Received: Added at production | Revised: Added at production | Accepted: Added at production

DOI: xxx/xxxx

Space Support Research in the Communication Sectors and Risk Determination Against Core Systems and Processes Targeted by Global Threats

Edward Smith | Dr. Chris Schweigert*

School of Technology and Engineering, National University
E-mail: e.smith8084@o365.ncu.edu (Edward Smith),

Correspondence
*Corresponding author: Dr. Chris Schweigert
Email: cschweigert@ncu.edu

Funding Information
This research was supported by the

Summary

The communication sector, also known as the telecommunications industry, plays a vital role in the economy by providing essential infrastructure and services for transmitting voice, data, and video traffic, contributing significantly to driving economic growth and fostering innovation[1]. It is crucial to prioritize safeguarding our communication networks, as it is vital to ensure the security of our data to maintain the trust of consumers and businesses, given the numerous cybersecurity threats that endanger the security of our communication sector[1]. The importance of security is due to increased private sector involvement in the space industry, resulting in a global market worth $269 billion as of 2017 and the attraction of new participants and initiatives[2]. This transition towards profit-driven economics has also led to faster research and development turnaround times and smaller, flexible teams resembling the IT industry rather than traditional aerospace or military organizations[2]. This research aims to deepen our understanding of the vulnerabilities and risks associated with Core Targeted Systems in the Communication Sector and provided insights into effective strategies for countering adversarial tactics in these critical domains. By examining Space System Risk Insights and exploring Space System Adversarial Tactics Use Case Tactics, the authors seeks to contribute to developing a more robust and resilient communication infrastructure in space.

1 | DISCUSSION

The Communications Sector relies on the Supply Chain, Information Technology (IT), and GPS. Moreover, its dependencies include the Information Technology Sector and the Defense Industrial Base (DIB) Sector[3] . Critical service in this sector consists of suppliers, networks, and service providers, creating a complex ecosystem such as the Internet[3]. Vulnerabilities or threats to non-communications sector functions and capabilities can impact network provider services, demanding continuous attention[3]. Threat actors employ innovative combinations of traditional espionage techniques, economic espionage, supply chain, and cyber operations. These actors also acquire valuable information, research, and technology from the nation's economy by infiltrating critical infrastructure[4]. Physical security and protection of communication sector infrastructure are equally important to digital vulnerabilities due to the susceptibility to attack, vandalism, and theft[1].

1.1 | Communication Risk in the National Infrastructure

The national communications infrastructure is a complex arrangement of networks managed by individual providers and divided into three functional domains: Services and Applications, Core, and Access Networks[3]. The diagram in Figure 1 illustrates the model of the Communications Sector architecture, which exhibits five primary approaches for accessing voice, video, and data services on the core network, namely broadcasting, cable, satellite, wireless, and wireline networks[5]. Space systems and their supporting infrastructure, including software, must be designed and operated with cybersecurity considerations and risk assessment[6].

As one of four access networks, satellites play a critical role in various aspects of our daily lives, such as global connectivity, positioning, navigation, timing, scientific research, exploration, weather tracking, and national defense[6]. This provision of end-to-end communication services for customers depends on the IT Sector's delivery of dependable products and services[3]. One of the main applications of GPS in the commercial communications industry, as part of the DIB sector, is to provide precise timing and network synchronization functions. This function allows for greater flexibility for end users due to the widespread coverage of GPS[3]. The significance of ensuring cybersecurity resilience is critical to both terrestrial and space-based communications. Resilience is paramount because the failure to implement proper practices in these domains can result in severe consequences[6]. To enhance national resilience, the United States government aims to promote measures in both government and commercial space operations. The aim is to safeguard space assets and infrastructure from cyber threats and maintain uninterrupted operations[7].

2 | RESEARCH ANALYSIS

The Memorandum on Space Policy Directive-5, released by the White House, contains a section on cybersecurity principles for space systems that is recommended for cybersecurity professionals[7]. The United States considers unrestricted space autonomy essential for promoting national security, economic well-being, and scientific understanding. These space systems enable critical functions such as global communication, navigation, scientific research, exploration, weather monitoring, and crucial national security applications[7]. The space environment is transforming due to technological advancements, societal acceptance, and increased investment. This transformation leads to increased accessibility for multiple stakeholders, expanding the threat landscape in the space industry due to the emergence of new constellations and the potential for a significant increase in the number of satellites in orbit[2]. Moreover, insufficient cybersecurity on land can result in typical consequences like losing intellectual property, disruptions in operations, and compromised devices, while lacking cybersecurity in space can lead to significant financial losses due to the diversion of vehicles[6].

