Military Cyber Affairs

Volume 7
Issue 1 *HammerCon 2024 Issue*

Article 2

May 2024

# Securing the Void: Assessing the Dynamic Threat Landscape of Space

Brianna Bace
*University at Albany*, bbace@albany.edu

Dr. Unal Tatar

# Securing the Void: Assessing the Dynamic Threat Landscape of Space

## Cover Page Footnote

This publication was supported by Award Number SA10012022020481 from the Griffiss Institute for VICEROY program. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of the sponsor.

# Securing the Void: Assessing the Dynamic Threat Landscape of Space

Brianna Bace and Dr. Unal Tatar

## Introduction

Outer space is a strategic and multifaceted domain that enables many of the essential functions a state must perform to safeguard the well-being of its citizens and maintain its competitiveness and resilience on the international stage. Space systems and assets are utilized by all critical infrastructure sectors and represent a single point of failure for many industries (Falco, 2018). Due to the range of uses and services that the space sector provides, the sector itself is considered a crossroads for political, strategic, military, and economic interests (Carlo, 2021). From a defense perspective, the U.S. military and intelligence community relies heavily on communication, reconnaissance, navigation, and weather satellite networks to meet national security objectives and carry out military operations and intelligence gathering.

Nation-states have acknowledged the capacity to disrupt their adversaries by targeting space systems and assets. In Russia's cyberattack on ViaSat's KA-SAT satellite broadband network at the start of the 2022 invasion of Ukraine, Russian threat actors were able to significantly impair military and police communication capabilities in Ukraine as they were suffering a ground military invasion (O'Neill, 2022). Given the substantial reliance on space systems and the interconnectedness of critical infrastructure, an attack on the space sector can trigger severe immediate consequences, as well as considerable cascading effects, potentially necessitating long-term recovery efforts.

The aim of this paper is to explore the current threat landscape of the space sector, particularly cyber threats and risks. This domain currently faces numerous threats, both natural and man-made. Some of these threats are unique to Space, while others are typical for any military asset, such as physical damage from a kinetic attack. Since space operations are largely cyber-enabled, the space sector is also vulnerable to cyber threats. The number of threat actors operating in this domain is also increasing, exhibiting significant variation in motivation and level of sophistication.

Additionally, in this study, we will focus on the repercussions of dual-use technology and the commercialization of Space. The employment of dual-use technology, or technology used for both military and civilian purposes, has resulted in several difficulties for the space sector. Since this technology has diluted the line between military and non-military, it is more challenging to define key terminology, ascertain if a state's actions are civil or military-based, and establish means of verification and regulation (Carlo, 2021). The commercialization of Space and growing usage of commercial off-the-shelf components have also changed the threat landscape of the space sector as a lower barrier to entry into this domain. This change has resulted in a more complex supply chain and a greater number of potential adversaries.

This paper's timing is notably relevant, coinciding with current discussions and legislative movements in the U.S. and abroad to recognize space as critical infrastructure. The bipartisan Space Infrastructure Act of 2023, introduced into the 118th Congress, calls for the Secretary of Homeland Security to issue guidance for designating space as a critical infrastructure sector (Space Infrastructure Act, 2023). Simultaneously, it corresponds with the European Union's recent Critical Entities Resilience (CER) Directive, which, among other things, acknowledges space as a critical sector (CER Directive, 2022).

The structure of this paper is as follows: Section 2 presents an overview of space system components, encompassing those within the Space, ground, link, and user segments, alongside a discussion of the primary services facilitated by these systems. Section 3 delves into the man-made and naturally occurring threats to the space sector and reviews the predominant threat actor types operating within this domain. Section 4 discusses the changing threat landscape of the space sector, with particular attention to the implications of dual-use infrastructure and commercial off-the-shelf components on the security and resiliency of space infrastructure. Section 5 offers an outline of legal efforts, international initiatives, published guidelines, and expert recommendations devised to combat the growing vulnerabilities within this domain. Section 6 is the conclusion.

## Space System Segments and Services

In this section, we review the four main segments of the space sector and examples of the assets that fall into each category. We also discuss some of the major services provided by space systems.

### Space Sector Segments

Space sector infrastructure typically falls into one of four segments: space, ground, link, and user (NATO, 2022b). The space segment consists of assets in Space, such as satellites, space probes, and both crewed and uncrewed spacecrafts. This segment has also been referred to as the “orbital segment” as spacecrafts follow an orbital path in space, including Geosynchronous Earth orbit (GEO), Highly Elliptical Orbit (HEO), Medium Earth Orbit (MEO), and Low Earth Orbit (LEO) (U.S. Space Force, 2022). Space vehicles or satellites consist of the bus, otherwise known as the control and processing systems needed to power and fly the satellite, and the payload, which is the equipment, instruments, and data needed to carry out the mission (Scholl & Suloway, 2022; Nguyen and Nguyen, 2020).

The ground segment refers to all terrestrial-based systems, equipment, and facilities (U.S. Space Force, 2022). This includes ground station terminals necessary for data handling and routing, as well as mission operation centers and payload control centers that communicate with satellites (Lightman et al., 2022).

The link segment consists of the electromagnetic signals traveling between the space and ground segments. These links include uplinks, which allow for the ground station to communicate with the spacecraft or satellite, and downlinks, which link the space asset down to the appropriate ground station or user (Manulis et al., 2021). These signals can also travel from space-to-space assets and from ground-to-ground stations.

The final segment of the space sector is the user segment, which relates to the use of space systems. This segment is made up of the consumers of space data "such as Global Positioning Systems (GPS) receivers, satellite phone users, satellite Television receivers, vehicles, 5G users, industrial systems, mobile devices, and aircraft" (Scholl & Suloway, 2022, p.13). The space, ground, and link segments work together for the successful execution of operations in the space domain, while the user segment demonstrates the multitude of applications of space systems.

