Cyber Wargaming in the Space Domain: Enhancing National Security Through Integration and Innovation

Mohammad Tasrif Khan (Mo Khan)

American Military University Alumni (Space Operations Studies), Embry-Riddle Aeronautical University, Florida Campus (Graduate Student-Cyber and Space Operations Major), Telecom Acquisitions Executive

Abstract

In the nascent era of outer space exploration and advancing technologies, this undertaking underscores that the need for cybersecurity in the space domain is a cornerstone for developing and maintaining a secure cyber environment during the entire lifecycle of space missions. It takes a relentless commitment: the complex coupling of disparate pieces of government, civil society, arms, and business into a single full-cycle operation. Cyber-attacks on space infrastructure such as malware installation, ransomware attack, and data/system hacking breaches are serious threats. The areas that are more susceptible to such attacks are revealed in this research, e.g., telecommunications, supply chain, national security, IoT/internet access, and global economies of scale. This project outlines primary goals, first by providing stakeholders insight into the state of play of current cyber wargaming, identifying trends, and closing with a sound framework for the integration of cyber and space-domain environments where impacts will be considerable.

The integrated assessment involves technical and non-technical methods of strategic planning and emphasizes cooperation between public and private organizations. This study design analyzes the questions about the history and significance of cyber wargaming, its vulnerabilities, and the need for its expansion in the cyber and space domains. It establishes objectives like analyzing the current status regarding cyber wargaming, identifying trends, and establishing a system of integration. The technical approaches will cover the areas of cyber wargaming, technology environment, integration of the space domain, state of advanced simulation technologies, and case studies within military (public) and civilian (private) sectors. Strategic approaches, much in the same vein, as that with a non-technical element, go under policy and legal issues, the

 doi: 10.18278/sesa.5.2.9

human factor, cooperation and information sharing, and ethical issues. The conclusion summarizes the main findings of this research while suggesting a framework and explaining the significance and future prospects, thereby advancing an ongoing debate on an innovative and strategic-level convergence of cyber operations and space wargaming as a means to enhance national security.

Keywords: cyber wargaming, cyberspace, national security, infrastructure, vulnerabilities

Título de la Conferencia en 2024: Juegos de guerra cibernéticos en el ámbito espacial: mejorar la seguridad nacional mediante la integración y la innovación

Resumen

En la era naciente de la exploración espacial y el avance tecnológico, este proyecto subraya que la necesidad de ciberseguridad en el ámbito espacial es fundamental para desarrollar y mantener un entorno cibernético seguro durante todo el ciclo de vida de las misiones espaciales. Requiere un compromiso inquebrantable: la compleja combinación de sectores dispares del gobierno, la sociedad civil, las fuerzas armadas y las empresas en una única operación de ciclo completo. Los ciberataques a la infraestructura espacial, como la instalación de malware, los ataques de ransomware y las violaciones de datos y sistemas, constituyen amenazas graves. Esta investigación revela las áreas más susceptibles a estos ataques, como las telecomunicaciones, la cadena de suministro, la seguridad nacional, el acceso a Internet (IoT) y las economías de escala globales. Este proyecto describe sus objetivos principales: primero, proporcionar a las partes interesadas información sobre el estado actual de los juegos de guerra cibernéticos, identificar tendencias y, finalmente, ofrecer un marco sólido para la integración de los entornos cibernéticos y espaciales, donde el impacto será considerable.

