An International Technical Standard for Commercial Space System Cybersecurity - A Call to Action

Gregory Falco *
Johns Hopkins University, Baltimore, MD, 21211, United States

Wayne C. Henry †
Air Force Institute of Technology, Wright-Patterson AFB, OH, 45433, United States

Marco Aliberti
European Space Policy Institute, Vienna, 1030, Austria

Brandon Bailey
The Aerospace Corporation, El Segundo, CA, 90245, United States

Mathieu Bailly
Cysec, Lausanne, 1015, Switzerland

Sebastien Bonnart and Giulia De Rossi
Space Generation Advisory Council, Vienna, 1030, Austria

Nicolò Boschetti, Nathaniel G Gordon, Adam B Byerly, and Damiano Marsili
Johns Hopkins University, Baltimore, MD, 21211, United States

Mirko Bottarelli, Gregory Epiphaniou, Duncan Greaves, and Carsten Maple
University of Warwick, Coventry, CV4 7AL, United Kingdom

Joseph Brule and Nick Tsamis
The MITRE Corporation, McLean, VA, 22102, United States

Antonio Carlo
TalTech - Tallinn University of Technology, Tallinn, 12616, Estonia

Matt Fetrow and Joseph Dan Trujillo
Air Force Research Laboratory, Wright-Patterson AFB, OH, 45433, United States

Daniel Floreani
CyberOps, Adelaide, 5001, Australia

Bruce Jackson
EV7 Systems Engineering and Integration, Huntsville, AL, 35808, United States

Garfield "Gary" Jones and Ronald Keen
Cybersecurity and Infrastructure Security Agency (CISA), U.S. Department of Homeland Security, Arlington, VA, 20528, United States

Steven Larson and Arun Viswanathan
NASA Jet Propulsion Laboratory, Pasadena, CA, 91109, United States

*Assistant Professor, Institute for Assured Autonomy, falco@jhu.edu, AIAA Member
†Assistant Professor, Air Force Institute of Technology, wayne.henry@afit.edu, AIAA Member

David Logsdon
Comptia, Downers Grove, IL, 60515, United States

Thomas Maillart
University of Geneva, Geneva, 1205, Switzerland

Nebile Pelin Mantı
Istanbul University Faculty of Law, Istanbul, 34116, Turkey

Erin Miller
Space ISAC, Colorado Springs, CO, 80907, United States

Kevin Pasay
European Space Agency, Noordwijk, 2201 AZ, The Netherlands

James Pavur
Defense Digital Service, Arlington, VA, 20310, United States

Garret Rose and John Thebarge
Air Force Institute of Technology, Wright-Patterson AFB, OH, 45433, United States

Johan Sigholm
Swedish Defence University, Stockholm, 114 28, Sweden

Jill Slay
University of South Australia, Adelaide, 5001, Australia

Chelsea Smethurst
Microsoft, Redmond, WA, 98052, United States

Mattias Wallen
Swedish Space Corporation, Solna, 171 54, Sweden

Christopher White
General Atomics, San Diego, CA 92121, United States

Ernest Wong
Science and Technology Directorate, U.S. Department of Homeland Security, Washington, DC 20528, United States

Matt Young
Space Dynamics Laboratory, North Logan, UT 84341, United States

Despite the significant increase in cyber threats to space systems, structured technical community engagement in space cybersecurity and mission resilience with an emphasis on the systematic advancement of technical guidance is lacking. The international group of co-authors propose the development of a space system cybersecurity technical standard intended for commercial-off-the-shelf (COTS) modular space systems, such as CubeSats.

I. Introduction

While not a new topic, space mission cybersecurity is a multifaceted and persistent challenge that historically concerned government agencies and the national security community. Space cybersecurity is no longer exclusively a nation state priority; the rapid commercialization of the space sector with private, civilian owners and operators has required a renewed, broader community of practice.