## Space Sector Services

The vast array of space systems in operation today enables the delivery of numerous essential services catering to both civilian and military needs (Bace et al., 2024). For example, Global Navigation Satellite Systems (GNSSs), like the U.S.'s Global Positioning System (GPS) or the European Union's GALILEO system, are the primary providers of Positioning, Navigation, And Timing (PNT) data (Georgescu et al., 2018). This data is used by different sectors and industries to perform basic but vital operations, such as the financial sector's ability to timestamp transactions and the aviation industry's capacity to monitor aircraft and prevent collisions.

Weather forecasting and earth observation are also made possible via satellites, which are equipped with various sensors to collect data on Earth's atmosphere, oceans, and surface. This information supports timely decision-making for both civilian and military purposes. Meteorologists can also use this data to develop long-term climate trends, and predict earthquakes, severe storms, and flooding. In the event of a natural disaster, remote-sensing satellites play a crucial role in search and rescue operations and the assessment of damage after the incident (National Coordination Office, 2021).

A third use of space infrastructure is its enablement of communication and connectivity. Space systems have played a vital role in the expansion of high-speed internet, and the provision of satellite communications, and television and radio broadcasting (Georgescu et al., 2018). Satellites have also been integrated into existing telecommunications infrastructure to enhance network coverage and capabilities (European Space Agency, n.d.-b). Utilizing space-based technologies can enhance the cost-effectiveness of telecommunications by minimizing infrastructure expenses. Deploying satellites is often more economical and straightforward compared to laying cables or constructing ground facilities, especially in remote regions lacking existing infrastructure or where it has been damaged (UNOOSA, n.d.; Hassan et al., 2020; Portillo et al., 2021).

Finally, space systems play an important role in national security and defense through intelligence gathering and missile warning systems. Another use of satellites is their ability to collect Signals Intelligence (SIGINT), Imagery Intelligence (IMINT), and Geospatial Intelligence (GEOINT), which is used by the military and intelligence community to advance U.S. national security interests and make operational and tactical decisions. Military early warning and reconnaissance satellites coupled with space-based and terrestrial missile warning sensors also provide further critical information (U.S. Space Force, 2022). These sensors are used to "provide launch detection, tracking, tactical warning, and attack assessment information to operational command centers" (U.S. Space Force, 2022, p.20). The U.S. Army Space and Missile Defense Command (SMDC) and the Defense Intelligence Agency (DIA) are just two of the U.S. defense and intelligence agencies involved in the space sector for the purposes of national security.

## Threats and Threat Actors

In this section, we examine various categories of threats confronting the space sector and discuss the array of threat actors in this domain.

### Threats

There is no shortage of threats against the space sector. As a sector with infrastructure on the ground and in orbit that relies on both electromagnetic signals to communicate and cyber-based systems to function, the sector is subject to many different types of threats. Some of these attacks are unique to space systems. This is true for the first category of threat: natural hazards. When operating in Space, certain phenomena must be considered, including the presence of meteoroids and the impact of space weather. Meteoroids pose a threat to space missions as they can collide and damage space assets, impacting their functionality (Falco & Boschetti, 2021). These collisions can also add to the space debris issue, which is an increasingly worsening problem where defunct space assets and fragments of derelict space vehicles remain in orbit for decades, posing an extended threat of collision to new missions. Space weather refers to the environmental threat of operating in Space. This hazard is primarily caused by the Sun, which can generate bursts of electromagnetic radiation (flares) or eruptions of material (coronal mass ejections, CMEs) that can not only impact the integrity of space assets in orbit but cause serious effects on ground infrastructure (Falco & Boschetti, 2021).

The next category of threats are physical attacks through kinetic and non-kinetic means. Kinetic physical attacks are attempts to cause physical damage to a space asset, either on Earth or in orbit. For example, ground stations could be targeted by close-range explosives like missiles or through a bombing, while satellites can be damaged or destroyed using Anti-Satellite Weapons (ASATs), which are launched either directly or co-orbitally (Amenabar, 2022). ASATs have yet to be utilized in warfare, but that trend may be changing. In February 2024, the White House announced that Russia was developing a new ASAT, with some American spy agencies worried that the weapon would be nuclear (Sanger & Barnes, 2024). Non-kinetic physical weapons cause physical damage without making contact with the asset. For example, directed energy weapons (DEW), such as lasers and High-Powered Microwaves (HPM), can cause thermal damage to a target through the rapid absorption of energy (Garino & Gibson, 2009). HPM weapons may also be used to damage electrical components and processors and then corrupt stored data (Harrison et al., 2022).

Electromagnetic attacks are a very common threat to the space sector. These attacks largely impact the link segment as attackers use these methods to attempt to damage the means by which space systems transmit and receive data. Electromagnetic attacks include jamming and spoofing. Jamming occurs when an attacker overpowers a Radio Frequency (RF) signal for a particular frequency band, temporarily disrupting communication between space assets (Rajagopalan, 2019; Manulis et al., 2021). Jamming technology is inexpensive and requires little technical competency to launch an attack, making it a growing concern for national security (Velkovsky et al., 2019). A spoofing attack occurs when an attacker mimics a legitimate RF signal in order to trick their target into locking into a fake signal and collecting false data (Way, 2019). Attackers can use this method to take control of a satellite by spoofing the command-and-control uplink (Way, 2019).

