-37/ (accessed: 31/12/2024).

controllers rely on this network to transmit messages and commands."[13] Spacecraft in orbit can communicate directly with ground stations on Earth only when they possess an unobstructed view of ground stations, an occurrence that is generally brief.[14] The feasibility of this endeavor is attributed to the existence of "tracking and data relay satellites," commonly referred to as TDRS.[15] "These satellites relay data from spacecraft to ground stations, allowing NASA to provide near-continuous global communications coverage to missions in low-Earth orbit."[16] The TDRS is an essential conduit for transmitting information, facilitating space-based research and exploration from its vantage point in geosynchronous orbit around our planet.[17] The satellite constellation guarantees an almost unbroken global communications network encompassing more than thirty-five LEO-orbiting spacecraft.[18] This useful technology may also have additional applications.

Consider, for example, a scenario of fourteen colonists traveling on their way to a habitable exoplanet. Philip K. Dick relates the story of fourteen colonists who travel to the planet *Delmak-O*.[19] Each of them is brought there with the promise of a new beginning.[20] Upon arrival, they attempt communication via satellite, however, the communication system fails, leaving the colonists without contact and unable to leave the planet.[21] Eventually, the situation spirals into chaos as more time passes.[22] These are the events depicted in Philip K. Dick's novel, *A Maze of Death*. While the exact condition of space explorers in the vastness of deep space will be revealed as time unfolds, the more significant challenge lies in the nature of human existence. These are some of the factors explored by the novel. Notions of space exploration will highlight the next fifty years when nations will increase their presence in space and endeavor to safeguard their infrastructure. This will require grappling with the legal complexities stemming from inherent cyber vulnerabilities associated with space exploration. In the same spirit, the use of outer space encompasses cyberspace with all its activities. The future of humanity and its expansion to off-world colonies are the inspiration that Philip K. Dick shares in his most famous novel, *Do Androids Dream of Electric Sheep?*[23] Most popularly known

13 *Ibidem*.
14 *Ibidem*.
15 *Ibidem*.
16 *Ibidem*.
17 *Tracking and Tada Relay Satellite (TDRS): Continuing the Critical Lifeline*, Goddard Space Flight Center, NASA. Available at: https://www.nasa.gov/wp-content/uploads/2022/04/tdrsfact-sheet_3.pdf (accessed: 31/12/2024).
18 *Ibidem*.
19 P.K. Dick, *op. cit.*
20 *Ibidem*, pp. 9–21.
21 *Ibidem*, pp. 48–59.
22 *Ibidem*.
23 D.E. Williams, Ideology as Dystopia: An Interpretation of 'Blade Runner', *Revue Internationale de Science Politique*, 1988, 9(4), p. 384 ["Ridley Scott's Blade Runner became first a 'cult' film, and then a national institution: it is one of only fifty films to be deposited in the Library

as the novel behind the motion picture *Blade Runner*, the visionary work is considered one of cinemas' most fascinating noir sci-fi stories.[24] Both, the book and the motion picture are concerned with the essence of humanity.[25] As humans enter the next space age, notions of technology may threaten or improve humanity's ability to develop a new age of discovery in outer space.

Matters of Law and Orbits

Planet Earth is in a galaxy like no other. From a distance, it may look like many others. The closest world with intelligent life—if any—is unknown. In between, there are millions of planets and thousands of potential exoplanets spreading across the galaxy. But life may be rare, for planets harboring life may be unique and hard to find in the universe. Yet, our existence's noble purpose is to explore new worlds. Occasionally, it is appropriate to take a moment to reflect on the past, if only to recognize the distance traveled and to contemplate the future. In the vast expanse of outer space, the concept of borders fades into irrelevance. Yet, as the legal field considers the LEO orbit, challenges surface to cast shadows over long-held notions, igniting uncertainties within the fabric of current realities. Simply said, technology is continuously developing. This is the technical progression of low-earth orbit communications. In terrestrial endeavors, those who venture into the cosmos will rely upon an intricate web of communication systems, including LEO satellites. For example, Starlink and Project Kuiper are deploying networks of LEO satellites to provide global connectivity to the Internet, especially to underserved or remote areas.[26] LEO satellites provide rapid, reliable communication, offering an ideal alternative for broadband Internet and cellular services.[27] These satellites present a pragmatic solution. Their orbit is ideally suited for the nascent phases of space exploration, the rigorous testing of satellites, and the essential training of astronauts.[28] The International Space Station (ISS) provides another LEO example by enabling sustained

---

of Congress, Washington DC, on the basis of its contribution to film culture"]. *See also* N. Wheale, Recognizing a 'Human-Thing': Cyborgs, Robots and Replicants in Philip K. Dick's 'Do Androids Dream of Electric Sheep?' and Ridley Scott's 'Blade Runner,' *Critical Survey*, 1991, 3(3), pp. 297–304.

24 B. Sherlock, Blade Runner: 10 Tropes Of Film Noir (& How It Puts A Sci-Fi Twist On Them), *Screenrant*, 22 August 2020. Available at: https://screenrant.com/blade-runner-film-noir-tropes-sci-fi-twist/ (accessed: 31/12/2024).

25 *Ibidem*.

26 L. Press, Amazon Project Kuiper vs SpaceX Starlink, *CircleID*, 19 January 2024. Available at: https://circleid.com/posts/20240119-amazon-project-kuiper-vs-spacex-starlink (accessed: 31/12/2024).

27 How will LEO satellites change wireless business models?, *Real Wireless*, 21 August 2024. Available at: https://real-wireless.com/how-will-leo-satellites-change-wireless-business-models/ (accessed: 31/12/2024).

28 A. Bowman, *op. cit*.

human presence in space and advancing technologies that may serve explorers in the vastness of deep space.[29] In this context, the legal inquiry necessitates clarifying the threats of failed communications relays that connect LEO satellites. Addressing this inescapable cyber threat necessitates the realization that an analysis of cybersecurity law and policy incorporates the consideration of cyberspace prioritized.

The evaluation of the present challenge must include the possibility of an external malicious actor disrupting satellite systems. Professor Carl Christol, an esteemed authority on space law, emphasized the imperative for a renewed dedication to the rule of law in global matters aimed at fulfilling the aspirations of humanity.[30] He seemed concerned with the rule of law significantly shaped by a progressive and pertinent legal framework governing the space environment and its natural resources, which aimed at fulfilling humanity's aspirations.[31] Accordingly, to effectively tackle illicit activities threatening LEO satellites, stakeholders must recognize that human endeavors shape cybersecurity in outer space. As the threat environment expands to include interconnected domains, stakeholders should be prepared to deal with increased vulnerabilities. Christol further noted that evolving an international legal framework governing outer space will undoubtedly enhance the thrill of uncovering an innovative model of human experiences and interactions.[32] The challenge here involves individuals acting alone or directed by rogue nations to interfere with space missions through cyber means. This state of affairs, grounded in reality, resides within a partial legal void. As legal experts search for the rule of law, there is a point of departure. Article I, paragraph 2 of the Outer Space Treaty, notes that:

> Outer space, including the Moon and other celestial bodies, shall be free for exploration and use by all States, without discrimination of any kind, on a basis of equality and in accordance with international law, and there shall be free access to all areas of celestial bodies.[33]

The spirit of the Outer Space Treaty must be contrasted with the realities of rising global conflicts. Satellite technology exists for use in space, where their military capability may be exploited for reconnaissance, guiding weapons, and supporting other warfare activities on the surface of the Earth.[34] The nature of the utilization of

29 *Ibidem*.

