INFORMATION SHARING AND ANALYSIS CENTER

YEAR 2024

WHITE PAPER

Space Cyber Security

REPORT BY

ISAC AND SIA-INDIA

ISAC

SIA INDIA

An association for space industry

TABLE OF CONTENTS

Executive Summary

The reliance on space systems for national security, defence, and daily life has never been greater, and with this reliance comes an increased risk of cyber-attacks. Adversaries possess sophisticated knowledge of satellite command and control, as well as space distribution networks, posing critical threats to these systems. The hybrid nature of space systems, which combine information technology (IT) and operational technology (OT), makes them particularly vulnerable.

The recent cyber incursions during the Ukraine crisis serve as a stark reminder of the potential impact on national security and global economic development if cybersecurity regulations are neglected.

This position paper highlights the importance of establishing a Cyber Range for training and testing purposes and developing cybersecurity measures and standards to ensure the integrity of space operations.

Introduction

The space domain has evolved significantly over the past decade, transforming from a purely scientific endeavor to a warfighting domain. The increasing reliance on space-based systems for global communication, navigation, and economic development has created a new set of challenges for space cyber security. The recent report by Booz Allen on emerging tech for the space sector underscores the importance of space domain awareness (SDA) in understanding the space operating environment and perceived threats.

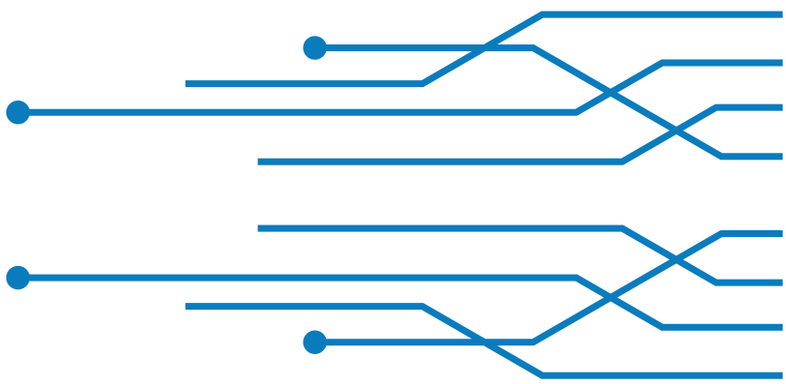
The problem of weaponization

The weaponization of space has become a critical aspect of modern warfare. Space-based systems play a vital role in supporting military operations, including communication, navigation, and surveillance. Cybersecurity is essential for ensuring the integrity of these systems and protecting against potential cyber threats. The U.S. Space Force has indicated the potential anti-satellite (ASAT) capabilities developed by Russia and China as a reason for the need for suitable space-based countermeasures. This highlights the importance of robust cybersecurity measures to prevent the exploitation of space-based systems.

Space cyber security faces unique challenges, including communication latency and signal security, limited physical access for remediation, harsh operational environments, dependency on ground-based infrastructure, and supply chain vulnerabilities. These challenges necessitate innovative solutions that go beyond traditional cybersecurity measures. Advanced monitoring, anomaly detection, and secure communication protocols must be integrated into the design and operation of space missions.

Emerging technologies such as quantum computing pose new challenges but also offer opportunities for advancing space cybersecurity. Quantum-resistant encryption is a burgeoning field that seeks to fortify communications against potential quantum decryption methods, thereby future-proofing space-based assets. Self-healing satellite networks are another forward-looking innovation that can autonomously detect, diagnose, and repair faults, including those induced by cyberattacks.

Rapid Innovations and lack of cyber security in the space sector



There is rapid innovation in the space sector in the following domains and may often lack the necessary cybersecurity practices and standards:

1. Satellite Mega-Constellations: Rapid deployment of large networks of small satellites for global internet coverage lacks comprehensive cybersecurity protocols to protect against hacking and signal interference.
2. Space Tourism: Companies developing commercial space travel services are primarily focused on safety and reliability, often neglecting robust cybersecurity measures to protect onboard systems and passenger data.
3. Autonomous Spacecraft and Rovers: Innovations in autonomous navigation and operations for spacecraft and planetary rovers have advanced significantly, yet they often lack adequate cybersecurity to defend against unauthorized access and control.
4. In-Space Manufacturing: The development of manufacturing processes in space, such as 3D printing and assembly of large structures, requires enhanced cybersecurity to protect intellectual property and ensure operational integrity.