La evaluación integrada implica métodos técnicos y no técnicos de planificación estratégica y enfatiza la cooperación entre organizaciones públicas y privadas. Este estudio analiza la historia y la importancia de los juegos de guerra cibernéticos, sus vulnerabilidades y la necesidad de expandirlos a los ámbitos cibernético y espacial. Establece objetivos como analizar el estado actual de los juegos de guerra cibernéticos, identificar tendencias y establecer un sistema

de integración. Los enfoques técnicos abarcarán las áreas de los juegos de guerra cibernéticos, el entorno tecnológico, la integración en el ámbito espacial, el estado de las tecnologías avanzadas de simulación y estudios de caso en los sectores militar (público) y civil (privado). Los enfoques estratégicos, similares a los de los que incluyen un componente no técnico, abarcan cuestiones políticas y legales, el factor humano, la cooperación y el intercambio de información, y las cuestiones éticas. La conclusión resume los principales hallazgos de esta investigación, a la vez que sugiere un marco y explica la importancia y las perspectivas futuras, impulsando así el debate sobre una convergencia innovadora y estratégica de las operaciones cibernéticas y los juegos de guerra espaciales como medio para mejorar la seguridad nacional.

Palabras clave: juegos de guerra cibernéticos, ciberespacio, seguridad nacional, infraestructura, vulnerabilidades

2024年会议主题：太空领域的网络战争：通过融合与创新来增强国家安全

摘要

在外层空间探索和先进技术的新生时代，本研究强调，太空领域的网络安全需求是“在整个太空任务生命周期内开发和维护安全网络环境”一事的基石。其需要不懈的承诺：将政府、公民社会、军备和企业的不同部分复杂地结合成一个全周期的运作。对太空基础设施的网络攻击（如恶意软件安装、勒索软件攻击和数据/系统黑客入侵）都是严重的威胁。本研究揭示了更容易受到此类攻击的领域，例如电信、供应链、国家安全、物联网/互联网接入和全球规模经济。本研究概述了主要目标，首先是让利益攸关方了解当前网络战争的现状，确定趋势，最后为影响巨大的网络和太空领域环境的整合制定一个完善的框架。

综合评估涉及战略规划的技术方法和非技术方法，并强调公共和私人组织之间的合作。本研究设计分析了网络战争的历史和意义、其脆弱性、以及其在网络和太空领域中扩展的必要性。本研究确立了一系列目标，例如分析网络战争的现状、确定趋势和建立集成系统。技术方法将涵盖网络战争、技术环境、太空领域的整合、先进模拟技术的状态、以及军事（公共）和民用（私人）部门的案例研究。战略方法与非技术要素的方法大致相同，涉及政策和法律问题、人为因

素、合作和信息共享、以及伦理问题。结论总结了本研究的主要发现，同时提出了一个框架并解释了其重要性和未来前景，从而推动了关于“网络操作和太空战争在创新和战略层面的融合，以作为增强国家安全的手段”的持续辩论。

关键词：网络战争，网络空间，国家安全，基础设施，脆弱性

Introduction

The pace of technological progress in space exploration and satellite technology has entered a new cyber vulnerability era. The need for strong cybersecurity in space operations has been reinforced by recent attacks. NASA's Terra AM-1 satellites, originally launched in 1999 and vital to NASA's Earth observation network, faced suspicious incidents in 2008—more specifically, potential cyber interference (U.S.-China Economic and Security Review Commission, 2011). In an illustration of real-life risks to space assets, the Russia-Ukraine conflict of 2022 included cyberattacks targeting ViaSat and Starlink satellites (Tidy, 2022).

Cybersecurity has become increasingly important in space as space infrastructure supports global communications, navigation, and national security. The Space Information Sharing and Analysis Center (ISAC) reported in June 2024 that it had observed more than 100 attempted cyberattacks against space systems on a weekly basis, emphasizing the increasing threat landscape faced by the sector (Space ISAC, 2024). This conference proceeding report will investigate the nexus of cybersecurity and space operations; specifically, investigating cyber wargaming as a venue to improve the security of space missions. It aims to accomplish the following three targets: analyze the current cyber threats to the space domain, assess the effectiveness of cyber wargaming, and recommend a framework for meeting space-based cybersecurity challenges. Through fulfilling these goals, this research aims to provide insight into the challenges of protecting essential space assets from the evolving cyber threat in an ever-increasingly connected globe.

