Cyber Security Threats - Summative

Contents

Created By: Christina Antonopoulou

1. Section A

1.1. Risk Management Methodology

The fortification of YSNC's defences against cyber incidents is imperative for the protection of its services and operations. This report relies on National Institute of Standards and Technology Special Publication 800-30 [1] for the risk assessment (RA). [1] is a widely recognised framework endorsed by national regulatory and advisory bodies [2-4] and academics [5-9].

[1] enables organisations regardless of their size and sector to conduct RAs in a consistent way similar to ISO standards [3], and assess specific security areas (e.g., operational) [5]. Unlike CRAMM [10] or OCTAVE [11], [1] supports the identification of relevant operational threats and the adoption of a risk-based approach to resource allocation [12]. Frameworks like [11] are generally suited to business, while [10] is aviation-focused [12]. [1] offers greater flexibility across sectors with a detailed step-by-step approach for adaptable risk analysis [6], [12]. In contrast, ISO/IEC 27005:2018 [13] is not as prescriptive and specialist teams are required for its implementation [3], while ISO/IEC 27001 [14] can be challenging due to complexity, cost, and undefined scope [15]. Given this RA's focus on YSNC's operations, the prescriptive nature of [1] is ideal, although it is voluntary and non-certifiable, unlike [3], [13-14]. As YSNC's satellites are already into orbit, compliance with UK spaceflight regulations [16] and valid licenses are assumed.

In order to bolster the relevancy of [1], YSNC's initial RA integrates threats, risks, and vulnerabilities specific to space missions following guidelines of space mission and cybersecurity standards [17-19] recognised by national regulatory bodies [2][20] It is also informed by LEO-specific and navigation satellite studies [9], [21-32] and cyberattack records [33-40].

1.2. Prepare

1.2.1. Purpose

This document's purpose is to evaluate the cybersecurity risks of YSNC's in-orbit LEO satellites, ground-based, and communication systems. This RA follows a qualitative approach to address threats, risks, vulnerabilities and security measures, providing guidance on security controls and regulatory compliance.

[1] includes four stages for the assessment process. Stage 1, "Prepare for Assessment" identifies assumptions, constraints, assets and defines the RA's scope. Stage 2, "Conduct Assessment", identifies threat sources, vulnerabilities and evaluates risks.

Stages 3 "Results communication" and 4 "RA maintenance" are beyond this document's scope, but they typically document risks for stakeholders and ongoing updates.

1.2.2. Scope and High-Level System Description

Following [1] guidelines, the organisational context is established. [1] defines three tiers: Tier 1 covers policies, Tier 2 focuses on enterprise-level decisions, and Tier 3, addresses design, implementation and operational decisions. This RA encompasses Tier 3, focusing on specific

system in place including (i) space assets (SA), (ii) communication systems (CS), and (iii) ground-based systems (GBS).

Space assets include in-orbit satellites or constellations, with each satellite being comprised by a platform (e.g. thermal control systems) and a payload (mission execution) [14, 19]. The ground segment includes the Satellite Control Centre and Network Operation Centre which handle the satellite command and network management [9]. Finally, the communications segment supports space-to-ground communication with systems such as transmitters, receivers, and network infrastructure [9].

This report also focuses on threats relevant to data integrity, availability, and confidentiality pertinent to YSNC's service, and will remain relevant until a new system release or emerging threats occur in the space cybersecurity landscape.

1.2.3. Assumptions and Constraints

This IRA does not exhaustively cover all potential cybersecurity risks to commercial space infrastructure, and several assumptions and constraints apply.

Firstly, it is assumed that infrastructure integrity checks and security policies are updated regularly and as such hardware failures are out-of-scope. Insider threats are also excluded, as it is assumed that due to YSNC's operations, controlled access, security training and policies are already established. Since the satellites are already in-orbit, it is also presumed that YSNC has acquired necessary licenses and already complies with cybersecurity standards, spectrum rules, privacy and export control regulations [42]. Non-cybersecurity risks and environmental threats like space debris, are also out-of-scope.

Constraints include an unknown number of satellites deployed into orbit. Additionally, in the absence of risk tolerance and historical YSNC data, threat events have been derived from [17-19] and impact analysis does not comprise all potential impacts to the general business model and user base. Likelihood and impact rely on industry standards but cannot verify specifics like mitigation effectiveness and failover capabilities of YSNC's systems.

1.2.4. Risk Model, Analytic Approach and Sources of Information

In the absence of historical data from previous RAs and limited time for data collection, this report primarily utilises a qualitative-approach which relies on external information from scholarly sources, past cybersecurity attacks, and established cybersecurity standards. An evaluation of threats, risks, vulnerabilities, and their potential impacts has been performed, emphasizing on their relevance to the organisation's service and assets. Therefore, this RA adopts a qualitative model (very low (VL), low (L), moderate (M), high (H), very high (VH)) as recommended by [1, p.16], and employs a threat-oriented analytic approach.

1.3. Conduct

1.3.1. Identify Threat Sources

Threat sources were categorised into three main types [1]:

Adversarial Sources: External actors, including hackers, and Nation-states with the capability and intent to compromise the system.

