Cybersecurity in the Era of Space Domain Awareness

Ulpia Elena BOTEZATU
National Institute for Research and Development in Informatics - ICI Bucharest
Romanian Space Agency, Romania
ulpia.botezatu@ici.ro, ulpia.botezatu@rosa.ro

Abstract: As society increasingly relies on space systems, this article explores the critical link between space operations and cybersecurity, highlighting the need to protect space assets from cyber threats. It emphasizes the role of Space Domain Awareness (SDA) in comprehending and securing activities in outer space. The article also discusses the challenges posed by the evolving space architecture and SpaceX's Starlink project, underlining the importance of cybersecurity in safeguarding space assets. In conclusion, it calls for vigilance, innovation, and international collaboration to secure the space frontier in an era marked by digital vulnerabilities.
Keywords: cybersecurity, Space Domain Awareness, emerging technologies, space governance, international cooperation, space security.

INTRODUCTION

The prominence of the space domain in contemporary society is indisputable, with space-based assets and digital systems permeating critical functions. From enabling global connectivity to monitoring Earth's well-being and expanding our presence beyond terrestrial boundaries, space operations are integral to modern life. However, this heightened dependence on space infrastructure also ushers in a new realm of vulnerabilities—cyber threats in outer space (Botezatu, 2023).

The imperative of addressing a dynamic intersection between space and cyber domains demands immediate recognition. As of early 2022, the World Economic Forum underscored the pressing concerns related to "digital dependencies and cyber vulnerabilities" in conjunction with the "crowding and competition in space" as prominent global threats (World Economic Forum, 2022). In subsequent months, the tangible convergence of these threats manifested during the Ukrainian crisis. Satellite-based broadband internet services assumed paramount significance for military operations and the Ukrainian military's resilience against a Russian incursion. However, these services also found themselves in the crosshairs of digital disruptions and efforts aimed at denying access, with repercussions extending far beyond the confines of the conflict zone.

The aim of this article is to explore the intricate interplay between space operations and cybersecurity in the context of Space Domain Awareness (SDA) (US Space Force Command, 2023). SDA encompasses the comprehensive understanding, management, and security of

https://doi.org/10.54851/v6i1y202403

activities in outer space (Di Mare, 2021). The convergence of space systems and cybersecurity is underscored as a critical element in ensuring the continued and reliable contributions of space systems to national critical infrastructure. By analysing the cybersecurity principles laid out in programmatic documents, such as the American SPD-5 Directive and the EU Space Strategy for Security and Defense, as well as addressing contemporary cyber threat landscape, this article underscores the indispensable role of cybersecurity in the future of space exploration.

SPACE DOMAIN AWARENESS: A COMPREHENSIVE FRAMEWORK

SDA, from both American and European perspectives, serves as a pivotal framework for comprehensively grasping, regulating, and securing operations in outer space. It has emerged as an indispensable paradigm in an environment where space is akin to traditional domains of warfare such as air, sea, and land. Space Domain Awareness encompasses the examination and surveillance of Earth's orbital satellites, encompassing tasks such as identifying, tracking, cataloging, and detecting artificial entities, including both operational and defunct satellites, expended rocket components, and fragments of space debris, in addition to other more complex activities, such as geointelligence.

Discussing a New Paradigm

Recent years have witnessed a significant transformation in the geopolitical landscape, ushering in a period characterized by increased uncertainty (Azoulay, et al., 2021). Within this shifting paradigm, Western alliance confront the pressing need to rapidly adapt to emerging threats on the international stage. Of particular note is the evolution of the space domain, marked by growing concerns regarding the development and deployment of anti-satellite capabilities.

In this context, the pivotal role of Space Domain Awareness (SDA) becomes evident. As nations navigate the changing dynamics of outer space, space-based intelligence platforms emerge as indispensable tools for decision-makers, providing clarity amid ambiguity. SDA's capacity to comprehensively understand, monitor, and secure activities in outer space aligns seamlessly with the need to adapt swiftly to emerging global challenges.