Background

As the importance of space-based assets for civilian and military uses has grown, so has the evolution of cyber threats in the space domain. It is a transition from the physical to the digital threat, punctuated by several salient private sector incidents and trends. During the early years of space exploration, the concern revolved mostly around physical threats to satellites. But the digital age has introduced an entirely new range of vulnerabilities. For example, in 2022, a cyberattack

against ViaSat, a private satellite communications company, disrupted internet service across Europe and impacted Ukrainian military communications (Tidy, 2022). The incident underscored the broad implications of cyber threats in space and their potential effects on civilian and military aspects alike.

Private corporations entering the field of space exploration and satellite deployment have complicated the cybersecurity landscape even further. An item that comes to mind is SpaceX's Starlink satellite network, which has been an indispensable asset in numerous situations, including offering internet access in combat zones. In 2022, in conflict zones in Ukraine, there were attempts to jam Starlink frequencies, which led to the company rapidly releasing a software update to mitigate future attempts (Sheetz, 2022). An example of private sector vulnerability is demonstrated in the 2019 cyberattack on Visser Precision, a contractor working for several space and defense companies, including SpaceX and Lockheed Martin. Similar to SolarWinds' other clients, the attack involved both ransomware and data theft, highlighting the risk of supply chain vulnerabilities for the space industry (Cimpanu, 2020).

Currently, there is a patchwork of government, military, and commercial interests in the world of space-based cybersecurity. Programs like those of the Space Information Sharing and Analysis Center (ISAC), which help create collaboration in the space industry, speak to this complexity. According to a report from the Space ISAC, there is an increasing number of attempted cyberattacks on space systems in recent months as of 2023, which has emphasized the increasing risk of the threat landscape (Space ISAC, 2023). It is clear a cohesive cybersecurity strategy across both private and public sectors is required. In turn, the U.S. government has acted in ways to improve cooperation. For example, the Cybersecurity and Infrastructure Security Agency (CISA) identified common sources of cyber risk to space systems and mitigation options mapped to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CISA, 2024).

Private companies are also taking the initiative. Salesforce partnered with Google, Okta, and Slack in 2021 to announce a Minimum Viable Secure Product (MVSP) effort, establishing minimum-security demands for business-to-business software and outsourcing suppliers (Center for Strategic and International Studies [CSIS], 2022). Though not space systems specific, this initiative is indicative of the increasingly important role of the private sector in codifying cybersecurity standards that can also potentially carry into the space domain. These examples highlight the dynamic nature of cyberattacks in the space domain and the importance of generic, collaborative cybersecurity strategies to safeguard the growing ecosystem of interwoven circumstances impacting the security of outer space with the public and private sector.

Methodology

This study employs a semantic approach to identify cybersecurity issues regarding the cyber threat in the space domain. The methodology is a hybrid of qualitative analysis leveraging existing literature and case studies, and a quantitative analysis of cyber incidents in the space sector. The input in question is the mentioning of data statistics dating as far as 2017 for the purpose of key statistical illustrations in this report among public and private sectors. Data collection consisted primarily of a literature review of relevant unclassified academic journals, industry reports, and government documents, typically found on web searches. The research was also aided by a daily influx of interactions with cybersecurity experts and space industry professionals through military and corporate service connections. These conversations offer useful perspectives on current approaches and emerging trends. It also includes an analysis of public data on cyber-attacks on space infrastructure, providing a quantitative view of the prevalence and types of such threats. The data was analyzed thematically to wrest key vulnerabilities, trends, and solutions on cybersecurity. By employing this multi-faceted analysis, the study captures the intricate relationship between cyber threats and space systems, which serves as a strong basis for its conclusions and recommendations.

Cyber Vulnerabilities in Space Infrastructure

Our research revealed some key segments of space infrastructure that are vulnerable to cyber-attacks. These vulnerabilities in both the military and private sectors pose growing threats that could have disastrous impacts on our space-based assets and operations. Telecom systems are a prime target for cyber criminals looking to tap into global communication or grab sensitive data. For instance, in the military domain, in 2018, hackers, thought to be state-sponsored, broke into a U.S. Navy contractor and made away with 614 gigabytes of undersea warfare-related data, including plans for a supersonic anti-ship missile (Nakashima & Sonne, 2018). This incident brought attention to the vulnerability of military communications and data storage systems connected to space-based infrastructure.

