Could Redefining U.S. Space Power Mitigate the Risk of Space Logistics Degradation by the Threat of Space Weaponization?

Ivan Gulmesoff
American Public University System

Abstract

This research article aims to assess U.S. space logistics and the threat of space weapons through the lens of proposed theories and concepts of space power. This analysis will begin with a brief introduction to space logistics, followed by the threat of space weapons, address concepts of space power, and end with recommendations and a new theory of space power. To this day, more states are gaining access to the space domain and challenging U.S. space dominance. As Smith suggests, the U.S. has been more focused on tracking objects in orbit instead of protecting space assets and deterring adversaries (M. V. Smith 2002). While the space treaties of the 1960s and 1970s attempted to establish the peaceful use of the space domain, preventing outer space's weaponization, its effectiveness has slowly declined over the decades with changes to global, national security objectives and technology advancements.

Advanced societies rely on the critical space infrastructure (CSI) for daily life to include supporting economies and government systems. From the day CSI's were established in the space domain, their technology has vastly improved to provide better services. Even though the expansion and reliance have enhanced technological capabilities with communications, remote sensing, global positioning/navigation, broadband, and entertainment, it has also exposed vulnerabilities. In 2016 the U.S. had 576 satellites in orbit while China had 181, and Russia had 140 (Johnson-Freese, 2016). A space-faring nation with significantly more satellites in orbit than other states could be viewed as threatening space dominance. As Georgescu et al. explain, "this dependency breeds vulnerability, both to natural and man-made risks arising from the specific environment in which space systems operate, as well as to deliberate attacks seeking to destabilize societies" (Georgescu et al. 2019).

Keywords: U.S. space power, risk, space logistics, degradation, threat, space weaponization

 doi: 10.18278/sesa.2.2.8

¿Podría la redefinición del poder espacial estadounidense mitigar el riesgo de degradación de la logística espacial por la amenaza del uso de armas espaciales?

Resumen

Este artículo de investigación tiene como objetivo evaluar la logística espacial de Estados Unidos y la amenaza de las armas espaciales a través de la lente de las teorías y conceptos propuestos del poder espacial. Este análisis comenzará con una breve introducción a la logística espacial, seguida de la amenaza de las armas espaciales, abordará los conceptos del poder espacial y finalizará con recomendaciones y una nueva teoría del poder espacial. Hasta el día de hoy, más estados están obteniendo acceso al dominio espacial y desafiando el dominio espacial de EE. UU. Como sugiere Smith, Estados Unidos se ha centrado más en rastrear objetos en órbita en lugar de proteger los activos espaciales y disuadir a los adversarios (M. V. Smith 2002). Si bien los tratados espaciales de las décadas de 1960 y 1970 intentaron establecer el uso pacífico del dominio espacial, evitando el uso de armas en el espacio ultraterrestre, su eficacia ha disminuido lentamente a lo largo de las décadas con los cambios en los objetivos de seguridad nacional y mundial y los avances tecnológicos.

Las sociedades avanzadas dependen de la infraestructura espacial crítica (CSI) para la vida diaria para incluir economías de apoyo y sistemas gubernamentales. Desde el día en que se establecieron los CSI en el dominio espacial, su tecnología ha mejorado enormemente para brindar mejores servicios. Aunque la expansión y la dependencia han mejorado las capacidades tecnológicas con comunicaciones, teledetección, posicionamiento / navegación global, banda ancha y entretenimiento, también ha expuesto vulnerabilidades. En 2016, Estados Unidos tenía 576 satélites en órbita, mientras que China tenía 181 y Rusia tenía 140 (Johnson-Freese, 2016). Una nación espacial con significativamente más satélites en órbita que otros estados podría verse como una amenaza para el dominio del espacio. Como Georgescu et al. explican, "esta dependencia genera vulnerabilidad, tanto a los riesgos naturales como provocados por el hombre que surgen del entorno específico en el que operan los sistemas espaciales, así como a los ataques deliberados que buscan desestabilizar las sociedades" (Georgescu et al. 2019).

Palabras clave: Poder espacial estadounidense, riesgo, logística espacial, degradación, amenaza, armamento espacial

重新定义美国太空实力能缓解由太空武器化威胁造成的太空后勤弱化风险吗？

摘要

该研究文章旨在透过所提理论和太空实力概念视角，评估美国太空后勤和太空武器威胁。本篇分析将首先简要介绍太空后勤、太空武器威胁，接着研究太空实力的概念，最后提出建议和关于太空实力的新理论。目前，更多的国家正在进入太空领域，挑战美国的太空主导权。正如学者Smith所暗示的那样，美国一直更多地聚焦于追踪轨道上的物体，而不是保护太空资产和威慑对手（M. V. Smith 2002）。尽管20世纪60年代和70年代的空间条约试图建立对太空领域的和平使用、防止外层空间的武器化，但随着全球、国家安全目标的改变和技术提升，条约的有效性在几十年里缓慢下降。