Within the North Atlantic Treaty Organization (NATO), member states operate in an environment marked by rapid transformation. This environment underscores the growing necessity for enhanced operational readiness and increased system resiliency. Recognizing space's significance within contemporary defense strategies, the Joint Air Power Competence Centre (JAPCC) has recently advocated for NATO to exert its political influence. The objective is to ensure that member nations not only integrate resilience concepts into the development of their space systems but also foster the selection of resilient, redundant, and synergetic national space systems, including commercial solutions, to bolster the Alliance's operational capabilities. This proactive approach aligns with the essence of SDA—preparing for an uncertain future by enhancing space systems' resiliency and effectiveness.

Technological Considerations

The drive to augment the resiliency of space infrastructure is intrinsically linked to the principles of Space Domain Awareness (SDA). As the world seeks to adapt to evolving challenges in outer space, one viable strategy involves enabling the production of satellites at scale. This approach not only expedites the replenishment of depleted or damaged space assets but also underscores the importance of SDA in safeguarding the space domain. Manufacturers, equipped with the ability to rapidly produce identical satellite units without compromising quality, exemplify the principles of SDA. Such resilience in infrastructure maintenance represents an essential aspect of deterrence by denial, which SDA promotes.

NASA's recent initiative, calling for the development of its next-generation fleet of multi-mission spacecraft, aligns with the tenets of SDA. The trend of batch-producible small spacecraft, pioneered by emerging space enterprises like SpaceX, OneWeb, and BlackSky, reflects a commercial market's shift toward the principles of SDA. These companies demonstrate heightened efficiency in harnessing compact satellites, underscoring the importance of adaptability and resiliency, central themes in SDA.

The accelerated pace of technological advancements, a hallmark of the modern era, reinforces the necessity of Space Domain Awareness in spacecraft development. Space systems must be agile enough to accommodate new capabilities during their development. SDA promotes this flexibility, as it emphasizes the swift assimilation of unplanned hardware without disrupting project timelines. Furthermore, the global dispersion of space enterprises necessitates cooperation among manufacturers from diverse sources. Often, these entities lack coordination regarding standards and protocols, highlighting the importance of genuine plug-and-play solutions, a concept consistent with SDA.

In summary, the evolving spacecraft domain, intimately connected with geopolitical dynamics, underscores the growing importance of Space Domain Awareness (Tadjdeh, 2021). SDA principles—resilience, adaptability, and interoperability—have emerged as cornerstones for safeguarding space assets and ensuring their continued effectiveness in a dynamic global context. Strategies such as batch production and plug-and-play solutions, closely aligned with the tenets of SDA, offer viable pathways to address evolving challenges within the space domain while enhancing the capabilities of Western alliances in an increasingly uncertain world.

The American Perspective

The transition from Space Situational Awareness (SSA) to SDA in the United States signifies an acknowledgment of the growing complexities in space operations. While SSA primarily focused on detecting, tracking, and identifying artificial objects in Earth's orbit, SDA encompasses a more expansive spectrum. It involves the identification, characterization, and comprehension of various factors—passive or active—that could affect space operations (Erwin, 2022; Erwin, 2019). These factors span from space debris and satellites to emerging threats from rival nations.

Furthermore, SDA underlines the imperative of comprehending and managing these multifaceted challenges within the dynamic space domain. This transition underscores the United States' commitment to maintaining a proactive and adaptive approach in safeguarding its interests and those of its allies in an environment marked by the continuous evolution of space-related technologies and threats.