Insider Sources: YSNC's personnel who could intentionally or unintentionally compromise the system security through actions such as data theft.

Structural Sources: Failures in software or hardware that could disrupt service availability and reliability.

1.3.2. Identify Threat Events

Threat events relevant to YSNC were identified from [17-19]. In the absence of historical data, this RA relied on external sources whose relevancy is evaluated per Table E-4 in [1]. Information acquired from [17-19] were categorised under the "Anticipated" classification, as they are derived from industry frameworks and are considered as trusted sources. "Expected" threat events are those derived from cyberattacks in similar organisations [38], [41], while academic articles [9] were categorised under the "Possible" classification.

Threat Event	Asset	Likelihood	Impact	Risk	Relevance
Software attack (TE-1)	SA, GBS, CS	M	H	M	Anticipated
Hijacking (TE-2)	SA, CS	VH	VH	VH	Anticipated
Compromised Ground System (TE-3)	SA, GBS, CS	H	VH	VH	Anticipated
Jamming (TE-4)	SA, CS	H	VH	VH	Expected
Data injection (TE-4)	SA	M	VH	H	Possible
Data manipulation (TE-5)	SA, GBS, CS	M	H	M	Anticipated
Replay (TE-6)	SA, GBS, CS	H	VH	VH	Anticipated
DoS (TE-7)	SA, GBS	M	M	M	Anticipated
Manoeuvre & Control (TE-8)	GBS	M	H	M	Anticipated
Gather Supply Chain Information: Known Vulnerabilities (TE-9)	GBS	H	H	H	Anticipated
Rogue External Entity (TE-10)	GBS, SA, CS	H	VH	VH	Anticipated
Link Eavesdropping	CS	M	M	M	Anticipated

(TE-11)					
Spoofing (TE-12)	CS	M	M	M	Expected
Masquerade (TE-13)	CS	M	M	M	Anticipated

***Table 1**: RA results*

1.3.3. Identify Vulnerabilities and Predisposing Conditions

Table 2 shows the identified vulnerabilities (V) and predisposing conditions (PC) of YSNC operations. The scoring was calculated based on guidelines of [1]'sAppendix F along with additional information retrieved from [19] and academic articles [21-28], [43-44]. Detailed description is included in Appendix A.

Vulnerability - PC	**Type**	**Severity/Pervasiveness**
Data	PC	H
Proximity and Low-Power Jamming	PC	M
Altitude	PC	M
Limited Resources	PC	H
Ground-based jamming/GS-SS communication/communication links	PC	M
Link Switching	V	H
Satellite software	V	VH
Tapping of communications links	V	VH
High Mobility and Limited Coverage of LEO Satellites	PC	M
Continuous User Tracking	V	M
Long Open Wireless Links	V	H

***Table 2**: Vulnerabilities and PCs*

1.3.4. Likelihood, Impact, and Risk Determination

According to [1]'s Appendix G, overall likelihood is calculated by combining likelihood of initiation and adverse impact likelihood from threat events. For this RA the scoring primarily relied on [18-19] assessments of likelihood. Each likelihood was cross-referenced with scholarly research and historical cases to maintain relevancy with YSNC's operations. For example, easily-exploitable cyber-attacks, observed in recent incidents (i.e. jamming) [38], [41], [45] were classified under the "Very High" category.

Impact scoring for YSNC's threat events followed a similar approach and relied on [18-19] suggestions. From a business perspective, depending on the score of each impact and threat event, consequences have different ramifications [1]. More specifically, all identified threats (TE-1 – TE-13) can disrupt YSNC's missions and cause delays for the restorations of its operations [17], [41]. Further these threats risk regulatory non-compliance and may result in

legal and financial costs. TE-1, TE-3 and TE-7 may lead to direct financial costs, while TE-5, TE-4 and TE-2 can damage YSNC's reputation and affect customer trust [6], [12]. Potential loss or damage to information systems and intellectual property could lead to significant financial and legal costs, especially if personally identifiable information are lost [5], [13]. Finally, all threats could danger critical infrastructure and national security, and therefore robust security measures are recommended [9], [27]. For more detailed information, please refer to Appendix B.

Lastly, according to [1]'s Appendix I, risk is calculated by combining the likelihood and impact per threat event. The results are shown in Table 1.

1.3.5. Treatments

To protect YSNC's network and operations, adherence to CYBOK's 21 knowledge areas [46] is recommended to ensure best practices. YSNC should implement physical controls, firewalls, and network segmentation via VLANs, air-gapping, and demilitarised zones. Additionally, security policies and insurances are essential for the mitigation of potential financial losses from cyberattacks. Table 3 shows specific treatments for identified threat events, with main treatment justifications from [19-29], [49-50]. Appendix C contains more detailed justifications.

