JPNT 12(4), 437-445 (2023)
https://doi.org/10.11003/JPNT.2023.12.4.437

JPNT Journal of Positioning, Navigation, and Timing

Efforts against Cybersecurity Attack of Space Systems

Jin-Keun Hong†
Next Convergence Tech/Division of Advanced IT, Baekseok University, Cheonan 31065, Korea

ABSTRACT

A space system refers to a network of sensors, ground systems, and space-craft operating in space. The security of space systems relies on information systems and networks that support the design, launch, and operation of space missions. Characteristics of space operations, including command and control (C2) between space-craft (including satellites) and ground communication, also depend on wireless frequency and communication channels. Attackers can potentially engage in malicious activities such as destruction, disruption, and degradation of systems, networks, communication channels, and space operations. These malicious cyber activities include sensor spoofing, system damage, denial of service attacks, jamming of unauthorized commands, and injection of malicious code. Such activities ultimately lead to a decrease in the lifespan and functionality of space systems, and may result in damage to space-craft and, lead to loss of control. The Cybersecurity Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) matrix, proposed by Massachusetts Institute of Technology Research and Engineering (MITRE), consists of the following stages: Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command & Control, Exfiltration, and Impact. This paper identifies cybersecurity activities in space systems and satellite navigation systems through the National Institute of Standards and Technology (NIST)'s standard documents, former U.S. President Trump's executive orders, and presents risk management activities. This paper also explores cybersecurity's tactics attack techniques within the context of space systems (space-craft) by referencing the Sparta ATT&CK Matrix. In this paper, security threats in space systems analyzed, focusing on the cybersecurity attack tactics, techniques, and countermeasures of space-craft presented by Space Attack Research and Tactic Analysis (SPARTA). Through this study, cybersecurity attack tactics, techniques, and countermeasures existing in space-craft are identified, and an understanding of the direction of application in the design and implementation of safe small satellites is provided.

Keywords: cybersecurity, ATT&CK, attack, space system, security threats

1. INTRODUCTION

The space system is consisted of space and terrestrial components. A part of the space component, the satellite system, is composed of payloads, equipment that performs the functions of the satellite, and a bus connecting the payload and the functional equipment. The space component also includes Telemetry, Tracking and Control (TT&C), Command and Data Handling, and Attitude Determination and Control Systems.

In the space system, attackers can maliciously be destroyed, disrupted, and degraded system, network, communication channels, and space operations. Malicious cyber activities targeting the space system include sensor spoofing, system damage, denial of service attacks, jamming of unauthorized commands, and malicious code injections. These malicious activities can be led to reduce life or functionality of the targeted space system and loss of control, including damage to space vehicles (ESPI 2022).

The U.S. government is interested in cybersecurity principles for the space system. Of course, the space system relies on information systems or networks that support

Received Nov 10, 2023 **Revised** Nov 18, 2023 **Accepted** Nov 26, 2023
†**Corresponding Author**
E-mail: jkhong@bu.ac.kr
Tel: +82-41-550-2445 Fax: +82-41-550-9107
Jin-Keun Hong https://orcid.org/0009-0008-1393-2647

design conceptualization, launch, and flight operations. Additionally, channels of command and control (C2) between the space and ground components, and mission information transmission performance in the space system, are depended on wireless frequency and wireless communication channel performance.

The U.S. government's emphasis on the space system and cybersecurity principles in the areas of Position, Navigation, and Timing (PNT) can be found in the president's executive orders or standard documents, which can be referred to in the cyber activities of this paper.

The U.S. government, leading in space cybersecurity policies, has incorporated space security plans into the national space policy master plan through the establishment of the National Space Policy Secretariat within the State Council (established April 2016), the Cybersecurity Strategy Headquarters within the Cabinet (established April 2015), the National Institute for Cybersecurity and Strategy (NISC, established September 2015), and the Space Policy and Strategy Headquarters (established June 2020) (Schmitt 2017). The plan includes securing space systems, disaster response, creating new knowledge based on space science and exploration, and realizing economic growth and innovation based on space.

The U.S. government has established six defense measures for responding to cyber-attacks in the space security system. These measures include strengthening the security of information systems; cyber-attack response for units, including cyber defense, system protection, communication protection, and computer security assessment; maintenance and development; cutting-edge technology research (education); manpower development; and inter-agency collaboration.