高等社会依赖关键空间基础设施（CSI）以供每日生活，把支持经济和政府系统包括在内。自CSI在太空领域建立之日起，相关技术已获得巨大提升，以期提供更好的服务。尽管CSI的扩张和依赖通过各方面提升了技术能力，包括传播、遥感、全球定位/导航、宽带、娱乐，但也暴露了弱点。2016年，美国在轨道中拥有576颗卫星、中国拥有181颗、俄罗斯拥有140颗（Johnson-Freese, 2016）。一个在轨道上拥有的卫星数量远超过其他国家的太空强国能被视为对太空主导权造成威胁。学者Georgescu等人解释道，“这种依赖性会在两方面催生脆弱性，一是空间系统所运作的特定环境中产生的自然风险和人为风险，二是企图混乱社会的蓄意攻击”（Georgescu et al. 2019）。

关键词：美国太空实力，风险，太空后勤，退化，威胁，太空武器化

Introduction

Unlike terrestrial logistics, space operations and the space environment's intricacies make logistics much more complex and demanding on supply chain management. In 2011 alone, 25 tons of supplies and equipment were transported to the ISS consisting of propellant, oxygen, water, food, spare parts, and medical equipment (Johnson 2011). By understanding this logistical complexity, vulnerabilities could be more easily evaluated to mitigate future space weapon attacks' damage. Johnson explains space logis-

tics as (1, 2011) "the theory and practice of driving space system design for operability, and of managing the flow of material, services, and information needed throughout a space life cycle." Within this concept are multiple factors that could lead space logistics to become vulnerable to adversaries and hinder space logistics' effectiveness. For example, the logistics involved with the Shuttle and ISS have demonstrated multiple areas that could improve current space logistics' efficiency.

Five key areas of contemporary space flight logistics could be improved. These areas include fragmented databases, storage problems on the ISS, real-time awareness of system health and logistics inventory levels, overly complicated and bureaucratic processes, and costly NASA logistic practices designed in program/project lines (Andy, Evans, and Laufer 2006). Each one of these critical areas contributes to inefficiencies that affect space logistics in one way or another. In addition to these vital elements, space logistics must also consider ground operations and the supplier network. While Laufer et al. explain each of these critical elements must be considered, the most significant inefficiency does not come from any technical aspects of space logistics but the administrative and managerial processes (Andy, Evans, and Laufer 2006). For example, the DoD Logistics Transformation Study identified a lack of perspectives being shared within engineers and logisticians to determine issues and improve many of the critical areas previously mentioned. While each key area has a specific function, the managerial aspect plays a significant role in space logistics efficiency. Each key area requiring improvement also exposed vulnerabilities.

The lack of security measures increases vulnerability. Security measures could be introduced in many forms. The Rumsfeld Commission was assigned in 2001 to review all U.S. space activities as they related to national security. After a thorough review, what they determined was two significant recommendations were required for all U.S. space activities:

1. A centralized management of space programs and overall acquisition of space platforms for national security.
2. Creation of a military space department when conditions allow.

Without these recommendations, the 2001 commission argued that the U.S. would risk an inventible conflict in space. The vulnerability of space weapons to space launch could range anywhere from the ground site, throughout the launch process up to 62 miles to space and continue in orbit. Augustyn explains how space logistics' safety and security are dependent on terrestrial network connections required for business and government agencies (Augustyn 2020). For example, space launch operations alone require the deployment of payloads into space, the sustainment, augmentation, or reconstituting satellite constellations for military or commercial uses (DIA 2019). The risk of conflict did not end in 2001 with the Rumsfeld Commission.

In fact, it continued, and in 2017 General Hyten suggested to Congress that the space domain required oversight of the acquisition, deployment of strategic ground control segments, oversight of the enterprise-wide defense system, the development of rapid space capabilities for experimental technology, the appointment of an oversight executive agent for the Joint Requirements Oversight Council, and the development of a national space security executive committee (Whitney, Thompson, and Park 2019). The oversight committee was the first step that later led to the development of the U.S. Space Force.

The Threat of Space Weapons to Space Logistics

The security of space logistics is dependent on the vigor and efficiency of the supply chain. The key to this dependency is the satellite command and control architecture (C2). The C2 is the primary control to uplink communication and downlink data to ground stations through antennas, transmitters, and receivers (DIA 2019). In addition to the C2, there are many variables associated with the supply chain and the space environment that can transport logistics very difficult, leading to costly mistakes. As Andy et al. explain (35, 2006), "we have also come to learn that the path to optimizing operability and sustainability is by consideration of the entire supply chain." The strength of the supply chain directly relates to the success of space logistics and space operations in general.