The final threat category facing space infrastructure is cyberattacks, given the extensive use of cyber systems and software within the space sector. Unlike electronic attacks that target RF signals, cyberattacks are used to intercept and corrupt data and disrupt and destroy the systems that use, transmit, and control this data (Way, 2019; Falco & Boschetti, 2021). The cyber threats category includes signal hijacking, denial-of-service, malicious code injection, data corruption, modification, and interception, among many others (Falco & Boschetti, 2021). Attackers have also been known to launch social engineering attacks on employees in the space sector with the goal of gaining access to satellite control systems (Falco, 2018). Cyberattacks, though capable of causing physical damage to an asset, are typically employed “to subvert the integrity of political, social, and economic systems” (Serra, 2021, p.91). This is particularly true for the space sector, whose job it is to provide PNT and GPS data used by other sectors and industries. If the space sector failed to provide this data, it would result in a loss of trust for both the space sector itself and the sectors reliant on this information to provide essential services. While attackers would need to understand the systems they are targeting, the cyberattack itself does not require significant resources or budgets to be executed (Falco & Boschetti, 2021).

### Threat Actors

Although state actors have historically dominated the space sector, the entry of numerous commercial and private companies into this domain, coupled with the reduced barriers to launching electronic and cyberattacks, has led potentially to a broader spectrum of potential adversaries for the space sector (Meyer, 2016). Threat actors have varying levels of sophistication, differing funding levels, and diverse motivations for launching attacks on space assets. More sophisticated threat actors include nation-states, state-sponsored attackers, and organized crime groups (Garrett, 2023). Nation-state actors and those operating at a state's direction often possess considerable resources and advanced cyber capabilities. The same can be said for cybercriminal organizations. Yet, where nation-state and state-sponsored actors are likely to target space assets for espionage, sabotage, or military purposes, the main motivation of a cybercriminal group is financial gain, typically through extortion or the sale of stolen data (Lopez, 2022).

Threat actors with less sophistication and more moderate resources include terrorist groups and non-state actors like hacktivists and lone malicious attackers. Terrorist groups may attempt to create a high-profile disruption to amplify their message or promote violence. For example, the bombing of a ground facility would kill analysts and technicians, stop data transmission, and prevent control of satellites (Garino & Gibson, 2009). Hacktivist individuals and groups may attempt to launch attacks for ideological reasons. Other malicious attackers can have variable levels of sophistication and resources, looking to disrupt space operations for purposes of revenge, financial gain, or just to show that they can. In sum, the presence of these numerous threat actors emphasizes the extensive threat landscape that the space domain must contend with.

## Changing Threat Landscape

In this section, we discuss two major reasons that have led to the changing threat landscape of space infrastructure: the utilization of dual-use technology and the increasing commercialization of the space domain.

### Dual-Use Technology

The distinction between civil and military is being blurred due to the proliferation of dual-use systems and components, which serve both peaceful and military objectives with equal efficiency. According to the U.S. Department of Defense, dual-use technology is defined as "a technology that has both military utility and sufficient commercial potential to support a viable industrial base" (Prazak, 2021, p.398). Essentially, the services that these technologies facilitate can be utilized for both civilian and military needs. When it comes to the military application of space assets, is generally understood that this usage will remain compliant with the "peaceful purposes" principle found in the Outer Space Treaty (Ortega, 2023). One example of dual-use space technology is GNSS satellites that enable a citizen to receive navigation data on their cell phone as well as provide situational awareness to soldiers on the battlefield (Serra, 2021). Another example would be how civilians use satellite communications (SATCOM) for things like television broadcasting or internet connectivity, while the military or intelligence community would utilize SATCOM for secure communication channels and intelligence collection. Considering that dual-use technology can serve both civilian and military functions, this infrastructure has the potential to bring increased investment to the sector and expand the market for space products and services to a broader group of customers (New Space Economy, n.d.).

The expansion of this technology also carries negative implications for the space sector. First, the presence of dual-use space infrastructure creates a setting in which the targeting of military infrastructure by an adversary yields repercussions that, whether deliberate or unintended, generate a ripple effect on civilian populations. Under International Humanitarian Law (IHL), civilian assets cannot be targeted by attacks, but assets that are used for military objectives can be (with certain conditions) (ICRC, n.d.; Ortega, 2023). Since there is no such thing as a dual-use object in IHL, arguably, any dual-use technology actively being used for a military function is targetable (Ortega, 2023). This issue will only worsen as military officials have declared their support for increasing the government's collaboration with the commercial space industry in the form of greater data sharing and interoperability (Erwin, 2023). In April 2024, the Department of Defense released its first ever Commercial Space Integration Strategy which "seeks to align the Department's efforts and drive more effective integration of commercial space solutions into national security space architectures" (U.S. Department of Defense, 2024, para. 1). In the near future, the U.S. Space Force is also set to release a strategy that outlines how they plan to integrate commercial space sector capabilities into Space Force missions (Easley, 2024).

A second complication arising from dual-use technology is the effect its operational ambiguity has on the security of the space domain. Without a clear line between civil and military, it is progressively challenging to establish definitions for key terminology (Carlo, 2021). This creates a dominion effect, making it harder to create adequate definitions for international agreements and laws, and hinders the development of multilateral arms control agreements (Carlo, 2021). All of this discourages cooperation and fosters mistrust, increasing tensions amongst states operating in this domain. The U.S. government has publicly stated that it believes that China relies on strategic ambiguity to achieve its objectives (Office of the Secretary of Defense, 2020).