Naturally, such U.S. government cybersecurity strategies and policies in the space system are closely linked with its ally such as the Japanese government. The Japan Self-Defense Forces, in collaboration with the U.S. Department of Defense, closely cooperate in the use of the electromagnetic spectrum (command communication surveillance area). Areas of cooperation are sensitive in terms of security, and include understanding and applying electronic warfare capabilities, visualizing, strengthening information collection, and analysis capabilities (establishing units, system upgrades), neutralizing capabilities (aircraft development and research, purchasing and Research & Development of laser systems), and manpower development (education) areas. The cooperation between the U.S. and Japanese governments in cybersecurity strategies and policies is very tight and solid.

The National Oceanic and Atmospheric Administration (NOAA)'s Commercial Remote Sensing Regulatory Affairs develops and implements appropriate cybersecurity plans, designs and practices that are necessary requirements for space operators. The Space Policy Guidelines identify the comprehensive processes needed to develop and operate systems flexible for cyberattacks based on Security Policy Directive (SPD)-5 (NOAA 2022). Of course, SPD-5 describes cybersecurity models for risk-based deep defense. In threatened informal risk-based engineering of space systems, operational technologies and software elements, along with comprehensive policies, procedures, controls, and technologies, must be considered for cybersecurity response.

This paper contributes to understanding the direction of attack tactics, techniques, and countermeasures focusing on the US government's cybersecurity principles, cybersecurity policies, and Space Attack Research and Tactic Analysis (SPARTA) for the space system described above.

In this paper, the significance of cybersecurity is initially discussed in the introduction, drawing from research on the background of U.S. cybersecurity strategies and policies in the space system. Following this, Chapter 2 aims to explore the security threats and attacks, activities of cybersecurity in the space system. Chapter 3 describes the tactics, techniques, countermeasures in the space system, and Chapter 4 seeks to conclude the paper.

2. THREATS AND ACTIVITIES OF CYBER SECURITY IN THE SPACE SYSTEMS

2.1 Security Threats and Attacks in a Space System

Security threats in the space system can also target the terrestrial counterpart of the communication system, causing it damage. Security threats occurring in the communication channel environment between the space and ground parts include jamming or eavesdropping attacks, hijacking or Global Positioning System (GPS) signal spoofing attacks. Damage to the terrestrial system allows attackers to control and track satellite systems.

Security threats to the terrestrial system include physical attacks on resources composing the terrestrial system, network attacks (exploits), infrastructure disruption attacks (cloud), software and hardware attacks (bugs, errors, data modification), supply chain attacks (leakage of software, source codes, etc.), and software attacks on existing equipment (Trump 2020).

On one hand, since the space system can be threatened from a supply chain perspective, there is a need to upgrade

https://doi.org/10.11003/JPNT.2023.12.4.437

risk assessment and vulnerability inspection paradigms. Commercial Off-The-Shelf (COTS)-based satellites can expand the cyber-attack surface. Vulnerabilities can be heightened when considering software, networks, and cloud in the terrestrial counterpart of satellites due to scalability and dependency issues.

Attacks in the space system include operational and security control attacks targeting space-craft or satellite systems (vulnerabilities in software and hardware), buffer overflows, denial of service, and memory attacks. To address such security threats in the space system, there are also issues with the security management system regarding key management problems (e.g., quantum key distribution, scalability, group management), software updates, secure software (e.g., memory safety, fault tolerance), and authentication (e.g., navigation message authentication, chip message authentication, stream loss-tolerant authentication). Countermeasures to respond to the security threats of the space system include kinetic operations and capabilities, electronic warfare capabilities, non-physical kinetic operations, and cyber warfare capabilities (Manulis et al. 2021).

When considering cybersecurity issues in the space system, the security principles advocated by Northern Sky Research (NSR) include authentication and authorization, minimum privilege allowance, network management and monitoring segmented into smaller areas, strong encryption and multi-factor authentication, and situational awareness-based access control policies. Absolute verification for new users, minimum connection settings, and dynamic authorization are also emphasized.

Naturally, the space system (including satellite systems) is considering the application of block-chain technology with an aim to ensure zero trust. In their research, Pavur and Martinovic evaluate the security techniques in space systems. The primary targets of these cyber-attacks are the Command Control Communications Computer Intelligence Surveillance and Reconnaissance (C4ISR) systems (Rajagopalan 2019).

Potential attackers can range from the military, deploying space system weapons, intelligence agencies involved in technical theft or eavesdropping, insiders who might commit technical theft, suppliers causing disruptions, to competitors engaged in technological theft.