According to the U.S. Space Policy, the space infrastructure is considered a vital national interest and must be protected (Weston 2009). The U.S. national interest in space has grown with the reliance and dependence on technological capabilities regarding communications, remote sensing, global positioning/navigation, broadband, and entertainment. As Georgescu et al. state, 90% of military communications are transmitted and routed through civilian satellite systems (Georgescu et al., 2019). This reliance by the U.S. military on civilian communication satellites and the U.S. infrastructure consisting of more satellites than any other state inevitably increases vulnerability. In 2009, the U.S.-owned 400 satellites worth over $123 billion out of the 900 active satellites in orbit (Weston 2009). However, an adversary could expose those vulnerabilities and render U.S. satellites or their associated space logistics useless or incapacitated by other means.

Space weapons could threaten space logistics in many ways—from an operational standpoint to administrative burdens. Logistical operations could be affected by the administrative burdens due to the internet-of-things that link humans to intelligent machines and robotics in space logistics (Augustyn 2020). The autonomous operations of satellite systems, as well as the logistics, expose valuable space assets to adversaries. To fully understand how a threat of space weapons could be possible, we must first define what space weapons are. Weidenheimer elaborates on the definition of space weapons that has also been accepted by the

United Nations. Weidenheimer states (16, 1998) "a space weapon is a device, located in space at the time of its attack, that is designed to damage or harmfully interfere with the normal operation of a target located anywhere (in space, in the air, on the ground, underground, on the sea, or under the sea); or a device, located anywhere, designed to damage or interfere with the normal operation of a target in space (where space means the volume 90 kilometers or more above the earth's surface)" (Weidenheimer 1998). While Weidenheimer's definition seems to encompass all space weapons, it fails to address or articulate an ever-growing and often concealed space weapon—cyberweapons. Weidenheimer implies cyberwarfare as a means of information warfare (IW). Cyberweapons have wreaked havoc among many industries to date and have already infiltrated the space domain as well. Knowing the space infrastructure depends on space logistics, vulnerabilities, and space weapons' threat should be clearly understood.

New space weapons include nuclear, kinetic energy, radio frequency (RF), high power microwave (HPM), laser, particle beam (PB), and information warfare (IW) (Weidenheimer 1998). In the United States, the Defense Intelligence Agency (DIA) categorizes these weapons. The DIA considers any weapon used to (9, 2019) "disrupt, damage, or destroy enemy equipment and facilities" a direct energy weapon and any weapon designed to "jam, spoof or control the electromagnetic spectrum" a weapon of electronic warfare (EW). However, for this analysis, more specific weapon terminology will be used for clarity and understanding. Each space weapon could be leveraged by adversaries knowing their effects on operations if a satellite or logistical system could be rendered inefficient. These weapons could be used as a means of kinetic attack, direct energy, or cyber-attack (information warfare) (Handberg 2019). What makes these weapons more difficult to detect in modern satellite technology is their inconspicuous use. For example, advanced satellites used various systems to operate. The various communications satellites used and relied on by societies worldwide include voice communications, television broadband internet, mobile services, and civilian and military data transfer services (DIA 2019). Unbeknownst to the U.S., an adversary's communication satellites could be orbiting with added ASAT (anti-satellite) technology (Johnson-Freese 2016). A commercial satellite could easily have concealed ASAT technology. Listed below are concise explanations of each space weapon with the anticipated effect on space assets or operations.

Nuclear Weapons

Even though the definition of a nuclear space weapon has not been clearly defined, what is clearly defined is fitting the category of weapons of mass destruction (Ferreira-Snyman 2015). A weapon of mass destruction would destroy space assets and be used as a significant deterrent for an adversary. Handberg explains how (299, 2019) "nuclear weapons provide a bigger bang for the buck which attacks sup-

port among weaker states for their development and possible use, increasing the probability of use when threatened." However, nuclear weapons were specifically mentioned in the Outer Space Treaty because of this reason—the bigger bang. In addition to the gravity of the explosion itself (that would be damaging but much different in the space environment), a primary concern is a radioactive fallout (Ferreira-Snyman 2015). The radioactive fallout could affect critical space-based assets damaging them or rendering them completely useless. Nuclear space weapons could come in various methods depending on the intended target. The majorly of these developed are projectile type weapons. Once they are detonated in the space atmosphere, they emit electromagnetic pulses. Emitting electromagnetic pulses could be used to deter an adversary elsewhere or distract them all together. One type of projectile is a nuclear-tipped intercontinental ballistic missile (ICBM) that could be used purposely as a space weapon because of its timing and accuracy. The U.S. alone can launch an ICBM within 30 minutes to any location on earth (Varni et al. 1996). Given this precision and timing, not only would space-based assets be threatened but also launch and landing platforms as well as ground operation centers.