Recently, space cybersecurity has been a matter of interest and discussed in a wide array of forums, ranging from policy think tanks [1, 29] to commercial conferences [2]. There is increased public awareness of space cybersecurity challenges after the recent and widely publicized ViaSat cyberattack [3]. Further, the space cybersecurity community of interest has dramatically expanded in recent years, as evidenced through the growth in popularity of Aerospace Village at DEFCON [4] and the rapid and robust emergence of the Space Information Sharing and Analysis Center (ISAC) [5]. Outside the United States, interest in space cybersecurity has also increased with major events such as CYSAT and an emergent commercial ecosystem engaging in space cybersecurity challenges [6].

Interest in and the urgency of space cybersecurity is unsurprising given the growing pressure on commercial space companies to acknowledge and account for cyber threats. Not only has the threat landscape evolved with new geopolitical tensions and actors, but the failure modes and attack surface have also significantly increased due to the digital nature of 'new space' systems. Now-prevalent modular space systems that are sold as commercial-off-the-shelf products are particularly vulnerable with several attacks demonstrated to date[7]. Digitization of space systems has afforded new robotic techniques and probabilistic autonomy, which presents an additional layer of mission cybersecurity challenges such as assured and trustworthy autonomy[8]. The digital transformation of space systems similarly raises their vulnerability to cyberattacks, akin to other critical infrastructure technology.

While the nature of space systems has evolved, so has the context of their missions. Space missions previously thought to be unaffordable and technologically impractical are no longer matters of science fiction. In-space servicing, assembly and manufacturing is one such type of mission segment that is expected to become commonplace in the coming decade that has a unique cyber risk profile[9]. Launch service provider diversification, also considered to be impractical from a financial standpoint, is not only viable, but a thriving marketplace. Startups have entered the sector with enthusiasm, bolstered by private capital investment. The heterogeneity of missions, the organizations enabling them, and advancements in the underlying technology stack presents a turning point in the sector.

Given the current market and threat landscape, a strategic, systematic effort is necessary to address new mission cybersecurity challenges in a rigorous, technical manner. The current pace of progress requires efforts to properly document and discuss technical cybersecurity needs to maintain the robustness of the sector. This paper is a call for action to the space systems community to formulate a technical standards committee that will define cybersecurity technical requirements for commercial-off-the-shelf (COTS), modular space system technology encompassing the ground segment, space segment, user segment, link segment and the integration layer across the system of systems. Such a standard will help to address considerable cybersecurity gaps in the commercial space community today.

II. Existing Space Cybersecurity Recommendations

The call for a cybersecurity technical standard for modular commercial space systems is necessary given the existing piecemeal (at either the component or segment level) guidance provided by governments and their agencies. One of the most critical cyber vulnerabilities of space systems - its status as a system-of-systems - is not fully realized via specific, actionable guidance. Below we describe existing guidance which falls short of addressing technical cybersecurity challenges for modular commercial space systems. Most outline systems engineering and risk management guardrails that lack technical specificity with regards to cybersecurity concerns. Thus far, no organizations listed have the mission or charter to build and maintain technical standards relating to space system cybersecurity - hence the call for action.

A. Space Policy Directive 5

Executive Order Space Policy Directive 5, also referred to as Cybersecurity Principles for Space Systems published in 2020 provides generic cyber risk management practices to those developing space systems. The Executive Order draws from research such as Cybersecurity Principles for Space Systems [16] and Defending Spacecraft In the Cyber Domain [17], which, while specifically written about space systems, does not provide technical cybersecurity specifications.

B. NIST

The National Institute of Standards and Technology (NIST) is a non-regulatory agency within the United States Department of Commerce that provides industry, academia, and other government agencies with standards and regulatory practices. NIST is in the process of developing several space-related security recommendations, including space segments [23] and ground segments [24]. [23] seeks to apply the Cybersecurity Framework (CSF) to commercial space business and defines a process for developing an organization's cybersecurity profile: establishment of scope, orientation, create a current risk profile, conduct of risk assessments, create a target profile, determine and prioritize

gaps, implement actions. [24] establishes a baseline profile for ground considerations. These recommendations are a good development but are still currently aimed at providing general guidance, not tailored recommendations for modular spacecraft.