Three primary victims in the space domain are the payloads, signals, and ground systems: In payloads, these refer to essential components like surveillance imaging equipment, required for specific tasks or functions of a satellite. Vulnerabilities in payloads can lead to various threats such as Denial of Service attacks, hardware backdoors, privilege escalation, hijacking, and sensor injection.

Also in signal channels, attacks on signal channels can manifest in various forms like jamming, eavesdropping, meta-data analysis, replay attacks, and signal injection or hijacking. In ground systems, these are susceptible to malware, social engineering attacks, physical access breaches, data destruction, and hardware backdoors. It is noteworthy that over 67% of security incidents in satellite systems arise from radio frequency communication attacks (NSR 2022).

The communication attack types on satellite systems include eavesdropping, signal injection, and signal spoofing. In an eavesdropping attack, unauthorized attackers intercept or decrypt signals. Signal injection attacks maliciously encapsulate legitimate transmission data. Meanwhile, signal spoofing involves malicious hijacking or overwriting of lawful radio signals. Addressing these vulnerabilities and potential threats is imperative for ensuring the security and functionality of space systems in an increasingly digital age (MOD 2020).

Notably, the lack of cybersecurity standards or regulations for commercial satellites exacerbates security vulnerabilities (Pavur & Martinovic 2022).

Spacecraft protection requires an understanding of how to manage cyber risks, along with the introduction of the Defense in Depth (DiD) concept (Ingols & Skowyra 2019). Security threats that impede secure small satellite design and implementation include aggressive approaches such as supply chain, physical manipulation, malicious insiders, credential theft, sandbox bypass, and channel intercept. A supply chain attack is an attack that targets components of hardware, firmware, and software in space systems through infusion prior to logistics delivery or integration. A physical manipulation attack is a tampers attack that acquires physical access to components of the system and uses system information to access other areas. There are attacks such as malicious insider attacks or credential theft. A credential theft attack is an attack that pretends to be the identity and authority of a normal user in the space system. Sandbox bypass attack refers to an attack that moves through a range of work or a limited boundary. It is an attack in which the control channel is controlled through the interception of the control channel.

Techniques that must be considered in the design process to mitigate the attacks include obtaining safety by minimizing or simplifying interfaces between system components, minimizing attack surfaces by minimizing the overall size and complexity of the system, isolating between components against interfaces in software or systems, data

protection (integrity, confidentiality, reliability, freshness, etc.), authentication and secure control to eliminate illegal data flows.

Satellites such as CubeSats, aiming for cost reduction by leveraging COTS technologies, may be exposed to vulnerabilities inherent in open-source components, such as the inclusion of backdoors or other exploitable weak points. CubeSats typically employ open-source software for their onboard operating systems, like FreeRTOS or KubOS. Of course, they can also operate in environments based on more general OS platforms, such as Windows or Linux (Starling et al. 2021).

2.2 Activities of Cybersecurity for Risk Management of Space System

There have been cybersecurity activities at the government level in terms of risk management for space systems. The European Commission (EC) has passed the Network Information System (NIS) 2 Executive Order (NIS2 Directive 2022). The CISA and FBI announced enhanced cybersecurity for SATCOM network providers and customers at AA22-076A (America's Cyber Defense Agency 2022). US Space Force started IA-Pre (USSF 2023). This program is a preliminary security assessment program for commercial satellite communication services.

The German BSI has announced basic cybersecurity measures for satellite systems and cybersecurity strategies for space infrastructure strategies (Federal Office for Information Security 2023). The UK Space Agency has released a cybersecurity toolkit, Ver.2, and the OSA has released commercial space system security guidelines (UK Space Agency 2020). DHS launched a pilot process working group in May 2021 to consider whether to add space systems to its 16 core infrastructure sectors.

Based on the threat information highlighted in SPD-5, risk-driven engineering approaches include threat recognition, risk assessment, security control design and implementation, monitoring and validation. The threat recognition process identifies and analyzes potential threats in space systems. The risk assessment phase assesses how identified threats can affect space systems and networks. In the design and implementation phase of security controls, security controls are implemented, policies are designed and deployed to minimize assessed risks. The monitoring and verification phase identifies the behavior of installed security controls and responds to new threats through continuous monitoring.