Kinetic Weapons

There are two types of kinetic space weapons—A kinetic space energy weapon is known as a "hit and kill" weapon and generally does not carry explosives. In contrast, a kinetic weapon system could be designed with robotic ASAT mechanisms. The high speed at the impact on their designated target is designed to be enough for a kinetic space energy weapon's intended purpose. In 1983, the Strategic Defense Initiative (Star Wars) planned to use kinetic energy weapons in the form of missiles that could be used to destroy other missiles in the launch stages (M. S. S. Smith 2003). Even though the concept of Star Wars was developed in 1983, this method could very well be applied to modern-day kinetic energy weapons in space. As Vari explains, kinetic weapons could be used to reach small satellites in low earth orbit (LEO) containing storage containers within minutes (Varni et al. 1996). Kinetic space weapons could also be used to destroy or disable critical satellites intended for communications or navigation.

One example of this was on January 11th, 2007, when China intentionally collided with two objects in space to destroy an old weather satellite (Gubrud 2011). Even though the Chinese government denied this was any form of ASAT, it demonstrated Chinese space capabilities. They were able to deploy accurately and collided with another object for their intended purpose. An unintentional or intentional collision with space assets would hinder not only objectives but also introduce more problems. One example could have come from the HTV2 flight. The HTV2 was deployed in 2011 to deliver necessary spare parts in orbit to another shuttle using a Japanese robotic arm (Johnson 2011). If an adversary were to destroy the robotic arm using a kinetic

weapon, critical parts would have never reached their destination. Whitney et al. explain how both China and Russia have prioritized the development of kinetic space weapons to counter U.S. Space Dominance (Whitney, Thompson, and Park 2019).

Radio Frequency Weapons

Radiofrequency weapons can be used primarily to disrupt communication and navigation systems. Radiofrequency weapons are a means of electronic warfare that encompass jamming and spoofing. Jamming can be accomplished by either downlink jamming where the damage is centralized to ground operators or uplink jamming where the satellite systems are affected.

Weidenheimer provides an example of uplink and downlink jamming. One is terminal guidance jamming, where a ground transmitter becomes inoperable, and another is terminal guidance jamming from a space-based system where communications cease completely (Weidenheimer 1998). Terminal guidance jamming could affect satellite systems in various ways and is not a new technology. As Howard explains, the Chinese government had developed jamming satellite technology in 2001. The Rumsfeld Commission report revealed that Iran and North Korea had also achieved similar advancements in technology (Howard 2010). Such advancements in radio frequency weapon technology could be devastating to space assets or operations.

A significant advancement in radio frequency weapons is the use of spoofing techniques. Spoofing can be used to compromise the entire electromagnetic spectrum by simulating fake signals or spreading erroneous information. Developing space logistics continue introducing more advanced technology such as autonomous UAV, e-mobility vehicles, and intelligent containers (Augustyn 2020). Many of these systems rely heavily on artificial intelligence. As Augustyn explains (361, 2020), "innovation machines join the logistics workforce not only through self-driving vehicles and IoT but also Augmented Reality (AR) in the environmental area of machine-human (anthropo-technical system) interaction and collaboration in space logistics systems." While the AR provides a whole picture using only a snapshot or small portion the environment area of machine-human provides the "human reasoning" to the machine. The Internet of Things (IoT) combines each computing device to work seamlessly and effectively together. Erroneous data introduced by spoofing could be devastating to space logistics causing excessive re-work and costs and ultimately not meeting logistical obligations.

High Power Microwave Weapons

High power microwave space weapons are only an orbital threat because current technology limits their capability solely from space-based satellites. The Soviets first introduced high power microwave space weapons in the mid-1980s by testing them on ballistic missile systems (Weidenheimer 1998). Not only did the Soviets take advantage of this technology, but the Chinese government did as well. As Blazejewski explains, intending to develop a strong

space program, the Chinese have conducted space-based testing jamming their satellites with high-power microwave technology (Blazejewski 2008). These weapons have continued to improve over the decades, becoming a more significant threat to satellite infrastructures to this day. According to the Defense Intelligence Agency, high power microwaves are considered a directed energy weapon that can be very difficult to detect where the attack came from (DIA 2019). High power microwave weapons can be used for jamming communication between satellite systems.

Leveraging electromagnetic radiation, these weapons do not require accurate pinpointing; instead, they are transmitted with an array of high-energy pulses between tens of megahertz to tens of gigahertz to broadener targets (Varni et al. 1996). Once the high-power microwaves hit their intended target, all electronics are either permanently or temporarily disabled. Like radiofrequency weapons, these weapons can easily disrupt space logistics or operations in general. Besides the benefit of not requiring pinpoint accuracy, high-power microwaves could also be a preferred weapon because they can operate in any weather atmospheric condition. Most electronics are vulnerable to damage (Varni et al. 1996). With modern technology relying on an abundance of electronics to operate, high energy weapons could be one of the greatest threats posed by an adversary.