30 C.Q. Christol, *Space Law: Past, Present, and Future*, Kluwer Law and Taxation Publishers, Deventer 1991, p. 495.

31 *Ibidem*.

32 *Ibidem*.

33 United Nations, *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, 27 January 1967, 610 UNTS 205, article II (entered into force 10 October 1967) [Outer Space Treaty].

34 R. Hagen, J. Scheffran, *International Space Law and Space Security. Expectations and Criteria for a Sustainable and Peaceful Use of Outer Space*, [in:] M. Benkö, K.-U. Schrogl (eds.), *Current Problems and Perspectives for Future Regulation*, Eleven International Publishing, AJ, Utrecht: The Netherlands 2005, p. 273.

space is tied directly to the activities of States, as Michel Bourély, former legal adviser to the European Space Agency, observed how space activities have emerged within the domain of nations, whether exclusively, as noted in certain cases, or in a more limited fashion, as seen in others.[35] Without a doubt, States have kept the primary control over those space activities that belong to the military.[36] But then again, military activities are linked to State sovereignty and, thus, the defense of the nation.[37] Along this line of reasoning, the rapid expansion of space-based systems to support military operations among the major powers has been observed. These activities have translated into real events, with "significant resources now devoted by each of them to the development of ever-more effective (and potent) space-related weaponry."[38] Sadly, the "prospect of a celestial war can no longer be regarded as mere fantasy."[39] In light of the legally ambiguous cyber threat landscape and the quest for meaning in a hostile environment, the noir in cybersecurity demands new guidance to delineate the future rule of law.

If humanity is to expand its exploration of the solar system and travel more frequently, its technology must be dependable. Yet, the concept of a nation engaging in cyber operations to disrupt the space infrastructure of another nation is more concerning, mainly if the nation permits the use of its territory for such operations.[40] The intersection of the cyber and space domains challenges all principles of space law and even all notions of international law. Michel Bourély also observed that operations conducted in outer space have a moral aspect that necessitates the rapid development of legal frameworks.[41] In the same vein, Bourély would agree that cyber activities in space are linked to state sovereignty. In other words, exploring outer space generally rests with responsible States.[42] While this concept is usually understood, it takes on a new meaning when cyberspace enters the analysis. Modern plans for the Moon and Mars should involve a forward-thinking approach, focusing on informed decision-making and risk reduction. The space industry should strive to be proactive rather than reactive to ensure a successful transition. And these proactive measures pose an intriguing question. Considering the challenge, it is essential to approach the analysis in a way that broadens the perspective of strategic threat intelligence for space activities. This approach should involve applying strategic thinking to the various factors in developing the LEO

35 M. Bourély, The Institutional Framework of Space Activities in Outer Space, *Journal of Space Law*, 1998, 26(1), p. 1.

36 *Ibidem*.

37 *Ibidem*, at 5.

38 J. Maogoto, S. Freeland, The Final Frontier: The Laws of Armed Conflict and Space Warfare, *Conn J Int'l L*, 2007, 23:1, p. 165.

39 *Ibidem*, p. 169.

40 D.E. Sanger, K. Conger, *Russia Was Behind Cyberattack in Run-Up to Ukraine War, Investigation Finds*, The New York Times, 10 May 2022. Available at: https://www.nytimes.com/2022/05/10/us/politics/russia-cyberattack-ukraine-war.html (accessed: 31/12/2024).

41 M. Bourély, *op. cit.*, p. 5.

42 *Ibidem*.

orbit. In the space industry, the process of intelligence gathering and understanding may begin with strategic threat intelligence. Thus, strategic threat intelligence is high-level knowledge of the global danger environment and an organization's role.[43] Strategic threat intelligence informs CEOs and other executives about cyber threats.[44] The research suggests that as traditional armed conflict becomes more risky and costly, cyberattacks are becoming increasingly attractive in the space between peace and full-scale war.[45] In this context, cyber operations emerge as an additional information security concern that can potentially extend to the far frontiers of space exploration.[46] These cyber operations have a specific goal, but their unpredictability can be intensified by additional disruptions that affect targets beyond the initial objective.[47]

While the space industry seeks solutions to new problems, Judge Manfred Lachs' advice acts as a guidepost.[48] It is thrilling to think of the other planets that await discovery and exploration. On such planets, colonists will arrive in one-way rockets, as in the case of *Delmak-O*, to participate in mystifying colonization programs.[49] Madred Lachs, former judge and president of the International Court of Justice, said that modern science's greatest feats are but a small part of a far larger epic.[50] In the same way, this approach could be considered the search for a strategic threat intelligence that seeks to avoid misjudging the threat actors and aims to discover informed business decisions.[51] Strategic threat intelligence may help LEO operations reduce cyber risks and better use existing data, which should lead to the development of laws that will manage the intricacies of the space domain. As the twenty-first century draws to a close, the LEO orbit may be poised to become increasingly congested with an array of satellites, space stations, and privately operated installations. The orbital lanes could stand on the precipice of chaos, where antiquated treaties provide inadequate protection against the encroaching influence of corporations, hackers, and rogue nations. The aspirations for peaceful exploration of the cosmos stand in stark contrast to the looming specter of armaments in the vastness of space. As the quest for power in the cosmos intensifies, nations engage in fierce competition to engineer anti-satellite weapons (ASATs)

43 IBM, What is threat intelligence? Available at: https://www.ibm.com/topics/threat-intelligence (accessed: 31/12/2024).

44 *Ibidem*.

45 J. Collier, Proxy Actors in the Cyber Domain: Implications for State Strategy, *St Antony's International Review*, 2017, 13(1), pp. 25–47.

46 D. E. Sanger, K. Conger, *op. cit.*

47 *Ibidem*.

48 M. Lachs, Thoughts on Science, Technology and World Law, *The American Journal of International Law*, 1992, 86(4), pp. 673–699.

49 P. K. Dick, *op. cit.*, p. 1.

50 M. Lachs, *op. cit.*, 45 at p. 677.

51 K. Barker, What is Cyber Threat Intelligence?, *CrowdStrike*, 23 March 2023. Available at: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/ (accessed: 31/12/2024).

designed to destroy orbiting satellites.[52] A distinct arena of anti-satellite technology that has recently garnered attention is the non-kinetic variant. Cyberattacks exemplify a remarkable form of non-kinetic anti-satellite strategies, harboring the capacity to cause significant damage to satellites.[53] A confrontation in space may very well extend beyond the confines of the LEO orbit. The existence of humanity, much like in any other sphere of endeavor, would find itself in peril. As time passes, it becomes increasingly apparent that an environment of rising tensions prevails.