The European Perspective: EU Space Strategy for Security and Defense

The European Union's Space Strategy for Security and Defence (EU External Action Service, 2023) signifies a significant step forward in bolstering the security and resilience of space assets on the continent. This comprehensive strategy encompasses five key areas: defining space threats, enhancing resilience and protection of space systems, responding to space threats, optimizing the use of space for security and defence, and promoting responsible behaviours in space. By embracing this strategy, the European Union not only strives to safeguard its own space assets but also to foster cooperation with global partners, including the United States and NATO, in addressing emerging challenges in the space domain. The EU's commitment to defining space threats and developing strategies for resilience reflects a proactive approach that aligns with the evolving landscape of space operations and the imperative of Space Domain Awareness (SDA) on a global scale. This strategy also emphasizes the need to cultivate a shared understanding of space threats and encourages responsible behaviours in outer space—a pivotal aspect

of international collaboration in an era where space is central to both security and innovation.

Furthermore, the European Union's Space Strategy for Security and Defense recognizes the intrinsic connection between this strategic approach and the principles of Space Domain Awareness (SDA) and cybersecurity. As SDA encompasses the comprehensive understanding, management, and security of activities in outer space, the EU's strategy aligns perfectly with the objectives of fostering a shared understanding of space threats, enhancing the resilience and protection of space systems, and responding effectively to space threats. By prioritizing these aspects, the EU aims not only to secure its space assets but also to promote responsible behaviours in space, emphasizing the importance of international cooperation and information sharing in the realm of space cybersecurity. This integrated approach underscores the imperative of combining SDA principles with robust cybersecurity measures to ensure the safe and sustainable use of outer space, reinforcing the importance of securing the space frontier in an era marked by digital vulnerabilities and increasing reliance on space-based assets.

To sum up, both the American and European perspectives underscore the significance of SDA in addressing the evolving challenges and dynamics of outer space. Regardless of the vantage point, SDA serves as a pivotal framework for enhancing security, safety, economic stability, and environmental protection in an increasingly congested and contested space environment.

THE ARCHITECTURE OF OUTER SPACE

The concept of Space Domain Awareness (SDA) extends beyond the essential tasks of monitoring and understanding space threats (Erwin, 2022). It encompasses the intricate architecture of outer space itself, which serves as the backdrop for all space operations and activities. To fully grasp the significance of SDA, we must delve into the multi-layered nature of this space domain.

- Physical Space Environment: At its core, the space domain encompasses the vast and boundless expanse of outer space, extending far beyond the Earth's atmosphere. This domain is home to celestial bodies, cosmic phenomena, and the electromagnetic spectrum. Understanding the intricacies of this physical space environment is imperative for the safe and effective conduct of space operations. It involves considerations such as radiation exposure, microgravity effects, and the impact of cosmic debris on spacecraft.
- Orbital Regions: Within the space domain, orbital regions represent distinct zones with unique characteristics and applications. These regions include Low Earth Orbit (LEO), Medium Earth Orbit (MEO), Geosynchronous Orbit (GEO), and more. Each altitude offers specific advantages and challenges for satellite deployments. LEO, for instance, is ideal for Earth observation satellites, while GEO is preferred for communication satellites due to its geostationary nature. Recognizing the diversity of orbital regions is essential for planning and optimizing satellite missions.
- Satellites and Spacecraft: At the heart of the space architecture are the artificial objects—satellites and spacecraft—that fulfill a myriad of functions. These space assets enable global communication, Earth monitoring, navigation, scientific exploration, and national security. Satellites are strategically positioned within orbital regions to achieve specific objectives, making them central components of the space domain's architecture. The continued operation and protection of these assets are crucial for various societal and defense needs.
- Ground Infrastructure: While much of the focus is on objects in orbit, the architecture of outer space also extends to Earth's surface, where ground infrastructure plays a pivotal role. This infrastructure includes satellite ground stations, launch facilities, tracking and control centers,

and communication hubs. Ground infrastructure facilitates communication with spacecraft, data reception, satellite tracking, and control operations. It forms an integral part of the broader space architecture and must be considered in any comprehensive space strategy.