Threat Event	**Main Treatment**	**Alternative Treatment**	**Main Treatment Justifications**
Software attack	Frequent updates	• Code signing	Promptly vulnerability patching reduces exploitation risk
Hijacking	Secure authentication mechanisms (MFA, cryptographic keys)	• Encryption of communication channels • IDS	Robust protection against unauthorised control and hijacking
Compromised Ground System	Access Control and Encryption	• Insider threat protection • Data transfer authorisation	Enforces strict protocols to ensure data confidentiality and integrity
Jamming	Standard RF-spectrum protections	• Encrypted communication	Successfully demonstrated to reduce jamming
Data injection	TCP Security	• Input validation and sanitisation • Code signing	Addresses vulnerabilities in data transmission which is essential for preventing data injection attacks
Data	Data integrity schemes	• Secure data backups	Maintain the accuracy, reliability, and integrity of

manipulation	(signatures)	• Verify integrity of backups	data
Replay	Time-based One-Time Password (TOTP)	• Encrypted timestamps • Session tokens	Passwords are time-bound, making them invalid after a short period – prevents attackers from re-using passwords
DoS	Access Control Lists	• Rate limiting • Service screening	Manage access and prevent unauthorised use of resources
Manoeuvre & Control	Strong data protection through ACLs, encryption, and data-loss prevention	• IDPS • Data Segmentation	Maintain operational security through restrict access, unreadable data, and protection against data deletion
Gather Supply Chain Information: Known Vulnerabilities	Access Enforcement	• Periodic review and update of access permissions • Penetration testing	Approved authorisations are enforced to access resources and data
Rogue External Entity	Cryptographic Mechanisms on TT&C	• Secure Key Storage and Access Controls • Relay Protection Mechanisms	Provide end-to-end protection – identify and reject wireless transmissions with intention to harm
Link Eavesdropping	Encrypted VPNs	• Secure Key Management • Disconnect or disable Access	Treat remote connections as internal networks through encrypted tunnels to detect malicious code
Spoofing	Authentication of signal sources	• Cryptographic verification • Robust signal processing	Verifies the legitimacy of the incoming signals before establishing connection
Masquerade	Two-person Rule	• Session tokens • Timestamps • Physical access control	For enhanced security, all critical actions require the presence of two authorised people at all times

***Table 3**: Threat Mitigations*

2. Section B

There is increased interest in the private sector for the use of space assets due to the plethora of applications and services such as geolocation services, global broadband services, communication, and Internet of Remote Things. However, satellite systems have significant cybersecurity vulnerabilities [51]. Therefore, two threats relevant to YSNC's service will be analysed.

Spoofing is an attack where the actor deceives a recipient into accepting a malicious signal as genuine [9]. The attack is relevant to civilian Global Position Systems (GPS), since the attacker can release spoof GPS signals to deceive systems and users, gain unauthorised access or manipulate data [51]. One such example occurred in September 2023, when a private aircraft crew allegedly ventured into the Iranian airspace due to GPS spoofing, leading to heightened tensions as Iranian military units issued threats to engage the aircraft in the absence of proper clearance [41]. A severe form of spoofing is satellite hijacking, where attackers exploit communication protocols to control satellites, potentially leading to collisions and national security risks [9]. The implications of these attacks are severe, potentially leading to unauthorized access, data compromise and disruption of critical services [9].

Jamming disrupts communication by overwhelming the signal with noise or false information. LEO satellites usually use a dedicated downlink pilot channel for the transmission of channel status, user management data, and other types of information [9]. Adversaries target this channel and to broadcast false information and cause network paralysis [9]. Notably, LEO satellites are more susceptible to jamming attacks, because they are placed closer to Earth and their downlink signal can be affected by antennas or a compromised MEO or GEO satellite [51]. During the 2022 Ukraine invasion, Russian hackers disrupted ViaSat's ground receivers across Europe. In response, Elon Musk offered Starlink's satellite network which also experienced jamming attacks, a fact that was also confirmed by the US Department of Defence [38]. This indicates an escalation in cyber warfare involving space-ground communication systems [41]. The implications of jamming can lead to navigation errors, accidents, and significant financial losses for businesses relying on satellite communications. In some cases, the impact of jamming can be overwhelming, as the attacker can deliberately flood communication channels with high-power interference signals and launch a DoS attack, severing legitimate communication links or disrupting communications [9].

To counter jamming, techniques such as standard RF-spectrum protections for telemetry, tracking and command systems (TT&C) and controlled reception pattern antennae have been proven by the U.S. military as effective measures against jamming and spoofing for lower RF band frequencies [47]. [52] also recommends spread spectrum techniques, frequency hopping and jamming detection. The importance of architecting a resilient infrastructure is highlighted, as systems must be able to withstand and recover from interference attacks. Redundant systems, secure data practices, alternative communication paths, and rapid response protocols assist in alleviating the impact of both jamming and spoofing incidents [52]. To address risks arising from spoofing attacks, YSNC is recommended to employ authentication of signal sources, cryptographic verification and

signal processing algorithms [52]. Secure key distribution and regular updates of encryptions standards are necessary to ensure minimum compromise [52]. The importance of updates was highlighted by the case of Starlink attack on 2022 which successfully resisted all hacking and jamming attacks due its latest update [25]. Finally, the adoption of ground segment-based protections measures for communications and traffic with space assets is pertinent [47].

3. Section C

In recent years, commercial space missions have grown exponentially [51] [53]. This expansion has challenged regulatory bodies to revise frameworks in line with the sector's growth. However, as [54] note "the presence of divergent priorities and interests has resulted in the creation of different frameworks that often involve costly solutions". In space, security interests of different states arise and often give way to conflicts of interest which might influence the security policies of space systems.