C. NASA Space Asset Protection Standard

The NASA Space Asset Protection Program (SAPP), established in 2008, has published a standard to establish protection requirements ensuring NASA missions are resilient to threats [21]. This standard defines several high-level mission protection objectives and derives corresponding requirements, such as maintenance of command authority. For example, the standard requires encryption and authentication to maintain command authority. While this mitigates specific cyber threats, the standard does not address the full range of possible attack vectors–such as supply chain attacks–leaving a large portion of attack surface unconsidered.

D. Japanese Guidelines on Cybersecurity Measures for Commercial Space Systems

The Japanese Ministry of Economy, Trade and Industry (METI) has assembled a set of guidelines tailed specifically for security commercial space assets. The guidance, most recently updated in July of 2022, highlights important risk scenarios and outlines necessary attack mitigation measures at a subsystem level [26]. These are excellent steps towards ensuring that the commercial sector is properly informed on the nature of cyber-threats their systems will face, but falls short of concrete governance and technical standards.

E. German IT Baseline Protection Profile for Space Infrastructure

Also the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik or BSI) released in June 2022 its own guidance for the security of space assets[27]. The guidance is the result of cooperative research by the German Aerospace Center (DLR), BSI, Airbus Defense Center, Airbus Defense and Space, and OHB Digital Connect. In the *IT-Grundschutz-Profil für Weltrauminfrastrukturen* (IT baseline protection profile for space infrastructures), BSI defined minimum requirements for cyber security for satellites. The document outlines protection options based on perceived cyberattack consequences to certain space missions.

F. European Cooperation for Space Standardization

The European Cooperation for Space Standardization (ECSS), a collaboration between the European Space Agency (ESA), the European space industry, and several space agencies develops and maintains a coherent, single set of user-friendly standards for use in all European space activities. The standards include guidance and methods to assure the processes and products of space engineering. In addition to standards for implementing system engineering methodology, the standard ECSS-Q-ST-80C Rev.1 [28] covers space software product assurance, including COTS and modified off-the-shelf (MOTS), with the aim of providing adequate confidence that procured software, whatever its' origin, is developed to perform properly and safely. This standard focuses on a risk-based, systems engineering practices to follow for software reliability and does not provide technical cybersecurity specifications or guidance for modular, COTS space systems.

G. Consultative Committee for Space Data Systems

The Consultative Committee for Space Data Systems (CCSDS) is an international organization of space agencies that develops standards and practices for communications and data systems for space missions. Recommendations begin as concept papers that bring technical suggestions to the CCSDS. As recommendations are developed and refined, they become "White Books" (proposed standards and practices) and ultimately "Red Books" (draft standards and practices). Once a standard or practice reaches the draft stage, it is reviewed by CCSDS member organizations for comment. Finally, it becomes a "Magenta Book" (recommended practice) or "Blue Book" (recommended standard) if approved. Along the way, various "Green Books" (information reports) containing supporting analysis may be developed and published in support of a recommended standard or practice.

The CCSDS has published a set of "Books" for security, including a Security Architecture for Space Data Systems [18], Security Threats against Space Missions [19], and Space Data Link Security Protocol [20]. [18] begins with several general security concepts, including physical security, information security, and transmission security, before introducing recommendations for the security aspects of system design. [19] considers various sources of threats,

including adversarial, insider, environmental, and structural, and characterizes these threats against mission archetypes, e.g., earth observation, communications, and human spaceflight. [20] defines a protocol for providing authentication and confidentially at the data link layer, both for telemetry downlink and telecommand uplink.

The need for a technical cybersecurity standard beyond CCSDS' Space Data Link Security Protocol can be met using commercial off-the-shelf encryption units such as the KI-700 [22] because there is more to a space system's cybersecurity than data security. The computing system and its component architecture are increasingly the targets of attackers, which must be accounted for by a technical standard. Attacks against these systems have been documented and published by the Aerospace Corporation [25].