- Communication Networks: The functionality of space assets heavily relies on intricate communication networks that facilitate data transmission between space assets and Earth. These networks encompass various components, such as radio frequency links, ground stations, and data relay satellites. A robust and resilient communication network is vital for maintaining continuous contact with satellites and ensuring the timely exchange of data, which is essential for various applications, including navigation, weather forecasting, and national security.
- Industrial Space Sector: The space industry comprises a diverse array of organizations, both public and private, that are engaged in space exploration, research, development, manufacturing, and launch services. These entities contribute significantly to the development and maintenance of space assets. Their role in advancing space technology, fostering innovation, and expanding the space frontier cannot be overstated.

The architecture of outer space, with its intricate and interconnected layers, testifies to human ingenuity, technological advancement, and the potential for scientific discovery. It represents a delicate equilibrium between the exploitation of space for myriad purposes and the responsibility of protecting these vital assets. Understanding the multi-layered nature of the space domain is not only essential for effective space operations but also for addressing the evolving challenges and complexities of the modern space era.

As Space Domain Awareness continues to evolve, recognizing the nuances of this architecture becomes paramount. This understanding serves as the foundation for ensuring the security, sustainability, and responsible use of outer space—an essential endeavor as humanity explores and exploits the final frontier while safeguarding it for future generations.

Interconnected Systems and Services

The architecture of outer space comprises interconnected systems and services, each contributing to the functionality and utility of space assets.

Navigation and Positioning Systems: Satellite navigation systems, exemplified by the ubiquitous Global Positioning System (GPS), play an indispensable role in providing precise positioning and timing information. These systems have transcended mere navigational aids, permeating various aspects of modern life. They underpin logistics operations, enabling the efficient movement of goods and services, and serve as critical tools in disaster management, facilitating rapid response and relief efforts during crises.

Earth Observation Satellites: A constellation of Earth observation satellites, equipped with advanced remote sensing instruments, serves as Earth's vigilant guardians. These satellites capture a wealth of data critical for a range of applications. They provide the foundation for weather forecasting, supplying meteorologists with real-time information about atmospheric conditions. Moreover, they empower environmental scientists to monitor changes in ecosystems, enabling the assessment of climate trends, natural disasters, and biodiversity dynamics. Earth observation satellites are vital tools for agriculture, offering insights into crop health and enabling precision farming practices. Additionally, their imagery aids in disaster response by assessing the impact of events such as wildfires, floods, and earthquakes.

Communication Satellites: Geostationary communication satellites occupy a pivotal position in the space architecture, forming the backbone of global telecommunications. These satellites, stationed in geosynchronous orbit, facilitate voice, data, and video communication

services that span the globe. They enable seamless international connectivity, supporting everything from international business transactions and global news dissemination to personal communication and entertainment. The uninterrupted flow of information through these communication satellites has transformed the way the world communicates, collaborates, and connects.

National Security Satellites: Governments deploy a cadre of reconnaissance and surveillance satellites to safeguard national interests and security. These satellites serve as the eyes and ears of nations, monitoring potential threats and gathering vital intelligence. They provide essential data to military and defense organizations, offering critical insights into adversary activities and ensuring early warning capabilities. National security satellites are integral to maintaining sovereignty and readiness, assisting in crisis management, and supporting strategic defense operations.

Space Science and Exploration Missions: Scientific spacecraft and exploration missions exemplify humanity's insatiable curiosity and quest for knowledge. These missions venture beyond Earth's confines to explore the cosmos, conduct experiments, and expand our understanding of the universe. They encompass a wide range of objectives, from studying distant celestial bodies and their composition to unraveling the mysteries of cosmic phenomena. The data and insights gleaned from these missions transcend scientific discovery, inspiring awe and wonder while pushing the boundaries of human achievement.