YSNC delivers a navigation service to users from multiple regions so the company must comply with a variety of regulations, including those related to security, privacy and export controls. Under the Outer Space Treaty, Article VII [56] and the Liability Convention [57], a strict and absolute liability for damage is enforced, which is geographically and financially unlimited providing maximum protection to potential victims harmed from space activities [55]. Therefore, acquiring liability risk insurance is necessary to safeguard YSNC from financial repercussions related to its operations. Moreover, the company must comply with data protection regulations including the General Data Protection Regulation in Europe [58] and the Data Protection Act 2018 [59] in the UK, as the proposed service might entail the processing and transmission of sensitive data. Non-compliance with these regulations could lead to significant fines and reputational damage, as was observed with Meta [60], which faced a €1.2 billion fine in 2023 for mishandling data transfers between Europe and the US. This case highlights the importance for YSNC to ensure robust data protection measures are in place to avoid similar repercussions.

Commercial satellite companies also have an ethical responsibility of protecting public data and user privacy. As [61] recommends, engineers could establish an ethical framework to inform the public of what information may be used against them and commit to preventing the development of technology that breaches user privacy. Secure data practices such as encrypted storage and strict data retention policies are essential for maintaining confidentiality and integrity, whereas the education of users about privacy practices and informed consent for data collection can improve transparency and trust towards YSNC's services. The significance of this ethical responsibility highlights the example of BetterHelp, which faced backlash and legal challenges in 2023 for the unauthorised disclosure of health information for advertising purposes [62].

Apart from legal and ethical responsibilities, YSNC should address several technical issues relevant to their operations. LEO satellites have limited computing power and storage, which restricts the use of complex encryption algorithms. Therefore. complex encryption should be used for authentication in the ground segment [22], [51]. [63] recommends implementing quantum encryption, which relies on generating a pseudo-random secret key

and then taking the modulo-two function of the key and the information to be encrypted, which is termed as plain text. This encryption has been utilised in various space missions however the evolving field of quantum computing poses a significant challenge to traditional methods. [64] highlights the emergence of Post-Quantum Cryptography (PQC); a cryptography type that reduces the capability of quantum computers to break the encryption, and recently [65] released three PQC standards designed to withstand such attacks which might prove beneficial for the protection of YSNC's communications and service.

Finally, YSNC should minimise the attack surface to ensure that only authorised ground-stations can communicate with the satellite(s) [9]. This can be achieved through access controls, surveillance, firewalls and network segmentation; VLANs, air-gapping, and demilitarised zones [52]. Integrating these measures would create a secure network, which combined with the use of intrusion detection systems (IDS) and the communication security protocol, would further bolster the company's security posture [52].

4. Appendices

4.1. APPENDIX A: Vulnerabilities and Predisposing Conditions

Vulnerability - Predisposing Conditions	**Description**	**Type**	**Severity/Pervasiveness**
Data	Due to resource constraints, LEO satellites cannot support complex encryption. Therefore, secure key management is essential.	PC	H
Proximity and Low-Power Jamming	Reliance on numerous satellites or gateways broaden the attack surface, increasing the risk of unauthorized access, eavesdropping, or node compromise.	PC	M
Altitude	The low altitude of LEO satellites makes them vulnerable to interference-based attacks from the ground.	PC	M
Limited Resources	With limited power, storage, and computational capabilities, LEO satellites are susceptible to jamming, hijacking, and DoS attacks.	PC	H
Ground-based jamming/GS-SS communication/communication links	Constant communication between ground stations and satellites heightens the risk of jamming attacks.	PC	M
Link Switching	Frequent link switching in LEO networks increases security complexity and introduces exploitable vulnerabilities.	V	H
Satellite software	Key satellite components are managed by software, making them targets for adversaries. Vulnerabilities such as bugs and insecure code can be critical due to the satellite's autonomous nature and reliance on onboard software.	V	VH
Tapping of communications links	Communication links are susceptible to tapping (whether wireline, RF, or network) and system jamming, often due to weak communication protocols.	V	VH
High Mobility and Limited Coverage of LEO Satellites	The high mobility of satellites and limited coverage per LEO increase management complexity and pose challenges for the ground segment, including	PC	M

	management errors and operational weaknesses.		
Continuous User Tracking	Continuous user tracking is required for efficient handovers between LEO satellites, which introduces the risk of unauthorized access to user location data.	V	M
Long Open Wireless Links	LEO satellites depend on long, open wireless links with ground stations, making them vulnerable to jamming or signal interception attacks.	V	H

4.2. APPENDIX B: Threat and Impact Analysis

Type of Impact	**Affected Asset**	**Maximum Impact**	**Applicable Threats**
Harm to Operations	Inability to perform current missions/business functions	High	ALL
	Inability to restore missions/business functions in a sufficiently timely manner	High	ALL
	Harms (e.g., financial costs, sanctions) due to noncompliance	High	ALL
	Direct financial costs	Moderate	TE-1, TE-2, TE-8
	Damage to image or reputation	High	TE-1, TE-2, TE-3, TE-5, TE-6, TE-7, TE-9 to TE-13
Harm to Assets	Damage to or loss of information systems or networks	High	ALL
	Damage to or loss of information technology or equipment	High	ALL
	Loss of intellectual property	High	ALL
Harm to Individuals	Loss of Personally Identifiable Information	Moderate	TE-1, TE-5, TE-6, TE-7, TE-10, TE-12
Harm to Other Organisations	Harms due to noncompliance with applicable laws or regulations	High	ALL
Harm to the Nation	Damage to or incapacitation of a critical infrastructure sector	Very High	ALL
	Harm to national security	Very High	ALL

