SUBCOMMITTEE ON SPACE AND AERONAUTICS
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES

HEARING CHARTER

Exploring Cyber Space: Cybersecurity Issues for Civil and Commercial Space Systems

July 28th, 2022
10:00 a.m. Eastern Time
Hybrid: 2318 Rayburn House Office Building and Online via Zoom

PURPOSE

The purpose of the hearing is to examine cybersecurity for civil and commercial space systems, including current and potential cybersecurity risks, the status of policies and guidance regarding cybersecurity for space systems, and opportunities for facilitating and strengthening cybersecurity for civil and commercial space systems, among other issues.

WITNESSES

- **Dr. Theresa Suloway**, Space Cybersecurity Engineer, The MITRE Corporation
- **Mr. Matthew Scholl**, Chief, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology
- **Mr. Brandon Bailey**, Senior Project Leader, Cyber Assessments and Research Department, The Aerospace Corporation

OVERARCHING QUESTIONS

- What are the range of issues regarding commercial and civilian space systems and cybersecurity that need to be addressed?
- What is needed to support the strengthening of cybersecurity for civil and commercial space systems?
- What is the status of the workforce and pipeline for space cybersecurity, and to what extent does the workforce need expertise in both space systems and cybersecurity?
- What is the role of standards for cybersecurity for commercial space systems and what is the status of standard development for such systems?
- To what extent do government entities coordinate and collaborate on cybersecurity issues in space systems?
- What can be done to encourage commercial companies to adopt cybersecurity principles into their space systems?

BACKGROUND

The space industry touches many aspects of citizens' everyday lives and supports the global economy. Space assets provide positioning, navigation, and timing services that enable navigation applications and telecommunication services. Remote sensing assets support improvements in agriculture through moisture monitoring and in the oil and gas industry through more accurate monitoring of methane leaks.[1] Global navigation satellite systems, such as the Global Positioning System, enable financial services such as ATM transactions.[2] Disruption of these and other space services and activities could have significant economic and societal impacts.

In addition, as Federal government agencies engage in partnerships with commercial entities and use commercial space services, ensuring that such systems are secure from cyber threats is an important factor in the implementation of government missions. For example, the National Aeronautics and Space Administration (NASA) uses commercial providers to provide cargo and crew transportation services to the International Space Station. NASA plans to retire its constellation of Tracking and Data Relay Satellites, which provide communications capabilities to NASA and other government agencies, and procure communications services from the commercial sector.[3] In addition, the National Oceanic and Atmospheric Administration (NOAA) procures commercial Earth remote sensing data to supplement NOAA satellite weather data in support of its operational weather forecasting mission.

Cyber threats for commercial space systems could also have significant effects on the global space economy. From 2005 to 2020, the global space economy grew from $161 billion to $447 billion. The majority of growth has been and is projected to be in the commercial space sector. [4]