The architecture of outer space serves as a testament to human ingenuity and technological advancement. It represents a harmonious balance between the pursuit of diverse purposes in space and the imperative to safeguard these invaluable assets (Young, et al., 2019; Chakraborty, et al., 2019; Rayner, 2017). As Space Domain Awareness (SDA) continues to evolve, acquiring a comprehensive understanding of this intricate architecture becomes paramount. It is through this understanding that we can ensure the security, sustainability, and responsible utilization of outer space—a tribute to humanity's capacity to explore and exploit the final frontier while steadfastly safeguarding it for the prosperity and enlightenment of future generations.

CYBERSECURITY CHALLENGES IN THE SPACE DOMAIN

In the context of the paradigmatic shift towards SDA, this section delves into the critical connection between cybersecurity and outer space. It emphasizes the growing importance of safeguarding space assets and systems from cyber threats—a concern as space operations become more integrated into daily life and national security strategies (Young, et al., 2019). SDA, at the forefront of comprehending and managing activities in outer space, accentuates the pressing issue of the intersection between space operations and cybersecurity. Just as SDA broadens our comprehension of the space environment, it underscores the imperative to secure this newfound domain from cyber threats.

The integration of space systems into global communication, navigation, defense, and economic infrastructure has introduced several key considerations at the intersection of cybersecurity and outer space:

- Space Assets Vulnerability: Satellites, space-based services, and ground infrastructure are susceptible to cyberattacks. Disrupting or compromising these assets can have far-reaching consequences, affecting national security and daily life, from GPS navigation to weather forecasting.
- Emerging Threat Landscape: The space domain has witnessed a proliferation of actors—both state and non-state—with the capacity and intent to conduct cyber operations in space. These threats encompass cyber espionage, data manipulation, and the potential to disable or control space systems.

- Data Security and Integrity: Ensuring the integrity and security of data transmitted to and from space assets is paramount. Unauthorized access or manipulation of data can distort situational awareness, potentially leading to misunderstandings or conflicts.
- Space Supply Chain Vulnerabilities: The space industry relies on a global supply chain, making it susceptible to cyber vulnerabilities at various development, manufacturing, and launch stages. Supply chain compromises can have cascading effects on space missions and services.

Addressing these challenges necessitates a concerted effort at the confluence of cybersecurity and outer space.

Key considerations encompass secure communication, data encryption, advanced threat detection, international collaboration, and security-by-design principles.

STARLINK SATELLITES AND SPACE DOMAIN AWARENESS

In May 2021, SpaceX, under the stewardship of Elon Musk, launched a cluster of 60 Starlink satellites into Low Earth Orbit (LEO), marking the commencement of a global satellite internet network. SpaceX's ambitious Starlink project exemplifies the expansion of the space architecture.

SpaceX's Starlink venture signifies a substantial augmentation of the space architecture, notably in LEO. With thousands of satellites in orbit and further launches planned, this mega-constellation aims to provide high-speed internet access to underserved regions worldwide. These satellites are integral components of the evolving space architecture.

As the number of active satellites and space objects escalates in LEO, space traffic management becomes increasingly complex. Operators must meticulously plan satellite trajectories to avoid collisions, minimize space debris generation, and ensure space environment safety and sustainability. This challenge underscores the importance of SDA (Skrzypiec, 2021).

To prevent collisions and ensure safe Starlink satellite operation and that of other space assets, coordination and monitoring are imperative. Space agencies, organizations, and private companies like SpaceX must rely on SDA systems to track precise satellite locations, predict their orbits, and adjust courses when potential collisions with other objects are detected.

Given that Starlink satellites constitute critical infrastructure, their cybersecurity is paramount. Malicious actors may endeavor to infiltrate satellite systems, disrupt communications, or interfere with satellite operations. This introduces a new dimension of cybersecurity concerns in the space domain.

SDA plays a pivotal role in averting space incidents by providing real-time data and forecasts about space object positions and movements. In the context of the Starlink project, SDA assists SpaceX in ensuring the safe deployment and operation of its extensive satellite constellation while also identifying potential cyber threats. Robust cybersecurity measures, including encryption, secure data transmission, and protection against unauthorized access, are indispensable for safeguarding against cyber threats. The integration of cybersecurity practices into SDA systems is vital for detecting and mitigating cyber risks.