Laser Weapons

Laser space weapons can be developed and designed from either ground operations or space-based platforms. According to Possel, laser weapons are the most technologically advanced and cost-effective weapon that could be used (Possel 1998). However, to be most cost-effective, the entire laser weapon must be space-based. The laser weapons would operate on either platform (land or space) using large mirrors to transmit the laser beam to its intended location. The laser weapons generally target sensors on satellite systems to either disrupt, degrade, or damage them (DIA 2019). The targeted sensors would most likely be the most vital to space-based assets. In space logistics, smart sensors are used and relied upon to make critical decisions based on timing and passion (Augustyn 2020). If these sensors are targeted, spare parts or supplies may not reach their intended destination.

The last shuttle flight of the STS-134 Endeavour is one example of how critical sensors are to space logistics. The last STS 134 Endeavour flight's impact was significant because it was one of the only STS with such a large payload capacity. The large payload capacity of STS 134 Endeavor's had previously been used to transport a 1,400-pound ammonia pump module back to earth from the ISS (Johnson 2011). This was a significant event in space logistics because, following STS 134 Endeavor's flight, the U.S. had to rely on the Soyuz (Soviet Space Program) for large transports. Knowing the U.S. only had one STS capable at the time of large transport capacity, its sensors could have easily become a laser weapon target from an adversary.

Theory & Concepts

While there is no universally accepted theory of Space Power, many concepts attempt to define and address space power. While Smith explains space power as (7, 2020) "the ability to use spacecraft to create military and political effects," the scope of this description seems broad and missing critical elements about the space environment. For example, the word "spacecraft" could easily be replaced with the word "aircraft" and then define air power. However, a much more comprehensive doctrine of space power was introduced by Lupton in 1988. Lupton explains how four schools of thought must be considered for space power—the sanctuary school is the ability for a state to oversee states from orbit. The survivability school considers the space environment and its vulnerability. The control school argues space should be a controlled environment, and the school of high ground implies the purview of space provides an advantage over adversaries (M. V. Smith 2002). Given current space operations, Lupton's four tenants could easily be applied to a space-faring state to determine their extent of space power. Below are a few key concepts of space power from various known authors on the topic to provide a better understanding. Each author varies in experience and profession. Some are from military occupations (USAF), others are experts in the field, or scholars. The differences, similarities, and perspectives could shed light on familiar themes and gaps in the theory itself.

U.S. Space Dominance Through the Lens of Space Power

Even though each Space Power definition is different, they each imply a sense of control and deterrence in support of national interests. While Varni et al., Smith and the USAF Doctrine imply conflict or war is a cornerstone of Space Power, Lupton and Oberg see it differently. A significant factor that may have contributed to this difference could have been the timing of these definitions and the global events affecting U.S. national interests at the time. In 1996 the U.S. was involved in Operation Desert Strike in Iraq, and on September 11, 2001, the U.S. experienced one of the worst combined terrorist attacks to date. However, regardless of the timeframe, these concepts were developed. They all had a clear understanding of our growing reliance on U.S. space infrastructures and the necessity to ensure their functionality, seamless operations, and security.

In 1997 General Estes explained (23, 1998), "To begin with, it must be made clear that space is becoming, or some would say, space has become the 4th medium in which the military operates in the protection of our national security interests." Unfortunately, it would take nearly two decades for the U.S. to establish a Space Force for General Estes's intended purpose. Along with U.S. Air Force leadership, General Estes understood the gravity of not having a specific U.S. armed service for the space domain. After all, the U.S. has a long history of displaying air and sea

Table 1. Concepts of Space Power by Various Authors

Author	Definition of Space Power
Oberg, Jim	(9, 2010) "Space power is the combination of technology, demographics, economic, industrial, military, national will, and other factors to contribute to the coercive and persuasive ability of a country to politically influence the actions of other states and other kinds of players, or to otherwise achieve national goals through space activity."
Varni, Jamie et al.	(73, 1996) "Global space power involves the application of the full spectrum of force, physical and virtual, from space on demand to an adversary's means of pursuing the conflict."
Smith, M. V	(49, 2002) "Space power is not composed alone of the war-making component of space. It is the total space activity; civil, commercial, defense, and intelligence, potential as well as existing.
October 1999 USAF Doctrine Center Publication	(7, 2002) "Space power, like airpower, can place an adversary at a disadvantage. Space Power is a subset of aerospace power."
Lupton, D	(141, 2013) "space power is the ability of a nation to exploit the space environment in pursuit of national goals and purposes and includes the entire astronautical capabilities of the nation."
Swilley, S	(146, 2013) "space exploration, commercial space endeavors, and space enablers serve as the core space activities associated with space power. These three core space power activities serve three distinct national processes: innovation, prosperity, and security"

superiority to ensure freedom of navigation and ensure national objectives are met with an assumption that conflict may be inevitable. However, to establish Space Power, the medium of the space domain where conflict could occur must be clearly understood.