The space sector also involves components from a complex network of suppliers involved in satellite manufacturing and launch operations, which poses multiple entry points for cyber-interference or attacks against its supply chains. Visser Precision, a contractor of space and defense companies such as SpaceX and Lockheed Martin, was also a victim of a ransomware and data theft cyberattack in 2019 (Cimpanu, 2020). The incident highlighted supply chain vulnerabilities for major players in the space world. Key systems of national security, such as military satellites and other space-based assets relevant to national security

In the private sector, telecommunications companies such as AT&T and T-Mobile have known vulnerabilities related to their operations, including satellite communications. For instance, the AT&T data breach affecting about 73 million current and past customers, discovered in March 2024. In this breach, the hackers managed to expose sensitive personal data, consisting of Global trade, personal, and private information, including Social Security numbers, passcodes, full names, email addresses, mailing addresses, phone numbers, dates of birth, and AT&T account numbers (AT&T, 2024). Although not specifically aimed at satellite systems, this event highlighted the interconnectedness of terrestrial and space assets communications infrastructure and the risk of cascading impacts from cyber-intrusions.

Figure 1. Millions of customers being impacted by AT&T data breach since March 2024, including identity theft from all walks of life (AT&T, 2024)

Another incident of data breach involved T-Mobile, which had a major data breach in 2021 that impacted more than 50 million customers; hackers accessed personal information through a vulnerable API (Whittaker, 2021). These examples illustrate the continuing difficulty of securing massive amounts of customer data and the possible aftermath to the space-based communications infrastructure. Sandoval's team for AT&T R&D was very involved in ensuring the cyber readiness of AT&T's space-based assets. The increasing convergence of terrestrial and space-based (and Navy) communications was raised with a press release by the recent 2022 announcement of a partnership with Northrop Grumman to create a 5G-enabled digital battle network for the U.S. Department of Defense (AT&T, 2022). Threats in this domain are emerging:

1. Complex spear-phishing assaults aimed at space agency personnel using human frailties to leverage entry into important systems.
2. Malware that used artificial intelligence to target weaknesses in satellite control systems, which could give unauthorized users the ability to change tracking or disable satellites.
3. Given the potential for quantum computing attacks against existing encryption used in space communications, existing security measures may become obsolete.
4. Supply chain attacks on the array of contractors and subcontractors that participate in space infrastructure building.

These developing dangers highlight the necessity to constantly adapt and strengthen cybersecurity initiatives in the military and non-public sector space operations. Let me encourage you to walk through some of AT&T's responses to what was one of the largest data breaches of 2024. It serves as a stark reminder of the need for strong data protection practices, frequent security checks, and quick incident response in an environment where cyber threats are constantly transforming.

Cyber Wargaming in Space Domain

Cyber wargaming has been identifying itself as a useful tool for cyber preparedness and aversion in the space domain. This method includes reflecting attacks in space companies and enables their vulnerabilities, along with the possibility of counters, to be identified. The practice is especially vital as so many systems now depend on space-based assets for functions as critical as communications, navigation, and Earth observation. With most exercises historically centering around terrestrial networks, cyber wargaming in the space domain remains in its infancy. However, space typology scenarios are increasingly being integrated into these simulations. This paradigm shift is necessitated by the unique characteristics of space systems, with their remote environments, challenges of physical access for repairs, and the potential for space effects to impact operations on Earth. Based on these empowered theoretical frameworks, there have been some positive developments demonstrating the evolution of space-centric cyber wargames in recent years. For example, the ICARUS matrix (Imagining Cyberattacks to Anticipate Risks Unique to Space), which is the product of the Ethics & Emerging Sciences Group, produces more than four million different scenarios to anticipate and prepare for space-based cyber threats.