SpaceX's Starlink endeavor underscores the necessity for international collaboration in managing the space architecture and addressing cybersecurity concerns. With satellites from various operators sharing the same orbital region, cooperation in data sharing, collision avoidance maneuvers, and cybersecurity information exchange is pivotal.

SpaceX's Starlink project serves as a contemporary example of the rapidly evolving outer space architecture with the deployment of mega-constellations. It underscores the critical role of Space Domain Awareness in ensuring the safe and responsible use of outer space while highlighting the growing importance of cybersecurity in shielding space assets from

malicious cyber threats. This real-life case illustrates how SDA principles, coupled with robust cybersecurity measures, are applied to navigate the complexities and security challenges of the modern space architecture.

CONCLUSION: SAFEGUARDING THE SPACE FRONTIER

In this new era of Space Domain Awareness, securing space assets and systems from cyber threats is integral to ensuring space security and resilience. The convergence of cybersecurity and outer space necessitates vigilance, innovation, and international collaboration to shield our space frontier from emerging digital risks. This paradigmatic shift elucidates that securing the final frontier is not solely a space mission—it is a cybersecurity imperative.

SDA, with its focus on tracking, monitoring, and predicting activities in outer space, stands as a pivotal framework for ensuring the safety and sustainability of space operations. However, the complexities inherent in modern space architectures, exemplified by initiatives such as SpaceX's Starlink project, underline the necessity of adapting SDA to the evolving landscape.

Cybersecurity, once confined to terrestrial concerns, now transcends Earth's boundaries. Satellite constellations, communication networks, and navigation systems are not immune to cyber threats. The malevolent manipulation of space assets can yield far-reaching consequences, affecting not only technological advancements but also national security and everyday life.

In response to this burgeoning challenge, the integration of robust cybersecurity measures into SDA systems assumes paramount importance. Elements such as encryption, secure communication protocols, and proactive threat detection mechanisms are essential components for safeguarding space assets against cyberattacks.

Moreover, international collaboration takes on heightened significance within the realm of space cybersecurity. The shared utilization of space mandates shared responsibilities. Nations, space agencies, and private space enterprises must collaboratively establish norms, rules, and principles to encourage responsible behavior in space and address emerging cyber threats.

As we contemplate the future of space exploration, resource utilization, and commercialization, we must acknowledge that preserving the space frontier is inseparable from our ability to protect it from cyber threats. The guardianship of outer space is not merely an obligation; it is a strategic imperative, vital for maintaining our presence beyond Earth and ensuring the sustainability of space endeavours.

In this new space age, where the final frontier signifies a realm of exploration, connectivity, innovation, and security, collaboration among space professionals, cybersecurity experts, and policymakers becomes indispensable. Collectively, we can secure the space frontier and embark on a future where the boundless potential of outer space remains within our grasp while shielding it from digital vulnerabilities.

The confluence of Space Domain Awareness and cybersecurity epitomizes the forefront of our endeavors to safeguard our space frontier—a frontier holding the key to scientific discovery, technological progress, and the resilience of our interconnected world. As we traverse this uncharted territory, one certainty prevails: securing the final frontier constitutes a mission transcending borders, disciplines, and generations. It is a mission defining our commitment to a safer and more prosperous future, both on Earth and among the stars.

BIBLIOGRAPHY

Anon. (2018) *Space Policy Directive-2, Streamlining Regulations on Commercial Use of Space.* https://trumpwhitehouse.archives.gov/presidential-actions/space-policy-directive-2-streamlining-regulations-commercial-use-space/ [Accessed 21st August 2022].

Anon. (2018) *Space Policy Directive-3, National Space Traffic Management Policy.* https://trumpwhitehouse.archives.gov/presidential-actions/space-policy-directive-3-national-space-traffic-management-policy/ [Accessed 21st August 2022].

Anon. (2019) *Space Policy Directive-4: Establishment of the United States Space Force.* https://trumpwhitehouse.archives.gov/presidential-actions/text-space-policy-directive-4-establishment-united-states-space-force/ [Accessed 21st August 2022].

Anon. (2020) *Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems.* https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/ [Accessed 21st August 2022].

Anon. (2021) *Memorandum on Space Policy Directive 7.* https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-7/ [Accessed 21st August 2022].

Association of Space Explorers. (2020) *Mitigation of Orbital Debris in the New Space Age.* https://www.space-explorers.org/resources/Documents/Mitigation%20of%20Orbital%20Debris%20in%20the%20New%20Space%20Age-ASE%202020.pdf [Accessed 7th May 2023].

Azoulay, T., Federico, G. & Qedar, R. (2021) Modular Satellite Manufacturing to Enhance Space Assets Resiliency. *Joint Air & Space Power Conference 2021.* Kalkar, Germany.

Barrie, J., Zawdie, G. & João , E. (2017) Leveraging triple helix and system intermediaries to enhance effectiveness of protected spaces and strategic niche management for transitioning to circular economy. *International Journal of Technology Management & Sustainable Development*, 16(1), 25 - 47.

Botezatu, U.-E. (2023) Attempted Cyber Security of Systems and Operations in Outer Space: an Overview of Space-based Vulnerabilities. *Romanian Cyber Security Journal*. 5 (1), 67-76.

Chakraborty, N., Agrawal, S. & Chauhan, P. (2019) Blockchain technology and applications in the space industry: A review. *Acta Astronautica*. 161, 96-114.

Chertoff, M. (2018) Space security and the Global Counterterrorism Forum's Space Security Initiative. *Journal of Space Law*. 42(1), 65-81.

Dennerley, J. (2016) Emerging space nations and the development of international regulatory regimes. *Space Policy.* 35, 27-32.

Di Mare, A. (2021) The Role of Space Domain Awareness: Space Asset Resilience thru Protection. *Joint Air & Space Power Conference.* Kalkar, Germany,

Dodge, M. & Kitchin, R. (2007) The automatic management of drivers and driving spaces. *Geoforum*. 38(2), 264-275.

Erwin, S. (2019) *Air Force: SSA is no more; it's 'Space Domain Awareness'.* https://spacenews.com/air-force-ssa-is-no-more-its-space-domain-awareness/ [Accessed 23rd September 2023].

Erwin, S. (2022) *Space domain awareness: A secret weapon against shadowy threats in orbit.* https://spacenews.com/space-domain-awareness-a-secret-weapon-against-shadowy-threats-in-orbit/ [Accessed 23rd September 2023].

EU External Action Service. (2023) *EU Space Strategy for Security and Defence.* https://www.eeas.europa.eu/eeas/eu-space-strategy-security-and-defence-0_en [Accessed 23rd September 2023].

European Space Agency. (2020) *The current state of space debris.* https://www.esa.int/Space_Safety/Space_Debris/The_current_state_of_space_debris [Accessed 7th May 2023].

European Space Agency. (2023) *Copernicus EMS: Earthquake in Turkey.* [Online] Available at: https://emergency.copernicus.eu/EMSN011/earthquake-turkey

European Space Agency. (2023) *How Satellites are Helping to Respond to Natural Disasters.* [Online] Available at: https://www.esa.int/Applications/Observing_the_Earth/Copernicus/Sentinel-1/How_satellites_are_helping_to_respond_to_natural_disasters

Finkleman, D. (2010) Chapter 12 - Space situational awareness and space traffic management standardization. Em: *Space Safety Regulations and Standards.* s.l.:s.n., pp. 137-145.

Fourati, F. & Alouini, M. (2021) Artificial intelligence for satellite communication: A review. *Intelligent and Converged Networks*, 2(3), pp. 213-243.

Froehlich, A., Seffinga, V. & Qiu, R. (2020) The Development of the Mandates of the Committee on the Peaceful Uses of Outer Space (COPUOS) and the Conference on Disarmament (CD) and the Collaboration Between the Forums. Em: T*he United Nations and Space Security. Studies in Space Policy, vol 21*. s.l.:Springer.

Fruhlinger, J. (2022) *Stuxnet explained: The first known cyberweapon.* https://www.csoonline.com/article/3218104/stuxnet-explained-the-first-known-cyberweapon.html

Gargalakos, M. (2021) The role of unmanned aerial vehicles in military communications: application scenarios, current trends, and beyond. *The Journal of Defense Modeling and Simulation*. doi: 10.1177/15485129211031

Georgescu, A. et al. (2016) Critical Infrastructure Dependency on Space Systems. *"Mircea cel Batran" Naval Academy Scientific Bulletin, XIX(1),* 398-404.

Hall, R. D. (2016) Cybersecurity in outer space: A new strategic frontier. *Georgetown Journal of International Affairs.* 17(2), 63-70.

Harrington, J. & Tsui, C. (2017) Securing space systems from cyber threats: A strategic approach. *The Journal of Strategic Studies.* 40(5-6), 669-699.

Hays, P. (2020) International Space Security Setting: An Introduction. Em: Handbook of Space Security. *Springer,* Cham.

Johnson, N. L. (2018) Securing the space commons: Resilience and strategic competition in the space domain. *Security Studies,* 27(3), 529-560.

Kolovos, A. (2023) Strengthening Links Between European Union Space and Defence: Adopting a Combined Approach. *Space Policy*, 63.

Lyall, F. & Scott, C. J. (2018) The Weaponisation of Space: Risks, Challenges and Opportunities for International Security. T*he Political Quarterly*, 89(4). 595-605.

Mackowski, D., Bai, Y. & Ouyang, Y. (2015) Parking Space Management via Dynamic Performance-based Pricing. *Transportation Research Procedia*. 7, 170-191.

Murdoch, S. (2018) The use of blockchain in space governance: An assessment of benefits and challenges. *Acta Astronautica*. 147, 243-250.

Nitoslawski , S., Galle, N. & Van Den Bosch, C. (2019) Smarter ecosystems for smarter cities? A review of trends, technologies, and turning points for smart urban forestry. *Sustainable Cities and Society.* 51.

Polkowska, M. (2020) Space diplomacy – future perspective. *Humanities and Social Sciences*, 27(3), 121-128.

Prantl, J. & Goh, E. (2022) Rethinking strategy and statecraft for the twenty-first century of complexity: a case for strategic diplomacy. *International Affairs | Oxford Academic.* 98(2).

Rayner, G. (2017) The Use of Autonomous Systems in Outer Space: Legal and Ethical Challenges. *Journal of Conflict & Security Law*. 22(3), 383-402.

Skrzypiec, P. J. (2021) Satellite Image Processing with Convolutional Neural Networks - A Review. *Remote Sensing*. 13(1), 1-26.

Tadjdeh, Y. (2021) *U.S. Strengthening Space Domain Awareness.* https://www.nationaldefensemagazine.org/articles/2021/7/30/us-strengthening--space-domain-awareness [Accessed 23rd September 2023].

US Space Force Command. (2023) Space Domain Awareness & Combat Power. https://www.ssc.spaceforce.mil/Program-Executive-Offices/Space-Domain-Awareness-Combat-Power [Accessed 23rd September 2023].

World Economic Forum. (2022) The Global Risks Report 2022. *Switzerland: World Economic Forum*. Geneva.

Young, R. et al. (2019) Artificial intelligence and machine learning in space weather. *Space Weather*. 17(12), 1682-1703.

This is an open access article distributed under the terms and conditions of the Creative Commons Attribution-NonCommercial 4.0 International License.