SPD-5 establishes cybersecurity principles for space systems. The principles of cybersecurity are as follows. First, infrastructure, including space systems and software, should be risk-based and developed and operated using engineering with cybersecurity in mind. Second, in the system of the owner or operator of the space system, and in the system of the control center, the cybersecurity plan should include the ability to ensure the maintenance and recovery of control of space vehicles. Third, the implementation of cybersecurity principles should reflect existing good case studies and norms of conduct. Fourth, operators and owners of space systems must discover good examples within the legal scope. Fifth, owners and operators of space systems should design security measures in a way that properly manages risks and minimizes unnecessary burdens.

2.3 Activities of Cybersecurity for Risk Management of Position, Navigation, and Timing

There have been cybersecurity activities at the government level in terms of risk management for PNT.

National Institute of Standards and Technology Interagency Report (NISTIR) 8270 addresses cybersecurity issues for commercial satellite operations (Scholl & Suloway 2023).

Of course, NIST IR 8270 presents the problem of cybersecurity in the commercial satellite part (Scholl & Suloway 2023). NIST IR 8323 deals with the problem of cybersecurity in the user part, and 8401 deals with the problem of cybersecurity in the ground part together. In addition, 8401 focuses on the issue of applying the framework of cybersecurity for command and control of satellites. A cybersecurity profile is presented in the satellite and the ground part, which is designed to be used as part of a risk management program for the purpose of managing cybersecurity risks to systems, networks and assets that make up the ground part of satellite operations. The focus of this issue is on risk management and cybersecurity frameworks.

In addition, NIST created a profile for cybersecurity in hybrid satellite networks in Certified Secure Web Application Program 27 (McCarthy et al. 2023). NISTIR 8401 created a document on the application of a cybersecurity framework for satellite command and control (Lightman et al. 2022). In NISTIR 8323 (Bartock et al. 2021), it is a security profile document relating to PNT services, which is linked to the national resilience enhancement policy for responsible use of PNT services as stated in Executive Order 13905 (Trump 2020).

As the number of suppliers grows, the attack surface for infiltrating the space system broadens, potentially leading

https://doi.org/10.11003/JPNT.2023.12.4.437

to an uptick in vulnerabilities. So far, we have explored the myriad security threats manifesting in space systems. In Chapter 3, it is described on attack tactics, techniques, and countermeasures for cybersecurity of space systems.

3. COUNTER-ATTACKS TACTICS, TECHNIQUES IN THE SPACE SYSTEMS & PNT

3.1 Attack Tactics in Space Systems

In the space domain, a cybersecurity framework should be established under the principles of minimizing the attack surface, protecting data, robust system design, continuous monitoring and vulnerability management, human factor management, and sharing of cyber threat intelligence.

Given the expansive attack surface of space systems, their security design must aim to minimize potential attack vectors. This includes reducing unnecessary network connections, segregating system components, and deactivating unused functionalities. Throughout its lifecycle - creation, transmission, storage, and processing - data within the space system must be safeguarded. The system should be designed to operate securely and resiliently against potential attacks or failures. Continuous real-time monitoring against potential threats and swift patching of vulnerabilities are paramount. Moreover, personnel involved in designing and operating the space system must undergo comprehensive security training. Organizations associated with the space system must actively share threat intelligence and collaborate in real time.

The primary objectives of establishing a cybersecurity attack matrix for space systems are to enhance security and collect strategic intelligence. Enhancing security pertains to protecting national space assets and their information, which can be prime targets for cyberattacks. Strategic intelligence collection revolves around understanding various attack scenarios that might target space systems and formulating counter-strategies. This intelligence aids in anticipating and defending against attempts to steal national secrets or disrupt systems.

Cyberattacks on satellite systems are associated with in Very Small Aperture Terminal (VSAT) terminal attacks, eavesdropping, and hijacking. Vulnerabilities can be found VSAT terminal software and the protocols used at higher layers. Embedded devices utilized in space systems and operating systems like Windows 10 occasionally can be presented vulnerabilities in TCP/IP and remote protocols.

If languages like C and C++ are employed, vulnerabilities can arise from unsafe memory command usage. The CubeSat Protocol is implemented in an open-source TCP/IP stack environment, and given that the CubeSat Space Protocol library is C-based, open-source, and implemented on CubeSats, it is potentially exposed to vulnerabilities. Libscp (CubeSat Space Protocol) reported three vulnerabilities (Common Vulnerabilities and Exposures (CVE) 2016-8596, 8597, 8598). The CVE 2016-8596 vulnerability is a common fragmentation vulnerability resulting from a memcpy buffer overflow attack, allowing an attacker's component to propagate through the internal Controller Area Network bus and compromise other components. The 8597 vulnerability relates to the Small Fragmentation Protocol (SFP) and can cause a buffer overflow from a single fragment. An attacker accessing the network layer of the SFP protocol can execute arbitrary code on the vulnerable module. The 8598 vulnerability is a simple buffer overflow issue due to insufficient verification of the length field in memcpy. Attackers with access to the ZeroMQ interface can execute arbitrary code on the vulnerable component through this interface.