One central consideration is the use of law as a tool for achieving a global order of human dignity, including the many aspects that this endeavor entails. Space industry stakeholders must search for legal norms that will offer certainty and promote the security of future space missions. The search for legal and technical standards does not respond to preordained theories or beliefs, instead, it is the response to tangible dynamics of cyber operations, their relations with governments, and their relevance to national security. The integration of cyberspace in the enhancement of space endeavors ought to be steered by the values of the Outer Space Treaty and the foundational tenets of relevant space law. Article I (2) of the Outer Space Treaty highlights the free exploration and use of outer space without discrimination of any kind.[54] While the expectation is that the use and exploration of outer space will be peaceful, the stakeholders must also acknowledge the rising threats and emerging attacks. The problem with assessing LEO orbit endeavors from the lens of space law, or even cyber law, is that it assumes that rules of behavior will be followed or that these rules are clearly defined and accepted. However, even for experts, the principles of behavior being drafted seem to "walk" carefully around geopolitics. However, the application of the rule of law to space operations should coincide with Article III of the Outer Space Treaty. This provision requires that space activities shall be conducted "in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international co-operation and understanding."[55] The task is to seamlessly integrate new cyber activities into evolving LEO endeavors.

The third decade of the twenty-first century is now emerging, and the US Space Operations Command has assigned cybersecurity and intelligence specialists to work with satellite operators to support military units and protect US systems with adequate cyber defenses.[56] US Admiral Michael Rogers, commander of US Cyber

52 M. Smith, Anti-satellite weapons: History, types and purpose, *Space*, 10 August 2022. Available at: https://www.space.com/anti-satellite-weapons-asats (accessed: 31/12/2024).

53 *Ibidem*.

54 Outer Space Treaty, *op. cit*.

55 *Ibidem*.

56 S. Erwin, Space Force shifting resources to intelligence and cybersecurity, *Space News*, 19 September 2022. Available at: https://spacenews.com/space-force-shifting-resources-to-intelligence-and-cybersecurity/ (accessed: 31/12/2024).

Command and director of the National Security Agency, once observed: "The seas around the world are, much like the cyber domain, not governed by one single nation."[57] He noted that humans needed to establish standards of conduct in the online world to maintain the free flow of knowledge and ideas, as had been done in the ocean.[58] It is now clear that a new and unified strategy is required to address the risks impacting space-enabled communications and associated human activities.

Dystopian Landscape

In 1958, Myers McDougal, a renowned international law scholar, warned that the conquest of space had barely begun.[59] His observations no doubt aroused interesting questions and encouraged further discussion. As if McDougal had a crystal ball to forecast the future, he anticipated a legal evolution necessitating the recognition of future difficulties, stressing the terrestrial basis of much of our law and the earthly methods in which, for some time, we would continue to think about law in outer space.[60] Today, as plans are drafted for the future, the inescapable truth lies within the human condition. McDougal correctly foresaw the increase in counterspace activities, which involve combining offensive and defensive operations to gain and sustain control and security in space.[61] To ensure the enduring essence of the Outer Space Treaty, security concerns must take precedence in any proposed plan. However, space law is failing to keep pace with the increasing number of objects being launched, the related cyber activities, and even the forthcoming astronaut missions.[62] This task presents a multitude of dangers that loom over humanity's progress as it seeks to explore the solar system. One of these threats emanates from the cyber domain.

The present state of cyberspace evokes images of a dystopian future where crime is rampant and law enforcement struggles to maintain order. This notion is clearly illustrated by the 1979 film *Mad Max*, released in the US by American International Pictures LLC/ Filmways.[63] This Australian dystopian action film tells the

57 M.S. Rogers, *Admiral, Address at the International Conference on Cyber Conflict*, NATO Cooperative Cyber Defense Centre of Excellence, Tallinn 2015.

58 *Ibidem*.

59 M.S. McDougal, Perspectives for A Law of Outer Space, *American Journal of International Law*, 1958, 52, pp. 407–431.

60 *Ibidem*.

61 Doctrine, Counterspace Operations, *Air Force Doctrine Publication 3–14*, LeMay Center for Doctrine Development and Education, United States Air Force, 1 April 2025. Available at: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-14/3-14-D05-SPACE-Counterspace-Ops.pdf (accessed: 01/04/2025).

62 See generally: R. Balleste, Cyber Conflicts in Outer Space: Lessons from SCADA Cybersecurity, *Emory Corporate Governance and Accountability Review*, 2021, 8(1).

63 B. Eggert, Mad Max, *Deep Focus Review*, 9 May 2015. Available at: https://www.deepfocusreview.com/reviews/mad-max/ (accessed: 31/12/2024).

story of a world with a declining rule of law.[64] Like the lawless hackers of present cyberspace, in the story, unbound motorcycle gangs roam the countryside.[65] The challenges of a lawless domain of human activity are illustrated by the efforts of the Australian Main Force Patrol (MFP) and their high-speed interceptors.[66] The story serves as an allegory for the present efforts of governments seeking to catch up to the hackers that race unbound across cyberspace. Whether with interceptors or computers, technology has been an excellent tool for improving the overall quality of human existence. It is the existence of humanity that defines behavior. In this setting, many cybercrimes may be considered traditional or "real world" crimes.[67] The borderless nature of cyberspace provides anonymity and a fertile environment to quickly impact victims globally.[68] This nature also makes it difficult to pinpoint a crime's origin. Given the disadvantages associated with forensic analysis, the time invested in attributing these activities is seen as a waste of time.[69] There is an additional drawback when dealing with criminals who exploit rapidly evolving technology to outsmart the government.[70] The intersection of technology and law highlights the glaring gap between legal frameworks and technological advancements, resulting in a pressing concern for public safety.[71]

Regrettably, a dystopian scenario is increasingly becoming a reality. Lately, there has been considerable discussion and study regarding the future of cyberspace and its impact on society. The Center for Strategic and International Studies conducted an analysis focused on warfare in cyberspace as part of their series "On Future War."[72] An innovative combination of public polls, expert forecasts, and AI-generated threat scenarios was employed to examine the evolving nature of cyber operations aimed at the United States.[73] The data is especially relevant because the study included a public survey of over 1,000 people from around the US and six tabletop

64 *Ibidem*.
65 *Ibidem*.
66 *Ibidem*.
67 K.M. Finklea, *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction. Issues Confronting U.S. Law Enforcement,* Congressional Research Service 2013, p. 5.
68 *Ibidem*.
69 K. Zurkus, What's the Value in Attack Attribution?, *CSO Online*, 2017. Available at: https://www.csoonline.com/article/560371/is-identifying-an-attacker-a-waste-of-time.html (accessed: 31/12/2024).
70 K.M. Finklea, *op. cit.*, p. 18.
71 J.B. Comey, *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?*, Federal Bureau of Investigation, Washington 2014. Available at: https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course (accessed: 31/12/2024).
72 Y. Atalan, J.M. Macias, B. Jensen, *Eroding Trust in Government: What Games, Surveys, and Scenarios Reveal about Alternative Cyber Futures*, Center for Strategic and International Studies 2024, p. 2. Available at: https://www.csis.org/analysis/eroding-trust-government-what-games-surveys-and-scenarios-reveal-about-alternative-cyber (accessed: 31/12/2024).
73 *Ibidem*.

exercises with more than 50 top cyber specialists and experts in foreign policy.[74] The findings unveiled a projection of a cyber future characterized by targeted assaults on governmental services, essential infrastructure, and public confidence.[75] The findings also emphasize the tendency of potential adversaries to undermine the United States by means of cyberattacks that result in extensive disruption in critical services and small companies, along with espionage operations aimed at pillaging patents.[76]