Cybersecurity for Space Systems

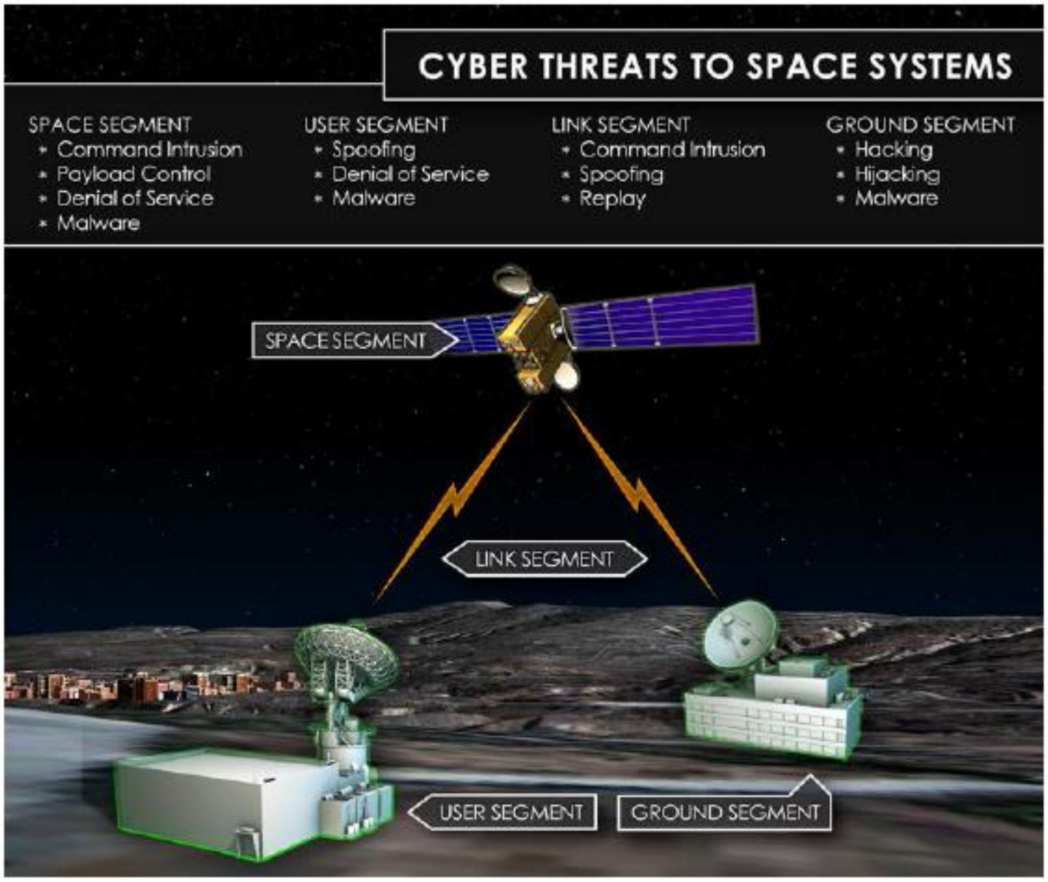
Space systems are composed of multiple segments: ground stations that operate the satellite in space; the communications and command link between the ground station and the satellite; the space segment including the satellite, its payload and spacecraft; and the user segment, which is also linked to the space segment and uses the data it provides. Each segment of a space system is exposed to different cybersecurity risks, as shown in the figure below, and mitigations differ across the type of segment, the lifecycle of the system, and the operator's risk posture.

[1] The Invisible Transformation of Global Industries – Part 1, Space Capital, Available at: https://www.spacecapital.com/publications/invisible-trans-global-industries-part-1

[2] The Invisible Transformation of Global Industries – Part 2, Space Capital, Available at: https://www.spacecapital.com/publications/invisible-trans-global-industries-part-2

[3] https://www1.grc.nasa.gov/space/communications-services-program/

[4] The Space Report 2022 Quarter 1, Space Foundation



Source: Defending Spacecraft in the Cyber Domain (The Aerospace Corporation. Nov. 2019)

Within the federal government, the National Institute of Standards and Technology (NIST) issues cybersecurity guidance for Federal government agencies and critical infrastructure owners and operators that can, when applied, strengthen the cybersecurity of their systems. In particular, NIST, under direction from Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," and the Cybersecurity Enhancement Act of 2015, has developed the Cybersecurity Framework to identify and develop risk frameworks for voluntary use by critical infrastructure owners and operators.[5,6]

CYBERSECURITY THREATS TO SPACE SYSTEMS

Cybersecurity threats against space systems are myriad and evolving. Traditionally, cybersecurity for space systems has concentrated on the ground segment, which largely resembled other information technology systems.[7] Spacecraft themselves were not considered highly susceptible to cyber-attacks because of their unique hardware and software architectures and because physical access to a spacecraft after launch was highly unlikely.[8] However, as the

[5] See *15 USC Sec. 272 (e)(1)(A)(i)*. The Cybersecurity Engagement Act of 2014 (S. 1353) became public law 113-274 on December 18, 2014 and may be found at https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.
[6] Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, National Institute of Standards and Technology, April 16, 2018, Available at: https://www.nist.gov/cyberframework/framework.
[7] Cybersecurity Protections for Spacecraft: A Threat Based Approach, The Aerospace Corporation, April 29, 2021
[8] Cybersecurity Protections for Spacecraft: A Threat Based Approach, The Aerospace Corporation, April 29, 2021

understanding of cyber threats has evolved, the range of cyber threats has expanded to include all segments of the space system.