Unlike other air and sea domains, where conflict has already taken place, the space domain is relatively new to conflict. As previously discussed, space weapons are vastly different to ensure functionality and effectiveness in the space environment. The key to achieving U.S. space superiority through Space power could be investing in space situational awareness networks. Situational awareness networks encompass radar, optical, and intelligence for ground and space operations as a means of anticipating conflicts (Szymanski 2019). Space situational awareness networks could not only monitor an adversary's terrestrial activity but also in space leveraging on space technology. As Robinson ex-

plains, to successfully ensure the principle of force employment is met, Space Power must leverage the space medium as an advantage over adversaries while remaining flexible during operations (Robinson 1998).

The U.S. Space Command (USSPACECOM) seems to have accepted Lupton's understanding of space power by prioritizing certain aspects of its vision for 2020. As Steele explains, four central tenants of USSPACECOM's vision: the control of space, global engagement, full force integration, and global partnerships (Steele 2001). The aspect that pertains most to Lupton's doctrine is the first aspect of USSPACECOM's vision. USSPACECOM's control aspects include surveillance as well as protection that are both vital elements of space power. However, should "control" be prioritized over other tenants of USSPACECOM? As Klien suggests, presence, coercion, and force should be prioritized as a means of commanding space (Townsend 2019). One of the primary reasons for this suggestion is leveraging the limited space-faring states. In other words, by the U.S. having the most space assets, it not only "controls" the space domain but also "commands" the space domain by its operational behavior.

While USSPACECOM appears to have adopted some of Lupton's space power concepts, there are many others. One gap that is unclear to have been adopted is Oberg's definition of space power in leveraging technology to achieve national security objectives. A common gap throughout the U.S.-centric space power literature is cybersecurity. This could be partly due to national security objectives and the clandestine nature of cybersecurity strategies. On the other hand, the Russian government (29, 2019) "considers the information sphere to be strategically decisive and has taken steps to modernize its military's information attack and defense organizations and capabilities." Russia's prioritization in this area of cyberspace has been ongoing contemporary cyber-attacks on U.S. systems.

Cyber Security and U.S. Space Power

To fully understand how the threat of cyber-attacks could limit U.S. space power, we must begin with a clear understanding of U.S. cybersecurity. In 2015 Astronaut Peake made an honest mistake. Using Skype, Astronaut Peake misdialed a call to a wrong number on the earth and established a data transfer connection to an unknown source for several minutes (Hannan 2018). While this breach in cybersecurity proved to be a low-level threat, it also raised awareness of cybersecurity vulnerabilities. As Nye states (45, 2017), "as recently as 2007, malicious cyber activities did not register on the director of national intelligence list of major threats to national security. In 2015 they ranked first." The United States relies on cyber capabilities in various aspects of space and critical terrestrial infrastructures. A significant threat was explained in 2012 by Defense Secretary Leon Panetta. He described how Russia and China have hacked into our

electrical grid and can take it down at any moment (Nye 2017). While the act of taking down the United States power grid might expose a vulnerability, it would also demonstrate a failure of U.S. deterrence and offensive capabilities.

The nature of American cyber dominance in many ways is different than other states worldwide. First, the United States government continues developing new technology to maintain strong offensive and defensive cyber capabilities. This continued development appears to some as (48, 2016) a "cyber arms race" with China. This perception of a "cyber arms race," as Mazanec explains, drives the development of new technology in cyber warfare (Mazanec, n.d.). Unlike the Space Domain with the Outer Space Treaty as a means of mitigating an arms race in space, the cyber domain has no such treaty. Each world superpower's unspoken objective is to dominate another state's technology in the best methods of offensive and defensive cyber capabilities. In other words, China, Russia, and the United States continue striving for better cyber warfare technology in a perceived "arms race." Coincidentally, China and Russia are also two of the space-faring states with the most space weapon capability. In 2007 alone, China successfully launched an ASAT missile exposing vulnerabilities to the U.S. satellite infrastructure (Weston 2009). Had a space-faring adversary infiltrated the Chinese cybersecurity systems, the ASAT missile launch could have been compromised and deemed unsuccessful.

A significant threat to U.S. cyber dominance that also affects U.S. space power is communication and transmissions in U.S. society. As Andres explains (96, 2017), "The United States is an open society, which means even adversaries are allowed to attempt to influence or compromise the integrity of U.S. policymaking institutions." While the United States might aim to achieve cyber dominance through different aspects, its open society will still introduce a means of vulnerability. In addition to the cyberspace vulnerability of an open society, the United States also relies heavily on cyberspace as a means of critical space and terrestrial infrastructures for electricity, water, banking, communication, transportation, and command and control military systems (Nye 2017). However, as Weston explains, the U.S. does have space-based electronic countermeasure capabilities that can render adversary satellite communication and transmissions useless (Weston 2009). While the United States' open society may expose vulnerability, the U.S. electronic countermeasures may minimize or deter the threat.

