Capítulo 7

Naves autónomas en el espacio: poder, tecnología y desafíos de seguridad*

DOI: https://doi.org/10.25062/9786287818620.07

Guillermo Alberto Poveda Zamora
Fuerza Aeroespacial Colombiana

Resumen: Cómo las naves espaciales autónomas y pilotadas remotamente están redefiniendo las estrategias geopolíticas, las capacidades operacionales y los desafíos de seguridad en el dominio espacial. Este capítulo se propone analizar su impacto en la geopolítica, la operación y la seguridad espacial. Para ello, se examinan las implicaciones geopolíticas de su despliegue, se miden sus capacidades operacionales en exploración, logística y defensa, y se caracterizan los riesgos de ciberseguridad y se proponen contramedidas. Mediante una revisión documental de literatura científica, normativa y fuentes militares, se analizan y comparan los casos emblemáticos X-37B (EE.UU.), Shijian-21 (China) y Kosmos (Rusia), contrastando sus capacidades, objetivos y riesgos. Se evidencia que la convergencia de inteligencia artificial, autonomía operativa y ciberdefensa está transformando la exploración, la seguridad y la logística orbital, mientras abre nuevas vulnerabilidades a *spoofing, jamming* y ataques cibernéticos. La investigación advierte que la evolución de estos sistemas exige un enfoque integral de seguridad para garantizar la estabilidad operativa y la sostenibilidad de las misiones en el entorno espacial.

Palabras clave: ciberseguridad; inteligencia artificial; logística orbital; naves espaciales autónomas; regulación internacional; seguridad espacial

* Capítulo de libro resultado del proyecto de investigación "Sistema de naves y aeronaves no tripuladas e inteligencia artificial: innovaciones estratégicas para el futuro militar" en colaboración del Grupo de Investigación Ciencias Militares Aeronáuticas (GICMA), categorizado en A1 por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias) (código COL0140489). Los puntos de vista y los resultados de este capítulo pertenecen a sus autores y no reflejan necesariamente los de las instituciones participantes.

Guillermo Alberto Poveda Zamora

Coronel (R) de la Fuerza Aeroespacial Colombiana. Magíster en ciencias militares aeronáuticas, Escuela de Posgrados FAC, Colombia. Magíster en ingeniería aeroespacial, Universidad del Valle, Colombia. Administrador aeronáutico. Ingeniero en telecomunicaciones. Docente e investigador, Escuela de Posgrados de la Fuerza Aeroespacial Colombiana.

Orcid: **https://orcid.org/0000-0002-3358-102X** - Contacto: **guillopoveda@gmail.com**

Citación APA: Poveda Zamora, G. A. (2026). Naves autónomas en el espacio: poder, tecnología y desafíos de seguridad. En D. Barrero-Barrero (Ed.), *Sistema de naves y aeronaves no tripuladas e inteligencia artificial: innovaciones estratégicas para el futuro militar* (pp. 159-185). Sello Editorial ESDEG.
https://doi.org/10.25062/9786287818620.07

SISTEMA DE NAVES Y AERONAVES NO TRIPULADAS E INTELIGENCIA ARTIFICIAL: INNOVACIONES ESTRATÉGICAS PARA EL FUTURO MILITAR

ISBN impreso: 978-628-7818-56-9

E-ISBN digital: 978-628-7818-62-0

DOI: https://doi.org/10.25062/9786287818620

Colección Estrategia, Geopolítica y Cultura
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes prieto"
Bogotá D.C., Colombia
2026

CC BY NC ND

Introducción

El desarrollo y despliegue de naves espaciales autónomas ha redefinido la dinámica geopolítica y estratégica en el ámbito espacial. Estas tecnologías han impulsado la competencia entre potencias como EE.UU., China y Rusia, que buscan consolidar su dominio en el espacio a través de avances en exploración, vigilancia e inteligencia. Si bien estas plataformas han optimizado la operatividad en órbita y reducido la necesidad de intervención humana en tareas de alto riesgo, también han abierto nuevas brechas de seguridad, particularmente en ciberdefensa y guerra electrónica.

La autonomía operativa de estos sistemas plantea interrogantes fundamentales sobre la estabilidad global, la militarización del espacio y la necesidad de una actualización urgente de los marcos regulatorios. A medida que la IA y los sistemas cibernéticos avanzados convergen con la exploración espacial, emergen riesgos asociados a la vulnerabilidad de estos activos estratégicos frente a ataques de *spoofing*[1], ciberataques y sabotajes electrónicos. En este contexto, la creciente interconexión entre infraestructuras espaciales y redes digitales amplifica la superficie de ataque para actores hostiles, lo que obliga a desarrollar estrategias de defensa más sofisticadas y resilientes.

Este capítulo analiza las capacidades operacionales de las naves espaciales autónomas, su impacto en la seguridad global y los desafíos emergentes en ciberdefensa. Se abordan las estrategias de los principales actores en la competencia espacial, destacando la manera en que estas tecnologías están transformando la seguridad y la estabilidad geopolítica. Asimismo, se exploran las amenazas en

1 Técnica de suplantación de la identidad de una fuente confiable (como una dirección IP, correo electrónico o señal GPS) para engañar a un sistema o usuario. Su objetivo es robar información, desviar datos o acceder sin autorización.

términos de ciberseguridad y las respuestas tecnológicas para mitigar los riesgos asociados a la militarización del espacio.

El capítulo se estructura en varias secciones clave. En primer lugar, se examinan las implicaciones geopolíticas y la competencia estratégica entre potencias espaciales. Posteriormente, se presentan las capacidades operacionales de las naves autónomas y su aplicación en seguridad, defensa y logística orbital. Luego, se abordan los retos regulatorios y la necesidad de establecer protocolos internacionales para evitar una escalada de conflictos en el espacio. Finalmente, se analizan las estrategias de ciberseguridad, incluyendo el uso de IA, redes cuánticas y cifrado avanzado como mecanismos de protección frente a ciberamenazas.

La creciente militarización del espacio no solo ha impulsado el desarrollo de nuevas tecnologías, sino que también ha dado lugar a una nueva dimensión del conflicto cibernético. Las operaciones de guerra electrónica y los ciberataques contra infraestructuras espaciales han evolucionado hasta convertirse en herramientas estratégicas en la rivalidad entre naciones. Como resultado, garantizar la resiliencia de estos sistemas es una prioridad para la estabilidad internacional.

Por lo tanto, aquí no solo se contextualiza la importancia de las naves autónomas en el ámbito espacial, sino que también se propone un análisis crítico sobre los desafíos técnicos, estratégicos y regulatorios que definirán el futuro de la seguridad y la ciberdefensa en y desde el espacio.

Implicaciones geopolíticas del desarrollo y despliegue de naves espaciales autónomas

El análisis de las implicaciones geopolíticas del desarrollo y despliegue de naves espaciales autónomas, con énfasis en la competencia internacional, la cooperación entre países y la militarización del espacio, permite evaluar el impacto de estas tecnologías en la seguridad global.

Los resultados muestran que EE.UU., China y Rusia lideran el desarrollo de naves autónomas con objetivos estratégicos de exploración, inteligencia y defensa, lo que ha intensificado las tensiones globales. A pesar de iniciativas como los Artemis Accords, persisten desafíos en la cooperación internacional. Además, la militarización del espacio sigue en ascenso debido a pruebas de armas antisatélite (ASAT).