This tool embraces everything from near-term worries to far reaches of the future, such as insider threats, AI weaponization, and false-flag attacks. Lessons learned from field exercises across industry and the military reveal the promise of cyber wargaming to improve space security. In the military arena, the U.S. Space Force recently ran a series of cyber wargames, simulating

ICARUS Matrix: generating novel scenarios in outer space cybersecurity

Instructions: Pick a variable from two or more columns to construct a scenario. This is not a comprehensive list but only a starter kit.

	A: Threat actors	B: Motivations	C: Cyberattack methods	D: Victims / stakeholders	E: Space capabilities affected
1	Major space-faring states	Nationalism	Insider attack	Major space-faring states	GPS / GNSS
2	Other space-faring states	Dominance / influence	Social engineering	Other space-faring states	Earth observation / remote sensing
3	Non-space-faring states	Financial / economic	Ransomware	Non-space-faring states	Military intelligence and capabilities
4	Insider threats	Fraud	Honeypot	State-owned entities	Spacecraft, robotic or crewed
5	Political terrorists	Employment	Sensor attack	Military and other contractors	Life-sustaining services
6	Mercenaries	Blackmail / coercion	Signals jamming	Scientific organizations	Other essential services
7	Eco-terrorists	Terror	Signals spoofing or hijacking	Corporations	Other safety of personnel / others
8	Corporations	Warfare	Eavesdrop / man-in-the-middle	Wealthy individuals	Loss of sovereignty / control
9	Mobile service providers	Disinformation	Network security	General population / society	Earthbound services
10	Launch service providers	Espionage	Supply chain, hardware	Indirect / secondary stakeholders	Emergency services
11	Social engineering groups	Sabotage	Supply chain, software	Marginalized populations	Financial transactions
12	Organized crime	Extremist ideology	AI / ML / computer vision	Social movements	Mining or manufacturing
13	Chaos agents	Cult of personality	Attack coverup	Cultural / religious groups	Scientific capability / research
14	Religious / apocalyptic	Paranoia / anti-technology	Software hacking	Unions / labor reps	Asteroid detection systems
15	Other ideological groups	Boredom / trolling	Systems security	Customers / users via their data	Space weather monitoring
16	Proxies / agents, esp. unwilling	See world burn / chaos	Multi-phase attack / APT	Individual targets	Space traffic management
17	Noncombatants, esp. unwilling	Social / distributive justice	Cloud hacking	Critical specialists	Space tourism
18	Amateur hackers / enthusiasts	Intellectual / tech demo	Account compromise	Critical infrastructure	Launch capabilities
19	AI / machine learning	Revenge / retaliation	Quantum computing / comms	Internet / media / entertainment	Communications
20	Unknown / anonymous	First contact, for and against	Death by 1,000 cuts / long game	AI / machine learning	News / social media

Figure 2. ICARUS Matrix for Space Cybersecurity Operational Readiness (Lin, 2023)

attacks on satellite networks. These exercises resulted in better incident response protocols and underscore the necessity for greater coordination between space and cyber operations. The wargames simulated various scenarios, including attempts to hijack satellite command and control systems, disrupt communications, and manipulate data transmitted from space-based assets. Consequently, the Space Force has honed its defensive tactics and beefed up its cybersecurity protocols for its space operations. For example, in the civilian sector, a leading satellite communications provider used cyber wargaming to find and fix vulnerabilities in their ground control systems, avoiding a potential data breach. This exercise was designed to simulate a range of cyber-attacks on the company's infrastructure, from its satellite control centers to its data downlink facilities and customer-facing systems. Through these simulations, the company discovered previously indeterminate vulnerabilities in the architecture of its network and its software systems. By creating a virtual version of its space and ground-based physical assets, the wargaming process was able to realistically simulate various scenarios without jeopardizing any physical infrastructure. Composed of ethical hackers, red teams tried to penetrate the systems, and blue teams defended against attacks. The drill un-

covered several major vulnerabilities, such as outdated software in ground stations, weak encryption protocols in satellite-to-ground communication links, and potential insider security threats. Based on these findings, the company made a number of improvements, including:

1. Upgrading software and firmware over all ground stations.
2. Enhancing encryption protocols for all space-to-ground communications.
3. Improving access controls and monitoring systems to defend against insider threats.
4. Creating new incident response plans specifically for space-based cyber-attacks.