Before establishing the U.S. Space Force, the Global Space Coordinating Authority identified several command-and-control issues in the space domain. As Brown explains through the C2 Air Mobility lessons learned, the fragmented coordination of on-orbit assets created more problems and compounded inefficiencies (Brown 2006). By introducing improvements in C2, all space assets eventually fell under one commander—the Joint Functional Component

Commander-Space and Global Strike. This may improve inefficiencies in C2 but also unintentionally introduce vulnerabilities to cyber-attacks focused on a single commander instead of fragmented management of the past.

Proposed Theory and Concept of Space Power

Considering the contemporary threat of space weapons from space-faring states, space operations and logistics in the space environment, the importance of cybersecurity, and the primary objective of protecting space assets through space dominance, I propose a new theory as follows. *Space power is the command and control of the space domain, leveraging sea and air power, ensuring national objectives are met while continually adapting and improving technological advancements. Space power is also dependent on the strength of cybersecurity measures because of the inherent and ever-increasing risks associated with cyber-attacks.* Even though space power is superior to sea and air power in many ways because of its global access and presence, there are many contributing factors associated with the sea and air. Mahan's theory of sea power intended to ruin an adversary's economy by denying them opportunities to trade, commerce, and sea access (France 2000). This concept relates to space power because space is a controlled environment in several ways. For one, only limited states have the capability to reach LOE and deploy a satellite successfully. Another reason is due to the growing global reliance on space-based systems such as communication and navigation. Sea Power could also benefit space operations by providing launching or recovery platforms like SpaceX.

The application of Air Power to Space Power is more concise. Robinson defines Air Power as (51, 1998) "the use of or denial of the air medium for military value." This aspect could be simply applied to space power because to reach the space domain (at a minimum altitude of 62 miles), any object must pass through the atmosphere—the airpower domain. Leveraging U.S. airpower capabilities, the U.S. could use this as an advantage against adversaries while maintaining space dominance. C2 of this definition is a foundational concept that directly contributes to the effectiveness of Space Power. As Robinson suggests, command and control are where optimum situational awareness exists to direct space force actions (Robinson 1998). Whatever becomes an action or event in the space domain is determined at the command-and-control sector.

Recommendations

The threat of space weapons on the U.S. space logistics must be considered a top national security priority, not only because of societal reliance on critical systems but also because of military dependence. As Pfaltzgraff explains (147, 2013), "space power enables and enhances a state's ability to achieve national security." Analyzing the space power of our adversaries could be key to determine and anticipate threats to space-critical

infrastructure. With several variations of space power concepts, the risk of space weapons on critical space logistical and operations, a common theme emerged—a space-faring nation's behavior in the space domain. As Lefebvre explained 2019), "the key to space power is acquiring the human and technical resources to increase one's freedom of action while aiming to reduce an opponent's." This definition suggests a continuous adaptation to technological changes to improve space operation and the associated logistical challenges. By the U.S. having the most space assets, it inevitably becomes the most vulnerable to adversaries and sets a standard of acceptable behavior.

A vital approach that has been introduced by the U.S. Air Force's space doctrine center that could be considered for other national and commercial space applications has been the Agile Combat Support (ACS). The ACS consists of essential areas of logistics to include civil engineering, maintenance, supply, transportation, logistics plans, and force protection (Hall 2003). The ACS incorporates essential areas of logistics to provide the necessary oversight to ensure efficiency. While the ACS was designed for anticipating war for the U.S. Air Force, it also ensures support systems within logistics to work more efficiently by less maintenance and more productivity. As Bruce DeBlois explained (80, 2009), "the decision to weaponize space does not lie within the military-seeking short-term military advantage in support of national security but at the higher level of national policy-seeking long-term national security, economic well-being, and world-wide legitimacy of U.S. constitutional values." Given the understanding that space weaponization may be unavoidable, lacking cybersecurity would compound any threat of conflict in the space domain.

In conclusion, due to the risk of vulnerability and civil and military reliance associated with the CSI, the United States must continually improve both its offensive and defensive cyber capabilities and never expose their shortcomings. Goines (1, 2017) states, "the Department of Defense reported in 2008 that it was probed hundreds of thousands of times each day, and the problem has only grown." By not maintaining a strong defensive posture could introduce an unnecessary vulnerability. Saxon explains how once and vulnerable individual is targeted, exploiting malware can be introduced, the individual is then attacked and covered up by obfuscating malware (Saxon 2016). This is just one example of what could happen with inadequate offensive or defensive cyber capabilities. One weakness in cyber defense could introduce "botnet" attacks. Botnet cyber-attacks are coordinated and strictly designed to gain command and control of computer servers (Saxon 2016). Any botnet cyber-attack on space logistics or operations would have devastating and costly effects. As Wang Xushing proclaimed in 1999, *"a 1-ounce integrated-circuit chip in a computer will perhaps be much more useful than a ton of uranium*" (Gauthier 1999). A nation once considered a space superpower might one day find themselves on their knees, rendered helpless and ineffective by a mere cyber-attack that they had not anticipated.