5. Space Debris Management: Technologies for tracking and mitigating space debris are critical for sustainable space operations but comprehensive cybersecurity measures to prevent potential vulnerabilities in implementation.

1. Commercial Satellite Constellations: Companies like SpaceX, OneWeb, and Amazon's Kuiper Systems are launching large constellations of low-Earth orbit (LEO) satellites for global internet connectivity. However, these constellations may be vulnerable to cyber attacks due to lack of proper standards for implementation in this domain.
2. Private Space Stations: Companies like Axiom Space and Bigelow Aerospace are developing private space stations for scientific research, tourism, and commercial activities. However, these space stations often have complex interplay of IT, IOT and OT technologies, making them vulnerable to cyber attacks.

The Need for Establishing a Cyber Range for the Space Sector

Simulation in Space Cybersecurity

The increasing complexity and critical nature of space infrastructure necessitate advanced training and testing facilities. Cyber ranges that integrate phygital labs and virtual simulations provide a safe and realistic platform to explore potential attack vectors and vulnerabilities. They enable the development and refinement of defensive strategies, ensuring that space systems are resilient against a wide range of cyber threats. This proactive approach is vital for maintaining the security and integrity of space operations, protecting both national security interests and commercial investments.

A cyber range, utilizing both virtual simulations and phygital labs that combine IT, OT, and IoT, is essential for preparing and defending against potential cyber threats. These environments provide realistic, hands-on training and testing, allowing for valuable experience without risking real-world operations.

Phygital labs, which integrate physical models and digital simulations, bring a tangible, visual element to cybersecurity training and testing. These labs can accurately represent various components of space infrastructure, from satellite arrays to ground control stations. Combined with virtual simulations, they create an immersive environment where both the physical and digital aspects of space systems are tested for vulnerabilities and resilience. This hybrid approach enables the simulation of complex attack scenarios, providing a comprehensive understanding of potential threats.

The integration of physical and virtual environments offers several advantages. It allows for detailed analysis and understanding of how cyber attacks can affect both the physical and digital components of space systems. Trainees can observe the direct consequences of attacks, improving their ability to develop effective response strategies.

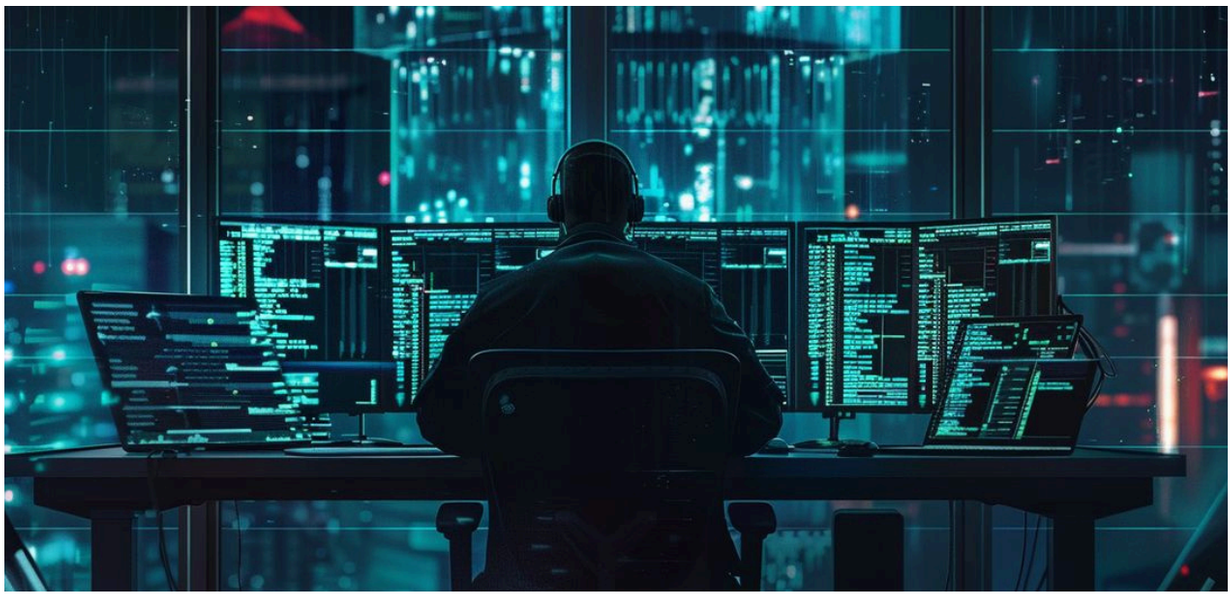
This approach also supports the testing of new security measures in a controlled setting, ensuring their effectiveness before real-world implementation. Additionally, it fosters collaboration among engineers, cybersecurity experts, and policymakers, addressing the multifaceted challenges of space cybersecurity.