The technical advancements over the last two decades have transformed into obstacles and drawbacks to overcome. In the US, for example, as criminals deliberately use new methods to commit the same crimes, the government, in contrast, finds itself in a defensive position when addressing illegal actions.[77] Sophisticated criminals can elude law enforcement due to their utilization of advanced technology and techniques that surpass the capabilities and knowledge of the government.[78] The utilization of advanced encryption to facilitate unlawful ventures exemplifies the challenge law enforcement faces in keeping pace with criminals.[79] The Department of Justice, Homeland Security, and numerous international organizations have identified impediments to assisting foreign governments in improving their ability to combat cybercrime.[80] Some significant drawbacks include a lack of specialized tools such as money, trained personnel, and a clear understanding of what constitutes a computer crime.[81] The cyberlandscape is mired by barriers stemming from the activities of hackers and similar actors, especially those engaged in malicious activities across national borders.[82] Cyber operations have become an easy tool of choice since these can be conducted anywhere in the world simply by accessing a computer and an Internet connection.[83]

The need for cybersecurity extends to satellite operations, which rely on a trio of interconnected segments. The US National Institute of Standards and Technology (NIST) defines the commercial space operations architecture as including space, ground, and user segments.[84] The *space segment* includes two parts. The first is the vehicle or satellite, which "consists of the platform and one or more

74 *Ibidem*.
75 *Ibidem*.
76 *Ibidem*.
77 K.M. Finklea, *op. cit.*, p. 18.
78 *Ibidem*.
79 *Ibidem*, p. 19.
80 Global Cybercrime, *Federal Agency Efforts to Address International Partners' Capacity to Combat Crime*, United States Government Accountability Office, Washington 2023. Available at: https://www.gao.gov/assets/gao-23-104768.pdf (accessed: 31/12/2024).
81 *Ibidem*.
82 I. Couzigou, Securing Cyber space: the Obligation of States to Prevent Harmful International Cyber operations, *International Review of Law, Computers & Technology*, 2018, 32(1), pp. 37–57.
83 *Ibidem*.
84 M. Scholl, T. Suloway, *Introduction to Cybersecurity for Commercial Satellite Operations*, National Institute of Standards and Technology, U.S. Department of Commerce, Washington 2023, p. 4.

payloads."[85] The second is the bus, which "consists of the components of the vehicle associated with the 'flying of the satellite,' such as power, structure, attitude control system, processing and command control, and telemetry."[86] Usually, the bus and the payload together comprise the satellite.[87] This space segment connects to the ground segment and user segment. The ground segment is comprised of ground operations (terrestrially-based) "that can be automated or conducted by human operators."[88] Lastly, the user segment includes the "consumers, such as Global Positioning Systems (GPS) receivers, satellite phone users, satellite Television receivers, vehicles, 5G users, industrial systems, mobile devices, and aircraft."[89] The US NIST has noted the associated threat to commercial space operations architectures, emphasizing the synergy of segments functioning as a cohesive whole.[90] Conversely, the realm of space communication represents a quintessential human endeavor, fraught with its own set of security challenges.

Nowadays, criminal behavior has taken root in cyberspace, which is both a complicated information highway and an arena for warfare. New laws are needed in every area where humans engage in activities, including on land, in the air, in space, and online. In other words, tackling the dangers of the cyber domain requires that scholars acknowledge that cybersecurity is at the core of human space activities. Information networks require practices and strategies to safeguard and defend them in an evolving new space arena. The core of information protection is reflected in *availability, integrity, and confidentiality*.[91] It involves an organization's overall risk assessment and considers law, due diligence, due care, and related risk management strategies. Indeed, an analysis of threats and challenges in the space industry from 1977 to 2019 reveals a broad attack surface.[92] The aforementioned discoveries, accessible in the public sphere, were classified according to the specific segment of space that was targeted, whether it was governmental, commercial, civilian, or military in nature.[93] Additionally, the incidents were classified based on the type of occurrence, such as jamming, spoofing, computer network exploitation, and hijacking.[94] The motivations behind these events were

85 *Ibidem*.
86 *Ibidem*.
87 *Ibidem*.
88 *Ibidem*, p. 6.
89 *Ibidem*.
90 *Ibidem*, p. 4.
91 J. Cawthra, M. Ekstrom, L. Lusty, J. Sexton, J. Sweetnam, *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events*, NIST Special Publication 1800-25, U.S. Department of Commerce, Washington 2020. Available at: https://www.nccoe.nist.gov/publication/1800-25/index.html (accessed: 31/12/2024).
92 M. Manulis, C. Bridges, R. Harrison, V. Sekar, A. Davis, Cyber security in New Space: Analysis of threats, key enabling technologies and challenges, *International Journal of Information Security*, 2021, 20, pp. 287–311.
93 *Ibidem*, p. 295.
94 *Ibidem*.

also identified, including State espionage, hack and leak operations, and illicit activities.[95] Space cybersecurity researchers would not be surprised to know that the ground segment was the most targeted segment from the events analyzed, followed by RF data transmission.[96] Experts predicted this outcome due to attackers' experience with ground-based tactics and the worldwide reach of RF communications.[97] The painful realization is that space objects have been on hackers' list of targets. The study revealed that, in spite of operational o challenges, the space industry remains vulnerable to attacks, with eight documented cases, with most of those attacks—91%—targeting government-owned assets.[98] This happens against the background of the Outer Space Treaty, Article II, which asserts that the space domain "is not subject to national appropriation by claim of sovereignty."[99] This statement is one of the cornerstones of international space law and supports the true spirit enshrined in Article I (2), emphasizing that outer space is accessible for exploration and use without any restrictions. In the same manner, Article 45(1) of the International Telecommunication Union (ITU) Constitution specifies that the functioning of all stations must be conducted in a manner that does not result in detrimental interference with "radio services or communications."[100] Unfortunately, the existing norms for cyber operations are inadequate and more troublesome when applied to the space domain.

The Russian war of aggression in Ukraine has been paradoxical against the backdrop of the global rule of law. The current situation has resulted in an environment lacking in law and order as the strength of the rule of law diminishes. Within this environment, military offensive operations are carried out in accordance with the legal and policy frameworks established by governments. Retired US Army Lieutenant Colonel J.W. Shipp, a cybersecurity expert, acknowledges that cyberspace and outer space are global arenas for military operations, where the objective is to achieve supremacy to gain control over information.[101] According to Shipp, the essential objective in every domain is to ensure allies' actions and, if necessary, prevent enemies from acting.[102] He suggests that common elements can be used to devise a strategy.[103] In this regard, Article IV of the Outer Space Treaty, notes in relevant part, as follows:

95 *Ibidem*.
96 *Ibidem*.
97 *Ibidem*.
98 *Ibidem*.
99 Outer Space Treaty, *op. cit.*
100 *Constitution and Convention of the International Telecommunication Union*, 22 December 1992, 1825 UNTS 330, ATS (1994) 28, BTS 24 (1996) (entered into force date 1 July 1994), as amended by the 2018 Plenipotentiary Conference [ITU Constitution].
101 J.W. Shipp, Space and Cyberspace: The Overlap and Intersection of Two Frontiers, *Army Space Journal*, 2011, 10(1), pp. 40–41.
102 *Ibidem.*
103 *Ibidem*.