H. Dangers of Defaulting to Reliance on Non-Space Cybersecurity Standards

In the absence of a comprehensive and holistic cybsersecurity technical standard, governing bodies may be inclined to apply traditional cybersecurity guidance to space-specific applications. However, the critical technical knowledge gaps described in this document have been acknowledged as a weakness in this approach by NATO [30]. Not having widespread technical standards make cybersecurity requirements to be defined on a per mission basis, usually as an afterthought. The mission may evaluate an expected threat model and then try to assess countermeasures that could be actively built and integrated in the system – only if the mission budget allows for a project-specific cybersecurity analysis. Having an internationally accepted standard would drive the integration of a minimum set of features for commercial, off-the-shelf components that should become expected as a cyber baseline for mission operations.

III. Target Standards Bodies

To facilitate a rigorous commercial technical international cybersecurity standard, we propose approaching either the International Electrical and Electronics Engineers Standards Association (IEEE SA) or the International Organization for Standardization to engage with for the standard development process.

A. IEEE

The IEEE SA is an operating unit of IEEE that develops global standards for technology across many industries. IEEE standards are developed through a consensus-based approach which involves technical experts from around the world. The development of a cybersecurity standard for space systems would benefit from drawing inspiration from current IEEE standards, which achieve a balance between technical and economic feasibility. IEEE is an internationally recognized and respected technical society and should the space cybersecurity technical standard be created with IEEE SA, its adoption could be accelerated due to its technical credibility amongst engineers.

B. ISO

The International Organization for Standardization (ISO) is an international standards development organization headquartered in Geneva, Switzerland. ISO develops global standards for all technical and non-technical fields, excluding electronic engineering. ISO is composed of national standards bodies comprising 167 countries. The development of a cybersecurity standard for space systems would benefit from drawing inspiration from current ISO standards, which have been adopted at scale across the world. ISO standards can include both technical and non-technical guidance, which could be valuable given non-techncial cybersecurity consierations for modular COTS space systems.

IV. Technical Standard Scoping

While deep-space missions are inherently bespoke, with missions designed explicitly for their target operating environment, e.g., interplanetary space, near-Earth and cisLunar operations are more amenable to mass-produced, assembly-line style space vehicles. In addition, initiatives such as on-orbit servicing, assembly, and manufacturing (OSAM) will continue to drive a transition to "flat-pack" style space assemblies.

A proposed cybersecurity standard would be scoped to specifically define cybersecurity parameters for modular, commercial-off-the-shelf space systems. As the space economy grows, commercial entities with limited space system expertise that aim to specialize in specific payloads and sensors will require COTS space systems to complete their mission objectives. Such commercial space companies will need assurance of the cybersecurity for the space system modules that they purchased - be they modules for the ground system (e.g. database), space vehicle (e.g. bus), link segment (e.g.communications protocol), or the integration layer (e.g. configuration).

Below we identify the various components of a space system for which technical cybersecurity standards are needed.

A. Ground Segment

Ground Segment refers to space infrastructure hosted on Earth, such as ground stations and the associated computing components. Ground segment functions include telemetry, tracking and control (TT&C) of space assets and space-launch mission functions. Securing assets on the ground segment is essential as they are the sole interface to space assets outside Earth. A proposed cybersecurity standard would need to detail appropriate measures in the configuration and operation of these systems and their component modules that could be individually offered for sale and inclusion as part of a space system.

B. Space Segment

Space Segment refers to space infrastructure not hosted on Earth, such as satellites, probes, and space stations. Securing assets in the space segment is important as they are difficult to repair once compromised due to their physical location. A proposed cybersecurity standard would need to detail appropriate technical specifications to be included in the development of these systems and their component modules available for purchase.

C. Link Segment

Link Segment refers to the communication links between the ground and space segment. Communication between space assets is typically achieved using either radio frequency (RF) communication or free-space optical (FSO) networks. Securing the link segment is critical as it controls the flow of information between space assets. A compromised link segment can result in a loss of confidentiality, integrity and availability of communications. A proposed cybersecurity standard would need to detail appropriate levels of communication security modules to be engaged in operating space communication links and their component modules offered for sale.

D. User Segment

User segment refers to any user-facing interfaces and infrastructure that exposes the services of a given space system to a consumer. This includes distributed antenna, routers, and the digital clients and applications that enhance a wide variety of products. The user segment serves as a 'last hop' from the service provider to the consumer that is just as critical to the system as a whole.

E. System-of-System Integration Layer

Space system cybersecurity is particularly unique to other sectors given the requirement for seamless operation across the segments in order to achieve a mission. In addition to threat actors individually attacking components that comprise each segment, the threat actor can undermine the interaction of the various segments, or what we call the integration layer. This systems-level cybersecurity challenge is more nuanced than describing a communication layer standard across the segments; instead it requires a systems-of-systems integration configuration cybersecurity technical standard.

V. Existing Space Cybersecurity Ecosystems

There are several organizations currently exploring opportunities to augment space cybersecurity. Each effort is in its early stages of program development and has yet to generate a demonstrable technical impact on the space cybersecurity community. A sampling of communities exploring how to augment current space cybersecurity capabilities include: the Space ISAC [5], the Air Force Research Laboratory's Space Cyber Summit [11], the Space Generation Advisory Council's Space and Cybersecurity Project Group[10], the AIAA Aerospace Cybersecurity Working Group (ACWG) [12], the Department of Homeland Security's Critical Infrastructure Partnership Advisory Council's Space Systems Critical Infrastructure Working Group [13], and the FBI's Space Systems and Security Working Group (S3WG) [14, 15]. While there is some collaboration among the working groups, none are systematically engaging in the technical cybersecurity challenges confronted by the sector. We expect that an international effort to align cybersecurity standards for the emergent spacecraft COTS ecosystem could help focus the attention of existing disparate efforts on a unified technical cause.

VI. Conclusion

We expect that an internationally recognized technical standard targeted at commercial, modular space systems will help to elevate the existing cybersecurity practices of space system developers. Detailed technical cybersecurity specifications will be actionable and advance beyond general risk management provided currently by NIST and SPD-5. If successful, such a technical standard will pave the way for future cybersecurity standards that may address a wider variety of space systems including bespoke space assets.

Our next step will be to approach one of the above standards organizations to elevate the formality of this process. We aim to be inclusive of diverse stakeholders and would value any help in developing a robust cybersecurity standard for space systems. Please do not hesitate to reach out to engage with our team.

References

[1] Rudiments of a Space Security Policy Framework, Richard J. Chasdi, Centre for International Governance Innovation, July 2022.

[2] CyberLeo, CyberSatSummit.com, Access Intelligence, LLC. May 2022.

[3] N. Boschetti, N. Gordon. G. Falco. Space Cybersecurity Lessons Learned from The ViaSat Cyberattack. ASCEND 2022. American Association for Aeronautics and Astronautics. October 2022.

[4] Aerospace Village. DEFCON 30. https://aerospacevillage.org/category/defcon/ August 2022.

[5] Space Information Sharing and Analysis Center. https://s-isac.org/ Accessed 9.13.2022.

[6] CYSAT 2022. Cysec. https://cysat.eu/ April 2022.

[7] Falco, Gregory, Arun Viswanathan, and Andrew Santangelo. "Cubesat security attack tree analysis." 2021 IEEE 8th International Conference on Space Mission Challenges for Information Technology (SMC-IT). IEEE, 2021.

[8] Falco, Gregory. "Autonomy's Hierarchy of Needs: Smart City Ecosystems for Autonomous Space Habitats." 2021 55th Annual Conference on Information Sciences and Systems (CISS). IEEE, 2021.

[9] Gordon, Nathaniel G., and Gregory Falco. "Reference architectures for autonomous on-orbit servicing, assembly and manufacturing (OSAM) mission resilience." 2022 IEEE International Conference on Assured Autonomy (ICAA). IEEE, 2022.

[10] Space and Cybersecurity Project Group. Space Generation Advisory Council. https://spacegeneration.org/projects/space-cybersecurity/advisors. Accessed 9.13.2022.

[11] Space Cyber Summit. Space Vehicles Directorate. Air Force Research Laboratory. https://www.afrl.af.mil/News/Article/2828102/afrl-space-vehicles-directorate-holds-first-ever-space-cyber-summit/ November 2021.