4.3. APPENDIX C: Treatments

Threat Event	**Main Treatment**	**Alternative Treatment**	**Main Treatment Justifications**
Software attack	Frequent updates	• Code signing	While code signing adds an extra layer of security, frequent updates offer a more comprehensive approach to mitigating attacks. They ensure that the software remains robust against new threats, providing a stronger defence overall.
Hijacking	Secure authentication mechanisms (MFA, cryptographic keys)	• Encryption of communication channels • IDS	Secure authentication mechanisms, such as MFA and cryptographic keys, offer a more direct approach to preventing the hijacking of commercial navigation satellites. These mechanisms ensure that only authenticated users can access and control a company's technical assets. While IDS and encryption are important, they do not provide direct protection against hijacking.
Compromised Ground System	Access Control and Encryption	• Insider threat protection • Data transfer authorisation	While the alternative mitigations are important for the broader security strategy, they do not directly assist in the prevention of the attack. Access control and encryption ensure that only authorised personnel can access critical satellite systems and that all transactions are encrypted.
Jamming	Standard RF-spectrum protections	• Encrypted communication	While encryption is crucial for securing data, it does not offer the same level of prevention for jamming attacks. Standards RF-spectrum protections are a proven approach by the U.S. military to reduce jamming impacts
Data injection	TCP Security	• Input validation and sanitisation • Code signing	TCP security ensures the integrity and security of data transactions, providing robust protection against unauthorised data injection. While the alternatives are important, the do not offer as direct prevention as TCP security offers.
Data manipulation	Data integrity schemes	• Secure data backups • Verify integrity of backups	Data integrity schemes offer a proactive defence ensuring unauthorised changes are detected in real-time. Both alternative mitigations are reactive and even though are essential for a company, in this case are

			complementary measures.
Replay	Time-based One-Time Password (TOTP)	• Encrypted timestamps • Session tokens	TOTP ensures that passwords are valid only for a specified period, thereby making it challenging for unauthorized actors to reuse them, which is crucial for preventing replay attacks. Although encrypted timestamps and session tokens do not directly prevent replay attacks, they serve as important complementary measures. Session tokens, in particular, contribute by ensuring the uniqueness of each token, though they are not as critical as TOTP.
DoS	Access Control Lists (ACLs)	• Rate limiting • Service screening	ACLs prevent unauthorised users from accessing the network which maintains integrity and network availability. Rate limiting is reactive and assists lowering the impact of a DoS attack after it occurs. Service screening is also reactive and mainly filters traffic after it enters the network. Both alternative mitigations do not prevent unauthorised access.
Manoeuvre & Control	Strong data protection through ACLs, encryption, and data-loss prevention	• IDPS • Data Segmentation	Strong data protection prevents unauthorised access whilst ensures data confidentiality and protection against data loss. IDPS and data segmentation are reactive mitigations and while they help limiting the impact of an unauthorised access in terms of breaching, they do not prevent the attack.
Gather Supply Chain Information: Known Vulnerabilities	Access Enforcement	• Periodic review and update of access permissions • Penetration testing	The main mitigation is to enforce approved authorisations to users accessing resources and data. Periodic reviews and update of access permissions, while important, is more focused on maintaining the accuracy of access controls over time. Penetration testing identifies vulnerabilities by mimicking attacks, but it does not prevent them.
Rogue External Entity	Cryptographic Mechanisms on	• Secure Key Storage and Access	Cryptographic mechanisms provide end-to-end protection for TT&C communications. It ensures that only authorised entities can interpret data transactions whilst identifying

	TT&C	Controls • Relay Protection Mechanisms	and rejecting harmful transmissions with intention to harm. The alternative mitigations while protecting cryptographic keys and relay of signals, they do not directly ensure secure communications themselves or provide comprehensive end-to-end encryption on their own.
Link Eavesdropping	Encrypted VPNs	• Secure Key Management • Disconnect or disable Access	Encrypted VPNs generate encrypted tunnels for transmitting data and treat remote connections as if they are part of the internal network. Encryption ensures that data is secure and unreadable to attackers, preventing eavesdropping. Secure key management is important for protecting cryptographic keys, but it is a complementary solution. Disconnect or disable access, while effective to stop eavesdropping, it does not prevent the attack in the first place.
Spoofing	Authentication of signal sources	• Cryptographic verification • Robust signal processing	Authentication of signal sources verifies the legitimacy of the incoming signals before establishing connection, ensuring only verified signals are accepted. This directly prevents spoofing attacks from malicious actors. Cryptographic verification does not specifically verify the source of the signal, but mainly verifies the integrity and authenticity of data. Robust signal processing analyses characteristic of signals to detect anomalies, and while it identifies suspicious signals, it does not have the same level of certainty.
Masquerade	Two-person Rule	• Session tokens • Timestamps • Physical access control	For enhanced security, all critical actions require the presence of two authorised individuals at all times, ensuring continuous oversight and verification of actions. While session tokens, timestamps and physical access control are important complementary measures, they do not directly prevent masquerade attacks.