> The moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes. The establishment of military bases, installations, and fortifications, the testing of any type of weapons, and the conduct of military maneuvers on celestial bodies shall be forbidden.[104]

On the other hand, a dystopian landscape is unfolding, where rising power competition among nations is highlighted by various hackers, such as mercenaries, privateers, and spies, who bid to advance diverse agendas.[105] The Outer Space Treaty appears to be on a path toward obsolescence, with some of its provisions no longer able to guide the development of new technologies. In the cyberspace domain, legal developments are equally troubling. While various government experts have considered the operative aspects of these hackers or cyber operations for over ten years, discussions have focused on aspirational or soft law principles that suggest a voluntary honor code. This honor code-in-formation or international cyber norms began to evolve with the 2013 Report of the UN Group of Governmental Experts on Information and Telecommunications in the Context of International Security.[106] In 2021, the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security presented their report, observing that "efforts should be conducted in accordance with their obligations under the Charter of the United Nations and other international law, with a view to preserving an open, secure, stable, accessible and peaceful ICT environment."[107] The GGE, in the same 2021 report, paragraph 71(g) notes in particular the following:

> The Group reaffirms that States must meet their international obligations regarding internationally wrongful acts attributable to them under international law. It also reaffirms that States must not use proxies to commit internationally wrongful acts using ICTs and should seek to ensure that their territory is not used by non-state actors to commit such acts.[108]

The efforts of the various UN Group of Governmental Experts considered the international community's expectations in search of norms for responsible state behavior. While these endeavors provide potential models for future guidelines or

104 Outer Space Treaty, *op. cit.*

105 *See generally*, T. Maurer, *Cyber Mercenaries: The State, Hackers, and Power*, Cambridge University Press, Cambridge 2018.

106 United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/68/98, 2013.

107 United Nations, Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security, UN Doc A/76/135, 14 July 2021, paragraph 18.

108 *Ibidem*.

codes of behavior, unfortunately, these are still ambitious and have not yet been fully realized. Therefore, other factors indicate the need for an alternative course of action. The world is more dangerous now than in the last decades of the twentieth century. In this tumultuous environment, due care continues to be crucial in launching best practices to protect organizations.[109] Given the offensive capabilities of hackers, terrorist groups, and criminal organizations engaged in transnational hostile cyber operations, stakeholders in the space sector have a vital responsibility to fulfill. It is imperative that they assume a proactive stance, exploring innovative avenues to confront these pressing cyber threats. In the grand tapestry of the cosmos, the true essence of peaceful exploration lies in the harmonious collaboration of nations and the collective spirit of humanity.

Gray-Zone Power

The concept of cyberspace has undergone significant development, expanding beyond its original scope of basic accessibility to encompass a multifaceted domain of human interactions and activities. The data sources driving humanity's progress have become essential to an intricate network of activities supporting the private sector, governments, and individual users. Human behavior is intricately linked to the pursuit of solutions and the addressing of illicit conduct in order to strengthen national and international justice.[110] The human perception of justice seems inherently consistent over many geographical locations and historical periods.[111] Accordingly, to effectively tackle illicit activities in cyberspace, stakeholders must recognize that human endeavors shape cybersecurity. Human action does not occur alone; instead, it is influenced by broader cultural ideas.[112] Familiarity with the thought process involved in combat is equally necessary for defense.[113] Similarly, understanding the cultural context helps to clarify the goals of policymaking and planning.[114] As the threat environment expands to include interconnected domains, stakeholders must prepare to deal with increased vulnerabilities.

The 2007 Estonian Distributed Denial of Service (DDoS) attack prompted cybersecurity experts to recognize the rapid evolution of cyberspace, as well as the

109 M. Whitman, H. Mattord, *Management of Information Security*, Cengage Learning, Boston 2016, p. 231.

110 D. Sznycer, C. Patrick, Intuitions about justice are a consistent part of human nature across cultures and millennia, *The Conversation*, 21 October 2022. Available at: https://theconversation.com/intuitions-about-justice-are-a-consistent-part-of-human-nature-across-cultures-and-millennia-190523 (accessed: 31/12/2024).

111 *Ibidem*.

112 R.E. Guadagno, A. Lankford, N.L. Muscanell, B.M. Okdie, D.M. McCallum, Social Influence in the Online Recruitment of Terrorists and Terrorist Sympathizers: Implications for Social Psychology Research, *Revue Internationale de Psychologie Sociale*, 2010, 23(1), pp. 25–56.

113 *Ibidem*.

114 *Ibidem*.

adaptation of traditional techniques to novel contexts. A novel cybersecurity threat emerged, causing a redefinition of covert transnational operations.[115] Consequently, the attack demonstrated the potential for disabling vulnerable systems, which could have severe consequences for a nation and its citizens.[116] This attack, which disregarded the rule of law, has been replicated multiple times since 2007. Ironically, the DDoS assault in Estonia likely laid the foundation, at least partially, for the current state of cyberspace.[117] Experts studying Russia's capabilities have observed that satellite-based systems might be a possible target.[118] This scenario is not too far-fetched, considering the hostile actions witnessed in Estonia that gradually intensified over the subsequent years.[119] The situation reached a tipping point in 2015, when Russian hackers carried out a significant cyberattack on an electric grid, targeting three power companies in Ukraine.[120] After the invasion of Ukraine, Russia launched variants of the wiper data destruction malware against Ukrainian targets.[121] It would have been a reasonable assumption to expect Russia to expand its cyber operations into space. The VIASAT case of 2022 became a cautionary tale of cyber operations that now intersect space services. However, to fully understand the lessons, it is necessary first to consider other factors.

From the beginning of the Russian invasion of Ukraine in 2022, Ukrainians experienced the effects of an assortment of cyber operations that included the deployment of multiple variations of malware—wipers—to destroy data.[122] This escalated with the Russian VIASAT-Skylogic breach, which revealed the existing susceptibility of a space network to exploitation by any actor with relevant technical skills.[123] Unfortunately, the criminal element lurking in cyberspace blurs the borderlines for law enforcement across jurisdictions.[124] Although national boundaries serve local, state, and federal jurisdictions, they also affect criminal activity and law enforcement operations.[125] Due to their transnational nature and wide-ranging consequences, these attacks should not be addressed solely through any State's efforts, no matter how powerful. Thus, it is imperative for stakeholders to acknowledge the 2022 Viasat KA-SAT Satellite hack as a clear indication of

115 G. Evron, Battling botnets and Online Mobs. Estonia's Defense Efforts During the Internet War, *Georgetown Journal of International Affairs*, 2008, 9(1), pp. 121–126.
116 *Ibidem*.
117 *Ibidem*.
118 S. Bendett, M. Boulègue, R. Connolly et al., *Advanced military technology in Russia. Capabilities and Implications*, Chatham House, Royal Institute of International Affairs, London 2021, p. 35.
119 *Ibidem*.
120 *Ibidem*.
121 M. Kaminska, J. Shires, M. Smeets, *Cyber Operations During the 2022 Russian Invasion of Ukraine. Lessons Learned (so far)*. European Cyber Conflict Research Initiative, Leiden 2022, p. 4.
122 *Ibidem*.
123 M. Manulis et al., *op. cit.*, p. 297.
124 K.M. Finklea, *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction. Issues Confronting U.S. Law Enforcement*, Congressional Research Service, Washington 2013.
125 *Ibidem*.

Russia's intensifying cyber operations interfering with the space domain. It is notable that several States have this capability.

