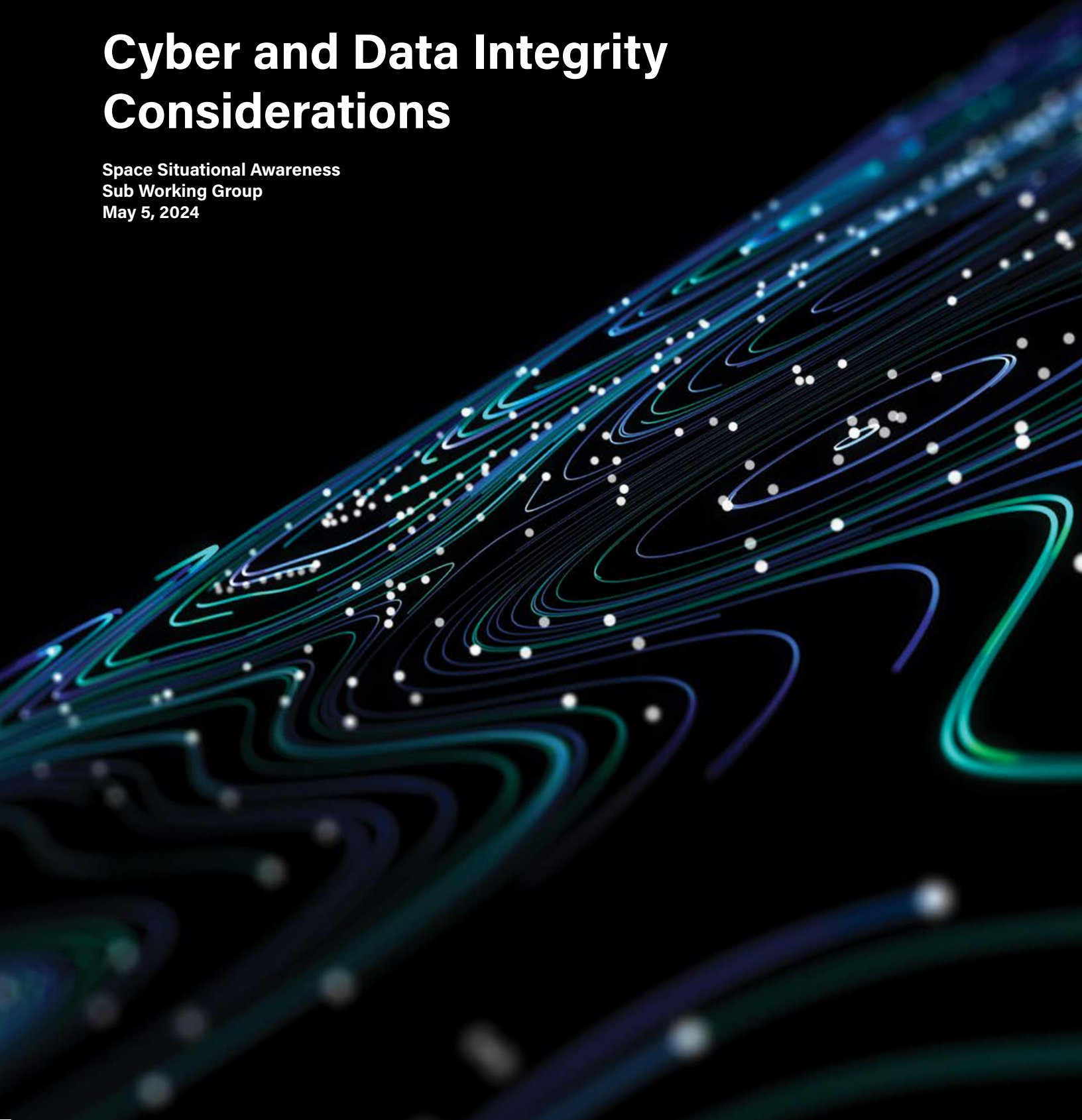




Cyber and Data Integrity Considerations

Space Situational Awareness
Sub Working Group
May 5, 2024





Cyber and Data Integrity Considerations

Background

The U.S Geospatial Intelligence Foundation's (USGIF) Space Situational Awareness Working Group (SSA WG) was established to advance two goals:

- To inform and educate the global Geospatial Intelligence (GEOINT) community about Space Situational Awareness (SSA); and
- Form a common understanding between government, industry, and academic stakeholders on how ground-and space-based sensors, information derived from those sensors, and space-domain analytics contribute to building a comprehensive understanding of the entire space domain.

In furtherance of these goals, the SSA WG reviewed national security implications of SSA and how commercial industry can improve SSA effectiveness, with a particular focus on cyber risks and data integrity assurance issues. This White Paper offers findings and recommendations which will be presented at the May 2024 GEOINT Symposium.