2.1 | Core Targeted Systems in the Communication Sector

One of the main focuses is on large global corporations involved in satellite, aerospace, and communication industries during research and development of advanced technological products[8]. Satellites employ ground-based and space-based features to link services, such as facilitating two-way voice, video, and data communication, gathering data, identifying events, maintaining accurate timing, and enabling navigation[3]. Users can acquire data through a direct connection to the satellite receiver or by transmitting it from a ground station gateway connected to a satellite to a user interface via terrestrial networks[2]. The motivation to upgrade and improve capabilities for countries is growing in almost all areas of the space industry, including satellite communications, remote sensing, navigation-related aspects, science, and technology demonstration[9].

2.2 | Space System Risk Insights

The current global threat landscape is becoming more diverse and dynamic, as emphasized in the most recent Annual Threat Assessment of the U.S. Intelligence Community (IC), with an increasing number of state and non-state entities focusing on the United States[4]. Threat actors focus on obtaining classified U.S. secrets and actively collect data from various U.S. Government agencies and all sectors of the U.S. economy[4]. According to the report, the primary targets are ground and radio frequency communications, however, the prominence of satellite constellations could lead to a shift in focus toward the space segment (Figure 2)[2]. They explicitly target personal data, trade secrets, intellectual property, technology, and research and development[4]. These actors utilize their capabilities, patience, and resources to accomplish their goals[4]. The success of civilian space missions

heavily depends on a vast network of interconnected resources and assets, both in space and on the ground, which could be exploited[10]. Any successful attack on these entities could have different impacts on the mission, ranging from minor software crashes to the complete loss of the mission, and could potentially undermine the mission's confidentiality, integrity, and availability[10]. This risk is especially concerning to telemetry, tracking, and command (TT&C) functions and network operations different from the communication activities associated with the satellite's service provision[2].

2.3 | Space System Adversarial Tactics Use Case Tactics

Active threats involve a threat source, like an Advanced Persistent Threat (APT) actor, initiating events that actively disrupt the system to exploit vulnerabilities. This risk includes communication system jamming, unauthorized access attempts, replaying recorded traffic, masquerading as authorized entities, exploiting software weaknesses, supply chain interference, unauthorized data modification, and introducing malicious software[10].

2.3.1 | Initial Access Approach.

Threat actors may focus on software-defined radios (SDRs) to gain access[11] . This tactic is used because SDRs have software-based features that allow for the creation of Command and Control (C2) channels[11]. If combined with attacks on the supply chain or development environment, the programmability of SDRs can be used to secretly configure C2 channels, enabling covert activities by a threat actor[11].

2.3.2 | Reconnaissance Approach.

Threat actors have the potential to gather critical intelligence about the flight termination system of a vehicle through reconnaissance[12]. These actors can then utilize this information to carry out future attacks and specifically target the termination system to achieve the desired impact on the mission[12].

2.3.3 | Exfiltration Approach

Threat actors may exploit the absence of emission security or tempest controls to extract information using a visiting spacecraft, similar to side-channel attacks but utilize an approaching spacecraft to measure the signals for decoding purposes[13].

2.3.4 | Resources Development

Threat actors can compromise ground systems owned and operated by a mission, enabling them to employ these systems in future campaigns or to perpetuate other tactics[14]. These ground systems have already been configured to set up for communication with the targeted spacecraf[14]. By infiltrating this infrastructure, threat actors can organize, initiate, and carry out an operation[14]. Threat actors can utilize these systems for various activities, including execution and exfiltratio[14]. Passive threats, unlike active threats, do not require a threat source to actively attack or interfere with the operations of the target system(s), and they encompass tapping of communications links, resulting in the loss of confidentiality and traffic analysis to determine communication entities without accessing the information[10].

3 | CONCLUSION

In conclusion, the research aimed to deepen our understanding of the vulnerabilities and risks associated with Core Targeted Systems in the Communication Sector and provided insights into effective strategies for countering adversarial tactics in these critical domains. It's clear that there is a need for further research in these areas to enhance our understanding and develop more robust strategies for safeguarding these systems. Furthermore, in-depth analysis is required by space security experts to identify emerging threats and vulnerabilities. In addition, there is a need for ongoing monitoring and risk assessment to adapt to the evolving threat landscape. Further investigation should prioritize the development of prognostic models and methods to mitigate risk in specific space system configurations. Scholars should study innovative technologies and strategies to enhance the resilience of space systems against hostile actions. The dynamic characteristics of space systems and the evolving threat landscape require a proactive approach to ensure the security of vital communication infrastructure in space.