A journey to the Moon, Mars, and other celestial bodies encompasses thoughts of optimism, high hopes, and a future-oriented perspective infused by human activity. Yet, if we are to look into the proverbial "crystal ball," the future shows satellite constellations, the Lunar Gateway, and increased crewed missions expanding human presence in the space landscape. If humanity is to achieve that success, then two realities must be recognized above all others. First, the nations of the planet, especially the spacefaring nations, must work together toward that common goal. Humanity as a whole must recognize how, in the event of a significant conflict involving major nations with space capabilities, the orbital region of Earth would be positioned to serve as a potential theater of warfare.[126] Second, while laws give guidelines that must be carried out under rule-governed direction, no legislation can ever ensure its honest implementation. [127] Indeed, the Outer Space Treaty has been in force for almost sixty years, yet, at present, a simple update of that treaty cannot be realized, even when the space law community recognizes the need for an update. Why does this idle status prevail? The truth is that the existing legal framework in cyberspace is more of a suggestion than an enforceable legal standard, and this status is slowly poisoning the activities of humanity in outer space. Other factors, such as mining for resources, and the race for the Moon and Mars, have increased competition among nations. As the conflict in Ukraine has demonstrated, a single factor is clear: the rule of law has no authority over transborder cyber operations, even when a space service is involved. Recognizing the gravity of space operations requires facing the truth: international cooperation is painfully slow and, at the moment, nonexistent.[128] The existing *legal lacunae*, better exemplified as *gray-zone conflict,* complicates matters. The gray-zone conflict is characterized by activities of subterfuge or malice utilized by States and non-State actors to "exploit gaps and ambiguities in the law."[129] Technology has made the gray-zone conflict more common and its effect more widespread.[130] This is supported by empirical data that shows how non-State actors use information technology to harm targeted infrastructure.[131]

The current landscape of activities is also profoundly influenced by the dynamics of the *great power competition*, a framework that elucidates the nature of global,

126 B.E. Bowen, *War in Space. Strategy, Spacepower, Geopolitics*, Edinburgh University Press, Edinburgh 2022, p. 281.

127 J.L. Esposito, *Law and Morality: A Survey of Ideas, Issues, and Cases*, Ethics International Press, West Yorkshire 2022, p. 12.

128 B. Ramsey, An Ethical Decision-Making Tool for Offensive Cyberspace Operations, *Air & Space Power Journal*, 2018, 32(3), p. 63.

129 R. Brooks, *Rule of Law in the Gray Zone*. Modern War Institute, 2 July 2018. Available at: https://mwi.westpoint.edu/rule-law-gray-zone/ (accessed: 31/12/2024).

130 *Ibidem*.

131 *Ibidem*.

interstate interactions shaped by political pursuits throughout history, culminating in the era preceding World War II.[132] Over time, numerous competition periods have seen strong national powers contend for prestige and prominence.[133] While the competition was limited to a two-state competition between the US and the USSR, it has resurfaced in international relations and security studies recently, due to globalization and American supremacy.[134] It has been noted how the US National Security Strategy of 2017 openly advanced the notion that the United States, Russia, China, and other national powers had formally transitioned from collaboration to competition.[135] The problem arises from the continuum of relations between governments, nonstate actors, and specific super-empowered individuals, ranging from cooperation to confrontation, ultimately culminating in warfare.[136] In the current era of global power dynamics, the shift towards a competitive-dominant engaging framework among the most influential nations and others has introduced greater conflict and confrontation into the realm of competition.[137] This scenario has led to heightened readiness for possible conflicts, encompassing advancements in antisatellite technology and exceeding all that has been witnessed in the recent past.[138]

The advancement of a solution necessitates an understanding of the purpose behind the technology that aids humanity's objectives and consciousness. The intricate tapestry of contemporary technology presents a complex challenge in the pursuit of a universal framework for human dignity. In an age where humanity finds itself intricately woven into a vast tapestry of connectivity, a paradox emerges: the stakeholders face an array of novel threats that seek to undermine their inherent dignity. This situation necessitates the establishment of a novel framework for space law. Myers MacDougal and Florentino Panlilio Feliciano, Associate Justice of the Supreme Court of the Philippines, noted how the rapid diffusion of weapons capable of shattering the globe, the hostile polarization of power in the world arena, the ever more precarious equilibrium between national actors, and many other aspects magnify with chilling insistence, even for the willful blind, the urgent need for rational inquiry into the inherited principles for controlling violence between peoples.[139] Indeed, should the inhabitants of Earth continue to find themselves in conflict, the prospects for the future appear bleak, fraught with tension, and shrouded in ambiguity.

---

132 T.F. Lynch III, *Introduction*, [in:] T.F. Lynch III (ed.), *Strategic Assessment 2020: Into a New Era of Great Power Competition*. Institute for National Strategic Studies, NDU Press, Washington 2020, p. 1.

133 *Ibidem*.

134 *Ibidem*.

135 *Ibidem*.

136 *Ibidem*, p. 2.

137 *Ibidem*, p. 3.

138 *Ibidem*.

139 M.S. McDougal, F.P. Feliciano, International Coercion and World Public Order: The General Principles of the Law of War, *Yale Law Journal*, 1958, 67(5), p. 771.

So, how should the space industry proceed? The solution resides in the steadfast adherence to the principles of law and order. The pursuit of space exploration serves as a mirror to the myriad activities of humanity. In the boundless expanse of the universe, human endeavors will transcend our wildest imaginings, unfolding in ways we have yet to comprehend. Thus, the inherent virtues of humanity, coupled with the principles of space law, shall ignite a renaissance of exploration beyond our terrestrial confines. If humanity must enter a new age of discovery, incorporating the entire solar system into its new domain, then "[a] more *substantive* concept of the rule of law [should] aspire to fill the idea of the law with notions of substantive justice."[140] Justice must illuminate the endeavors of those embarking upon this new era of exploration, for it is impossible to overlook the escalating demands, unmatched in their breadth and intricacy, for the expansion of sovereign authority.[141] In a similar vein, this observation extends to the vast cosmic ocean and the principles governing its exploration. The principles and regulations governing the Low Earth Orbit are of particular significance. Striking a balance between essential order and inevitable chaos means achieving a common point of reference and a tool to protect the world. The direction of threat intelligence depends much on this. The current state of space cybersecurity evolves from valuable lessons originating in past knowledge based on security strategy, legal principles, and industry standards. However, this knowledge must be intended for risk assessments, security requirements, and an innovative space law. While an argument can be made that new norms in international law are emerging and applicable to cyberspace and its intersection with the space domain, the same can be said of the existing grey area surrounding that law.

Beyond the Horizon: Conclusion

The future of space exploration is one of hope and awe. Due to the complexities of present geopolitics, the need to explore outer space in search of new worlds seems far removed from the trivialities of human existence. The future of humanity holds the potential for interstellar space travel. These tasks are theoretically possible, albeit costly and challenging from the current perspective. The noir in cybersecurity, however, is simply a disappointment with the current state of the law at the intersection of cyberspace and outer space. This noir is literal pessimism. "Film noir is a stylized genre of film marked by pessimism, fatalism, and cynicism. The term was originally used in France after WWII, to describe American thriller or detective films in the 1940s and 50s."[142] To encapsulate the essence of noir, space

140 S. Wiessner, The Rule of Law: Prolegomena, *Zeitschrift für deutsches und amerikanisches Recht*, 2018, 82, p. 83.

141 *Ibidem*.