Introduction

The study team reviewed the DoD-authored report, "[Space Policy Review and Strategy on Protection of Satellites](#)," issued September 2023, in which space systems and architectures required to implement the Department's assured space access policies and priorities are highlighted. This study team's White Paper focuses on Space Systems Cyber Defense, while also considering findings and recommendations—highlighting technology-based risk mitigations—as the DoD transitions to a Hybrid Space Architecture with additional reliance on commercial capabilities.

U.S. Government (USG) space strategies address the rapidly evolving space operating environment. Currently, approximately 7,000 satellites are in Earth orbit, both operational and non-operational.¹ With the advent of mega-constellations—such as those operated by Planet, SpaceX, and Amazon Kuiper—the next decade could see as many as 28,000 satellites in low earth orbit.² In addition, there is an enormous number of discrete orbital debris—estimated at 36,500 pieces that are a centimeter or larger than 10 centimeters; one million pieces between 1cm and 10cm; and another 130 million smaller than 1cm which—when combined with man-made ways to interfere with satellites—dramatically increases threats to satellite operations in space across all operational domains.³

The SSA domain represents the foundational knowledge and characterization of objects in space as a basis for threat assessment and mitigation and is essential for effective U.S. space operations, but Space Domain Awareness (SDA) is more exacting as it is "identification, characterization and understanding of any factor, passive or active, associated with the space domain that could affect space operations and thereby impact the security, safety, economy or environment of our nation."⁴ This definition also aligns with U.S. Joint Publication 3-14, Joint Space Operations in which SSA is "the requisite foundational, current, and predictive knowledge and characterization of space objects and the operational environment upon which space operations depend—including physical, virtual, information, and human dimensions—as well as all factors, activities, and events of all entities conducting, or preparing to conduct, space operations."⁵

Advancing and maturing national SDA capabilities is a priority given the growth in satellite population, corresponding economic significance to the U.S. economy,

and ever-increasing critical national security reliance on these platforms. SDA will rely and build-upon the legacy SSA enterprise which has not kept pace with the growth of the space environment. In September 2023, U.S. Representatives Don Beyer (D-VA) and Donald Norcross (D-NJ) co-authored the Space Safety and Situational Awareness Transition Act of 2023, which emphasizes the importance of the space domain thusly: "*Space-based operations are essential for systems our society and our national security rely on, and the number of satellites powering those systems is growing at a rapid pace. Unfortunately, federal leadership on space situational awareness has not kept pace with this growing footprint in space.*" Capability gaps and challenges in the U.S. SSA and SDA system present real and growing challenges to U.S. and allied space operations. For example, gaps in geographical coverage, limited deep space object sensor coverage, an aging SSA infrastructure, growing counterspace threats, emerging commercial SSA capabilities, and a daunting variety and volume of SSA data that present challenges for storage, retrieval, discovery, processing, data interpretation, and use.⁶

Cyber and Data Integrity Threats

Both China and Russia consider offensive cyber capabilities and electronic warfare as key assets for maintaining military advantage and are researching, developing, and deploying cyber capabilities and modernized electronic warfare assets. These emergent cyber threats could target space systems, data links, and ground infrastructure with the aim to disrupt, deny, deceive, or degrade space services.⁷ Beyond this, cyberattacks could monitor data traffic patterns, intercept data, or insert false or corrupted data in a system. Permanent effects are possible as well, should an adversary conduct a cyber-attack against a satellite's command and control. Notably, cyber-attacks are relatively inexpensive, although they require detailed technical knowledge of the system being targeted and—because there are multiple methods to conceal the identity of the attacker—timely attribution and response are complicated.⁸

In particular, threats to cyber security and data integrity assurance stand out as two especially high-priority SSA challenges and to the SDA mission. The SSA WG considered several threats to cyber security and data integrity and associated mitigations. Threats include Distributed Denial

of Service (DDoS) type attacks and data poisoning, and related approaches to degrade trust in networks and data sources. As space capabilities and missions evolve, and the underlying networked infrastructure expands, the attack surface will create vulnerability vectors and attack opportunities with a commensurate need for protection—much like our terrestrial-based internet infrastructure has experienced as it has grown in size and complexity.