The operational ambiguity of dual-use technologies also means that intent and motivation are harder to determine. The verification and monitoring of state behavior in space is already a difficult task, with most of the effort focused on tracking the presence of space debris and avoiding collisions, not on verifying state assets (Meyer, 2016). This makes ensuring that states remain compliant with current agreements and regulations exceedingly complex. The presence of dual-use technology exacerbates this issue as the duality of these systems makes it hard to know with a high level of certainty if a state's actions are civil or military-based.

After all, while dual-use technology is not, in essence, a weapon, it is possible for it to be used for the weaponization of space (Prazak, 2021). For example, dual-use co-orbital systems tasked with the removal of space debris are equipped with nets, harpoons, magnets, and robotic arms to accomplish their task. Yet, this equipment could also be utilized to damage, degrade, and destroy satellites (United States, 2021). Furthermore, any "satellite with maneuvering capabilities, if launched into the proper orbit, could technically be used to attempt to collide with another satellite, even if not optimized to do so" (United States, 2021, p.4). Considering the importance of the space domain as a vital sector for defense and security, it is not inconceivable that a state would pursue dominance through the development of a military program. Therefore, any uncertainty surrounding motivations fosters mistrust and stimulates the escalation of conflict.

## Commercialization of Space

Another cause of increasing vulnerability in the space sector is the growing involvement of commercial entities in space-related activities. SpaceX, Blue Origin, Planet Labs, OneWeb, and Rocket Lab are just a few of the commercial space companies making a name for themselves in this new frontier. Made In Space Inc., Maxar Technologies, and Axiom Space are three of the companies from the past few years that have received multi-million-dollar contracts from the National Aeronautics and Space Administration (NASA) (Weinzierl & Sarang, 2021). According to a report by the Space Foundation, the global space economy reached 546 billion in 2022, with commercial revenue constituting 78% of the total space economy (Space Foundation Editorial Team, 2023). This growing commercialization signals the beginning of Space 4.0, the fourth industrial revolution in the space domain, also marked by greater technological innovation, global collaboration, and a broadened range of participants engaging in space activities (Serra, 2021; European Space Agency, n.d.-a).

Part of the growing commercialization of space is the increase of Commercial Off-The-Shelf (COTS) components. The term "commercial off the shelf" refers to the fact that they were not explicitly designed for space operations but were designed by the vendor pursuant to market forces (Pellish, 2018). These parts are largely considered to be cost-effective and innovative solutions for developing space assets and launching space missions. For example, low-cost satellites called "CubeSats" require less technical sophistication and limited resources as they are made largely from COTS technology (Falco, 2018). It should be noted that COTS technology refers to a broad population of parts that can vary greatly by reliability based on radiation robustness and expected lifetime (Hodson et al., 2022). Therefore, while it is not fair to make generalizations about the quality of all COTS parts, it is certainly possible that some COTS components are of a lower grade than others (Hodson et al., 2022).

The increased usage of COTS components introduces vulnerability in the space sector. First, due to their wide distribution, a threat actor, such as a hacker, could get ahold of COTS software or hardware and analyze it with the goal of exploiting any vulnerabilities they find when the technology is in use. Second, threat actors may intentionally plant code with back-doors to open-source technology and COTS software, with the intent of leveraging the flaw at a later date (Falco, 2018). Third, this technology requires that users maintain regular patching and software updating regimes to prevent the presence of exploitable security flaws (Falco, 2018; Nussbaum and Berg, 2020). Since this kind of cyber risk management is difficult for users in terrestrial environments, it is unlikely that it will be any easy when dealing with assets in orbit (Nussbaum and Berg, 2020). Again, while COTS technology is important for the advanced innovation of the space industry, it introduces significant risk, particularly in the digital ecosystem.

The growth of commercial space activity and the availability of COTS technology have significantly lowered the barrier of entry to operate in the space domain. In particular, these changes have lowered technical and financial thresholds, increasing the number of objects being launched into orbit (Serra, 2021). The decreasing cost of building and launching satellites adds to the existing problem of space debris. The U.S. government currently tracks more than 20,000 pieces of space debris, with NASA's Orbital Debris Program Office created to track and mitigate the risk this debris has (Mukherjee, 2021). The more space assets launched into orbit, the greater the probability of two assets colliding, resulting in their degradation or destruction. These collisions then result in further space debris and the potential disruption of services based on that asset's purpose.

The final vulnerability worsened by greater commercial activity in the space domain relates to supply chain security. With the increasing number of vendors and manufacturers in the space sector, supply chains for space systems and assets have become increasingly complex. Constructing a satellite involves procuring components from various manufacturers that specialize in specific parts or services, some of whom may further subcontract components from additional companies (Falco, 2018). This intricacy has only escalated in recent years. Decreased visibility into the supply chains of space assets makes it difficult to investigate and audit suppliers properly, significantly heightening the risk of threat actors successfully installing software vulnerabilities like backdoors in encryption (Bailey et al., 2019). Though software can be patched and upgraded after launch, malicious actors could exploit this weakness in the software, potentially giving them the ability to disrupt the asset's functions or take over command and control. In terms of hardware issues, remedying these problems becomes extremely challenging once a spacecraft has been put in orbit (Scholl & Suloway, 2022). When dealing with technologies characterized by their high precision and volatility, one flaw can result in serious damage (Serra, 2021).

## Efforts to Strengthen the Space Sector

In this section, we provide an overview of legal efforts, international initiatives, published guidelines, and expert recommendations devised to combat the growing vulnerabilities within this domain.