142 *What is Film Noir? A Brief History with Examples from Cinema*, Studiobinder, 27 June 2021. Available at: https://www.studiobinder.com/blog/what-is-film-noir/ (accessed: 31/12/2024).

industry stakeholders must acknowledge the intricate web of satellite communication, coupled with the shortcomings of existing regulations, underscoring the urgent necessity for a cohesive framework of principles.

"Noir stories typically feature gritty urban settings, morally compromised protagonists, dark mysteries, and a bleak outlook on human nature."[143] Will humanity find and settle in *Delmak-O* or similar exoplanets? Astronauts and relevant stakeholders will surely face dangers after they land on the Moon and travel on to Mars. The process begins with the LEO orbit. Such guidelines are essential to safeguarding data as it traverses the vast expanse between Earth, satellites, and the cosmos.[144] "Launch servicing companies, remote sensing companies, and data access and analytics firms all share a desire to capitalize on the development and growth primarily in LEO satellites."[145]

In this landscape, cyber operations emerge as another information security risk that touches the spirit of human space exploration.[146] Utilizing cyber threat intelligence, which facilitates gathering, examining, and distributing data to identify, monitor, and predict possibilities and risks within cyberspace, enhances decision-making.[147] By leveraging threat intelligence, stakeholders gain a valuable perspective on the ever-evolving landscape of threats, vulnerabilities, and tactics malicious actors employ.[148] The noir in cybersecurity encourages new practices, standards, and norms to help secure the space industry. The attractive promise of providing global internet access via LEO satellite constellations is expected to generate around $400 billion in growth for the space sector by 2040.[149] Observing the landscape of the next twenty years, and even one hundred years, offers a beginning that traces its wisdom into the past and evolves into the future. The path to a workable space cybersecurity framework that ensures defensive capabilities in LEO can be developed from the wisdom of those scholars who long ago identified the benefits of space exploration, recognizing that peace and security evolve from uncertainty. The immediate solutions are contained in a new cybersecurity framework that, anchored in space law, will inspire the development of novel legal principles.

---

143 *What Is Noir Fiction?*, MasterClass, 27 Jan 2022. Available at: https://www.masterclass.com/articles/noir-fiction (accessed: 31/12/2024).

144 *Ibidem*.

145 A. Saboorian, A Brave New World: Using the Outer Space Treaty to Design International Data Protection Standards for Low- Earth Orbit Satellite Operators, *Journal of Air Law and Commerce*, 2019, 84(4), pp. 575–604, 580.

146 D.E. Sanger, K. Conger, *op. cit.*

147 J. Kotsias, A. Ahmad, R. Scheepers, Adopting and Integrating Cyber-threat Intelligence in a Commercial Organization, *European Journal of Information Systems*, 2022, 31(1), p. 35.

148 Shweta, K. Aditham, M. Hoeper, *What Is Threat Intelligence? Definition, Types & Process*, Forbes Advisor, 12 October 2023. Available at: https://www.forbes.com/advisor/business/what-is-threat-intelligence/ (accessed: 31/12/2024).

149 A. Saboorian, *op. cit.*, p. 582.

Bibliography

Atalan, Y., **Macias J.M.**, **Jensen B.**, *Eroding Trust in Government: What Games, Surveys, and Scenarios Reveal about Alternative Cyber Futures*, Center for Strategic and International Studies 2024. Available at: https://www.csis.org/analysis/eroding-trust-government-what-games-surveys-and-scenarios-reveal-about-alternative-cyber (accessed: 31/12/2024).

Balleste, R., Cyber Conflicts in Outer Space: Lessons from SCADA Cybersecurity, *Emory Corporate Governance and Accountability Review*, 2021, 8(1).

Barker, K., What is Cyber Threat Intelligence?, *CrowdStrike*, 23 March 2023. Available at: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/ (accessed: 31/12/2024).

Bendett, S., **Boulègue, M.**, **Connolly, R. et al.**, *Advanced military technology in Russia. Capabilities and Implications*, Chatham House, Royal Institute of International Affairs, London 2021.

Bourély, M., The Institutional Framework of Space Activities in Outer Space, *Journal of Space Law*, 1998, 26(1).

Bowen, E., *War in Space. Strategy, Spacepower, Geopolitics*, Edinburgh University Press, Edinburgh 2022.

Bowman, A., *Commercial Space Frequently Asked Questions*, NASA, 7 April 2024. Available at: https://www.nasa.gov/humans-in-space/leo-economy-frequently-asked-questions/#:~:text=What%20is%20the%20LEO%20Economy,services%20this%20region%20of%20space (accessed: 31/12/2024).

Brooks, R., *Rule of Law in the Gray Zone*. Modern War Institute, 2 July 2018. Available at: https://mwi.westpoint.edu/rule-law-gray-zone/ (accessed: 31/12/2024).

Cawthra, J., **Ekstrom, M.**, **Lusty, L.**, **Sexton, J.**, **Sweetnam, J.**, *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events*, NIST Special Publication 1800-25, U.S. Department of Commerce, Washington 2020. Available at: https://www.nccoe.nist.gov/publication/1800-25/index.html (accessed: 31/12/2024).

Christol, Q.A., *Space Law: Past, Present, and Future*, Kluwer Law and Taxation Publishers, Deventer 1991.

Collier, J., Proxy Actors in the Cyber Domain: Implications for State Strategy, *St Antony's International Review*, 2017, 13(1), pp. 25–47.

Comey, J.B., *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?*, Federal Bureau of Investigation, Washington 2014. Available at: https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course (accessed: 31/12/2024).

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

Couzigou, I., Securing Cyber space: the Obligation of States to Prevent Harmful International Cyber operations, *International Review of Law, Computers & Technology*, 2018, 32(1), pp. 37–57.

Dick, P.K., *A Maze of Death*, First Mariner Books edition 2013, New York 1970.

Doctrine, Counterspace Operations, *Air Force Doctrine Publication 3–14*, LeMay Center for Doctrine Development and Education, United States Air Force, 1 April 2025. Available at: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-14/3-14-D05-SPACE-Counterspace-Ops.pdf (accessed: 01/04/2025).

Eggert, A., Mad Max, *Deep Focus Review*, 9 May 2015. Available at: https://www.deepfocusreview.com/reviews/mad-max/ (accessed: 31/12/2024).

Erwin, S., Space Force shifting resources to intelligence and cybersecurity, *Space News*, 19 September 2022.

Esposito, J.L., *Law and Morality: A Survey of Ideas, Issues, and Cases*, Ethics International Press, West Yorkshire 2022.

Evron, A., Battling botnets and Online Mobs. Estonia's Defense Efforts During the Internet War, *Georgetown Journal of International Affairs*, 2008, 9(1), pp. 121–126.

Finklea, K.M., *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction. Issues Confronting U.S. Law Enforcement*, Congressional Research Service 2013.

Global Cybercrime, *Federal Agency Efforts to Address International Partners' Capacity to Combat Crime*, United States Government Accountability Office, Washington 2023. Available at: https://www.gao.gov/assets/gao-23-104768.pdf (accessed: 31/12/2024).