5. References

[1] National Institute of Standards and Technology, *Guide for Conducting Risk Assessments*, NIST Special Publication 800-30, Revision 1, Sep. 2012. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-30r1

[2] UK Civil Aviation Authority, *Guidance on Cyber Security Strategies for Applicants and Licensees*, CAP 2535, 2nd ed., Crawley, West Sussex, UK: UK Civil Aviation Authority, Sep. 2024.

[3] National Cyber Security Centre, "Component driven risk management methods," accessed Oct. 2024. [Online]. Available: https://www.ncsc.gov.uk/collection/risk-management/component-driven-risk-management-methods

[4] A. Rashid, R. Chivers, S. Shaikh, M. A. Walker, S. Maitland, S. Spencer, D. Hutchison, and A. M. Creese, "Scoping the Cyber Security Body of Knowledge," *IEEE Security Privacy*, vol. 16, no. 3, pp. 96–102, May 2018, doi: 10.1109/MSP.2018.2701150.

[5] R. D. Pambudi and K. Ramli, "Information security risk management design of supervision management information system at xyz ministry using nist sp 800-30," *Jurnal Teknik Informatika*, vol. 4, no. 3, pp. 591–599, Jun. 2023. [Online]. Available: https://jutif.if.unsoed.ac.id/index.php/jurnal/article/download/978/318

[6] M. al Fikri, F. A. Putra, Y. Suryanto, and K. Ramli, "Risk assessment using NIST SP 800-30 revision 1 and ISO 27005 combination technique in profit-based organization: Case study of ZZZ information system application in ABC agency," *Procedia Computer Science*, vol. 161, pp. 1206–1215, 2019, doi: 10.1016/j.procs.2019.11.234.

[7] V. Levy Cahyani, Aristoteles, A. Yani, and Tristiyanto, "Analisis Manajemen Risiko Sistem Informasi Balai Pengkajian Teknologi Pertanian Lampung Menggunakan Metode NIST SP 800-30," *Jurnal Pepadun*, vol. 2, no. 1, pp. 13–20, 2021, doi: 10.23960/pepadun.v2i1.21.

[8] M. E. Johan, M. F. Rizqon, and J. S. Suroso, "University information system security risk assessment using NIST 800-30," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 3, pp. 8380–8385, Sep. 2019, doi: 10.35940/ijrte.c6511.098319.

[9] S. Salim, N. Moustafa, and M. Reisslein, "Cybersecurity of satellite communications systems: A comprehensive survey of the space, ground, and links segments," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 4, pp. 1–1, 2024, doi: 10.1109/COMST.2024.3408277.

[10] "A Qualitative Risk Analysis and Management Tool - CRAMM | SANS Institute," SANS Institute, accessed Oct. 2024. [Online]. Available: https://www.sans.org/white-papers/83

[11] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*, 2007.

[12] N. A. Hashim, Z. Zainal, A. P. Puvanasvaran, N. Azma, and R. Ahmad, "Risk assessment method for insider threats in cyber security: A review," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 11, 2018.

[13] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), *Information technology - Security techniques - Information security risk management*, ISO/IEC 27005:2018, 2018.

[14] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), *Information technology - Security techniques - Information security management systems — Requirements*, ISO/IEC 27001:2013, 2013.

[15] A. Longras, T. Pereira, P. Carneiro, and P. Pinto, "On the Track of ISO/IEC 27001:2013 implementation difficulties in Portuguese organizations," in *2018 International Conference on Intelligent Systems (IS)*, IEEE, Sep. 2018, pp. 886–890, doi: 10.1109/IS.2018.8710558.

[16] UK Space Agency, "Spaceflight legislation and guidance," GOV.UK, accessed Oct. 2024. [Online]. Available: https://www.gov.uk/guidance/apply-for-a-license-under-the-outer-space-act-1986

[17] The Consultative Committee for Space Data Systems, *Report Concerning Space Data System Standards - Security Threats Against Space Missions*, CCSDS 350.1-G-3, Feb. 2022.

[18] M. Scholl and T. Suloway, *Introduction to Cybersecurity for Commercial Satellite Operations (2nd Draft)*, NISTIR 8270, Gaithersburg, MD: National Institute of Standards and Technology, 2022.

[19] "SPARTA," *Aerospace.org*, accessed Oct. 2024. [Online]. Available: https://sparta.aerospace.org/

[20] European Union Agency for Cybersecurity (ENISA), *Low Earth Orbit (LEO) SATCOM Cybersecurity Assessment*, Feb. 15, 2024.

[21] G. Falco et al., "An international technical standard for commercial space system cybersecurity - A call to action," in *ASCEND 2022*, Reston, VA: American Institute of Aeronautics and Astronautics, Oct. 2022, doi: 10.2514/6.2022-4302.