Figure 1
Overview of the Communication Sectors Network Infrastructure

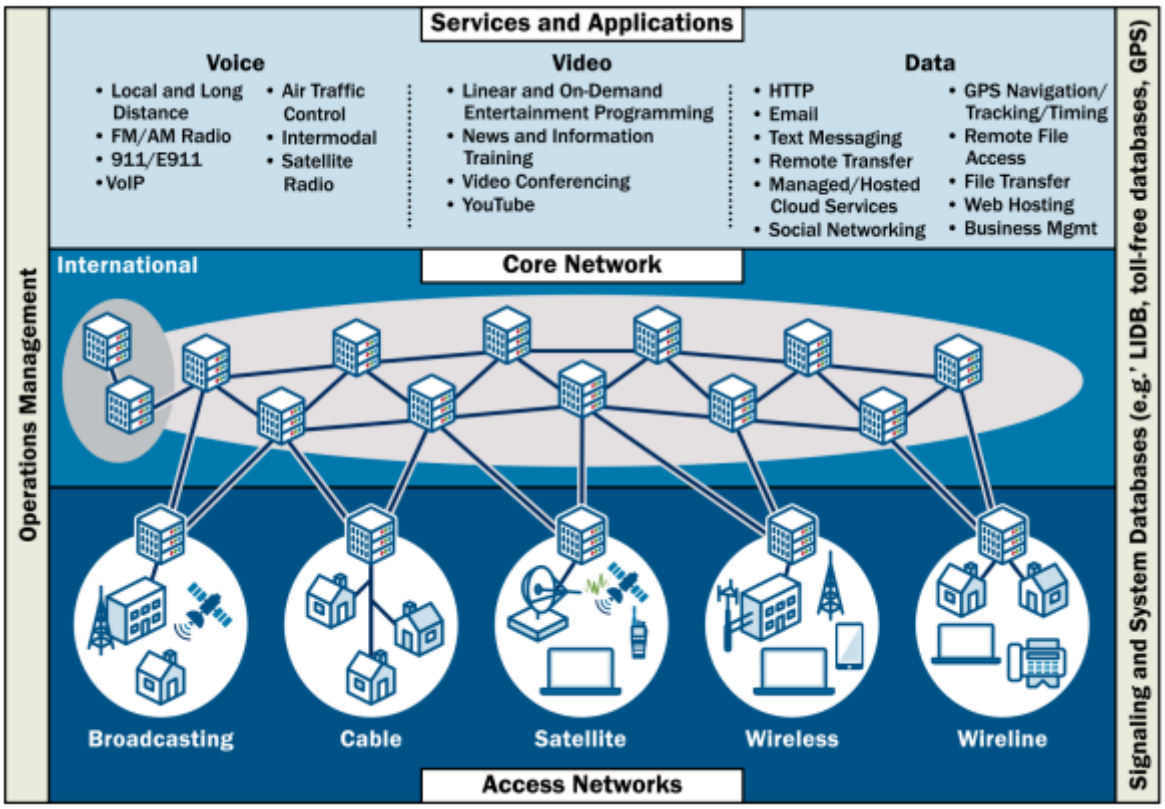

Figure 1 Note. The image captures a simplistic overiew of the layers involved in the communcation sector supported and distributed across various national services. Sources: Introduction to the Communications Sector Risk Management Agency (cisa.gov)