Cybersecurity risks to commercial space systems have recently been highlighted due to the commercial communications and remote sensing sectors' support during the war in Ukraine and subsequent attacks on their systems. For example, a cyber-attack on Viasat's modems in Ukraine and other parts of Europe resulted in temporary loss of service for tens of thousands of customers throughout Europe. [9]

Examples of potential and realized cybersecurity threats to space systems include:

- Cyber weapons developed and targeted to specific spacecraft systems.[10]
- Potential vulnerabilities in the supply chain.[11]
- Hacking of ground systems, causing service disruptions to commercial and government customers, as seen in the recent Viasat hack.[12]
- Command intrusion into an operational satellite presenting potential physical risks to other satellites and the orbital ecosystem.
- Spoofing of the link between the satellite and the user, providing false information to the user.[13]
- Disruption or intentional or unintentional manipulation of signals.

SPACE POLICY DIRECTIVE-5 (SPD-5) CYBERSECURITY PRINCIPLES FOR SPACE SYSTEMS

Issued in September 2020 SPD-5 describes government policy regarding cybersecurity in space systems.[14] It states that cybersecurity principles that apply to terrestrial systems also apply to space systems and directs the government to work with industry to establish cybersecurity norms and behaviors throughout the industrial base for space systems.

Principles related in the policy include:

- Space systems should be developed and operated using risk-based cybersecurity-informed engineering.

[9] On 24 February 2022, a multifaceted and deliberate cyber-attack against Viasat's KA-SAT network resulted in a partial interruption of KA-SAT's consumer-oriented satellite broadband service. Viasat is a communications company that provide satellite broadband internet services. See more: https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/

[10] Cybersecurity Protections for Spacecraft: A Threat Based Approach, The Aerospace Corporation, April 29, 2021

[11] Space Information and Sharing Center Overview at CISA Advanced Threat Technical Exchange. Available at: https://s-isac.org/resources/

[12] https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/-

[13] Defending Spacecraft in the Cyber Domain, The Aerospace Corporation, November 2019, Available at https://aerospace.org/sites/default/files/2019-11/Bailey_DefendingSpacecraft_11052019.pdf.

[14] Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems, September 4, 2020, Available at: https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/

- Space systems operators should protect against unauthorized access to space vehicle functions, communications jamming and spoofing, and should protect ground systems through practices that align with NIST's Cybersecurity Framework.
- Space systems owners and operators should develop and implement cybersecurity plans that ensure operators or automated control center systems can retain control or recover control of their space vehicles.

The policy encourages space system owners and operators to collaborate through an Information Sharing and Analysis Center (ISAC), and states that security measures should be effective while permitting space system owners and operators to manage according to their risk tolerances, as consistent with mission requirements.

CYBERSECURITY STANDARDS FOR COMMERCIAL SPACE SYSTEMS AND INFORMATION SHARING

A variety of entities have published cybersecurity standards for space systems, including the Committee on National Security Systems—an intergovernmental organization that sets policy for U.S. security systems— for national security space systems,[15,16] the Consultative Committee for Space Data Systems—a multi-national forum for the development of standards for spaceflight—for international civilian space systems,[17,18] the Aerospace Industries Association for Department of Defense space systems,[19] and NASA for their space systems.[20]

In addition, in response to direction in SPD-5, the Space Information Sharing and Analysis Center (Space ISAC) was established to encourage collaboration and coordination regarding cybersecurity threats across the global space industry.[21] The Space ISAC is a private, non-profit organization that is funded by member companies who are in turn granted access to cybersecurity trainings and resources. Similar ISACs have been created for other sectors, including aviation, communications, energy management, and financial services. The Space ISAC plans to establish a Watch Center that would allow members access to unclassified, real-time cyber threat information.