[22] P. Yue et al., "On the security of LEO satellite communication systems: Vulnerabilities, countermeasures, and future trends," *arXiv* [eess.SP], 2022.

[23] K. M. Kareem, "Cyber threat landscape analysis for Starlink assessing risks and mitigation strategies in the global satellite internet infrastructure," *arXiv* [cs.CR], 2024.

[24] M. Kang, S. Park, and Y. Lee, "A survey on satellite communication system security," *Sensors (Basel)*, vol. 24, no. 9, p. 2897, 2024.

[25] N. Boschetti, N. G. Gordon, and G. Falco, "Space cybersecurity lessons learned from the ViaSat cyberattack," in *ASCEND 2022*, 2022.

[26] X. Wei, J. Ma, and C. Sun, "A survey on security of unmanned aerial vehicle systems: Attacks and countermeasures," *IEEE Internet of Things Journal*, vol. 11, no. 21, pp. 34826–34847, 2024.

[27] G. Falco and N. Boschetti, "A security risk taxonomy for commercial space missions," in *ASCEND 2021*, 2021.

[28] L. Vessels, K. Heffner, and D. Johnson, “Cybersecurity risk assessment for space systems,” in *2019 IEEE Space Computing Conference (SCC)*, 2019.

[29] S. S. Visner and S. Kordella, “Cyber best practices for small satellites,” in *ASCEND 2020*, 2020.

[30] N. Tsamis, B. Bailey, and G. Falco, “Translating space cybersecurity policy into actionable guidance for space vehicles,” in *ASCEND 2021*, 2021.

[31] L. Wang, R. Chen, B. Xu, X. Zhang, T. Li, and C. Wu, “The challenges of LEO based navigation augmentation system – Lessons learned from Luojia-1A satellite,” in *Lecture Notes in Electrical Engineering*, Singapore: Springer Singapore, 2019, pp. 298–310.

[32] G. Kavallieratos and S. Katsikas, “An exploratory analysis of the last frontier: A systematic literature review of cybersecurity in space,” *International Journal of Critical Infrastructure Protection*, vol. 43, p. 100640, Dec. 2023, doi: 10.1016/j.ijcip.2023.100640.

[33] K. Brumbaugh and E. G. Lightsey, “A risk management plan for CubeSats,” in *AIAA SPACE 2012 Conference & Exposition*, 2012.

[34] Cyberpeace Institute, “Case study: Viasat attack,” *CyberPeace Institute*, Jun. 2022, accessed Oct. 2024. [Online]. Available: https://cyberconflicts.cyberpeaceinstitute.org

[35] G. Yılmaz, “Cybersecurity threats in global satellite internet,” *Cyber Defense Magazine*, Mar. 25, 2024, Accessed Oct. 2024. [Online]. Available: https://www.cyberdefensemagazine.com/cybersecurity-threats-in-global-satellite-internet/

[36] R. Santamarta, “SATCOM Terminals: Hacking by Air, Sea, and Land.” Accessed Oct. 2024. [Online]. Available: https://www.blackhat.com/docs/us-14/materials/us-14-Santamarta-SATCOM-Terminals-Hacking-By-Air-Sea-And-Land-WP.pdf

[37] “Spread Spectrum Satcom Hacking: Attacking The GlobalStar Simplex Data Service.” Accessed Oct. 2024. [Online]. Available: https://www.blackhat.com/docs/us-15/materials/us-15-Moore-Spread-Spectrum-Satcom-Hacking-Attacking-The-GlobalStar-Simplex-Data-Service-wp.pdf

[38] L. Laursen, “Satellite signal jamming reaches new lows,” *IEEE Spectrum*, May 2023, Accessed Oct. 2024. [Online]. Available: https://spectrum.ieee.org/satellite-jamming

[39] L. Wouters, “Glitched on Earth by humans: A black-box security evaluation of the SpaceX Starlink user terminal,” *Proceedings of the Blackhat US 2022 Conference*, Accessed Oct. 2024. [Online]. Available: https://i.blackhat.com/USA-22/Wednesday/US-22-Wouters-GlitchedOn-Earth.pdf

[40] F. Bussoletti, “Cyber warfare, Team OneFist hits Russia in space again,” *Difesa & Sicurezza*, Oct. 2022, Accessed Oct. 2024. [Online]. Available: https://www.difesaesicurezza.com/en/defence-and-security/cyber-warfare-team-onefist-hits-russia-in-space-again/

[41] C. Swope, K. A. Bingen, M. Young, M. Chang, S. Songer, and J. Tammelleo, “Space Threat Assessment 2024,” *CSIS*, 2024. [Online]. Available: https://www.csis.org/analysis/space-threat-assessment-2024

[42] “Spaceflight legislation and guidance,” *Gov.uk*, Accessed Oct. 2024. [Online]. Available: https://www.gov.uk/guidance/spaceflight-legislation-and-guidance

[43] S.-J. Chen, T.-Y. Wang, C.-S. Fang, and I.-W. Chiang, “Security assessment of low earth orbit (LEO) with software-defined networking (SDN) structure,” in *2023 IEEE 6th International Conference on Knowledge Innovation and Invention (ICKII)*, 2023.