Figure 2
Space Segment Risk Factors to Infrastructure

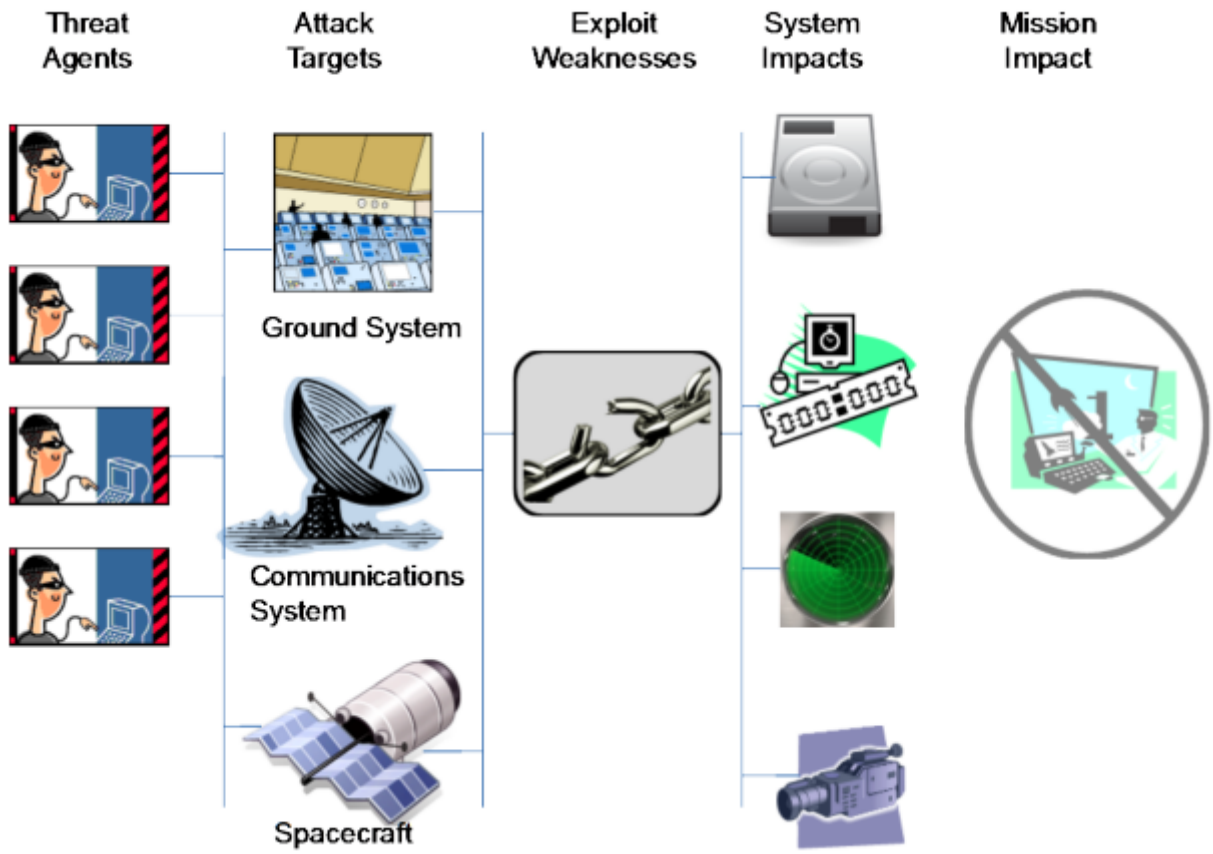

Figure 2 Note. The image is provided by CCSDS showing the layers in which space system are at risk during network and telecommuncation operations. Sources: Security Threats against Space Missions (ccsds.org)

References

1. Senstar . *Communication Sector Threats.* 2023.
2. Manulis M, Bridges C P, Harrison R, Sekar V, Davis A. Cyber security in New Space: Analysis of threats, key enabling technologies and challenges. *International Journal of Information Security.* 2021;20(3):287-311.
3. Security Homeland, An Annex to the NIPP 2013 . *Communications Sector-Specific Plan.* 2015.
4. Orlando M J. *Protect Your Organization from the Foreign Intelligence Threat.* 2021.
5. CISA . *Introduction to the Communication Sector Risk Management Agency.* 2021.
6. Platisis G. *Space Cybersecurity: How Lessons Learned on Earth Apply in Orbit.* 2021.
7. Presidential Documents 56155 Title 3-The President Space Policy Directive-5 of September 4, 2020 Cybersecurity Principles for Space Systems. *Federal Register.* 2020;.
8. Kose J. Cyber Warfare: An Era of Nation-State Actors and Global Corporate Espionage. *Information Systems Security Association.* 2021;.
9. DIA . *Challenges to security in space : space reliance in an era of competition and expansion.* 2022.
10. CCSDS , Report Concerning Space Data System Standards . *Security Threats Against Space Missions.* CCSDS 350.1-G-3; 2022.

11. Compromise Software Defined Radio, Technique IA-0002 | SPARTA. *Aerospace Corporation.* 2022;.

12. Flight Termination, Technique REC-0004.01 | SPARTA. *Aerospace Corporation.* 2022;.

13. Proximity Operations, Technique EXF-0005 | SPARTA. *Aerospace Corporation.* 2022;.

14. Mission-Operated Ground System. *Aerospace Corporation.* 2022;.

How to cite this article: Edward Smith, and Dr. Chris Schweigert (), **Space Support Research in the Communication Sectors and Risk Determination Against Core Systems and Processes Targeted by Global Threats**, *International Journal of Communication Systems, :: .*