## U.S. and Ally Legal Efforts

The criticality of the space sector, combined with its growing and evolving threat landscape, means that meaningful strides will need to be made to ensure the domain's security and resiliency. Last year, the bipartisan Space Infrastructure Act of 2023 was introduced into the 118th Congress. If passed, the bill would direct the Secretary of Homeland Security to issue guidance for designating space systems, services, and technology as critical infrastructure (Space Infrastructure Act, 2023). The designation as "critical infrastructure sector" carries many important benefits, including increased funding for security enhancements and disaster preparedness, as well as greater inter-sector collaboration and information sharing. This designation would also send an important signal to the public that the protection of space-dependent services is a priority for the government. It may also work to deter adversaries by signaling that the sector is well-defended and any attack would be met with significant consequences. The European Union is slightly ahead of the U.S. in this regard. Their recent Critical Entities Resilience (CER) Directive, issued in January 2023, acknowledges space as a critical sector and mandates that EU Member States identify critical entities in all 11 critical sectors (CER Directive, 2022).

The United States Space Priorities Framework has previously acknowledged how "space systems are an essential component of U.S. critical infrastructure [because they] directly provide important services and enable other critical infrastructure sectors and industries" (The White House, 2021, para. 16). Furthermore, the Cybersecurity and Infrastructure Security Agency formed the Space Systems Critical Infrastructure Working Group, signaling the U.S. government's commitment to space security.

## NATO Initiatives

Owing to the critical role space plays in the political, strategic, military, and economic realms, it is also a focal point in international relations and collaboration (Carlo, 2021). The North Atlantic Treaty Organization (NATO) has declared space to be an operational domain and has made efforts to bolster space domain awareness, deterrence, and resilience (NATO, 2022b). NATO's 2019 Space Policy also consists of seven principles and tenets that members are expected to adhere to, three of which come directly from the Outer Space Treaty, which entered into force in 1967. NATO reinforces that the free access, exploration, and use of outer space for peaceful purposes is in the common interest of all nations.; that Space is not subject to national appropriation by claim of sovereignty, and that allies will retain jurisdiction and control over their objects in space (NATO, 2022b).

NATO's 2022 Strategic Concept stated unequivocally that secure use of and access to space was vital to maintaining their deterrence and defense posture (NATO, 2022a). It is the goal of NATO to "enhance [their] ability to operate effectively in space and cyberspace to prevent, detect, counter, and respond to the full spectrum of threats, using all available tools" (NATO, 2022a, p. 7). Reflecting this position, NATO announced in July 2023 that it was launching the NATO Space Centre of Excellence, which will "act as a focal point for Space-related education and training, analysis and lessons learned, concept development and experimentation, as well as doctrine development and standards" (NATO, 2023, para. 3). The Center hopes to act as a bridge between NATO and all relevant national and international Space organizations, including the commercial sector and academia (NATO, 2023). The U.S. Space Command's Joint Commercial Operations cell, formerly named the Joint Task Force-Space Defense Commercial Operations cell, is another initiative where Allies, partners, academia, and industry work together to provide timely and accurate identification, analysis, and warning of potential counterspace activity (Bonnette, 2023). Collectively, these endeavors showcase a commitment to safeguarding the space domain and the maintenance of an open dialogue in this field. Enhanced collaboration and communication prove invaluable in addressing persistent threats, minimizing uncertainty, and articulating intentions unequivocally.

## NIST and NASA Guidelines

When discussing the increased security of Space, it is important to note that most conversations include a discussion of cybersecurity. This overlap is due to the close relationship between activities in both realms, particularly dealing with communication mechanisms and the use of information technology, exemplified by COTS components. The majority of space communications take place in cyberspace, including those that utilize the electromagnetic spectrum, which is part of the infrastructure of cyberspace (Housen-Couriel, 2023). Naturally, whenever software is being employed in the ground and space segments, the potential for cyber threats arises. For this reason, many experts see the security of the space domain to be closely interconnected, if not entirely reliant on the cybersecurity practices of those operating in this field (Falco, 2018; Nussbaum and Berg, 2020; Housen-Couriel, 2023; Unal, 2019).

Consequently, the National Institute of Standards and Technology (NIST) has released several pieces of guidance to combat cybersecurity threats and vulnerabilities in the space domain. NIST Interagency Report (IR) 8270, NIST IR 8323, NIST IR 8401, and NIST IR 8441 all apply the NIST Cybersecurity Framework to different facets of the space domain, including commercial satellite operations, the use of PNT services, the satellite ground segment, and hybrid satellite networks, respectively (Scholl & Suloway, 2022; Bartock et al., 2023; Lightman et al., 2022; McCarthy et al., 2023). With this guidance, space domain operators receive an introduction to cybersecurity and the risk management process and are shown how to assess their current security posture, which can help them in their future decision-making. NASA has also released the first iteration of its Space Security Best Practices Guide (BPG) to assist public and private sector participants in the space realm in bolstering the security of space-related missions, programs, or projects (Dooren, 2023). NASA's BPG uses both NIST security controls and

MITRE ATT&CK Framework to produce "guidance on mission security implementation in the form of principles coupled with applicable controls that cover both the space vehicle and the ground segment" (NASA, 2023, p.4). Similar to MITRE's ATT&CK framework, The Aerospace Corporation created the Space Attack Research and Tactic Analysis (SPARTA) matrix for space system tactics, techniques, and procedures (TTP). SPARTA is an analysis tool for space professionals, providing them with unclassified information on potential spacecraft vulnerabilities, both through cyber and conventional counterspace methods (Aerospace Corporation, 2024). With this guidance, vendors, manufacturers, organizations, and other space operators can effectively confront the expanding range of threats and threat actors while also addressing vulnerabilities stemming from the use of COTS technology, like supply chain security risks.