3.2 Attack Techniques in Space System

The MITRE ATT&CK is a framework for identifying and analyzing the behavior of attackers such as APT. In this framework, the attacker's behavior is approached from a technical point of view and classified into tactics and techniques. ATT&CK represents attack tactics and techniques for attackers to infiltrate systems, steal information, and achieve their goals. MITRE ATT&CK is used to analyze the behavior of attackers and prepare defense strategies.

The ATT&CK Matrix consists of matrix format. Each row is a tactic, and each column means a specific skill. Each cell describes how the corresponding tactics and technologies interact, and means whether the corresponding technologies belong to the corresponding tactics.

The SPARTA matrix, proposed by Aerospace Corporation, provides relevant techniques concerning the attack processes in space systems (Bailey 2021). This matrix defines and categorizes activities that could harm spacecraft and offers insightful analytical information on cybersecurity and attack & tactical research in space systems.

The SPARTA ATT&CK Matrix is similar to MITRE's matrix format. The difference deals with attack tactics, techniques, and countermeasures that take place against the spacecraft environment.

In a space system comprising terrestrial, space, and communication components, one can approach the ATT&CK matrix primarily as proposed by MITRE. The

terrestrial component can be distinguished into the physical layer, boundary layer, Computer Network Defense (CND)/ Incident Response (IR) layer, network layer, end-to-end layer, and software layer. The space component consists of the spacecraft software layer (including satellites), Single Board Computer (SBC) layer, Intrusion Detection/Intrusion Prevention System (IDS/IPS) layer, encryption layer, communication link layer, and terrestrial layer (Bailey 2021).

Data layer applies security such as transport encryption (including Date at Rest and Data in Transit) and Telecommunications Electronics Material Protected from Emanating Spurious Transmissions (TEMPEST) and protects data.

The electromagnetic field generated when the information technology device is operating causes unintended emission. In cybersecurity, TEMPEST refers to technology or equipment that detects emitted electromagnetic signals and steals information. At this time, the emitted signal may be collected and reconstructed, thereby damaging the confidentiality (Martin et al. 2023).

Spacecraft layer protects software through measures such as configuration management, secure coding standards, dynamic testing, software component analysis, and static code analysis. SBC/bus/processor layer protects hardware such as command authorization, memory protection, root of trust, bus disconnection, logging, and auditing. IDS/IPS layers detect and respond to network monitoring and anomalies. Crypto layers apply powerful passwords at the National Security Agency type-1 encryption level (authentication, encryption, and password bypass). The communication layer maintains the security of the communication link itself by measures such as secure protocols and frequency band selection. Ground layer protects software and data with physical boundary setting, network, and computer network defense/accident response. Prevention layers are defended at the administrative level, such as governance, policies, acquisition procedures, risk management, and supply chain security.

The MITRE ATT&CK framework can be divided into stages like Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Exfiltration, and Command and Control.

Reconnaissance refers to methods of collecting information about a target. Resource Development involves obtaining access rights to a target, securing infrastructure, and setting up accounts. Initial Access refers to the methods an attacker might use to gain first-time access to a system (e.g., social engineering, phishing, malicious attachments). Execution is about methods an attacker uses to execute malicious code on a device or network. Persistence describes how an attacker maintains continual access within a system. Privilege Escalation is about how an attacker gains higher-level permissions. Defense Evasion involves methods to bypass or evade security mechanisms. Credential Access pertains to ways an attacker obtains authentication details from a system. Discovery is about collecting information about a system. Lateral Movement involves methods to access additional systems within a network. Collection is about methods to gather crucial data. Exfiltration concerns sending the collected data outside the system. Command & Control (C2) is about how an attacker controls the system remotely.

Hence, in this paper, it is analyzed around the attack processes in space systems and summarized the relevant attack matrix of space systems (SPARTA).

In reconnaissance tactics & attack technique stage (9 techniques), there are focused as follows: Gather spacecraft design information, Gather Spacecraft descriptors, Gather spacecraft communication information, Gather launch information, Eavesdropping, Gather flight software development information, Monitor for safety mode indicators, Gather supply chain information and mission information.