The proactive lesson learned not only prevented a potential information breach but also significantly improved the overall security posture of the company's space operations. The success of this exercise led to a new regular schedule of cyber wargaming as part of the company's overall security strategy. This work highlights a few case studies in leveraging cyber wargaming and the increasing significance and effectiveness of cyber wargaming within the space domain. However, as global infrastructure and the economy rely more and more on space systems, the natural tendency to protect their physical property must be complemented with cybersecurity practices. Winters (2018) explains why cyber wargaming is an ideal solution: "*It's a powerful tool for organizations to validate their defenses and identify weaknesses, this is especially critical when considering the unpredictable and evolving nature of cyber adversaries seeking to attack space assets*."

Framework for Integrated Cyber-Space Security Wargaming Operations

The findings of the research are foundational and lead to the proposition of a holistic framework to harmonize cyber and space-related security environments for both technical and non-technical measures. Technically, the important measure is to develop more advanced simulation technology. Data up to October 2023 for simulation will bring the best cyber wargame scenario solutions for space-based systems. For example, tools such as SimSpace Cyber Range provide customized solutions that can drastically improve detection capabilities by using realistic emulation of actual cyber threats. Cybersecurity needs must be addressed through space domain-specific measures as well. This includes setting up personalized security protocols allowing satellite communications to take into account the distinctive problems posed in the space environment, e.g., the necessity for radiation-resistant algorithms and onboard, real-time threat detection systems. The policy and legal aspects are also an important part of this paradigm. We must urgently shape international norms and treaties around cybersecurity in space. Initiatives like some of NASA's recent work applying artificial

intelligence, blockchain, and nanosatellites to improve satellite security could provide useful models. Public-private partnerships are also a key element of this framework. Creating information-sharing forums and conducting joint cybersecurity exercises between government and commercial space companies would help greatly improve overall space cybersecurity. The U.S. Government and industry have become increasingly reliant on satellites, requiring a "Defense-in-Depth" approach to space cybersecurity. This framework attempts to foster a holistic cyber environment for space domain problems by attempting to leverage both technical and non-technical mechanisms.

Conclusion

Implementation Barriers

The proposed framework for integrated cyber-space security faces several implementation challenges:

1. **Technological limitations:** Accurately simulating complex space systems remains a significant hurdle. The unique environment of space and the intricate nature of satellite networks pose challenges in creating realistic cyber wargaming scenarios.
2. **Regulatory hurdles:** International cooperation on space cybersecurity is hampered by varying national interests and the lack of a comprehensive global regulatory framework. Establishing common standards and protocols across different countries and space agencies presents a formidable challenge.
3. **Resource constraints among national and global entities:** Smaller space agencies and companies often lack the financial and technical resources necessary to implement robust cybersecurity measures. This disparity in capabilities could create vulnerabilities in the overall space infrastructure ecosystem.

Emerging Trends

Several trends are shaping the future of space cybersecurity:

1. **Mega-constellations:** The deployment of large satellite constellations, such as those for global internet coverage, introduces new cyber risks due to their increased attack surface and complex network architecture.
2. **Increasing autonomy:** As satellite operations become more autonomous, the cybersecurity implications grow. AI-driven systems present both opportunities for enhanced security and potential vulnerabilities if compromised.
3. **Blockchain technology:** The potential of blockchain in securing space-to-ground communications is being explored, offering new possibilities for data integrity and secure transactions in space operations.