Grey, W., Troubles with Time Travel, *Philosophy*, 1999, 74(287).

Guadagno, R.E., **Lankford, A.**, **Muscanell, N.L.**, **Okdie, B.M.**, **McCallum, D.M.**, Social Influence in the Online Recruitment of Terrorists and Terrorist Sympathizers: Implications for Social Psychology Research, *Revue Internationale de Psychologie Sociale*, 2010, 23(1), pp. 25–56.

Guzman, A., *What is the Commercial Low Earth Orbit Economy?*, NASA, 26 July 2023.

Hagen, R., **Scheffran, J.**, *International Space Law and Space Security. Expectations and Criteria for a Sustainable and Peaceful Use of Outer Space*, [in:] M. Benkö, K.-U. Schrogl (eds.), *Current Problems and Perspectives for Future Regulation*, Eleven International Publishing, AJ Utrecht, The Netherlands 2005.

Holmes, M., 10 Defining Moments in Cybersecurity and Satellite in 2023, *Via Satellite*, 22 January 2024.

How Do We Communicate with Spacecraft? We Asked a NASA Technologist: Episode 37, NASA. Available at: https://www.nasa.gov/general/how-do-we-communicate-with-spacecraft-we-asked-a-nasa-technologist-episode-37/ (accessed: 31/12/2024).

IBM, *What is threat intelligence?*Available at: https://www.ibm.com/topics/threat-intelligence (accessed: 31/12/2024).

Kaminska, M., **Shires, J.**, **Smeets, M.**, *Cyber Operations During the 2022 Russian Invasion of Ukraine. Lessons Learned (so far)*, European Cyber Conflict Research Initiative, Leiden 2022.

Kotsias, J., **Ahmad, A.**, **Scheepers, R.**, Adopting and Integrating Cyber-threat Intelligence in a Commercial Organization, *European Journal of Information Systems*, 2022, 31(1), pp. 35–51.

Lachs, M., Thoughts on Science, Technology and World Law, *The American Journal of International Law*, 1992, 86(4), pp. 673–699.

Lynch III, T.F., *Introduction*, [in:] T. F. Lynch III (ed.), *Strategic Assessment 2020: Into a New Era of Great Power Competition*, Institute for National Strategic Studies, NDU Press, Washington 2020.

Manulis, M., **Bridges, C.**, **Harrison, R.**, **Sekar, V.**, **Davis, A.**, Cyber security in New Space: Analysis of threats, key enabling technologies and challenges, *International Journal of Information Security*, 2021, 20, pp. 287–311.

Maogoto, J., **Freeland, S.**, The Final Frontier: The Laws of Armed Conflict and Space Warfare, *Conn J Int'l L*, 2007, 23:1.

Maurer, T., *Cyber Mercenaries: The State, Hackers, and Power*, Cambridge University Press, Cambridge 2018.

McDougal, M.S., Perspectives for A Law of Outer Space, *American Journal of International Law*, 1958, 52, pp. 407–431.

McDougal, M.S., **Feliciano, F.P.**, International Coercion and World Public Order: The General Principles of the Law of War, *Yale Law Journal*, 1958, 67(5).

McDowell, J.C., The Low Earth Orbit Satellite Population and Impacts of the SpaceX Starlink Constellation, *The Astrophysical Journal Letters*, 2020, 892(2).

Press, L., Amazon Project Kuiper vs SpaceX Starlink, *CircleID*, 19 January 2024. Available at: https://circleid.com/posts/20240119-amazon-project-kuiper-vs-spacex-starlink (accessed: 31/12/2024).

Ramsey, B., An Ethical Decision-Making Tool for Offensive Cyberspace Operations, *Air & Space Power Journal*, 2018, 32(3).

Rogers, M.S., *Admiral, Address at the International Conference on Cyber Conflict*, NATO Cooperative Cyber Defense Centre of Excellence, Tallinn 2015.

Saboorian, A., A Brave New World: Using the Outer Space Treaty to Design International Data Protection Standards for Low-Earth Orbit Satellite Operators, *Journal of Air Law and Commerce*, 2019, 84(4), pp. 575–604.

Sanger, E., **Conger, K.**, Russia Was Behind Cyberattack in Run-Up to Ukraine War, Investigation Finds, *The New York Times*, 10 May 2022. Available at: https://www.nytimes.com/2022/05/10/us/politics/russia-cyberattack-ukraine-war.html (accessed: 31/12/2024).

Scholl, M., **Suloway, T.**, *Introduction to Cybersecurity for Commercial Satellite Operations*, National Institute of Standards and Technology, U.S. Department of Commerce, Washington 2023.

Sherlock, A., Blade Runner: 10 Tropes Of Film Noir (& How It Puts A Sci-Fi Twist On Them), *Screenrant*, 22 August 2020. Available at: https://screenrant.com/blade-runner-film-noir-tropes-sci-fi-twist/ (accessed: 31/12/2024).

Shipp, J.W., Space and Cyberspace: The Overlap and Intersection of Two Frontiers, *Army Space Journal*, 2011, 10(1), pp. 40–41.

Shweta, Aditham, K., **Hoeper, M.**, *What Is Threat Intelligence? Definition, Types & Process*, *Forbes Advisor*, 12 October 2023. Available at: https://www.forbes.com/advisor/business/what-is-threat-intelligence/ (accessed: 31/12/2024).

Smith, M., Anti-satellite weapons: History, types and purpose. *Space*, 10 August 2022. Available at: https://www.space.com/anti-satellite-weapons-asats (accessed: 31/12/2024).

Suwijak, Ch., Li, S., Global Internet Access from the Low Earth Orbit: Legal Issues regarding Cybersecurity in Outer Space, *Journal of East Asia and International Law*, 2022, 15(1).

Sznycer, A., **Patrick, C.**, Intuitions about justice are a consistent part of human nature across cultures and millennia, *The Conversation*, 21 October 2022. Available at: https://theconversation.com/intuitions-about-justice-are-a-consistent-part-of-human-nature-across-cultures-and-millennia-190523 (accessed: 31/12/2024).

Tracking and Tada Relay Satellite (TDRS): Continuing the Critical Lifeline, Goddard Space Flight Center, NASA. Available at: https://www.nasa.gov/wp-content/uploads/2022/04/tdrsfactsheet_3.pdf (accessed: 31/12/2024).

United Nations, *Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security*, UN Doc A/76/135, 14 July 2021, paragraph 18.

United Nations, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc A/68/98, 2013.

United Nations, *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, 27 January 1967, 610 UNTS 205, article II (entered into force 10 October 1967) [Outer Space Treaty].

Wheale, N., Recognizing a 'Human-Thing': Cyborgs, Robots and Replicants in Philip K. Dick's 'Do Androids Dream of Electric Sheep?' And Ridley Scott's 'Blade Runner', *Critical Survey*, 1991, 3(3), pp. 297–304.

Whitman, M., **Mattord, H.**, *Management of Information Security*, Cengage Learning, Boston 2016.

Williams, E., Ideology as Dystopia: An Interpretation of 'Blade Runner', *Revue Internationale de Science Politique*, 1988, 9(4).

Zurkus, K., What's the Value in Attack Attribution?, *CSO Online*, 2017. Available at: https://www.csoonline.com/article/560371/is-identifying-an-attacker-a-waste-of-time.html (accessed: 31/12/2024).