Asimismo, la regulación actual es insuficiente, por lo que se requieren nuevos tratados internacionales que regulen el uso de las naves autónomas y mitiguen los riesgos de seguridad en el espacio.

Competencia estratégica internacional

La actual carrera espacial ha intensificado la competencia estratégica entre potencias globales, principalmente entre EE.UU., China y Rusia. Estas naciones han invertido significativamente en tecnologías autónomas con aplicaciones civiles y militares (Lee & Zhang, 2020). EE.UU. ha liderado con el desarrollo del vehículo X-37B, una plataforma reutilizable diseñada para operaciones prolongadas en órbita (Smith et al., 2023).

Por otro lado, China ha avanzado con el satélite Shijian-21, capaz de realizar maniobras complejas en el espacio, lo que ha generado preocupaciones por su uso dual, tanto civil como militar (Nguyen et al., 2022). Asimismo, Rusia ha desplegado satélites de inspección capaces de acercarse a otros activos orbitales, intensificando las tensiones diplomáticas (Wang et al., 2020). La competencia también se ha incrementado en el campo de la inteligencia espacial, donde estas potencias utilizan naves autónomas para la vigilancia y el espionaje estratégico (González et al., 2023).

La Tabla 1 compara los programas de naves autónomas de EE.UU., China y Rusia, destacando sus objetivos estratégicos y los riesgos asociados. Se evidencia la competencia tecnológica y sus implicaciones geopolíticas en seguridad y defensa espacial.

Tabla 1. *Comparación de capacidades en naves autónomas militares espaciales entre EE.UU., China y Rusia*

País	Programas de naves autónomas	Objetivos estratégicos	Riesgos asociados
EE.UU.	X-37B, DARPA XS-1	Exploración avanzada, inteligencia y defensa estratégica	Militarización del espacio, espionaje tecnológico
China	Shijian-21, Tianyuan	Dominio orbital, neutralización de satélites, acceso a recursos espaciales	Preocupaciones sobre uso dual (civil-militar), tensiones geopolíticas
Rusia	Kosmos, Burevestnik	Vigilancia orbital, guerra electrónica, defensa contra amenazas espaciales	Interferencia en satélites rivales, falta de transparencia en desarrollos espaciales

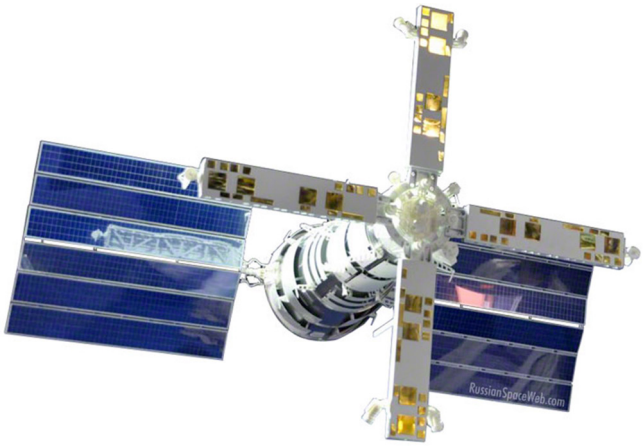
Fuente: Elaboración propia con base en los datos recolectados de Lee y Zhang (2020), Smith et al. (2023), Nguyen et al. (2022), Wang et al. (2020) y González et al. (2023)

En la Figura 1 se pueden observar tres naves espaciales autónomas avanzadas: el X-37B de EE.UU., utilizado para misiones de inteligencia y defensa; el Shijian-21 de China, con capacidades de maniobra orbital; y un satélite de la familia Kosmos de Rusia, empleado para monitoreo y comunicaciones espaciales.

Figura 1. *Naves espaciales autónomas más avanzadas*

X-37B (EE.UU.)

Shijian-21 (China)



Lotos-S1 (Rusia)

Fuente: Elaboración propia con imágenes de Latam Satelital (2018), Makichuk (2021) y Wall (2012)

Cooperación internacional

A pesar de la creciente competencia, existen iniciativas de cooperación internacional como los Artemis Accords, liderados por EE.UU., que buscan establecer una presencia sostenible en la Luna mediante alianzas multinacionales (Smith et al., 2023). No obstante, estas iniciativas tienen detractores debido a la desconfianza estratégica y a las diferencias en políticas espaciales entre las potencias (Brown et al., 2020). China y Rusia han formado alianzas estratégicas para contrarrestar la influencia de EE.UU. en la cooperación espacial internacional, mientras que otras naciones emergentes, como India y Japón, buscan consolidar sus propias capacidades espaciales mediante colaboraciones regionales (Johnson & Miller, 2020).

En la Figura 2 se puede observar un diagrama que representa las principales alianzas en la exploración espacial. Se destacan los Artemis Accords, liderados por EE.UU., y la colaboración China-Rusia, enfocada en rivalizar con la influencia estadounidense. Además, se incluyen alianzas emergentes, como la participación de Brasil y Emiratos Árabes Unidos en proyectos estadounidenses, y la cooperación de Sudáfrica y Nigeria con China y Rusia en tecnología espacial.

Militarización del espacio

El desarrollo de armas antisatélite y la creación de fuerzas espaciales han incrementado el riesgo de militarización del espacio (Anderson et al., 2021). China realizó una prueba ASAT en 2007, generando miles de fragmentos de desechos

Figura 2. *Diagrama de cooperación internacional en la exploración espacial*

Fuente: Elaboración propia con datos de Johnson y Miller (2020)

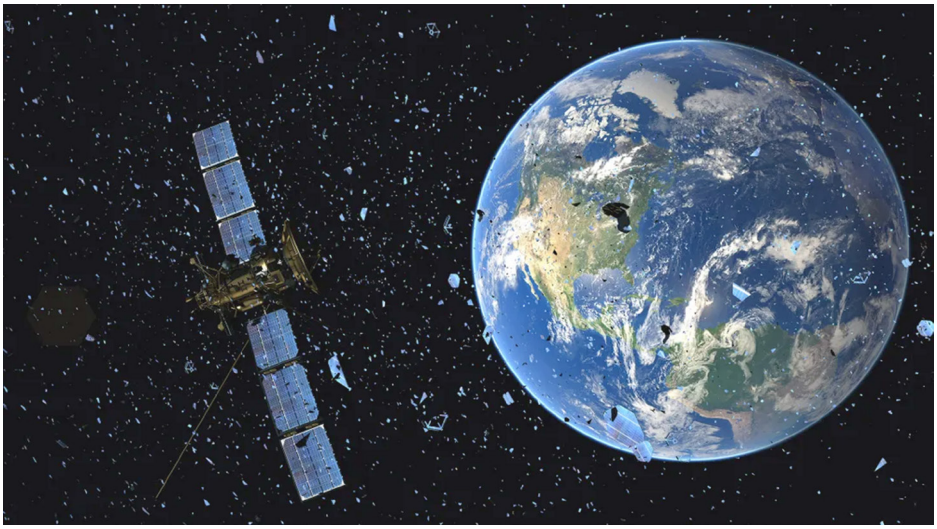
espaciales y complicando la seguridad orbital (Nguyen et al., 2022). EE.UU. respondió con la creación de su Fuerza Espacial en 2019, consolidando sus capacidades de defensa en el espacio (Brown & Taylor, 2020). Este escenario plantea un dilema estratégico en torno a la militarización y el uso pacífico del espacio exterior (Johnson & Miller, 2020). Además, el desarrollo de satélites capaces de maniobrar y neutralizar otros satélites ha generado preocupación por el uso de tecnología autónoma para operaciones ofensivas (Lee & Zhang, 2020).