Zero Trust Adoption in Phygital Labs

The increasing accessibility of satellite technology has expanded the number of countries and enterprises in space, necessitating distributed cybersecurity measures within phygital labs. These labs integrate IT, OT, and IoT, making the adoption of zero trust technology critical. This approach ensures secure connections and data sharing across various organizations and classification levels, protecting sensitive data among space assets.

AI in Phygital Labs

Phygital labs leverage AI and digital twins for rapid decision-making and democratizing space exploration. AI monitors space debris, enhances satellite navigation, and facilitates autonomous spacecraft operations. However, AI integration raises cybersecurity concerns, including the risk of AI-powered cyberattacks. To mitigate these risks, robust cybersecurity measures must be implemented. AI and machine learning are also used to predict threats and automate responses, providing advanced security for space systems within phygital labs.



The Urgent Need of Establishing cybersecurity standards for Space Sector

Establishing cybersecurity standards for testing space technology is crucial for ensuring the integrity of space operations. As space systems become more integral to national security, communication, and economic activities, they are increasingly targeted by sophisticated cyber threats. Also, countries are expected to increasingly focus on incorporating the space domain into the development of Mosaic warfare, aiming to weaponize the space sector. Mosaic warfare strategies involve the integration of multiple domains, including space, cyber, and ground-based systems.

Establishing comprehensive cybersecurity standards is crucial to mitigate these risks. These standards ensure that space technology is tested rigorously against potential vulnerabilities, from software flaws to hardware weaknesses. By implementing uniform cybersecurity protocols, we can safeguard critical space infrastructure, maintain operational integrity, and protect against adversaries seeking to exploit these vital systems.

Key Benefits of Standards

- Enhanced Security: Standardized testing procedures help identify and rectify vulnerabilities, ensuring robust defences against cyber threats.
- Operational Integrity: Consistent cybersecurity measures prevent disruptions, maintaining the reliability of space operations.
- Global Collaboration: Establishing international cybersecurity standards fosters cooperation, creating a unified defence against global threats.
- Innovation and Resilience: Rigorous standards encourage the development of advanced technologies, enhancing the resilience of space systems.

Cooperation required in the space sector

Global Concerns and the Need for Cooperation

With the expected launch of 25,000 satellites by 2030, the vulnerabilities are becoming increasingly apparent. Global cooperation is deemed essential to cyber-secure space systems, as no formal global treaties currently exist to forbid cyberattacks against them. We must recognize the importance of space for defense and security, linking space security with terrestrial resilience.

International cooperation is crucial for harmonizing regulations across countries to address the complexities of space cybersecurity

- The development and adherence to global cybersecurity standards and treaties are essential for maintaining the security and integrity of space missions
- NATO and its partners are working towards a coordinated approach to ensure the continuous availability of space-based capabilities.

Conclusion

The space sector's rapid innovation highlights the urgent need for comprehensive cybersecurity measures. Establishing cyber ranges that integrate phygital labs and virtual simulations is critical for training and testing against potential threats. These facilities provide realistic environments to explore vulnerabilities, develop defensive strategies, and ensure the resilience of space systems. Adopting zero trust technology and leveraging AI within these labs are essential for maintaining secure and efficient operations. Furthermore, developing and adhering to global cybersecurity standards is crucial for safeguarding space assets and fostering international cooperation. By addressing these challenges, we can protect critical space infrastructure, support national security, and promote sustainable space exploration and utilization.

About ISAC

Information Sharing and Analysis Center, ISAC is India's leading cyber security non-profit foundation and a Partner with the Ministry of Education, CERT-IN, AICTE, Ministry of Defence (MoD), Government of India, Karnataka Digital Economy Mission, IIT Gandhinagar, etc. Established in 2011, ISAC is focused on solving everyday cybersecurity challenges that impact individuals, networks, and organizations.

About SIA-India

As a dynamic, not-for-profit space sector association, SIA-India is dedicated to advancing sectoral interests, accelerating industry growth, and catalysing innovation through strategic engagements with key governmental and global stakeholders, policymakers, regulatory bodies, and standardization entities, aiming to create a vibrant and innovative ecosystem.