Areas for Further Research

To address future challenges, further research is needed in:

1. **Quantum-resistant encryption:** Developing encryption methods that can withstand attacks from quantum computers is crucial for long-term space communications security.
2. **AI-driven threat detection:** Advancing AI and machine learning capabilities for real-time threat detection and response in satellite networks.
3. **Legal and ethical frameworks:** Establishing guidelines for offensive cyber operations in space, balancing national security interests with international cooperation and ethical considerations for private sector entities additionally.

The findings highlight the urgent need to embed cybersecurity in space operations throughout the boardroom. A proposed integration framework for cyber-space security integration has been developed as a basis for these sectors to face challenges within the cyberspace and outer space rendezvous. Understanding that as space activities grow and change, so too does the need for cybersecurity, all stakeholders, from government to the private sector, need to ensure that cyber is the first order of business for their space missions. Addressing these issues requires collaboration and innovation, ensuring that our increasingly space-dependent world remains secure and reliable. This is a crucial development in proactive cybersecurity — integrating cyber wargaming with space mission planning. Simulating possible attacks and responses can help organizations prepare for the complex threat environment of the future and comes from protecting critical space infrastructure for generations ahead. This not only makes sure that current security measures are strengthened but also promotes a spirit of sustainability and evolution against cybersecurity attacks in the space domain.

References

AT&T. (2022, January 11). AT&T and Northrop Grumman to deliver 5G-enabled capabilities to U.S. Department of Defense. *AT&T Newsroom.* https://about.att.com/story/2022/att-northrop-grumman-5g-dod.html

AT&T. (2024, March 30). AT&T provides update on cybersecurity incident. *AT&T Newsroom.* https://www.att.com

Center for Strategic and International Studies (CSIS). (2022, March 22). A shared responsibility: Public-private cooperation for cybersecurity. https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity

Cimpanu, C. (2020, March 2). Ransomware gang targets space and defense industry. *ZDNet*. https://www.zdnet.com/article/ransomware-gang-targets-space-and-defense-industry/

Cybersecurity and Infrastructure Security Agency (CISA). (2024). Partnerships and collaboration. https://www.cisa.gov/topics/partnerships-and-collaboration

Kan, S. (2007). China's anti-satellite weapon test. *Congressional Research Service*. https://fas.org/sgp/crs/row/RS22652.pdf

Lin, P. (2023). Why Space Cybersecurity Needs More Imagination. *Via Satellite*. https://interactive.satellitetoday.com/via/articles/why-space-cybersecurity-needs-more-imagination

Nakashima, E., & Sonne, P. (2018, June 8). China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare. *The Washington Post*. https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html

Sheetz, M. (2022, March 5). Elon Musk says SpaceX's Starlink satellite internet service is activated in Ukraine. *CNBC*. https://www.cnbc.com/2022/03/05/elon-musk-says-spacexs-starlink-satellite-internet-service-is-activated-in-ukraine.html

Space ISAC. (2023). *Annual threat report: 2023*. Space Information Sharing and Analysis Center.

Space ISAC. (2024). *Quarterly threat report: Q2 2024*. Space Information Sharing and Analysis Center.

Tidy, J. (2022, March 31). Ukraine war: 'Cyberattack' on satellite internet service. *BBC News*. https://www.bbc.com/news/technology-60912789

U.S.-China Economic and Security Review Commission. (2011). *2011 report to Congress*. U.S. Government Printing Office.

Whittaker, Z. (2021, August 18). T-Mobile confirms it was hacked after customer data posted online. *TechCrunch*. https://techcrunch.com/2021/08/16/t-mobile-confirms-it-was-hacked-after-customer-data-posted-online/

Conflict of Interest Statement

The author declares no conflicts of interest related to the research and findings presented in this publication. The author's telecom sector work experiences with AT&T and Charter Communications Inc., does not pose a conflict of interest, as the research focuses on broader cybersecurity and space domain issues from unclassified reports, rather than specific company interests or technologies.