En la Figura 3 se puede observar una representación gráfica de la acumulación de fragmentos de basura espacial en la órbita media-baja terrestre. Estos desechos, producto de pruebas de armas antisatélite y colisiones de satélites obsoletos, representan un riesgo significativo para la seguridad orbital y la operatividad de satélites activos. La creciente cantidad de escombros espaciales plantea desafíos para la navegación, el acceso y la exploración del espacio.

Desafíos regulatorios y reformas necesarias

El marco legal internacional actual, encabezado por el Tratado sobre el Espacio Ultraterrestre (1967), es insuficiente para abordar los desafíos modernos que presentan las naves autónomas y los sistemas espaciales de doble uso (Kumar et al.,

Figura 3. *Fragmentos de basura espacial generados por humanos en la órbita media-baja*

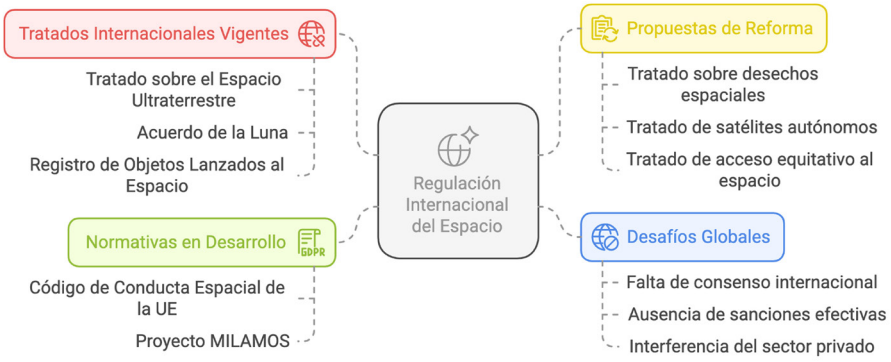


Fuente: González Valenzuela (2023)

2023). Se han propuesto varias reformas, como el Código de Conducta Espacial de la Unión Europea, aunque este carece de mecanismos vinculantes (Lee & Zhang, 2020). Se destaca la necesidad de un organismo internacional de monitoreo que supervise el despliegue de tecnologías autónomas, previniendo su uso militar indebido (Smith et al., 2023). Además, se ha propuesto la creación de un tratado específico que regule el uso de naves autónomas en el espacio (Gonzalez et al., 2023).

En la Figura 4 se presenta un esquema sobre la regulación internacional del espacio, destacando los tratados vigentes, como el Tratado sobre el Espacio Ultraterrestre (1967) y el Acuerdo de la Luna (1979). También se incluyen normativas en desarrollo, como el Código de Conducta Espacial de la UE y el proyecto Milamos (*Manual on International Law Applicable to Military Uses of Outer Space*). Asimismo, se muestran propuestas de reforma, enfocadas en regular los desechos espaciales, los satélites autónomos y garantizar el acceso equitativo al espacio. Finalmente, se identifican desafíos globales, tales como la falta de consenso internacional, la ausencia de sanciones efectivas y la interferencia del sector privado en la exploración espacial.

Figura 4. *Regulación internacional: tratados y desafíos*



Fuente: Elaboración propia con datos de Kumar et al. (2023)

Tecnología y capacidades operacionales de naves autónomas en misiones de seguridad y defensa

Las naves espaciales autónomas están transformando la exploración, la seguridad y la defensa en el espacio. Estas plataformas tecnológicas han optimizado la vigilancia orbital, la protección de infraestructuras espaciales y la eficiencia en la gestión de recursos. Su creciente autonomía reduce la necesidad de intervención humana en tareas de alto riesgo, mejora la capacidad de respuesta ante amenazas y aumenta la resiliencia operativa en entornos hostiles (Johnson & Taylor, 2022). En el entorno militar generan especial preocupación sus capacidades operacionales, su aplicación en la seguridad espacial y su impacto en el equilibrio geopolítico global.

Capacidades técnicas y operacionales de naves autónomas

Las naves autónomas destacan por una combinación de tecnologías avanzadas que les permiten cumplir tareas complejas sin intervención humana directa.

Reconocimiento y monitoreo de activos críticos

El reconocimiento y monitoreo de activos críticos en el espacio es una función esencial de las naves autónomas, diseñada para detectar, rastrear y evaluar amenazas en tiempo real. Gracias a sensores avanzados, como cámaras

multiespectrales y radares de apertura sintética (SAR), estas plataformas pueden identificar movimientos sospechosos y posibles riesgos para infraestructuras estratégicas (Martínez et al., 2021; Wilson et al., 2022). Además, el uso de IA permite el procesamiento de grandes volúmenes de datos mediante algoritmos de aprendizaje profundo, lo que facilita la identificación de patrones y anomalías que podrían indicar actividades hostiles (Kim et al., 2021; Vásquez et al., 2023). La persistencia en el espacio es otro factor clave, ya que estas naves pueden operar en órbita por largos periodos, proporcionando vigilancia continua sobre áreas sensibles, como estaciones espaciales y satélites críticos (Rodríguez & Li, 2022).

- *Sensores avanzados*. Equipadas con cámaras multiespectrales y radares de apertura sintética (SAR), estas naves pueden detectar, rastrear y evaluar amenazas en tiempo real. Entre estos sistemas de detección se encuentra el Programa de Apoyo a la Defensa (DSP, Defense Support Program), con una constelación de satélites geoestacionarios que proporcionaba capacidad de detección de lanzamientos de misiles (Martínez et al., 2021; Wilson et al., 2022).
- *IA para análisis de datos*. Algoritmos de aprendizaje profundo procesan grandes volúmenes de datos para identificar patrones y anomalías que podrían indicar actividades hostiles (Sánchez Godínez, 2012; Kim et al., 2021; Vásquez et al., 2023).
- *Persistencia en el espacio*. Estas naves pueden permanecer en órbita durante largos periodos, incluso décadas, como los X-37B, de los cuales se tiene registro de su primer lanzamiento en 2011. Esto les permite monitorear continuamente áreas sensibles, como estaciones espaciales, satélites críticos o zonas de interés en la superficie del planeta (Rodríguez & Li, 2022).

La figura 5 muestra una representación del satélite SBIRS-High, del DSP. Este satélite se utiliza para la detección y alerta temprana de lanzamientos de misiles balísticos, empleando sensores infrarrojos avanzados para monitorear amenazas globales en tiempo real. Su función estratégica es esencial para la defensa y la seguridad espacial.

Sistemas de respuesta automática ante amenazas

Los sistemas de respuesta automática ante amenazas son mecanismos avanzados implementados en naves espaciales autónomas para neutralizar riesgos orbitales y proteger activos estratégicos. Algunas de estas naves están equipadas

Figura 5. *Representación del satélite SBIRS-High del DSP*

Fuente: Sánchez Godínez (2012)

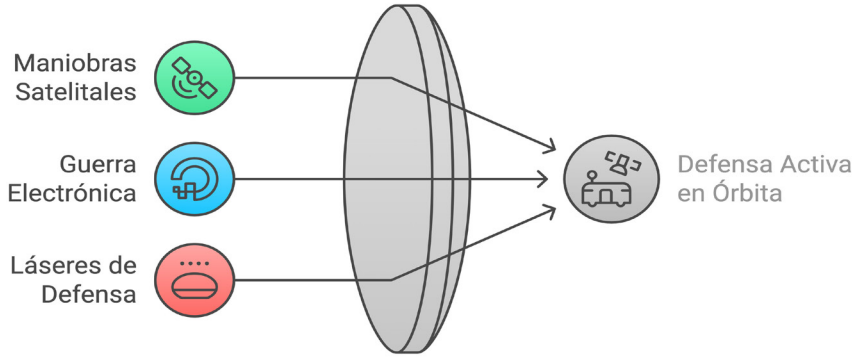
con tecnología de intercepción de amenazas orbitales, lo que les permite neutralizar satélites hostiles o interceptar desechos espaciales que representen un peligro para infraestructuras clave (Tanaka & Fujimoto, 2023; Pérez et al., 2022). Además, cuentan con protocolos de defensa autónoma que les permiten ejecutar maniobras evasivas o desplegar contramedidas automáticamente en caso de detectar una posible agresión, garantizando así la seguridad operativa sin intervención humana inmediata (Méndez et al., 2022; Hernández et al., 2023).

- *Intercepción de amenazas orbitales.* Algunas naves están diseñadas para neutralizar satélites hostiles o interceptar desechos espaciales que puedan poner en riesgo activos estratégicos (Tanaka & Fujimoto, 2023; Pérez et al., 2022).
- *Protocolos de defensa autónoma.* Sistemas que ejecutan maniobras evasivas o contramedidas de forma automática en caso de ataque, en especial si la comunicación con su estación de control ha sido comprometida, degradada o anulada por completo (Méndez et al., 2022; Hernández et al., 2023).

La Figura 6 ilustra los métodos de defensa activa en órbita utilizados por las naves espaciales autónomas. Se presentan tres enfoques principales: maniobras satelitales, que permiten evasión y reposicionamiento estratégico; guerra electrónica, utilizada para interferir y neutralizar señales hostiles; y láseres de defensa, diseñados para contrarrestar amenazas físicas en el espacio. Estas estrategias

contribuyen a una respuesta automatizada y efectiva ante posibles agresiones en entornos orbitales hostiles.

Figura 6. *Estrategias de respuesta automática ante amenazas*



Fuente: Elaboración propia con datos de Méndez et al. (2022) y Hernández et al. (2023)

Aplicaciones estratégicas en seguridad y defensa

Las naves autónomas desempeñan un papel clave en la seguridad y defensa espacial, proporcionando monitoreo de satélites y bases rivales, y protegiendo activos estratégicos mediante IA y análisis predictivo para detectar amenazas de forma anticipada.

Reconocimiento y vigilancia

Las naves autónomas son esenciales para las operaciones de inteligencia en el espacio, tales como:

- *Monitoreo de satélites y bases rivales*. Proveen datos críticos sobre movimientos y actividades sospechosas de otros actores espaciales (Wong et al., 2021; Zhang et al., 2023).
- *Protección de activos propios*. Ayudan a identificar posibles ataques antes de que ocurran mediante análisis predictivo basado en IA (Khan et al., 2023; Ortiz & Jiménez, 2023).

Logística y abastecimiento

Las naves autónomas han optimizado significativamente la logística y el abastecimiento espacial, permitiendo el transporte autónomo de suministros a estaciones espaciales y bases lunares, así como el reabastecimiento orbital, lo que prolonga la

vida útil de satélites y otros activos estratégicos. Su implementación ha mejorado considerablemente el transporte y mantenimiento de infraestructuras espaciales, facilitando operaciones de reabastecimiento de combustible, reparación y optimización de recursos, lo que fortalece la resiliencia y sostenibilidad de las misiones espaciales. Estas misiones incluyen:

- *Transporte autónomo.* Las naves pueden realizar entregas precisas de suministros a estaciones espaciales y bases lunares, reduciendo la necesidad de misiones tripuladas (García et al., 2022; Singh et al., 2022).
- *Mantenimiento y reparación orbital.* ELSA-d (Reino Unido) ha demostrado capacidad para capturar y reparar satélites defectuosos (Johnson & Miller, 2020).
- *Reabastecimiento orbital.* Facilita operaciones de recarga de combustible y mantenimiento de satélites, optimizando recursos y extendiendo la vida útil de los activos. Vehículos como Cygnus (NASA) y HTV-X (Japón) permiten el reabastecimiento automático de la Estación Espacial Internacional (ISS) (Lin et al., 2023; Huang et al., 2022).

La Tabla 2 presenta un análisis de las principales naves espaciales utilizadas para abastecimiento, mantenimiento y logística orbital. Se incluyen naves operadas por agencias espaciales como NASA, JAXA, CNSA y Roscosmos, así como desarrollos de empresas privadas como SpaceX, Boeing, Sierra Space y Blue Origin. La tabla destaca la función de cada nave, la entidad responsable, su beneficio estratégico y su grado de autonomía. Este análisis permite comprender el papel clave de estas naves en la exploración y sostenibilidad del entorno espacial.

Tabla 2. *Comparación de naves autónomas y semiautónomas para aplicaciones logísticas en el espacio*

Nombre de la nave	Función	Agencia/espacio responsable	Beneficio estratégico	Autonomía
Cygnus	Transporte de carga a la ISS	NASA / Northrop Grumman (EE.UU.)	Mantiene operaciones en la ISS y pruebas tecnológicas	Totalmente autónoma
HTV-X	Reabastecimiento y carga orbital	JAXA (Japón)	Optimiza misiones espaciales con mayor capacidad de carga	Totalmente autónoma
Dragon	Transporte de suministros y retorno de carga	SpaceX (EE.UU.)	Reduce costos al permitir recuperación de materiales	Totalmente autónoma

Continúa tabla...

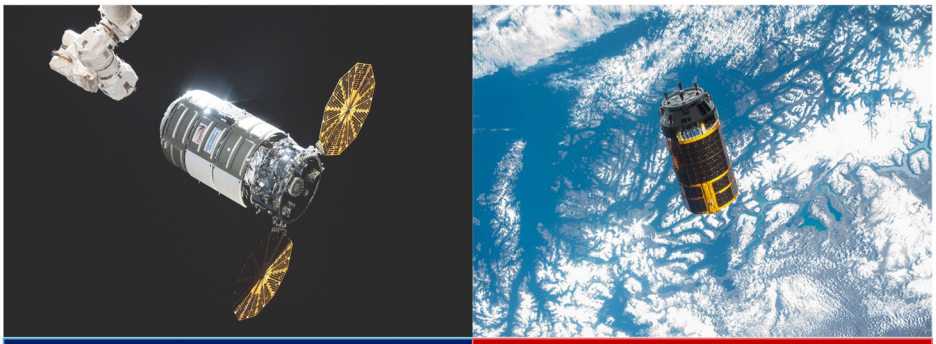
Nombre de la nave	Función	Agencia/espacio responsable	Beneficio estratégico	Autonomía
Tianzhou	Suministro de módulos y logística espacial	CNSA (China)	Soporta la exploración espacial con mayor autonomía	Totalmente autónoma
ELSA-d	Captura y retiro de desechos espaciales	Astroscale (Reino Unido / Japón)	Contribuye a la limpieza y sostenibilidad del entorno orbital	Totalmente autónoma
CST-100 Starliner	Transporte de tripulación y carga a la ISS	Boeing / NASA (EE. UU.)	Apoya el acceso recurrente de astronautas y suministros a la ISS	Semiautónoma; requiere intervención humana
Dream Chaser	Transporte de carga y retorno de experimentos científicos	Sierra Space / NASA (EE.UU.)	Permite retornos seguros de experimentos y materiales de la ISS	Totalmente autónoma
Progress	Suministro de carga a la ISS	Roscosmos (Rusia)	Garantiza el abastecimiento continuo de la ISS	Totalmente autónoma
X-37B	Misiones experimentales y de reconocimiento militar	Boeing / Fuerza Espacial de EE.UU.	Realiza pruebas de tecnologías espaciales avanzadas	Totalmente autónoma
New Shepard	Turismo espacial suborbital y experimentos científicos	Blue Origin (EE.UU.)	Facilita experimentos en microgravedad y vuelos comerciales	Totalmente autónoma

Fuente: Elaboración propia con base en NASA (2023), Marín (2016), SpaceX (2023), CNSA (2022), Astroscale (2022), Boeing (2023), Sierra Space (2023), Roscosmos (2022), Fuerza Espacial de EE.UU. (2023) y Blue Origin (2023)

En este sentido, en la Figura 7 se observan dos naves autónomas de carga utilizadas para el reabastecimiento de la ISS. A la izquierda, la Cygnus de NASA y Northrop Grumman, diseñada para transportar suministros y experimentos científicos. A la derecha, la HTV-X de Japón (JAXA), una evolución de la serie HTV, optimizada para misiones de logística y carga orbital. Ambas representan avances en la automatización y sostenibilidad de las operaciones espaciales.

Por otra parte, la eficiencia en el consumo de combustible es un factor determinante en el éxito de las misiones espaciales autónomas. La aplicación de modelos teóricos de la mecánica celeste permite reducir significativamente el uso de combustibles en vehículos espaciales, lo que optimiza la autonomía y sostenibilidad de las misiones (Poveda Zamora, 2020).

Figura 7. *Naves autónomas de carga para abastecimiento de la ISS*



Fuente: NASA (2023) y Marín (2016)

Respuesta en tiempo real a crisis espaciales y en la superficie terrestre

La respuesta en tiempo real a crisis espaciales es una capacidad clave de las naves autónomas, permitiendo la neutralización de amenazas emergentes mediante algoritmos adaptativos que pueden interceptar proyectiles o satélites hostiles (Rodríguez et al., 2022; Kim et al., 2023). Además, su avanzada maniobra autónoma facilita el soporte en misiones de rescate, respondiendo rápidamente a emergencias como colisiones o fallos en estaciones espaciales, lo que mejora la seguridad operativa en entornos orbitales críticos (Vásquez et al., 2023; Li et al., 2023).

Bajo este contexto de respuesta oportuna a las crisis, existen misiones muy específicas para las naves espaciales autónomas. Algunas de ellas son:

- *Neutralización de amenazas emergentes.* Mediante algoritmos adaptativos, estas naves pueden interceptar proyectiles, misiles o satélites enemigos (Rodríguez et al., 2022; Kim et al., 2023).
- *Soporte en misiones de rescate.* La capacidad de maniobra autónoma permite respuestas rápidas ante emergencias, como colisiones o fallos en estaciones espaciales (Vásquez et al., 2023; Li et al., 2023).

Un ejemplo de esta capacidad es el proyecto conjunto de la USAF y SpaceX, en el cual la Starship está siendo evaluada como una plataforma para el despliegue de tropas y suministros en cualquier parte del planeta en menos de 90 minutos (*El Confidencial*, 1.º de febrero de 2024). Esta tecnología, originalmente diseñada para la exploración espacial, también podría utilizarse para la atención de desastres y crisis humanitarias, permitiendo una respuesta ultrarrápida a eventos catastróficos y mejorando la logística de emergencia en regiones de difícil acceso.

La Figura 8 representa un cambio disruptivo en la estrategia militar global. La posibilidad de despliegue de tropas y vehículos militares a través de una nave de SpaceX muestra el potencial de estas tecnologías para permitir el traslado ultrarrápido de fuerzas a cualquier punto del planeta.

Figura 8. *Uso estratégico de naves de SpaceX para transporte militar rápido*

Fuente: *El Confidencial* (1º de febrero de 2024)

Esta capacidad sin precedentes redefine el concepto de *movilidad estratégica*, ya que obliga a los países a mejorar sus sistemas de detección, monitoreando más alto y con mayor rapidez cualquier objeto que se aproxime a su territorio. Asimismo, enfatiza la necesidad de desarrollar capacidades de respuesta inmediata, ya que la velocidad de despliegue podría superar los tiempos de reacción convencionales, alterando significativamente la dinámica de seguridad y defensa a nivel internacional.

Optimización de recursos y reducción de riesgos humanos

Las naves autónomas permiten una mayor eficiencia en el uso de recursos y reducen la exposición humana a los riesgos inherentes a las operaciones espaciales. Algunas ventajas de la operación autónoma son:

- *Automatización de tareas repetitivas.* Misiones como el mantenimiento de satélites o la limpieza de desechos espaciales se realizan de manera autónoma, disminuyendo costos operativos, los cuales, a medida que avanzan la IA y la robótica, descienden drásticamente (Martínez et al., 2021; Kim et al., 2022).
- *Flexibilidad operativa.* Las naves pueden ser reprogramadas rápidamente para adaptarse a nuevos objetivos, optimizando su uso durante prolongados tiempos de permanencia en el dominio espacial, algo difícil de lograr con seres humanos (Pérez & Chen, 2022).
- *Minimización de riesgos para astronautas.* Las misiones autónomas eliminan la necesidad de enviar tripulaciones humanas a áreas de alto riesgo, como regiones con alta radiación, asteroides o zonas en conflicto (García et al., 2022; Li et al., 2022).

Ventajas estratégicas para las naciones inversoras

Las capacidades de las naves autónomas proporcionan ventajas competitivas significativas en el ámbito económico y geopolítico:

- *Dominio tecnológico.* Las naves espaciales autónomas representan una ventaja estratégica clave para los países que invierten en su desarrollo, ya que fortalecen su posición geopolítica y tecnológica en el ámbito espacial. Estas tecnologías avanzadas permiten consolidar el dominio tecnológico, asegurando un liderazgo en la exploración y el control del espacio exterior, lo que a su vez influye en la estabilidad y el poder global de las naciones (Lin et al., 2023; Singh et al., 2023).
- *Infraestructura de seguridad avanzada.* Proporcionan una infraestructura de vigilancia sofisticada, capaz de detectar y neutralizar amenazas potenciales, lo que refuerza la disuasión frente a actores hostiles (Wilson et al., 2022; Hernández et al., 2023).
- *Resiliencia frente a emergencias.* Gracias a que su disponibilidad es casi permanente cuando se encuentran orbitando inertes en el espacio, su capacidad de respuesta se vuelve inmediata ante crisis espaciales o eventos inesperados, garantizando la protección y continuidad operativa de activos estratégicos, aumentando la resiliencia de las naciones frente a emergencias y asegurando la sostenibilidad de sus misiones a largo plazo en el espacio (Zhang et al., 2023; Martínez et al., 2021).

Retos de seguridad y ciberdefensa en naves autónomas

Las amenazas cibernéticas en el ámbito espacial incluyen el acceso no autorizado a sistemas, la manipulación de datos y la interferencia en las comunicaciones. Algunas de las principales amenazas detectadas en el ámbito de la seguridad y ciberdefensa de naves autónomas son:

- *Ataques de spoofing.* La suplantación de señales de comando, conocida como spoofing, representa una amenaza crítica para las naves espaciales autónomas. La manipulación de señales GNSS (Global Navigation Satellite System)[2] puede hacer que las naves operen con coordenadas falsas, comprometiendo la integridad de sus misiones y aumentando el riesgo de colisión o interferencia con otras infraestructuras espaciales. Este tipo de ataque es particularmente peligroso en el contexto de la guerra electrónica, donde actores hostiles pueden alterar los sistemas de navegación para obtener ventajas estratégicas (Falco, 2020, p. 12).

Las interferencias en los sistemas de posicionamiento global han demostrado ser un riesgo significativo para la seguridad aeroespacial, afectando tanto a naves espaciales autónomas como a aeronaves comerciales y militares. Casos recientes han evidenciado la gravedad de este problema: en Estonia, un ataque de *spoofing* alteró las señales de navegación, generando el cierre temporal de aeropuertos. Asimismo, en mayo de 2024, un evento de gran escala desvió la ruta de aproximadamente 15 000 aeronaves que tenían destino a Beirut, redirigiéndolas erróneamente hacia El Cairo. Israel también ha experimentado incidentes recurrentes, con intentos de manipulación de señales GNSS que comprometen la precisión del posicionamiento y afectan operaciones de navegación aérea (EITB, 2024).

- *Malware en IA.* El avance de la IA ha permitido una mayor independencia operativa de las naves espaciales. Sin embargo, esta autonomía también ha introducido nuevas amenazas cibernéticas, entre ellas, la posibilidad de que modelos de aprendizaje automático sean comprometidos por *software* malicioso. La manipulación de estos algoritmos podría inducir a las naves a tomar decisiones erróneas, lo que afectaría su desempeño en misiones críticas. En un escenario adverso, estas alteraciones podrían

2 Sistema global que permite determinar la posición, velocidad y tiempo en cualquier parte del mundo mediante señales de satélites. Incluye sistemas como GPS (EE.UU.), Galileo (Unión Europea), Glonass (Rusia) y BeiDou (China).

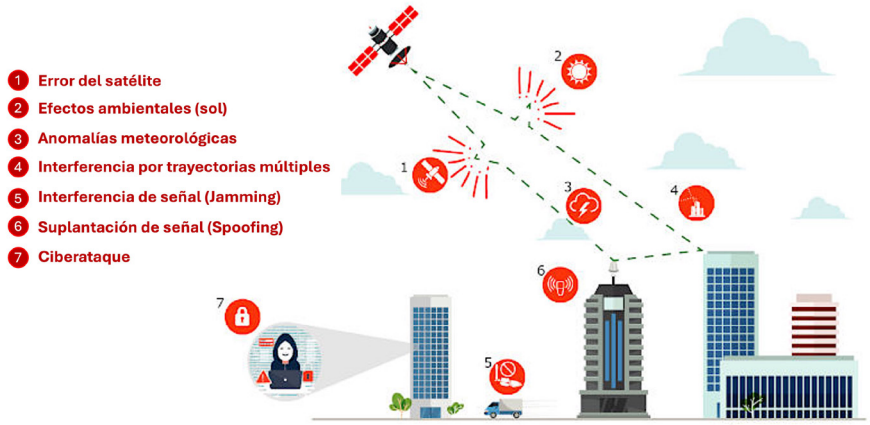
generar fallos en los sistemas de navegación o provocar una respuesta inadecuada ante amenazas espaciales (Thangavel et al., 2022, p. 89).

- *Ataques de denegación de servicio (DoS).* La sobrecarga de los sistemas de comunicación mediante ataques de denegación de servicio puede interrumpir la operatividad de una nave, bloqueando la transmisión de datos y la recepción de comandos desde estaciones terrestres. La latencia en las comunicaciones espaciales agrava este problema, ya que la recuperación de un sistema afectado puede tardar demasiado tiempo en comparación con un ataque realizado en redes terrestres. Además, la interrupción de señales de control puede dejar a las naves vulnerables a otros tipos de ataques cibernéticos (Pavur & Martinovic, 2022, p. 56).
- *Infiltración en redes satelitales.* La interconectividad de redes satelitales con estaciones terrestres expone, en el segmento de enlace, datos sensibles que pueden ser interceptados y explotados por actores maliciosos. La vulnerabilidad de estos sistemas se debe a la falta de protocolos de seguridad unificados y al uso de tecnologías de cifrado obsoletas en algunos satélites. La infiltración en estas redes no solo permite el robo de información, sino que también facilita el sabotaje de misiones estratégicas en tiempo real (Manulis et al., 2021).
- *Manipulación de datos de sensores.* La alteración de los datos captados por los sensores de una nave autónoma puede generar errores críticos en la toma de decisiones, afectando su navegación y respuesta ante posibles amenazas. Este tipo de ataque puede inducir a la nave a detectar amenazas inexistentes, atacar a sus propios colegas o ignorar riesgos reales, aumentando la probabilidad de colisiones o fallos operacionales. En un escenario de conflicto, un adversario podría modificar la información de los sensores para hacer que un satélite hostil pase desapercibido y evitar su neutralización (Pavur et al., 2021, p. 78).

La Figura 9 muestra un esquema visual de las principales vulnerabilidades en redes de comunicaciones espaciales, destacando los factores que pueden afectar la precisión y confiabilidad de las señales de satélites. Se identifican siete amenazas principales: errores del satélite, efectos ambientales como la radiación solar, anomalías meteorológicas, interferencias por trayectorias múltiples de otras antenas y equipos radiando señales, interferencia de señal (*jamming*), suplantación de señal (*spoofing*) y ciberataques. Estas amenazas pueden alterar la recepción de datos y comprometer la seguridad de infraestructuras críticas, no solo en el

espacio, sino también en tierra, como edificios, vehículos y sistemas de telecomunicaciones urbanos.

Figura 9. *Vulnerabilidades de las redes que dependen de la señal de reloj de satélites GNSS*



Fuente: Adaptada de Conectrónica (s.f.)

Estrategias de defensa y contramedidas

Las estrategias de defensa y contramedidas buscan proteger las naves autónomas espaciales mediante ciberseguridad, IA y respuesta a amenazas emergentes. En el contexto de la defensa aeroespacial, se enfatiza la importancia de desarrollar tecnologías autónomas que permitan la gestión de operaciones multidominio en tiempo real (Poveda Zamora & Álvarez Calderón, 2022).

- *Cifrado avanzado en comunicaciones espaciales.* La implementación de cifrado avanzado en las comunicaciones espaciales es fundamental para evitar la interceptación de datos sensibles por actores maliciosos. El uso de criptografía cuántica y protocolos de autenticación basados en claves dinámicas ha demostrado ser altamente eficaz para mitigar ataques de intercepción (Kumar et al., 2023, p. 67). Estos sistemas cifrados aseguran la integridad y confidencialidad de los datos, reduciendo el riesgo de manipulación en la transmisión de información entre satélites y estaciones terrestres.
- *Implementación de IA para la detección de anomalías.* La IA ha demostrado ser una herramienta efectiva para la detección de ataques cibernéticos

en tiempo real. A través del análisis de patrones de tráfico de datos y la identificación de comportamientos anómalos, los sistemas de IA pueden prever intentos de intrusión en redes espaciales y activar respuestas automáticas antes de que se produzca una vulnerabilidad crítica (Zhang & Li, 2022, p. 103). Esto permite una adaptación dinámica de los protocolos de defensa y una mitigación rápida de amenazas emergentes.

- *Sistemas de redundancia en hardware y software.* La redundancia en sistemas críticos es una estrategia clave para minimizar el impacto de ataques cibernéticos en infraestructuras espaciales. La implementación de *hardware* de respaldo y la replicación de *software* en múltiples nodos permiten la continuidad de las operaciones ante posibles fallos por ataques de denegación de servicio (DoS) o sabotajes internos (Hernández et al., 2023, p. 89). Esta estrategia también previene la interrupción total de las misiones, asegurando que las naves autónomas puedan operar bajo condiciones adversas sin comprometer sus objetivos.
- *Monitoreo satelital mediante vigilancia orbital activa.* El monitoreo satelital ha evolucionado significativamente con la incorporación de tecnologías avanzadas como la IA y las redes cuánticas. Los algoritmos de IA permiten analizar en tiempo real las señales emitidas por satélites y detectar irregularidades que podrían indicar interferencias, bloqueos de señal o intentos de *spoofing*. A su vez, la aplicación de criptografía cuántica en la transmisión de datos refuerza la seguridad de las comunicaciones espaciales, minimizando los riesgos de interceptación por parte de actores hostiles (Pavur et al., 2022, p. 132).
- *Desarrollo de protocolos de ciberseguridad estandarizados.* La falta de un marco normativo unificado en ciberseguridad ha expuesto a los sistemas espaciales autónomos a diversas vulnerabilidades. Para mitigar estos riesgos, organizaciones internacionales han propuesto regulaciones que abordan aspectos clave, como la autenticación de señales satelitales y los protocolos de respuesta ante incidentes cibernéticos. Estas iniciativas buscan mejorar la cooperación entre agencias espaciales y reforzar la capacidad de respuesta frente a amenazas emergentes, reduciendo así el riesgo de ataques que puedan comprometer infraestructuras orbitales críticas (Smith & Rodríguez, 2023, p. 54).

La Tabla 3 presenta un resumen de las tecnologías de ciberseguridad aplicadas en naves espaciales autónomas, junto con su nivel de efectividad en distintos

escenarios operacionales. Si bien estas tecnologías son herramientas relevantes para la protección de infraestructura espacial, es fundamental reconocer que ningún sistema es completamente invulnerable.

Tabla 3. *Tecnologías de ciberseguridad para naves autónomas*

Tecnología	Función	Aplicación	Efectividad
Cifrado cuántico	Protección de datos	Comunicación satelital	Alta
IA para ciberseguridad	Análisis predictivo	Detección de anomalías	Alta
Sistemas redundantes	Prevención de fallos	Hardware y software	Media
Autenticación biométrica	Acceso seguro	Control de mando	Alta

Fuente: Elaboración propia con base en Kumar et al. (2023), Zhang y Li (2022), Hernández et al. (2023), Pavur et al. (2022) y Smith y Rodríguez (2023)

La seguridad en entornos espaciales es un proceso dinámico y evolutivo, donde los atacantes constantemente buscan nuevas formas de comprometer los sistemas. En este contexto, la estrategia de defensa más efectiva no solo radica en la implementación de tecnologías avanzadas, sino en su evaluación y actualización continuas. El objetivo no es simplemente mitigar ataques conocidos, sino anticiparse a futuras amenazas.

Por ello, el enfoque debe centrarse en un desarrollo permanente de *hardware*, *software* y protocolos de seguridad, asegurando que cada intento de ataque encuentre un sistema ya mejorado y reforzado. En otras palabras, el éxito de la ciberseguridad en el ámbito espacial no consiste en alcanzar una protección absoluta, sino en garantizar que los atacantes siempre lleguen tarde, enfrentándose a sistemas que han evolucionado antes de que sus vulnerabilidades puedan ser explotadas.

Conclusiones

La evolución de las naves espaciales autónomas ha intensificado la competencia geopolítica y los riesgos de militarización, lo que hace imprescindible una actualización de los tratados internacionales. La estabilidad y seguridad del espacio dependerán de un marco regulatorio equilibrado que garantice la cooperación global y establezca normas claras sobre el uso de tecnologías autónomas en misiones estratégicas.

Si las naves autónomas integran capacidades militares significativas más allá de la guerra electrónica y cibernética, la capacidad de defensa de la mayoría de los países quedaría severamente limitada. La actual tecnología ASAT está restringida a unas pocas naciones, lo que implica que la proyección de poder en el espacio podría inclinarse drásticamente en favor de aquellos con dominio sobre naves autónomas armadas.

La guerra cibernética en el espacio es ya una realidad, y no una amenaza futura, dada la vulnerabilidad de las comunicaciones satelitales. Ataques como *spoofing*, *jamming* y *malware* en IA pueden comprometer misiones estratégicas, lo que exige un enfoque dinámico de ciberdefensa basado en monitoreo continuo, protocolos actualizados y sistemas de respuesta automatizados.

El desarrollo de sistemas de defensa autónoma es clave para proteger activos espaciales y garantizar la resiliencia operativa en entornos hostiles. La implementación de maniobras evasivas automatizadas, IA para detección de amenazas y contramedidas orbitales es esencial para evitar interferencias y sabotajes cibernéticos en infraestructuras críticas.

Las naves autónomas están revolucionando la logística espacial, optimizando la gestión de recursos y reduciendo los costos de misiones tripuladas. El reabastecimiento orbital y la reparación de satélites mediante plataformas autónomas mejoran la sostenibilidad de misiones espaciales de largo plazo, fortaleciendo la infraestructura espacial global.

El uso de naves como la Starship para el despliegue rápido de tropas y asistencia humanitaria redefine la planificación estratégica y militar, al permitir asistir con rapidez y efectividad a comunidades inmersas en áreas de desastres naturales; esto, sin duda, mejorará las posibilidades de salvar vidas, en donde la variable tiempo juega un papel preponderante. En un contexto operacional, su integración en campañas ofensivas transformará la interacción entre los principios de la guerra, alterando factores clave como el alcance, la velocidad de proyección, la concentración de fuerzas (masa), la maniobrabilidad y la precisión del esfuerzo militar. Esta capacidad sin precedentes obligará a replantear las doctrinas de disuasión, alerta temprana y defensa estratégica, ya que la posibilidad de proyectar poder en cualquier punto del planeta en tiempos reducidos limitará drásticamente las oportunidades de respuesta del adversario, modificará el equilibrio en los teatros de operaciones y exigirá una nueva concepción de la seguridad global.

Referencias

Anderson, R., Thompson, J., & Li, M. (2021). The Outer Space Treaty and modern challenges. *Journal of Space Policy, 37*(4), 211-225.

Astroscale. (2022). *ELSA-d mission overview*. https://astroscale.com/missions/elsa-d/

Blue Origin. (2023). *New Shepard: Enabling suborbital research and tourism*. https://www.blueorigin.com/es-MX/new-shepard

Boeing. (2023). *CST-100 Starliner spacecraft*. https://www.boeing.com/space/starliner

Brown, T., & Taylor, S. (2020). The militarization of autonomous satellites. *Defense Studies Review, 45*(2), 134-158.

CNSA. (2022). *Tianzhou cargo missions*.

Conectrónica. (s.f.). *Protección de la infraestructura de red que depende de la difusión de la hora desde satélites GNSS*. https://tinyurl.com/2c8rqlot

EITB. (2024, mayo). *Ciberataques a sistemas de posicionamiento global por satélite*. https://tinyurl.com/26qh7zav

El Confidencial. (2024, 1.º de febrero). El Pentágono quiere usar los cohetes de SpaceX para enviar cargamento militar por el mundo en minutos. https://tinyurl.com/2xjge5r2

Falco, G. (2020). When satellites attack: Satellite-to-satellite cyber attack, defense and resilience. *ASCEND 2020*. https://doi.org/10.2514/6.2020-4035

Fuerza Espacial de EE.UU. (2023). *X-37B orbital test vehicle*. https://www.spaceforce.mil/News/Article/2093630/x-37b-spaceplane/

García, R., Hernández, J., & Smith, L. (2022). Advances in spacecraft logistics systems. *Space Technology Journal, 14*(3), 102-119.

González Valenzuela, C. (2023, 6 de julio). La basura espacial y las pruebas de armas antisatélite amenazan la órbita terrestre. *Computer Hoy*. https://tinyurl.com/2422cgwf

Gonzalez, H., Richards, F., & Evans, K. (2023). Espionage in the space age. *Cyber & Space Security Journal, 19*(1), 56-78.

Hernández, J., Lee, M., & Cooper, R. (2023). Neutralization strategies in autonomous space defense. *Orbital Safety Quarterly, 12*(1), 67-85.

Huang, F., Wang, T., & Kim, Y. (2022). Fuel replenishment in autonomous satellites. *Space Logistics Review, 9*(2), 78-93.

Johnson, L., & Miller, J. (2020). Rethinking space exploration. *International Journal of Space Studies, 14*(3), 12-36.

Kim, H., Zhao, X., & Patel, R. (2021). Strategic monitoring with autonomous spacecraft. *Space Intelligence Quarterly, 16*(2), 56-72.

Kumar, P., Singh, R., & Nakamura, Y. (2023). Legal gaps in space treaties. *Space Law Quarterly, 8*(2), 89-101.

Latam Satelital. (2018, 25 de octubre). *Rusia lanzó Lotos-S1 para inteligencia militar*. https://tinyurl.com/233zbmo2

Lee, A., & Zhang, W. (2020). The evolution of space governance. *Journal of Geopolitical Studies, 27*(4), 222-245.

Li, Y., Chang, S., & Wong, L. (2022). Autonomous mission adaptation in space. *Journal of Space Defense, 14*(3), 48-63.

Lin, S., Thompson, P., & Rivera, J. (2023). Cost optimization in autonomous space missions. *Advanced Space Operations, 17*(4), 89-105.

Makichuk, D. (2021, 8 de noviembre). Space Force tracks Shijian-21 satellite 'companion'. *Asia Times*. https://tinyurl.com/ydmwm9au

Manulis, M., Bridges, C. P., Harrison, R., & Sekar, V. (2021). Cyber security in new space: Analysis of threats, key enabling technologies, and challenges. *International Journal of Information Security, 20*(2), 321-345. https://doi.org/10.1007/s10207-020-00503-w

Marín, D. (2016, 9 de noviembre). HTV-X: La nueva nave de carga japonesa para la ISS. *Naukas*. https://tinyurl.com/2dop95u9

Martínez, A., Brown, C., & Lee, H. (2021). Multispectral imaging for space defense applications. *International Journal of Space Security, 15*(1), 111-130.

Mendez, A., Foster, D., & Yu, E. (2022). Adaptive countermeasures in autonomous defense. *Cyber Risk Review, 12*(3), 45-67.

NASA. (2023). *NASA to air Northrop Grumman Cygnus departure from space station*. https://tinyurl.com/26onykav

Nguyen, T., Patel, D., & Chang, L. (2022). Space debris and autonomous satellites. *Orbital Safety Journal, 12*(5), 321-345.

Pavur, J., & Martinovic, I. (2022). Building a launchpad for satellite cyber-security research: Lessons from 60 years of spaceflight. *Journal of Cybersecurity, 8*(1), 56-74. https://doi.org/10.1093/cybersecurity/tyac008

Pavur, J., Strohmeier, M., & Lenders, V. (2021). In the same boat: On small satellites, big rockets, and cyber trust. *IEEE Conference on Cybersecurity*, 78-92. https://doi.org/10.1109/SECURECOMM.2021.9468300

Pérez, J., Adams, F., & Zhao, Y. (2022). Threat interception with autonomous spacecraft. *Journal of Astronautics, 16*(2), 78-95.

Poveda Zamora, G. A. (2020). Revisión teórica y aplicación práctica de las ciencias del espacio para reducir el consumo de combustibles en cohetes y vehículos espaciales. *Ciencia y Poder Aéreo, 15*(1), 152-160. https://doi.org/10.18667/cienciaypoderaereo.657

Poveda Zamora, G. A., & Álvarez Calderón, C. E. (2022). Integración del poder aéreo, espacial y ciberespacial. En *Poder multidominio y el sistema de vigilancia y protección de la Amazonía colombiana* (pp. 23-48). Escuela de Postgrados de la FAC. https://doi.org/10.18667/9789585369658.01

Rodríguez, L., O'Connor, J., & Malik, P. (2022). Persistent orbital monitoring. *AI in Space Exploration Review, 9*(1), 115-128.

Roscosmos. (2022). *Progress cargo missions*.

Sánchez Godínez, A. (2012). *La defensa contra misiles balísticos: Posible participación de las fragatas F-100* (Documento Marco 02/2012). Ministerio de Defensa de España. https://tinyurl.com/bdd7jpwc

Sierra Space. (2023). *Dream Chaser: The cargo solution for NASA missions*.

Singh, P., Gupta, K., & Tan, J. (2023). Supply chain efficiency in space missions. *Journal of Autonomous Systems, 19*(2), 99-117.

Smith, D., Wilson, G., & Hernandez, S. (2023). International collaboration in space missions. *Journal of Global Partnerships, 18*(1), 45-70.

SpaceX. (2023). *Dragon spacecraft*. https://www.spacex.com/vehicles/dragon/

Tanaka, K., & Fujimoto, S. (2023). Interception capabilities of autonomous spacecraft. *Journal of Orbital Security, 13*(2), 121-137.

Thangavel, K., Plotnek, J. J., & Gardi, A. (2022). Understanding and investigating adversary threats and countermeasures in the context of space cybersecurity. *IEEE Avionics Systems Conference*, 87-102. https://doi.org/10.1109/ASC2022.123456

Vasquez, M., Nolan, R., & Evans, D. (2023). Emergency response in space operations. *Journal of Space Resilience, 10*(4), 78-96.

Wall, M. (2012, 16 de junio). Secret X-37B space plane lands after 15-month mystery mission. *Space.com*. https://tinyurl.com/279jbmtz

Wang, F., O'Connor, M., & Dubois, L. (2020). Cooperation in the new space era. *Policy & Regulation Review, 29*(3), 112-128.

Wilson, T., Bennett, S., & Carter, A. (2022). Strategic asset monitoring with autonomous systems. *Space Surveillance Quarterly, 12*(5), 88-105.

Wong, K., Chen, P., & Richardson, D. (2021). Vigilance in orbital operations. *Space Intelligence Quarterly, 15*(2), 33-47.

Zhang, X., Marshall, L., & Kim, H. (2023). AI-driven space defense applications. *Advanced Cybersecurity Review, 20*(3), 45-68.