In resource development tactics & attack technique stage (5 techniques), there are focused as follows: Acquire and compromise infrastructure, Obtain cyber capabilities, Obtain non-cyber capabilities, Stage (rocket stage) capabilities.

In initial access tactics & attack technique stage (12 techniques), there are focused as follows: Compromise supply chain, Compromised Software Defined Radio, Cross-link via compromised neighbors, Secondary/ backup communication channels, Rendezvous/proximity operations, Compromise Hosted Payload, Compromise ground system, Rogue external entity, Trusted relationships, Exploit reduced protection during safe mode, Compromised ancillary device, Assembly/testing/launch operation compromise.

In execution tactics & attack technique stage (18 techniques), there are focused as follows: Replay, PNT geo-fencing, Authentication process modification, Boot memory compromise, Exploit due to unpatched hardware/firmware, Disable/bypass encryption, Trigger single event upset, Time-synchronized execution, Exploit due to code flaws, Malicious code, Exploiting reduced protection during safety mode, Onboard values modification, Flooding, Jamming, Spoofing, Side-channel attacks, Kinetic physical attacks, Non-kinetic physical attacks.

In persistence tactics & attack technique stage (5 techniques), there are focused as follows: Memory compromise, Backdoors, Ground system presence,

Table 1. Number of countermeasures in cyber attack of space system's SPARTA model.

# of counter measures	Data	Spacecraft software	Single board computer	IDS/IPS	Crypto graphy	Comm. link	Ground	Prevention
	4	20	16	8	5	1	6	27

Cryptographic key replacement, and Valid credentials.

In defense evasion tactics & attack technique stage (11 techniques), there are focused as follows: Disable fault management, Prevent Downlink, Modify On board values, Masquerading, Exploitation of reduced protections during safe mode, Modify Whitelist, Rootkit, Boot kit, Camouflage/ Concealment/Decoys, Overflow Audit log, Valid credentials.

In lateral movement tactics & attack technique stage (7 techniques), there are focused as follows: Hosted payload, Exploitation due to insufficient bus segregation, Constellation hopping via cross-link, Visiting vehicle interfaces, Virtualization escape, Launch vehicle interfaces, Valid credentials.

In exfiltration tactics & attack technique stage (10 techniques), there are focused as follows: Replay attack, Side-channel attacks, Eavesdropping, Out-of-Band communication link, Proximity operations, Modifying communication configuration, Compromised ground system, Compromised developer site, Compromised partner site, Payload communication channel.

In impact tactics & attack technique stage (6 techniques), there are focused as follows: Deception (or misdirection), Disruption, Denial, Degradation, Destruction, and Theft.

As radio interference or spoofing technology advances, the problem of interference in GPS and GNSS is increasingly threatened. There are attempts to provide PNT information at all times as an alternative to the threat of service interruptions targeting GPS and GNSS. The U.S. military introduces technologies such as Assured Positioning, Navigation, and Timing (A-PNT) Converged Computer - Embedded & Scalable (AC2ES). AC2ES can provide location, navigation, and timing information by strengthening existing GPS PNT sources through technologies such as anti-jam and anti-spoof, M-code receivers, imaged based terminals, and instrumental measurement devices (Leonardo DRS 2023).

3.3 Counter Attacks in Space Systems

The space system is made up of parts of the earth and space, links, and users. Protection for cybersecurity should be applied to each of these parts. Space systems should have various deep layers of defense. In view of DiD, counter attacks for each layers are follows in Table 1.

For Data layer: TEMPEST, integrity of machine learning against poisoning about training data sets, encryption of on board message.

For Spacecraft Software layer: development environment security (zero trust access control and monitoring against malicious code), security of software version number (checklist of exploit), software update (condition checklist), vulnerability scanning (checklist & test procedure formatting and testing), software bill of materials (relational check of total software supplier chain), dependency confusion (from private storage), software source control, Common Weakness Enumeration list management (priority management), applied coding standard, dynamic analysis, static analysis for source code, software digital signature, configuration management (condition of spacecraft), session termination, least privilege, long duration testing.

For Single Board Computer layer: secure boot (trust chain path for software & firmware), disable physical ports, segmentation of components (system, function), backdoor commands analysis, resilient PNT (authentication & synchronization), tamper resistant body (power reduction), power randomization (insert noise), power consumption obfuscation (hardware design), secret shared, power masking, increased cycles & timing, dual layer protection, Open Source Access Manager authorization (multi stage authentication), communication physical medium (optic fiber), protocol update/refactoring (vulnerability/threats in rule sets).