References

Andy, William A., E. Evans, and Deanna Laufer. 2006. "Logistics Lessons Learned in NASA Space Flight." http://www.sti.nasa.gov.

Augustyn, Sławomir. 2020. "A New Strategy for Developing of Space Logistics." *Journal of Konbin* 50 (1): 359–70. https://doi.org/10.2478/jok-2020-0021.

Blazejewski, Kenneth S. 2008. "Strategic Studies Quarterly • Spring 2008 [33] Space Weaponization and US-China Relations."

Brown, Kendall. 2006. "Space Power Integration." *Air University*.

DIA. 2019. "Challenges to Security in Space." www.dia.mil/Military-Power-Publications.

Ferreira-Snyman, Anél. 2015. "Selected Legal Challenges Relating to the Military Use of Outer Space, with Specific Reference to Article IV of the Outer Space Treaty." *Potchefstroom Electronic Law Journal* 18 (3): 488–529. https://doi.org/10.4314/pelj.v18i3.02.

France, Martin. 2000. "Mahan's Elements of Sea Power Applied to the Development of Space Power." *National Defense University*.

Gauthier, Kathryn L. 1999. "China as Peer Competitor! Trends in Nuclear Weapons, Space, and Information Warfare." *Air University*.

Georgescu, Alexandru, Adrian V. Gheorghe, Marius Ioan Piso, and Polinpapilinho F. Katina. 2019. "Critical Space Infrastructures." In *Topics in Safety, Risk, Reliability and Quality*, 36:21–36. Springer Netherlands. https://doi.org/10.1007/978-3-030-12604-9_2.

Gubrud, Mark A. 2011. "Chinese and US Kinetic Energy Space Weapons and Arms Control." *Asian Perspective*.

Hall, J. Reggie. 2003. *Agile Combat Support Doctrine and Logistics Officer Training : Do We Need an Integrated Logistics School for the Expeditionary Air and Space Force?* Air University Press.

Handberg, Roger. 2019. "Standing up the Space Force: Knowns and Unknowns." *Comparative Strategy* 38 (4): 289–301. https://doi.org/10.1080/01495933.2019.1633182.

Hannan, Noel. 2018. "An Assessment of Supply-Chain Cyber Resilience for the International Space Station." *RUSI Journal* 163 (2): 28–32. https://doi.org/10.1080/03071847.2018.1469249.

Howard, Michael. 2010. "Program Research Project Rendezvous in Space-A Look in on Military Space Power." US ArmyWar College.

Johnson, Alan. 2011. "Space Logistics."

Mazanec, Brian M. n.d. "Military Matters Constraining Norms for Cyber Warfare Are Unlikely."

Nye, Joseph S. 2017. "Deterrence and Dissuasion in Cyberspace." *International Security* 41 (3): 44–71. https://doi.org/10.1162/ISEC_a_00266.

Possel, William H. 1998. "Lasers and Missile Defense New Concepts for Space-Based and Ground-Based Laser Weapons." http://www.au.af.mil/au/awc/awccsat.htm.

Robinson, Alec. 1998. "Distingushing Space Power From Air Power: Implications For The Space Force Debate." Air University.

Smith, M. V. 2002. "Ten Propositions Regarding Spacepower," 140.

Smith, Marcia S. Smith. 2003. "US Space Programs: Civilian, Military, and Commercial." *Congressional Research Service*.

Steele, Claire. 2001. "The Weaponization of Space, a Strategic Estimate." U.S. Army Command and General Staff College in.

Szymanski, Paul. 2019. "Techniques for Great Power Space WarAuthor(s): Paul Szymanski Source: Strategic Studies Quarterly." *Air University*. https://doi.org/10.2307/26815047.

Townsend, Brad. 2019. "Space Power and the Foundations of an Independent Space Force." *AIR & SPACE POWER JOURNAL-FEATURE*.

Varni, Jamie G G, Mr Gregory, M Powers, Maj Dan, S Crawford Maj, Craig E Jordan Maj, and Douglas L Kendall. 1996. "Space Operations: Through The Looking Glass (Global Area Strike System)."

Weidenheimer, Randall. 1998. "Increasing the Weaponization of Space: A Prescription for Further Progress."

Weston, Scott. 2009. "Examining Space Warfare." *AIR & SPACE POWER JOURNAL-FEATURE* Spring.

Whitney, Jonathan, Kai Thompson, and Ji Hwan Park. 2019. "A Plan for a US Space Force." *AIR & SPACE POWER JOURNAL-FEATURE*.