### Expert Recommendations

Numerous researchers have also contributed recommendations regarding space sector cybersecurity. Falco (2018) supports a number of mitigation techniques like access control management, developing specialized security workforces, and fostering a security culture. Research Housen-Couriel (2023) strongly supports information sharing in regard to cyber threats in the space domain, as the exchange of operational data can help in risk mitigation and the establishment and maintenance of trust. Fortunately, the Space Information Sharing and Analysis Center (Space ISAC) was launched in 2019. The Space ISAC regularly sends alerts and advisories to members and partners detailing adversary activity (Space ISAC, n.d.). Georgescu et al. (2020) recommends that NATO create a Space Cyber Range, either separately or in conjunction with the Cyber Range in the Tallinn Center for Excellence on Cyber. The Range would give NATO member states and militaries the ability to build and test scenarios for cyberattacks, but with the added specificities of space system hardware and connections. This allows for "adequate training and the identification and mitigation of risks, vulnerabilities and threats" (Georgescu et al., 2020, p.5). Finally, Nussbaum and Berg (2020) highlight the similarities between satellites and the Internet of Things (IoT), particularly for their reliance on COTS components. They believe that recognizing that "more and more devices [are] addressable in Internet Protocol space" is critical in "understanding the trajectory of cybersecurity concerns in space" (p.97). The correlation between space systems and cyber systems cannot be overstated, and any effort to secure the space domain necessitates a comprehensive consideration of the cyber threat landscape alongside broader threat assessments.

## Conclusion

Incipient changes in the space domain have brought about significant strides in innovation, interconnectivity, and collaboration. Space has evolved beyond being a domain solely for exploration; it now serves as a playing field for researchers, entrepreneurs, and militaries alike. This additional human activity promises to further transform the space domain and augment the array of space-based capabilities relied upon for the delivery of essential services. The expansion of threats and threat actors, including the vulnerabilities from greater utilization of dual-use technology and commercial off-the-shelf components, are the inevitable growing pains of an expanding frontier. International organizations, governments, industry, and academia must continue their efforts to protect and secure the space sector and reduce the ambiguity that breeds mistrust and infringes on the peaceful employment of space systems. To achieve their purpose, they will have to strike a balance between implementing greater security without stifling innovation. Overcoming these hurdles is paramount for the establishment of a secure and resilient space realm that can benefit humankind for years to come.

## About the Authors

### Brianna Bace

Brianna Bace is a Senior Research Aide at the SUNY Research Foundation and a graduate student at the University at Albany, where she previously graduated summa cum laude with a bachelor's degree in Emergency Preparedness, Homeland Security, And Cybersecurity (EHC). In her senior year, she was selected as a VICEROY Research Fellow. Bace's expertise lies in cybersecurity law and policy.

### Dr. Unal Tatar

Dr. Unal Tatar is an assistant professor of Cybersecurity at the University at Albany. He served as the head of Turkey's National Computer Emergency Response Team and an academic advisor at the NATO Center of Excellence Defense Against Terrorism on cyber threats. Dr. Tatar has three main lines of research: the economics of cybersecurity and risk management, critical infrastructure protection and national security, and cybersecurity capacity building.

## Acknowledgement

This publication was supported by Award Number SA10012022020481 from the Griffiss Institute for VICEROY program. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of the sponsor.

## References

Aerospace Corporation. (2024). Space Attack Research & Tactic Analysis (SPARTA). https://sparta.aerospace.org/

Amenabar, C. (2022, June 14). "Counterspace Weapons 101 - Aerospace Security," *Aerospace Security Project*. https://aerospace.csis.org/aerospace101/counterspace-weapons-101/

Bace, B., Gökce, Y., & Tatar, U. (2024). Law in orbit: International legal perspectives on cyberattacks targeting space systems. *Telecommunications Policy*, 102739. https://doi.org/10.1016/j.telpol.2024.102739

Bailey, B., Speelman, R. J., Doshi, P. A., Cohen, N. C., & Wheeler, W. A. (2019).
"Defending Spacecraft in the Cyber Domain," The Aerospace Corporation. Available at: https://aerospace.org/sites/default/files/2019-11/Bailey_DefendingSpacecraft_11052019.pdf

Bartock, M., Brule, J., Li-Baboud Y.-S., Lightman, S., McCarthy, J., Meldorf, K., Reczek, K., Northrip, D., Scholz., A and Suloway, T. (2023). Foundational PNT profile: Applying the cybersecurity framework for the responsible use of positioning, navigation, and timing (PNT) services (NIST IR 8323r1; p. NIST IR 8323r1). *National Institute of Standards and Technology* (U.S.). https://doi.org/10.6028/NIST.IR.8323r1

Bonnette, B. (2023, December, 29). "Joint Task Force-Space Defense Commercial Operations Cell Receives New Name." *U.S. Space Command*. https://www.spacecom.mil/Newsroom/News/Article-Display/Article/3629834/joint-task-force-space-defense-commercial-operations-cell-receives-new-name/

Carlo, A. (2021). Cyber Threats to Space Communications: Space and cyberspace policies. In A. Froehlich (Ed.), Outer Space and Cyber Space: Similarities, interrelations and legal perspectives (pp. 55-66). Springer Cham.