General Spacecraft Cyber Security Mechanisms

Modern spacecraft busses require robust cyber protection—not only for collected and distributed SDA data, but also for internal processing systems as well. Unlike legacy spacecraft architectures relying on centralized processing, modern spacecraft may include several independent computer systems, each presenting a potential vulnerability for cyberattacks. Each processing system on a spacecraft should incorporate several mitigations to provide robust, defense-in-depth cyber protection:

- First, each processor must implement a boot security system that is based on a secure hardware Root-of-Trust and a corresponding authentication chain. This boot system should include both Secure Boot and TPM capabilities.
- Second, the processing system must be implemented on a secure operation system platform. For applications that involve multiple security levels, a hypervisor may be used in order to provide the necessary isolation between software components that operate at different security levels. Regardless of the type of operating system or hypervisor that is used, the platform must be based on components with a known pedigree that are updated periodically in order to address security bugs that are detected either in space or terrestrial applications.
- Third, the processing system should include a number of cyber security monitoring features for validation, profiling, anomaly detection, and auditing. These features cover a wide range of specific technologies. A firewall system and IDS are essential for blocking both unknown traffic and known threats. An intelligent profiling and traffic analysis system that is based on AI/ML techniques is important for detecting changes from the nominal behavior of the processing system. Low-level device monitoring systems that are coupled closely to the processing hardware also can detect anomalous

system behavior that are the result of a cyberattack.

- Finally, a robust and flexible auditing system is essential for making optimal use of limited space-to-ground bandwidth in providing security alerts to mission operators for real-time and offline analysis of potential security events.

Cross Domain Solution

The sophistication of modern busses relies upon advanced processing architectures resulting in information sharing between different security domains in order to enable the wide slew of mission objectives. To date, the implementation of a Cross Domain Solution (CDS) for spacecraft has been limited to elementary bypass signals. In July 2022, DoD released the Zero Trust Reference Architecture (Version 2.0), documenting the Zero Trust approach for future systems. Traditional cyber security approaches rely on single dimension authorization with related bulk permissions. As the cybersecurity space becomes more sophisticated, we can no longer apply this paradigm since it provides too wide of an attack surface for our adversaries.

A versatile and mission responsive solution is required to securely exchange traffic between security domains using both the National Security Agency (NSA's) "Raise The Bar" and DoD's Zero Trust architectures. Key attributes for this implementation should include:

- Multi-port, Multi-protocol interfaces;
- Inter-protocol bridging;
- NSA High Assurance architecture;
- Intrusion Detection System (IDS) based on AI/ML (Artificial Intelligence / Machine Learning);
- Zero Trust architecture with high resolution policy controls;
- Inter security domain interfacing: Unclassified up to Top Secret;
- Integrator configurable system policies, rules, and configuration.

Mitigation Concepts

For both government or commercial spacecraft, maintaining data integrity from space systems requires robust systems design, effective error detection and correction techniques, strong cybersecurity measures, and careful data management. The following mitigation concepts are reviewed: Decentralized Digital Identities or DDIs,

Decentralized identifiers (DIDs), Distributed Ledger Technology (DLT), Encryption Techniques (Privacy Enhancement Techniques), and general spacecraft platform cyber security protection mechanisms.

Decentralized Identities (DIDs)

DIDs are an emerging identifier method enabling a verifiable, decentralized digital identity. A DID attaches to any data object (e.g., a person, organization, thing, data model, abstract entity, etc.) designated by the originator and “owner” of the DID. The DIDs enable access controls and system rules, establishing an environment for variable trust leveraging Distributed Ledger Technology (DLT) or similar form of a decentralized network. DLT provides the capability to ensure immutability of a data set, image, or asset, track its location, and verify the existence of a record, trade, or sale. Furthermore, this approach can layer onto the latest available privacy and security protocols providing security in-depth. The ability to assign a traceable and verifiable identity to data elements aids in expanding security protocols and hinders the ability of adversaries to perform sensor data manipulation without detection.

Distributed Ledger Technology (DLT)

When looking to secure data and explore new ways to protect that data, DLTs establish a mechanism to “fingerprint” discrete data element at the initial data capture point (i.e. the sensor), maintaining and verifying data provenance and integrity throughout the data lifecycle through application of cryptographic signatures and timestamps within the ledger to provide an immutable audit trail of transactions. This approach provides a mechanism to detect data poisoning across the data supply chain. DLTs provide the capability to analyze and review each data transaction enabling an end-to-end data transaction audit. At a more granular level, DLT provides for rule-based workflow through a ‘Smart Contract’ implementation approach i.e. an auto-executing agreement or ‘contract’ which, once satisfied, results in a trackable and irreversible data transaction. The transaction ledger and metadata on data access is viewable to all authorized participants in the data life-cycle automatically implementing “need to know” constraints throughout, facilitating easy consumption of data across the data supply chain. Additionally, given the distributed and immutable nature of the DLTs environment, it is exceptionally difficult to alter the information in an undetectable fashion once recorded in the ledger using present computational tech-

niques. While potential adversarial countermeasures can be posited—such as the application of quantum processing and other exotic emerging computational approaches—they are presently unproven. However, the eternal dance between new capability and innovative countermeasure will undoubtedly continue indefinitely into the future.