[44] Z. Xiao et al., “LEO satellite access network (LEO-SAN) towards 6G: Challenges and approaches,” *IEEE Wireless Communications*, vol. 1, pp. 1–8, 2024.

[45] P. Velkovsky, J. Mohan, and M. Simon, “Satellite jamming,” *On the Radar*, Apr. 3, 2019, Accessed Oct. 2024. [Online]. Available: https://ontheradar.csis.org/issue-briefs/satellite-jamming/

[46] CyBOK, “CyBOK – The Cyber Security Body of Knowledge v1.1,” Cybok.org. Accessed Oct. 2024. [Online]. Available: https://www.cybok.org/knowledgebase1_1/

[47] Cybersecurity and Infrastructure Security Agency, “Recommendations to Space System Operators for Improving Cybersecurity.” Accessed Oct. 2024. [Online]. Available: https://www.cisa.gov/sites/default/files/2024-06/Recommendations%20to%20Space%20System%20Operators%20for%20Improving%20Cybersecurity%20%28508%29.pdf

[48] Z. Liu, L. Ren, R. Li, Q. Liu, and Y. Zhao, “ID-based sanitizable signature data integrity auditing scheme with privacy-preserving,” *Computers & Security*, vol. 121, no. 102858, pp. 1–10, 2022.

[49] “AC-3: Access enforcement,” *CSF Tools - The Cybersecurity Framework for Humans*, Accessed Oct. 27, 2024. [Online]. Available: https://csf.tools/reference/nist-sp-800-53/r5/ac/ac-3/

[50] “AC-17: Remote access,” *CSF Tools - The Cybersecurity Framework for Humans*, Mar. 5, 2021. Accessed Oct. 27, 2024. [Online]. Available: https://csf.tools/reference/nist-sp-800-53/r5/ac/ac-17/

[51] P. Yue et al., “Low earth orbit satellite security and reliability: Issues, solutions, and the road ahead,” *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1604–1652, 2023.

[52] O. J. Okeyo, “A comprehensive systematic review of privacy and security issues in Satellite Networks,” *GSC Advanced Research and Reviews*, vol. 20, no. 1, pp. 349–375, 2024.

[53] “Large constellations of low-altitude satellites: A primer,” *Congressional Budget Office*, May 17, 2023, Accessed Oct. 2024. [Online]. Available: https://www.cbo.gov/publication/59175

[54] E. Georgiades and M. Pedram, “The role of regulatory frameworks in balancing between national security and competition in LEO satellite market,” *Journal of National Security Law & Policy*, May 10, 2024, Accessed Oct. 2024. [Online]. Available: https://jnslp.com/2024/05/10/the-role-of-regulatory-frameworks-in-balancing-between-national-security-and-competition-in-leo-satellite-market/

[55] D. Kong, “International Space Law for GNSS Civil Liability: A Possible Solution?,” *Space Policy*, vol. 48, pp. 76–86, May 2019, doi: 10.1016/j.spacepol.2019.01.001.

[56] “Outer space treaty,” Unoosa.org, Accessed Oct. 2024. [Online]. Available: https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html

[57] “Liability Convention,” Unoosa.org, Accessed Oct. 2024. [Online]. Available: https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/liability-convention.html

[58] “General Data Protection Regulation (GDPR) compliance guidelines,” *GDPR.eu*, Jun. 18, 2018, Accessed Oct. 2024. [Online]. Available: https://gdpr.eu/

[59] “Data protection,” *Gov.uk*, Nov. 15, 2011, Accessed Oct. 2024. [Online]. Available: https://www.gov.uk/data-protection

[60] D. Milmo and L. O’Carroll, “Facebook owner Meta fined €1.2bn for mishandling user information,” *The Guardian*, May 22, 2023.

[61] R. Pak, “Eyes in the sky: Ethical considerations of commercial satellite surveillance,” *Viterbi Conversations in Ethics*, Jun. 25, 2024, Accessed Oct. 2024. [Online]. Available: https://vce.usc.edu/featured/eyes-in-the-sky-ethical-considerations-of-commercial-satellite-surveillance/

[62] K. J. Nahra, A. A. Jessani, and A. Olivero, “Year in review: The top 10 US data privacy developments from 2023,” *Wilmerhale*, Jan. 5, 2024, Accessed Oct. 2024. [Online]. Available: https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20240105-year-in-review-the-top-10-us-data-privacy-developments-from-2023

[63] E. Verco, “Satellites are cyber insecure: We need regulation to avoid a disaster,” *ANU Journal of Law and Technology*, vol. 2, no. 2, pp. 57–94, Dec. 2021, Accessed Oct. 2024. [Online]. Available: https://anujolt.org/article/30203-satellites-are-cyber-insecure-we-need-regulation-to-avoid-a-disaster

[64] N. Smart, “Cryptography Knowledge Area Issue 1.0,” KU Leuven, *Cyber Security Body of Knowledge (CyBOK)*, Oct. 2019, Accessed Oct. 2024. [Online]. Available: https://www.cybok.org/media/downloads/Cryptography-issue-1.0.pdf

[65] NIST, “NIST releases first 3 finalized post-quantum encryption standards,” *NIST*, Aug. 13, 2024, Accessed Oct. 2024. [Online]. Available: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards