Ciberseguridad en sistemas espaciales

Conceptos, tensiones y retos

DOI: 10.29236/sistemas.n174a6

Resumen
El espacio es la frontera final de la humanidad. Un contexto de oportunidades, riesgos, tensiones y retos que genera diferentes perspectivas y reflexiones entre las naciones. Las misiones espaciales se convierten en los nuevos escenarios de confrontación a nivel político, económico, social, tecnológico, ecológico y legal, donde lo que está en juego, no sólo es el posicionamiento estratégico y geopolítico de los países, sino la construcción de una visión global para la humanidad. En este sentido, este artículo desarrolla los conceptos básicos de las misiones espaciales, las tensiones que se generan y los retos asociados con los riesgos cibernéticos que pueden comprometer el ecosistema de componentes especializados de dichas misiones, con los impactos que se pueden generar tanto para la seguridad nacional de los Estados, como a nivel global en el escenario de las infraestructuras críticas cibernéticas interconectadas con sistemas satelitales.

Palabras clave
Ciberconflicto, ciberseguridad, geopolítica, satélites, sistemas espaciales,

Introducción

El dominio y la carrera espacial se han convertido en una renovada materia de interés de las naciones en la actualidad, comoquiera que es en este escenario, donde ahora se localizan nuevas fuentes de ventajas competitivas y dominios de poder, que tanto empresas como naciones quieren desarrollar para tomar posiciones estratégicas, no sólo para concretar sus promesas de valor, sino para mostrar sus nuevas capacidades de influencia y control más allá de un territorio conocido (WEF & Mckinsey, 2024)

El dominio espacial es un ecosistema complejo donde los sectores público y privado convergen, motivando inversiones y proyectos de frontera, que buscan concretar agendas políticas, económicas y estratégicas que configuren una manera distinta de entender la dinámica de las naciones, y así ubicar nuevas propuestas de productos y servicios que sean de uso global, superando las limitaciones propias de las condiciones naturales del dominio terrestre (Schrogl, 2020).

Desde la perspectiva de la ciberseguridad, los sistemas espaciales presentan retos únicos. La naturaleza de las misiones, que pueden ser militares, científicas o comerciales, determina el nivel de riesgo y los controles necesarios que se deben aplicar con el fin de disminuir las amenazas, reducir las vulnerabilidades y limitar los impactos. Un ciberataque exitoso podría tener consecuencias importantes, incluyendo temas como, la pérdida del control del satélite, la alteración de datos y de hardware, la interrupción de servicios críticos, entre otros, que revela la sensibilidad de este dominio y sus implicaciones para la sociedad actual (Falco & Boschetti, 2021).

Así las cosas, en un contexto internacional cada vez más inestable y con tensiones geopolíticas crecientes, el espacio es una arena para la proyección del poder y la disputa entre naciones, en donde la ciberseguridad de los sistemas espaciales se convierte en un elemento clave para la seguridad nacional e internacional. En este sentido, se hace necesario revisar algunos elementos básicos de los sistemas espaciales en clave de ciberseguridad con el fin de entender los desafíos que tanto empresas como naciones van a enfrentar de cara a la acelerada carrera tecnológica que supone explorar y explotar el espacio (Livingstone & Lewis, 2016).

En consecuencia, este artículo hace una breve revisión de los elementos básicos de los sistemas espaciales, cómo se configura y articula este ecosistema tecnológico alrededor de la dinámica de las misiones espaciales, con un énfasis

particular en las consideraciones de seguridad nacional y la ciberseguridad que se requiere para hacer más resistentes estas infraestructuras críticas de las empresas y las naciones que circundan la órbita terrestre, y que en el futuro, podrán operar desde otros planetas.

Fundamentos de los sistemas espaciales

Los sistemas espaciales son complejos y requieren un enfoque holístico para abordar no sólo los retos asociados a la seguridad, la gestión de riesgos, la arquitectura y el entorno orbital, sino para comprender la dinámica de su funcionamiento como sistemas altamente integrados y acoplados. En este sentido, a colaboración y la innovación son fundamentales para asegurar operaciones seguras y sostenibles en el espacio, con el fin de lograr misiones exitosas y alcanzar nuevos horizontes y alcances en la exploración de este nuevo dominio (Gerstein et al., 2016).

Un sistema espacial se puede definir como una red de componentes interconectados (de tecnología espacial y terrestre) que operan conjuntamente para llevar a cabo una misión específica, con cada segmento y componente desempeñando roles vitales, entre otros, comunicación, navegación, observación terrestre y seguridad nacional.

A continuación, se detallan los diferentes elementos de los sistemas espaciales: (Oakley, 2024)

- Segmento espacial:
- Incluye los satélites y otros vehículos espaciales en órbita, los cuales son el núcleo de cualquier sistema espacial. Los satélites pueden ser de diferentes tipos según su misión, desde satélites de comunicaciones hasta observatorios científicos o inclusos con labores militares (inteligencia y espionaje).
- Segmento terrestre:
- Comprende la infraestructura en tierra necesaria para controlar los satélites y procesar los datos. Esto incluye estaciones terrestres, centros de control de misión, redes de comunicación y centros de procesamiento de datos.
- Segmento de enlace:
- Son los enlaces de comunicación entre el segmento espacial y el segmento terrestre, y entre los diferentes componentes del sistema espacial. La seguridad y confiabilidad de estos enlaces es vital para articular las operaciones espaciales.
- Segmento de usuario:
- Son los profesionales y sus equipos que utilizan los servicios proporcionados por el sistema espacial. Esto incluye receptores GPS (*Global Position System*), terminales de comunicación por satélite y sistemas de análisis de datos.
- Segmento de interoperabilidad:
- Es la integración de todos los segmentos del sistema espacial y sus componentes para que funcionen de manera armónica

en las relaciones interdependientes que se tienen entre ellos.

Desde el punto de vista geopolítico los sistemas espaciales se encuentran en un entorno de competencia y cooperación internacional, donde la soberanía espacial y la seguridad nacional juegan un papel fundamental. Las tensiones geopolíticas y los conflictos internacionales pueden crear escenarios inciertos con un impacto directo en la disponibilidad y seguridad de los sistemas espaciales. La dependencia de componentes o tecnologías extranjeras puede generar vulnerabilidades estratégicas y dificultar la autonomía de los países en el espacio, particularmente de las potencias globales (Flanagan et al., 2023)

De otra parte, la creciente dependencia de los sistemas espaciales en sus roles vitales previamente comentados, los convierte en objetivos atractivos para ciberataques. Estos ataques pueden comprometer los principios de la seguridad de la información, así como el control de los satélites, con consecuencias potencialmente inesperadas por posibles efectos dominó que inicien en el espacio y lleguen a la tierra, o viceversa. La protección contra estas amenazas requiere la implementación de sistemas de seguridad en todos los segmentos, desde los satélites en órbita hasta las estaciones terrestres y los enlaces de comunicación (Falco et al., 2024)

El desafío de la ciberseguridad en los sistemas espaciales

La ciberseguridad se ha convertido en un desafío primordial para los sistemas espaciales, representando un riesgo significativo tanto para las operaciones como para la viabilidad a largo plazo tanto de las empresas como de las naciones.

Por tanto, comprender la alta interdependencia e interconexión de estos sistemas, implica entender que no son inmunes a las ciberamenazas, a las operaciones cibernéticas ni a las agendas militares de países desarrollados, sino que, por el contrario, su creciente digitalización y dependencia de las redes los hacen particularmente vulnerables y expuestos a diferentes estrategias y ataques especializados (Ear et al., 2024).

Para un director de misión espacial, la ciberseguridad representa un desafío crítico que debe abordarse de manera integral. Los cinco retos más importantes desde la perspectiva de la ciberseguridad incluyen la protección de los componentes básicos (control de altitud, sistemas de propulsión, sistemas de comunicaciones), la gestión de la cadena de suministro, la defensa cibernética, la integridad de los datos, y la capacidad resiliente del sistema ante incidentes (Manulis et al., 2021)

A continuación, se presenta un resumen de cada uno de estos retos con sus posibles controles:

Tabla 1. *Retos claves de la ciberseguridad en los sistemas espaciales*

Retos de ciberseguridad	Riesgos	Posibles controles
Protección de Componentes básicos	• Pérdida de control del satélite, • Interrupción de servicios • Fallas en operaciones • Manipulación de sistemas de propulsión, altitud o comunicaciones	• Controles de acceso • Cifrado • Verificación de integridad de sistemas • Segmentación y aislamiento de componentes • Pruebas en entornos simulados
Gestión de la Cadena de Suministro	• Inyección de código malicioso • Alteración de software • Compromiso de componentes	• Verificación y validación de componentes • Evaluación y diversificación de proveedores
Defensa cibernética	• Malware • Ransomware • Ataques DDoS • Manipulación de datos	• Sistemas de detección y prevención de intrusiones • Análisis de vulnerabilidades • Planes de respuesta a incidentes • Inteligencia de amenazas
Integridad de los Datos	• Degradación de datos • Errores en operaciones • Pérdida de información crítica	• Autenticación, • Integridad de datos • Funciones hash • Firmas digitales • Canales confiables y cifrados • Protocolo de gestión de datos
Capacidad resiliente	• Interrupción de la misión • Pérdida de datos • Incapacidad de recuperación • Pérdida de activo espacial	• Medidas de redundancia • Planes de recuperación • Copias de seguridad • Capacitación del personal • Simulaciones • Centro de operaciones de ciberseguridad

Nota: Basado en: Kaczmarek, 2024; Livingstone & Lewis, 2016; Hodgson et al, 2024

Abordar los desafíos de ciberseguridad en el contexto actual en un dominio espacial marcado por tensiones geopolíticas y amenazas cibernéticas emergentes, requiere una estrategia proactiva y adaptable, así como una comprensión en detalle de los riesgos y sus posibles implicaciones a nivel empresarial y nacional. En razón con lo anterior, un director de misión debe estar articulado desde su conceptualización y puesta operación con diferentes marcos y estándares de trabajo en ciberseguridad, con el fin de asegurar su entorno de operaciones frente a la materialización de un riesgo cibernético en su ecosistema tecnológico convergente (Gerstein et al., 2016).

En razón con lo anterior, para los sistemas espaciales se cuenta con varios marcos y estándares que buscan proporcionar una guía para la implementación de prácticas seguras en el diseño, desarrollo y operación de estos sistemas. Una breve lista se presenta a continuación: (Hodgson et al., 2024; Falco et al., 2024)

- NIST SP 800-53: *Security and Privacy Controls for Information Systems and Organizations*.

- NIST SP 800-37: *Risk Management Framework for Information Systems and Organizations*.

- *NIST Cybersecurity Framework*

- NIST IR 8270: *Introduction to Cybersecurity for Commercial Satellite Operations*.

- NIST IR 8323: *Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services*.

- NIST IR 8401: *Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control*.

- NIST IR 8441: *Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN)*.

- CMMC (*Cybersecurity Maturity Model Certification*)

- *IEEE Standard for Space System Cybersecurity*: Este estándar propone una especificación centrada en la seguridad y basada en componentes para el desarrollo de futuras misiones espaciales. Busca asegurar que las misiones espaciales estén diseñadas con resiliencia inherente contra amenazas cibernéticas, priorizando un enfoque fundacional de seguridad y haciendo referencia a trabajos existentes de otros organismos.

- *IT-Grundschutz Profile for Space Infrastructures*: Este perfil, desarrollado por la Oficina Federal Alemana para la Seguridad de la Información (BSI), ofrece una plantilla para conceptos de seguridad relacionados con el espacio. Enfatiza perfiles de seguridad específicos de la empresa basados en requisitos mínimos de seguridad, adaptables a necesidades únicas de la misión.

- *Cybersecurity Guidelines for Commercial Space Systems*: Desarrolladas por el Ministerio de Economía, Comercio e Industria de Japón (METI), estas directrices fomentan medidas voluntarias de ciberseguridad en el sector espacial comercial. Las directrices incluyen riesgos de seguridad, medidas básicas y referencias para obtener más orientación.

- *SPARTA (Space Attack Research and Tactic Analysis) Framework*: Es una base de conocimiento de la *Aerospace Corporation* que proporciona información no clasificada a los profesionales del espacio sobre cómo las naves espaciales pueden verse comprometidas por medios cibernéticos. La matriz define y categoriza las actividades comúnmente identificadas que

contribuyen a comprometer las naves espaciales.

- CCSDS (*Consultative Committee for Space Data Systems*): Aunque no se menciona específicamente como un marco, se hace referencia a los algoritmos criptográficos de CCSDS.

Los sistemas espaciales: seguridad nacional en clave del riesgo cibernético

El espacio se ha convertido en un escenario de tensiones geopolíticas internacionales. Las grandes potencias han identificado en los sistemas espaciales posibilidades concretas para continuar expandiendo su influencia, presencia y dominio en el contexto global (Tretter, 2025). Diferentes misiones se han concretado durante los últimos cinco años donde cada uno de los países del G7 (Canadá, Francia, Alemania, Italia, Japón, Reino Unido y Estados Unidos) han avanzado en su posicionamiento geoespacial bien con satélites de diferentes tipos, o misiones científicas generalmente situadas en la estación espacial internacional.

Cada una de estas naciones encuentra en el espacio una forma de mostrar su capacidad de inversión, investigación y proyección, que más allá de su liderazgo económico, revela una presencia internacional que sugiere avances y progresos que definen los jugadores principales en esta área. En este sentido, los intereses nacionales a menudo compiten con la necesidad de cooperación, lo que dificulta el establecimiento de acuerdos multilaterales efectivos. La competencia entre grandes potencias espaciales también se extiende a la conquista de mercados y el desarrollo de nuevas tecnologías, creando un entorno dinámico y desafiante donde la soberanía espacial y la seguridad nacional juegan un papel determinante (Livingstone & Lewis, 2016).

En este sentido, las tensiones geopolíticas y los conflictos internacionales pueden tener un impacto directo en la disponibilidad y seguridad de los sistemas espaciales. De igual forma, la dependencia de componentes o tecnologías extranjeras puede generar vulnerabilidades estratégicas y dificultar la autonomía de los países en el espacio. Por ejemplo, el uso de componentes de Estados Unidos puede estar sujeto a regulaciones de exportación que impiden su uso en algunos sistemas espaciales, creando condiciones asimétricas de competencia que exacerban los inciertos internacionales (Falco & Boschetti, 2021).

Así las cosas, lo anterior genera mayores tensiones por el control del espacio y sus oportunidades, motivando a actores maliciosos, incluyendo estados-nación, grupos terroristas, organizaciones criminales o individuos, para robar propiedad intelectual, información sensible, o simplemente causar da-

ño, aprovechando las vulnerabilidades en la infraestructura espacial, para mantener un conflicto de baja intensidad que busca debilitar al adversario, obtener información, interrumpir operaciones, influir en la opinión pública, sabotear infraestructura crítica, que termina comprometiendo los intereses nacionales y estratégicos de los países debilitando los fundamentos de su seguridad nacional (Hamill-Stewart, 2025).

La carrera espacial implica la participación de múltiples actores y proveedores para lograr articular de la mejor forma las misiones al espacio. En consecuencia, la complejidad de la cadena de suministro refleja no sólo la necesidad de cooperación y colaboración para el logro de los objetivos trazados, sino el punto de mayor vulnerabilidad en para concretar la independencia tecnológica en los temas espaciales (Kaczmarek, 2024).

La interconexión global de proveedores y fabricantes introduce múltiples puntos de vulnerabilidad que pueden ser explotados por adversarios. La diversidad de partes interesadas en la cadena de suministro, incluyendo formuladores de políticas, especialistas en adquisiciones, tecnólogos y expertos en seguridad, complica aún más la situación. La seguridad de los sistemas espaciales también se ve afectada por la dependencia en componentes producidos por proveedores con limitaciones financieras o con vínculos en países que representan riesgos para la seguridad nacional. La integración de inteligencia artificial (IA) en la iniciativa espacial, aunque esencial para el éxito y la confiabilidad de las operaciones, introduce riesgos adicionales como comportamientos maliciosos de la IA, problemas de integridad de datos y la explotación de sistemas de IA para control o sabotaje no autorizados (Kaczmarek, 2024; Ear et al., 2023).

Conclusiones

Al inicio de la exploración espacial los sistemas utilizados estaban aislados de las redes y conexiones. Funcionaban en un dominio cerrado y con controladores específicos, donde se conocía no sólo la infraestructura, sino a las personas que tenían los accesos para operarlos. Sin embargo, a medida que la tecnología avanzaba, la necesidad de interconectar los sistemas espaciales con las redes terrestres para mejorar la eficiencia operativa y la recopilación de datos llevó a una expansión significativa de la superficie de ataque. Esta transición marcó el inicio de la era de la ciberseguridad espacial, donde las vulnerabilidades y las amenazas cibernéticas se convierten en una preocupación clave (Schrogl, 2020).

Dentro de los riesgos críticos que se tienen para las misiones espaciales se detallan los siguientes, los cuales revelan la sensibilidad del tema, no sólo para industria espa-

cial, sino para los retos y propósitos de la seguridad nacional: (Falco & Boschetti, 2021)

- Robo y Corrupción de Datos: Los ataques cibernéticos pueden resultar en el robo de datos confidenciales, como datos de investigación o información de inteligencia, o la corrupción de datos críticos, comprometiendo la integridad de la misión.

- Interrupción de Operaciones: Los ataques de denegación de servicio y otros ataques cibernéticos pueden interrumpir las operaciones de los sistemas espaciales, causando retrasos, pérdida de ingresos y daño a la reputación.

- Secuestro de activos espaciales: Los atacantes pueden tomar el control de satélites y otros vehículos espaciales, comprometiendo su funcionalidad, alterando su trayectoria o incluso utilizándolos con fines maliciosos o armas cinéticas.

- Conflicto cibernético en el Espacio: Los satélites y la infraestructura espacial son objetivos potenciales en conflictos cibernéticos, lo que podría tener consecuencias devastadoras para las comunicaciones, la navegación y la seguridad nacional.

- Ataques a la Investigación Científica: Los ciberataques pueden afectar las actividades de investigación y la integridad de los datos científicos, obstaculizando la cooperación internacional en la exploración espacial.

En línea con lo anterior, y dado que, la naturaleza global de la industria espacial demanda una colaboración estrecha entre agencias espaciales, gobiernos, el sector privado y organizaciones internacionales, el intercambio de información sobre amenazas y vulnerabilidades, se convierte en un elemento y práctica fundamental para asegurar el buen desarrollo de las misiones, no sólo para mantener la integridad de las comunicaciones y el aseguramiento de los instrumentos de operación de las naves, sino para consolidar una postura de defensa cibernética espacial que permita anticipar distintas acciones adversas sobre activos espaciales sensibles y los planes estratégicos de las naciones (Oakley, 2024).

Por tanto, la ciberseguridad en las misiones espaciales es un campo en constante evolución que requiere atención permanente y una inversión significativa. Al abordar los retos actuales e implementar las acciones y alianzas adecuadas a nivel político, económico, social, tecnológico, ecológico y legal, la industria espacial puede proteger sus activos, asegurar la continuidad y resiliencia de sus operaciones y así, fomentar la innovación en un entorno cada vez más inestable y con tensiones geopolíticas crecientes. Esto exige de los Estados,

priorizar la ciberseguridad como un imperativo estratégico para el éxito y la sostenibilidad a largo plazo de la misión: posicionar el espacio como fuente de oportunidades y ventajas competitivas para los países (Flanagan et al., 2023).

El espacio es un recurso finito y valioso que debe ser gestionado con cuidado y responsabilidad, como un ejercicio de exploración conjunta para retar y superar las fronteras del conocimiento, y deponer las diferencias basadas en control y poder. Al asegurar el espacio como un bien común (Jah, 2024), es posible encontrar nuevas oportunidades para la investigación científica, la innovación tecnológica y el desarrollo económico, mejorando la vida de todos en el planeta. Ignorar estos desafíos multidimensionales que se tienen, y particularmente lo relativo al riesgo cibernético, y no actuar ahora, puede poner en riesgo el futuro de la exploración espacial y los beneficios potenciales para la humanidad.

Referencias

Ear, E., Remy, J. L. C., Feffer, A. & Xu, S. (2023). Characterizing cyber attacks against space systems with missing data: Framework and case study. *2023 IEEE Conference on Communications and Network Security (CNS)*. https://doi.org/10.1109/CNS59707.2023.10289045

Falco, G. & Boschetti, N. (2021). A security risk taxonomy for commercial space missions. *ASCEND 2021*. https://doi.org/10.2514/6.2021-4241

Falco, G., Boschetti, N., Viswanathan, A., Bailey, B., Maple, C., Kurt, G. K., Willbold, J., Slay, J., Birrane, E., Logsdon, D., Bennett, S., Ferguson, W., Curbo, J., Oakley, J., Schloegel, M., Hagen, S., Sigholm, J., Mehlman, C., Thummala, R., … Yahia, O. B. (2024). Minimum requirements for space system cybersecurity - ensuring cyber access to space. *2024 IEEE 10th International Conference on Space Mission Challenges for Information Technology (SMC-IT)*, 78–88. https://doi.org/10.1109/SMC-IT61443.2024.00016

Flanagan, S., Martin, N., Blanc, A. & Beauchamp-Mustafaga, N. (2023). A Framework of Deterrence in Space Operations. Research Report. *RAND Corporation*. https://www.rand.org/pubs/research_reports/RRA820-1.html

Gerstein, D., Kallimani, J., Mayer, L., Meshkat, L., Osburg, J., Davis, P., Cignarella, B. & Grammich, C. (2016). Developing a Risk Assessment Methodology for the National Aeronautics and Space Administration. *RAND Corporation*. https://www.rand.org/pubs/research_reports/RR1537.html

Hamill-Stewart, J. (2025). The Sendai Framework and satellite security. *International Journal of Disaster Risk Science*. https://doi.org/10.1007/s13753-025-00614-9

Hodgson, Q., Warren, K., Brosmer, J., Alhajjar, E., Fujiwara, J., Grossfeld, E., Hartunian, A., Kim, Y., Lee, M., López III, E., Rodgers, M., Van Abel, K. & Johnson, R. (2024). Enhancing Space Mission Assurance to Cyber Threats: Findings and Recommendations for the U.S. Space Force. *RAND Corporation*. https://www.rand.org/pubs/research_reports/RRA2319-1.html

Jah, M. (2024). The Tragedy of the Commons in Orbital Space: Toward a Circular Economy. *Amplify*. *37*(2). 36-43. https://www.cutter.com/article/tragedy-commons-orbital-space-toward-circular-economy

Kaczmarek, S. (2024). Cybersecurity challenges in space exploration. *Amplify*. *37*(2). 26-35. https://www.cutter.com/article/cybersecurity-challenges-space-exploration

Livingstone, D. & Lewis, P. (2016). Space, the Final Frontier for Cybersecurity? *Chatham House*. Research Paper. https://www.chathamhouse.org/2016/09/space-final-frontier-cybersecurity

Manulis, M., Bridges, C. P., Harrison, R., Sekar, V. & Davis, A. (2021). Cyber security in New Space: Analysis of threats, key enabling technologies and challenges. *International Journal of Information Security*, *20*(3), 287–311. https://doi.org/10.1007/s10207-020-00503-w

Oakley, J. G. (2024). *Cybersecurity for space: A guide to foundations and challenges*. Apress.

Schrogl, K.-U. (Ed.). (2020). *Handbook of space security: Policies, applications and programs*. Springer International Publishing.

Tretter, C. (2025). Exploring Factors for U.S.-Russia Crisis Stability in Space. *RAND Corporation*. https://www.rand.org/pubs/research_reports/RRA2313-3.html

WEF-World Economic Forum & Mckinsey (2024). Space: The $1.8 Trillion Opportunity for Global Economic Growth. *Insight Report*. https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/space-the-1-point-8-trillion-dollar-opportunity-for-global-economic-growth

Jeimy J. Cano M., Ph.D, CFE, CICA*. Ingeniero y Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes. Especialista en Derecho Disciplinario, Universidad Externado de Colombia; Ph.D en Business Administration, Newport University, CA. USA. y Ph.D en Educación, Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Profesor Distinguido de la Facultad de Derecho, Universidad de los Andes. Es director de la Revista SISTEMAS de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*