[15] Security Categorization and Control Selection for National Security Systems Instruction No. 1253, The Committee on National Security Systems, March 27, 2014, Available at: https://www.dcsa.mil/portals/91/documents/ctp/nao/CNSSI_No1253.pdf.

[16] National Information Assurance Instruction for Space Systems Used to Support National Security Missions Instruction No. 1200, The Committee on National Security Systems, May 7, 2014, Available at: https://www.cnss.gov/CNSS/openDoc.cfm?wrwBe/vSzqs7t2cCcl82Hg==.

[17] CCSDS Cryptographic Algorithms CCSDS 352.0-B-2, The Consultative Committee for Space Data Systems, August 2019, Available at: https://public.ccsds.org/Pubs/352x0b2.pdf.

[18] Network Layer Security Adaptation Profile CCSDS 356.0-B-1, The Consultative Committee for Space Data Systems, June 2018, Available at: https://public.ccsds.org/Pubs/356xb1.pdf.

[19] Critical Security Controls for Effective Capability in Cyber Defense, NAS 9933, Aerospace Industries Association, Available at: http://www.aia-aerospace.org/wp-content/uploads/2018/12/AIA-Cybersecurity-standard-onepager.pdf.

[20] Space System Protection Standard, National Aeronautics and Space Administration, October 29, 2019, Available at: https://discovery.larc.nasa.gov/PDF_FILES/2019AO/nasa-std-1006.pdf

[21] https://s-isac.org/about-us/

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) GUIDANCE

In response to SPD-5, NIST has developed three documents providing voluntary guidance to commercial space companies to help them apply NIST's Cybersecurity Framework to their space systems.[22] The three documents were formulated with the input of commercial industry. The three documents are:

- *Introduction to Cybersecurity for Commercial Satellite Operations*: focuses on introducing NIST's cybersecurity framework to commercial space systems.[23] It describes methods for applying the framework to a small portion of commercial satellite operations, creates an example framework of desired security outcomes, and describes a set of cybersecurity outcomes, requirements, and suggested controls.
- *Foundational Position, Navigation, and Timing (PNT) Profile: Applying the Cybersecurity Framework for the Responsible Use of PNT Services*: provides a flexible framework for users of PNT services to manage risks when forming and using PNT signals and data.[24]
- *Satellite Ground Segment: Applying the Cybersecurity Framework to Assure Satellite Command and Control:* creates a profile for ground segment operators to use to manage risks in the context of their own cybersecurity actions, systems architecture, and risk tolerance.[25] The goal of a profile is to supplement existing cybersecurity measures that ground segment operators have put in place to ensure resilience in their systems and to increase understanding and adoption of newer cybersecurity initiatives.

REGULATORY ENVIRONMENT

Federal agencies that have regulatory authority for aspects of commercial space activities stipulate certain cybersecurity measures as part of their respective licensing requirements to private space system operators. For example, NOAA's Commercial Remote Sensing Regulatory Affairs office, which licenses commercial remote sensing satellite systems, requires that satellites with propulsion control use encrypted communication so cyber attackers cannot take physical control of the satellite, among other cybersecurity related requirements. The Federal Aviation Administration's Office of Commercial Space Transportation, which licenses commercial space launch and reentry activities, has safety requirements for computing systems, among others. In addition, the Federal Communications Commission, which issues communications licenses for commercial satellite systems, stipulates, among other security-related requirements, that ground station facilities are protected by appropriate security measures to prevent unauthorized entry or operations.

[22] Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, National Institute of Standards and Technology, April 16, 2018, Available at: https://www.nist.gov/cyberframework/framework

[23] Introduction to Cybersecurity for Commercial Satellite Operations NISTIR 8270, the National Institute of Standards and Technology, February 2022, Available at: https://csrc.nist.gov/publications/detail/nistir/8270/draft.

[24] Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Service NISTIR 8323, the National Institute of Standards and Technology, February 2021, Available at: https://csrc.nist.gov/publications/detail/nistir/8323/final

[25] Satellite Ground Segment: Applying the Cybersecurity Framework to Assure Satellite Command and Control NIST IR 8401, the National Institute for Standards and Technology, April 2022, Available at: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8401.ipd.pdf