[12] Aerospace Cybersecurity Working Group. American Association of Aeronautics and Astronautics. https://engage.aiaa.org/communities/community-home/digestviewer?tab=digestviewer&CommunityKey=e37e3069-a9eb-4595-ab73-1765800b989d. Accessed 9.13.2022.

[13] Department of Homeland Security. Cybersecurity and Infrastructure Security Agency. Critical Infrastructure Partnership Advisory Council. Space Systems Critical Infrastructure Working Group. https://www.cisa.gov/news/2021/05/13/cisa-launches-space-systems-critical-infrastructure-working-group. May 2021.

[14] Space Systems and Security Working Group. Federal Bureau of Investigation. https://www.comptia.org/events/view/comptia-space-enterprise-council-fbi-s3-working-group-overview. Accessed 9.13.2022.

[15] Cybersecurity for Remote Sensing. 31st ACCRES FBI-DHS presentation. August 2022. https://www.nesdis.noaa.gov/commercial-space/regulatory-affairs/accres/accres-reports-and-minutes.

[16] G. Falco. Cybersecurity Principles for Space Systems. Journal of Aerospace Information Systems. American Institute of Aeronautics and Astronautics. Volume 16. Number 2. December 2018.

[17] Ryan Speelman, Prashant Doshi, Brandon Bailey. Defending Spacecraft in the Cyber Domain. Aerospace Corporation. November 2019.

[18] Security Architecture for Space Data Systems. Recommendation for Space Data System Practices (Magenta Book), CCSDS 351.0-M-1. Washington, D.C.: CCSDS, November 2012.

[19] Security Threats against Space Missions. Report Concerning Space Data System Standards (Green Book), CCSDS 350.1-G-3. Washington, D.C.: CCSDS, February 2022.

[20] Space Data Link Security Protocol. Recommendation for Space Data System Standards (Blue Book), CCSDS 355.0-B-2. Washington, D.C.: CCSDS, July 2022.

[21] NASA-STD-1006A, Space Asset Protection Standard. Rev A. July 15, 2022.

[22] L3Harris. Medium Rate Advanced Encryption Standard (AES) Unit (KI-700). https://www.l3harris.com/all-capabilities/medium-rate-advanced-encryption-standard-aes-unit-ki-700.

[23] National Institute of Standards and Technology (2022) Introduction to Cybersecurity for Commercial Satellite Operations. (Department of Commerce, Washington, D.C.), February 25, 2022

[24] National Institute of Standards and Technology (2022) Satellite Ground Segment: Applying the Cybersecurity Framework to Assure Satellite Command and Control. (Department of Commerce, Washington, D.C.), April 18, 2002

[25] Brandon Bailey The Aerospace Corporation Cyber Assessment and Research Department (CARD) Cybersecurity Subdivision (CSS) https://aerospace.org/sites/default/files/2022-07/DistroA-TOR-2021-01333-Cybersecurity%20Protections%20for%20Spacecraft–A%20Threat%20Based%20Approach.pdf April 29, 2021.

[26] Space Industry Office, Manufacturing Industries Bureau, Ministry of Economy, Trade and Industry Guidelines on Cybersecurity Measures for Commercial Space Systems https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_uchu_sangyo/pdf/20220721_3.pdf July 21, 2022

[27] Federal Office for Information Security IT-Grundschutz-Profil für Weltrauminfrastrukturen (IT baseline protection profile for space infrastructures) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/ Profil_Weltrauminfrastrukturen.html June 30, 2022

[28] European Cooperation for Space Standardization Space Product Assurance Standard ECSS-Q-ST-80C rev 1 https://www.esa.int/Enabling_Support/Space_Engineering_Technology/Requirements_and_standards June 30, 2022

[29] Chatham House Space, the Final Fromtier for Cybersecurity? https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf June 30, 2022

[30] Hennecken, Dennis G. "Beyza Unal: Cybersecurity of NATO's Space-based Strategic Assets. London: Chatham House, Juli 2019." SIRIUS–Zeitschrift für Strategische Analysen 4.2 (2020): 227-228.