For IDS/IPS: clocking safe mode (default protection check), on board IDS/IPS (monitoring, audit, fault check), cyber safe mode, fault insertion redundancy, model based system verification (date input & control sequence check & verification), smart contracts, reinforcement learning.

For Cryptography layer: Communication Security, Crypto key management, Replay protection, traffic flow analysis defence.

For Communication layer: Transmission Security (TRANSEC) (robustness of RF signal resistance).

For Ground layer: ground based countermeasures (identify-protect-detect-recover-response), monitor critical telemetry (for malicious activities), protect authenticators, controls physical security (badge, gate, guard), data backup (Disaster Recovery Plan & Business Continuity Plan), alternate communications paths for risk reduction.

For Prevention layer: protect critical data, secure test results, threat modeling, critical analysis, supplier review, original component manufacturing, Application Specific Integrated Circuit/Field Programmable Gate Array

manufacturing, tamper protection, user training, insider threats protection, two person rule, districted constellations, diversified architectures, space domain awareness, space RF mapping, maneuverability, stealth technology, defensive jamming/spoofing, deceptive /decoys, antenna nulling and adaptive filtering, physical seizure, electromagnetic shielding, filtering/shuttering, defensive dazzling/blinding.

Of course, there is a jamming problem with security threats targeting PNT. To solve the jamming problem, we first run a threat intelligence program and try to mitigate the risk. In addition, it is to solve the jamming problem by applying the technique of nulling the antenna or adaptive filtering. In addition, measures such as session termination, monitoring of a set measurement point to identify jamming attempts, setting up an alternative communication path when jamming occurs, utilizing an on-board intrusion detection and prevention system, identifying the use of a defect management system, activating encryption and authentication status under cyber safety mode, introducing reinforcement learning machines, using an authentication mechanism that can verify reliability for flexible PNT, and applying TRANSEC by analyzing transmission characteristics can be suggested.

4. CONCLUSIONS

The primary focus of this paper was to examine security threats within the cosmic system, followed by a detailed exploration centered on the cyber security tactical attack matrix. The cybersecurity tactics attack matrix is focused from SPARTA model as follows: initial access, execution, persistence, defense evasion, lateral movement, exfiltration, impact.

In addition, the attack techniques that may occur in the space system were analyzed focusing on the contents classified in SPARTA.

Also, there are identified and introduced countermeasures against attacks on space systems in terms of in-depth defense. Of course, these technologies refer to defense technologies in the space system layer, the data layer, the spacecraft software layer, the single board computer layer, the IDS/IPS layer, the cryptographic layer, the communication layer, the ground layer, and the prevention layer.

ACKNOWLEDGMENTS

This research was supported by Baekseok University.

AUTHOR CONTRIBUTIONS

Conceptualization, J.K.; Investigation; writing – original draft preparation, J.K.; writing-review and editing, J.K.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

America's Cyber Defense Agency 2022, Strengthening Cybersecurity of SATCOM Network Providers and Customers, [Internet], cited 2023 Nov 10, available from: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-076a

Bailey, B. 2021, Cybersecurity Protections for Spacecraft: A Threat Based Approach, Aerospace report, TOR-2021-01333-REV A. https://aerospace.org/sites/default/files/2022-07/DistroA-TOR-2021-01333-Cybersecurity%20Protections%20for%20Spacecraft--A%20Threat%20Based%20Approach.pdf

Bartock, M., Brule, J., Li-Baboud, Y. S., Reczek, K., Northrip, D., et al.2022, Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services, NIST IR 8323r1 ipd. https://doi.org/10.6028/NIST.IR.8323r1.ipd

European Space Policy Institute (ESPI) 2022, The War in Ukraine from a Space Cybersecurity Perspective, Short report. https://www.espi.or.at/reports/new-espi-short-report%e2%80%95the-war-in-ukraine-from-a-space-cybersecurity-perspective/

Federal Office for Information Security, Cyber Security for Air and Space Applications, [Internet], cited 2023 Nov 10, available from: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/IT-Sicherheit-in-Luft-und-Raumfahrt/it-sicherheit-in-luft-und-raumfahrt.html