Encryption Techniques (Privacy Enhancement Techniques)

With the routine integration of commercially owned and operated assets into space-based military operations, trust that the systems are secure is key to mission assurance. Zero-Knowledge Proofs (ZKP) enable data integrity validation without the need to expose or read the data requiring validation. In cryptography, a ZKP or zero-knowledge protocol, is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, while avoiding conveying to the verifier any information beyond the mere fact of the statement’s truth.

Secure multiparty computation (SMPC) permits analytics on encrypted, distributed data from diverse sources. The goal of SMPC is to provide a protocol where no individual can view the other parties’ data while enabling distribution of the data across multiple parties. SMPC can enable data scientists and analysts to compute privately on the distributed data without exposing it to other viewers, whether friendly or adversarial.

Fully homomorphic encryption (FHE) supports computations on encrypted datasets—ensuring data remains shielded—fostering privacy and collaboration. Like traditional encryption, homomorphic encryption schemes use a public key to encrypt the data. Unlike traditional encryption, homomorphic cryptosystems use more complex mathematical algorithms to ensure the data cannot be hacked, this providing a more secure encryption scheme.

Recommendations

Advances in commercial capabilities offer the government opportunities to increase its capacity, offload some mission requirements, and to focus on the hardest mission challenges. Commercial systems can help “operationalize” U.S. alliances and partnerships with key space faring nations and, together with government systems, complement USG capabilities and leverage shared and variable trust protocols.

1. Increase commercial cyber resiliency. The USG requires commercial space capabilities for its national security and therefore an interoperable/hybrid communications architecture demands greater commercial space resiliency to known data integrity threats. Knowledge of commercial space resiliency is critical to mission trust and therefore a cyber-rating system should be created. As part of this effort, the U.S. Government could consider reviewing the use of DLTs to existing security mechanisms and encryption techniques.

2. Increase U.S. commercial integration into the USG reference architecture. Commercial industry now offers real SSA and SDA capabilities that offer opportunities for integration. The United States Space Force and the Space Development Agency are encouraged to finalize the requirements for commercial SDA integration, including identifying gaps in the architecture that the commercial space industry could fill. Planning for privacy-enhancing techniques and common standards to enable government and commercial systems to cooperatively provide SSA capabilities should be an enabling priority. These techniques and standards should hold data privacy and opportunities for economies of scale as central guiding principles.

3. Increase commercial interoperability with international partners. On orbit SDA capabilities exist, as do analytic capacity to make rapid sense of SDA data. Further leveraging commercial capabilities and the sharing of unclassified data in this mission area would accelerate the operationalization of key U.S. relationships with allies and partners, complicate adversary decision making, and contribute to deterrence. But without knowing what capabilities the United States Space Force requires from its space faring allies and partners, they are starting to go out on their own, which is potentially a waste of resources and a missed opportunity. The U.S. Space Force is encouraged to proactively engage with allies and partners on requirements and gaps.

4. Pilot Advanced Mitigations Techniques and Technologies. Opportunities to pilot advanced mitigation approaches i.e. DIDs, DLTs and other privacy enhancement techniques and technologies should be pursued, including public-private partnering opportunities where feasible and appropriate. Where feasible and cost-effective, smallsat and rideshare platforms should be leveraged to take advantage of (relatively) low cost orbital insertion costs. Ground segment technol-

ogy insertion should also be considered to ensure a complete end-to-end data supply chain approach to risk mitigation.

In furtherance of these goals, the SSA WG with a particular focus on cyber risks and data integrity assurance issues feels the approaches outlined above can help bolster the Hybrid environment building in a trust-centric Operational Requirement of commercial space systems to drive the development of an architecture that can accommodate variable trust levels depending on the circumstances, constraints, and objectives of each mission.

Endnotes

1. NSIC, *Competing in Space*, 2nd Edition, December 2023, p. 6.
2. *Ibid*, p. 15.
3. *Ibid*.
4. Sandra Erwin, "Air Force: SSA is no more; it's 'Space Domain Awareness'", *Space News*, November 14, 2019.
5. U.S. Joint Pub 3-14, *Joint Space Operations*, August 2023, p. ix. For purposes of this white paper, we will use the term SDA, not SSA.
6. U.S. GAO, "Space Situational Awareness: DOD Should Evaluate How It Can Use Commercial Data," GAO-23-105565, Published: Apr 24, 2023.
7. NASIC, *Competing in Space*, December 2018, p. 18
8. CSIS, *Space Threat Assessment 2021*, April 2021, p. 5.

Contributors

Hudson Sutherland, CGI Federal, SSA Working Group Member

Taylor Senf, CGI Federal, SSA Working Group Member

Phil Ritcheson, Ph.D., SSA Working Group Member

Scott Lawler, SSA Working Group Member

Daniel Twomey, SSA Working Group Member

Copyright © 2024 United States Geospatial Intelligence Foundation.

This USGIF White Paper is provided for information purposes only, and its contents are subject to change without notice.