CER Directive. (2022). Official Journal of the European Union. PP. 164-198. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557

Dooren, J. M. (2023, December 22). NASA Issues New Space Security Best Practices Guide. *NASA.* https://www.nasa.gov/general/nasa-issues-new-space-security-best-practices-guide/

Easley, M. (2024, January). Space Force 'days away' from signing first commercial strategy. *DEFENSESCOOP.* https://defensescoop.com/2024/01/05/space-force-commercial-strategy-deanna-burt

Erwin, S. (2023, September 13). Space Force to release guidelines for the use of commercial satellite services. *Space News.* https://spacenews.com/space-force-to-release-guidelines-for-the-use-of-commercial-satellite-services/

European Space Agency. (n.d.-b) *From Space to Earth: Satellite integration for 5G*. [Blog] https://commercialisation.esa.int/2021/01/from-space-to-earth-satellite- integration-for-5g/

European Space Agency (n.d.-a). "What is space 4.0?" https://www.esa.int/About_Us/Ministerial_Council_2016/What_is_space_4.0

Falco, G (2018, September 17). The Vacuum of Space Cyber Security. *2018 AIAA SPACE and Astronautics Forum and Exposition.* 2018 AIAA SPACE and Astronautics Forum and Exposition, Orlando, FL. https://doi.org/10.2514/6.2018-5275

Falco, G. & Boschetti, N. (2021). A Security Risk Taxonomy for Commercial Space Missions. *AIAA Ascend 2021 Conference.* DOI: 10.2514/6.2021-4241.

Garrett, G. A. (2023). “Cyber Innovations Needed for Space Mission Assurance.” *Peraton.* https://www.actiac.org/documents/cyber-innovations-needed-space-mission-assurance

Garino, B., & Gibson, J. (2009). “Space System Threats” in AU-18 Space Primer Air University Press. pp. 273–281. https://www.airuniversity.af.edu/Portals/10/AUPress /Books/AU-18.PDF

Georgescu, A., Tatar, U., Muylaert, J., & Gheorghe, A. V. (2020). Critical Space Infrastructures: Perspectives and a Critical Review. In U. Tatar, A. V. Gheorghe, O. Keskin, & J. Muylaert (Eds.), Space Infrastructures: From Risk to Resilience Governance. (pp. 3-6). IOS Press

Georgescu, A., Bucovetchi, O., & Tatar, U. (2018). Space systems as critical infrastructures. *FAIMA Business & Management Journal.*

Harrison, T., Johnson, K., Young, M., Wood, N., & Goessler, A. (2022). “Space Threat Assessment 2022,” *Center for Strategic and International Studies*. https://www.csis.org/analysis/space-threat-assessment-2022

Hassan, N. U. L., Huang, C., Yuen, C., Ahmad, A., & Zhang, Y. (2020). “Dense Small Satellite Networks for Modern Terrestrial Communication Systems: Benefits, Infrastructure, and Technologies,” in *IEEE Wireless Communications*, *27*(5), pp. 96-103. doi: 10.1109/ MWC.001

Hodson, R. F., Chen, Y., Pandolf, J. E., Ling, K., Boomer, K. T., Green, C. M., Douglas, S. P., Leitner, J. A., Majewicz, P., Gore, S. H., Faller, C. S., Denson, E. C., Hodge, R. E., Thoren, A. P., & Defrancis, M. A. (2022, December). Recommendations on the Use of Commercial-Off-The-Shelf (COTS) Electrical, Electronic, and Electromechanical (EEE) Parts for NASA Missions – Phase II. *NASA.* [NASA/TM−20220018183]. https://ntrs.nasa.gov/api/citations/20220018183/downloads/20220018183.pdf

Housen-Couriel, D. (2023). IAC-21-E-9 (Paper ID: 67116) Information sharing for the mitigation of outer space–related cybersecurity threats. *Acta Astronautica*, *203*, 546–550. https://doi.org/10.1016/j.actaastro.2022.11.012

ICRC. (n.d.) Article 52 - General protection of civilian objects. *International Humanitarian Law Databases.* https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-52

Lightman, S., Suloway, T., and Brule, J. (2022, December). Satellite Ground Segment: Applying the cybersecurity framework to satellite command and control. *National Institute of Standards and Technology.* (NIST IR 8401). https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8401.pdf

Lopez, C. T. (2022). DoD: “It's Not Just State Actors Who Pose Cyber Threat to U.S.” *U.S. Department of Defense*. https://www.defense.gov/News/News-Stories/Article/Article/3039462/dod-its-not-just-state-actors-who-pose-cyber-threat-to-us/

Manulis, M., Bridges, C., Harrison, R. M., Sekar, V., & Davis, A. K. (2021). “Cyber Security in New Space,” International Journal of Information Security, 20(3), p287–311. https://doi.org/10.1007/s10207-020-00503-w

McCarthy, J., Mamula, D., Brule, J., Meldorf, K., Jennings, R., Wiltberger, J., Thorpe, C., Dombrowski, J., Lattin, O., & Sepassi, S. (2023). *Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN)* (NIST Internal or

Interagency Report (NISTIR) 8441). *National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.IR.8441

Meyer, P. (2016). Outer Space and Cyberspace: A tale of two security realms. In A. Osula and H. Rõigas (Eds.), International Cyber Norms: Legal, Policy & Industry Perspectives, NATO CCD COE Publications, Tallinn

Mukherjee, S. (202, November 16). "Q+A What is space debris and how dangerous is it?" *Reuters*. https://www.reuters.com/lifestyle/science/qa-what-is-space-debris-how-dangerous-is-it-2021-11-16/

NASA. (2023, October 13). Space Security: Best Practices Guide (BPG). Document No: SS BPG https://swehb.nasa.gov/display/SWEHBVD/7.22+-+Space+Security%3A+Best+Practices+Guide

National Coordination Office for Space-Based Positioning, Navigation, and Timing. (2021). *Public Safety & Disaster Relief Applications*. [Online]. https://www.gps.gov/applications/safety

NATO. (2023, July 17). Lift-off, NATO Launches New Space Centre of Excellence. https://www.act.nato.int/article/space-newest-coe/

NATO. (2022a, June 29). 2022 Strategic Concept. https://www.nato.int/strategic-concept/

NATO. (2022b, January 17). NATO's overarching Space Policy. https://www.nato.int/cps/en/natohq/official_texts_190862.htm

New Space Economy. (n.d.). *Dual Dimensions: The Impact of Dual-Use Space Technologies on the Space Economy.* https://newspaceeconomy.ca/2023/04/04/dual-dimensions-the-impact-of-dual-use-space-technologies-on-the-space-economy/

Nussbaum, B. & Berg, G. (2020). Cybersecurity Implications of Commercial Off The Shelf (COTS) Equipment in Space Infrastructure. In U. Tatar, A. V. Gheorghe, O. Keskin, and J. Muylaert (Eds.), Space Infrastructures: From Risk to Resilience Governance. (pp. 91-99). IOS Press

Nguyen, H. H., & Nguyen, P. S. (2020). Communication Subsystems for Satellite Design. In T.M. Nguyen (Ed.) Satellite Systems - Design, Modeling, Simulation and Analysis. *IntechOpen*. https://doi.org/10.5772/intechopen.93010

Office of the Secretary of Defense. (2020). Military and Security Developments Involving the People's Republic Of China. [Annual Report to Congress]. https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF

O'Neill, P. H. (2022, May). Russia hacked an American satellite company one hour before the Ukraine invasion. *MIT Technology Review.* https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/

Ortega, A. A. (2023, June 5). Not a Rose by Any Other Name: Dual-Use and Dual-Purpose Space Systems. *Lawfare*. https://www.lawfaremedia.org/article/not-a-rose-by-any-other-name-dual-use-and-dual-purpose-space-systems

Pellish, J. Commercial Off-The-Shelf (COTS) Electronics Reliability for Space Applications. *NASA*. https://ntrs.nasa.gov/citations/20180002659

Portillo, I., Eiskowitz, S., Crawey, E. F., and Cameron, B. G. (2021). Connecting the other half: Exploring options for the 50% of the population unconnected to the internet. *Telecommunications Policy, 45*(3), https://doi.org/10.1016/j.telpol.2020.102092

Prazak, J. (2021). "Dual-use conundrum: Towards the weaponization of outer space?" *Acta Astronautica*, 187, p397-405. https://doi.org/10.1016/j.actaastro.2020.12.051

Rajagopalan, R. P. (2019, May). Electronic and Cyber Warfare in Outer Space. *United Nations Institute for Disarmament Research (UNIDIR).* https://unidir.org/files/publication/pdfs/electronic-and-cyber-warfare-in-outer-space-en-784.pdf

Sanger, D. E. & Barnes, J. E. (2024, February 17). U.S. Fears Russia Might Put a Nuclear Weapon in Space. *The New York Times.*

Scholl, M., & Suloway, T. (2022). Introduction to Cybersecurity for Commercial Satellite Operations, *National Institute of Standards and Technology*. (Draft (2nd) NIST IR 8270). https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8270-draft2.pdf

Serra, J. F. (2021). Cybersecurity and Outer Space: Learning from connected challenges. In A. Froehlich (Ed.), Outer Space and Cyber Space: Similarities, Interrelations and Legal Perspectives (pp. 87-103). Springer Cham.

Space Foundation Editorial Team. (2023, July 25). Space Foundation Releases The Space Report 2023 Q2, Showing Annual Growth of Global Space Economy to $546B. *Space Foundation.* https://www.spacefoundation.org/2023/07/25/the-space-report-2023-q2/

Space ISAC (n.d.) *Space ISAC Frequently Asked Questions.* https://s-isac.org/resources/

Space Infrastructure Act, H.R.5017, 118th Cong. (2023). Available at: https://lieu.house.gov/sites/evo-subsites/lieu.house.gov/files/evo-media-document/space-infrastructure-act.pd

Unal, B. (2019, July). Cybersecurity of NATO's Space-based Strategic Assets. *Chatham House.* https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf

United States. (2021). National Submission to the United Nations Secretary General Pursuant to UN General Assembly Resolution 75/36 Reducing space threats through norms, rules and principles of responsible behaviours. https://documents.unoda.org/wp-content/uploads/2022/05/04292021-US-National-Submission-for-UNGA-Resolution-75.36.pdf

UNOOSA (United Nations Office of Outer Space Affairs). (n.d.). *Benefits of Space: Communication.* https://www.unoosa.org/oosa/en/benefits-of-space/communication.html

U.S. Department of Defense. (2024, April). DoD Releases 2024 DoD Commercial Space Integration Strategy. https://www.defense.gov/News/Releases/Release/Article/3728370/dod-releases-2024-dod-commercial-space-integration-strategy/

U.S. Space Force (2022, January). Space Doctrine Note *Operations*. https://media.defense.gov/2022/Feb/02/2002931717/-1/-1/0/SDN%20OPERATIONS%2025%20JANUARY%202022.PDF

Velkovsky, P., Mohan, J., & Simon, M. (2019). 'Satellite Jamming: A Technology Primer,' *CSIS*. https://res.cloudinary.com/csisideaslab/image/upload/v1565982911/on-the-radar/Satellite_Jamming_Primer_FINAL_pdf_bdzxwn.pdf

Way, T. (2019, October). Counterspace Weapons 101. *Aerospace Security Project.* https://aerospace.csis.org/aerospace101/counterspace-weapons-101/

Weinzierl, M & Sarang, M. (2021, February 12). The Commercial Space Age Is Here. *Harvard Business Review.* https://hbr.org/2021/02/the-commercial-space-age-is-here

The White House. (2021). United States Space Priorities Framework [Press release]. https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/01/united-states-space-priorities-framework