Ingols, K. W. & Skowyra, R. W. 2019, Guidelines for Secure Small Satellite Design and Implementation: FY18 Cyber Security Line-Supported Program, Project Report LSP-249 MIT. https://www.ll.mit.edu/sites/default/files/publication/doc/guidelines-secure-small-satellite-design-ingols-lsp-249.pdf

Leonardo DRS, [Internet], cited 2023 Nov 18, available from: https://www.leonardodrs.com/what-we-do/products-

and-services/a-pnt/
Lightman, S., Suloway, T., & Brule, J. 2022, Satellite Ground Segment, NIST IR 8401. https://doi.org/10.6028/NIST.IR.8401
Manulis, M., Bridges, C. P., Harrison, R., Sekar, V., & Davis, A. 2021, Cyber security in New Space, International Journal of Information Security, 20, 287-311. https://doi.org/10.1007/s10207-020-00503-w
Martin, M., Sunmola, F., & Lauder, D. 2023, A TEMPEST vulnerability prediction method for cyber security practitioners, Alexandria Engineering Journal, 78, 561-575. https://doi.org/10.1016/j.aej.2023.07.059
McCarthy, J., Mamula, D., Brule, J., Meldorf, K., Jennings, R., et al. 2023, Cybersecurity Framework Profile for Hybrid Satellite Networks, NIST IR 8441. https://doi.org/10.6028/NIST.IR.8441
MOD 2020, Responses in the Domains of Space, Cyberspace and Electromagnetic Spectrum, Part 3, Three Pillars of Japan's Defense (Means to Achieve the Objectives of Defense), Defense of Japan, pp.266-274. https://www.mod.go.jp/en/publ/w_paper/wp2020/pdf/R02030103.pdf
NIS2 Directive 2022, [Internet], cited 2023 Nov 10, available from: https://www.nis-2-directive.com/NIS_2_Directive_Articles.html
NOAA 2022, Guidance for Licensees – Cybersecurity measures. Commercial Remote Sensing Regulatory Affairs, 16 August 2022, pp.1-58. https://www.nesdis.noaa.gov/s3/2022-10/960.9%20(a)%201-3%20and%20960.10%20(a)(1)(i)%20(A%20&%20B)%20Guidance_%20Cybersecurity%20Measures_10032022.pdf
Northern SKY Research (NSR) 2022, Space Cybersecurity - current state and future needs, [Internet], cited 2022 April 18, available from: https://www.nsr.com/nsr-space-cybersecurity-white-paper/
Pavur, J. & Martinovic, I. 2022, Building a Launchpad for satellite cyber-security research: lessons from 60 years of spaceflight, Journal of Cybersecurity, 8, 1-17. https://doi.org/10.1093/cybsec/tyac008
Rajagopalan, R. P. 2019, Electronic and Cyber Warfare in Outer Space, Space Dossier 3, UNIDIR. https://unidir.org/sites/default/files/publication/pdfs//electronic-and-cyber-warfare-in-outer-space-en-784.pdf
Schmitt, M. N. 2017, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, NATO Cooperative Cyber Defence Centre of Excellence (Cambridge: Cambridge University Press). https://doi.org/10.1017/9781316822524
Scholl, M. & Suloway, T. 2023, Introduction to Cybersecurity for Commercial Satellite Operations, NIST IR 8270. https://doi.org/10.6028/NIST.IR.8270
Starling, C. G., Massa, M. J., Mulder, L. C. C. P., & Siegel, J. T. 2021, The Future of Security in Space: A Thirty-Year US Strategy, Atlantic Council Strategy Papers. https://www.atlanticcouncil.org/wp-content/uploads/2021/04/TheFutureofSecurityinSpace.pdf
Trump, D. 2020, Presidential Documents: Cybersecurity Principles for Space Systems. Space Policy Directive-5 of Sept. 4, 2020, Federal Register, Vol.85, No.176, [Internet], cited 2020 September 4, available from: https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/
UK Space Agency 2020, Cyber Security Toolkit – Space Assets. https://assets.publishing.service.gov.uk/media/5ec298a3e90e071e2f955ebc/Space_cyber_toolkit_final_v4.pdf
USSF, [Internet], cited 2023 Nov 10, available from: https://www.spaceforce.mil/News/Article/2230831/ussf-commercial-satcom-office-announces-development-of-new-security-program/

Jin-Keun Hong received the Ph.D. degrees in the Electronics from Kyungpook National University in 2000. From 2000 to 2004, He was the National Security Research (NSR). He is Full Professor in Division of Advanced IT of Baekseok University since 2004.