CENTRO DE ESTUDIOS ESTRATÉGICOS Y AEROESPACIALES

BOLETÍN INFORMATIVO Y DE ANÁLISIS N° 13 / 2025
Santiago, 06 de mayo de 2025

CIBERATAQUES A SATÉLITES

Por Álvaro Aguirre. 10 Min. de lectura

El espacio es una parte vital de las actividades de los seres humanos y de los países que lo han utilizado para fines de comunicación, monitoreo del medio ambiente, recopilación de inteligencia, realización de experimentos científicos vitales y suministro de datos para el posicionamiento global, la navegación y el cronometraje.

Asimismo, los países dependen cada vez más de las capacidades mundiales de los satélites para las infraestructuras nacionales e internacionales, que incluyen los sistemas que rigen la navegación de aeronaves, barcos, vehículos terrestres y sistemas de armas, las maniobras de las fuerzas armadas, las transacciones financieras, Internet y las telecomunicaciones.

La arquitectura basada en el espacio es fundamental para el suministro de datos y servicios en lo que genera una dependencia crítica del espacio, que da lugar a nuevos riesgos cibernéticos que afectan de manera significativa al desarrollo de las diferentes actividades que son soportadas por la información entregada por los satélites.

Los ciberataques a satélites son intentos de comprometer la seguridad y funcionalidad de estos dispositivos mediante técnicas digitales. Estos ataques pueden tener consecuencias graves, como interrupciones en las comunicaciones, errores en la navegación, impacto en servicios financieros y riesgos para la seguridad nacional.

Todos los satélites dependen de la tecnología cibernética, incluidos el software, el hardware y otros componentes digitales. Cualquier amenaza al sistema de control de un satélite o al ancho de banda disponible plantea un desafío directo a los activos críticos nacionales.

Principales amenazas cibernéticas para satélites.

Los satélites están expuestos a múltiples formas de ciberataques, desde interferencias hasta la toma de control total de los sistemas de gestión. Las técnicas más comunes utilizadas por los hackers incluyen:

- Spoofing.
  Este ataque implica suplantar la identidad de un satélite, alterando las señales y datos que transmite. Esto puede causar errores en los sistemas de navegación y comunicaciones, comprometiendo servicios críticos como el GPS.
- Jamming.
  La interferencia deliberada de señales satelitales puede interrumpir su funcionamiento, afectando a servicios dependientes de estas señales, como las telecomunicaciones y los sistemas de posicionamiento global.
- Ataques a Software.
  Los hackers pueden explotar vulnerabilidades en el software de los satélites o de las estaciones terrestres para tomar control de las operaciones.
  Un atacante podría desviar un satélite, interferir en sus comunicaciones o desactivar sistemas esenciales.
- Ataques de Denegación de Servicio (DoS).
  Los satélites pueden ser inundados con solicitudes falsas, lo que los sobrecarga y los deja temporalmente inoperativos. Esto puede causar fallos en las comunicaciones o la incapacidad para controlar los dispositivos en órbita.

Consecuencias de los ciberataques a satélites.

Los ciberataques dirigidos a satélites tienen repercusiones potencialmente devastadoras. No solo afectan las comunicaciones y la navegación, sino que

también pueden poner en riesgo la seguridad nacional y la economía global. Algunas de las principales consecuencias incluyen:

- Interrupción de comunicaciones globales.

  Muchos de los sistemas de telecomunicaciones globales dependen de satélites, y un ataque exitoso puede dejar sin servicio a millones de usuarios de telefonía, televisión e internet. Esto puede causar interrupciones generalizadas en las actividades comerciales y cotidianas.

- Fallos en la navegación y el transporte.

  Los sistemas GPS, fundamentales para la aviación, el transporte terrestre y marítimo, pueden ser gravemente afectados por ataques de spoofing o jamming. Esto puede provocar accidentes, desvíos o incluso retrasos significativos en la logística global.

- Compromiso de la seguridad nacional.

  Los satélites son vitales para las capacidades de defensa y vigilancia de los países. Un ataque cibernético podría comprometer la capacidad de un país para detectar amenazas en tiempo real o coordinar acciones militares.

Últimos ataques a satélites (2020-2024).

- Ciberataque a la red satelital de Viasat (2022).
  Uno de los incidentes más graves ocurrió en marzo de 2022, cuando un ataque cibernético dirigido contra la red satelital KA-SAT de Viasat, una empresa de comunicaciones por satélite, interrumpió las comunicaciones en Europa, afectando a decenas de miles de usuarios. El ataque coincidió con la invasión rusa de Ucrania y tenía como objetivo desestabilizar las comunicaciones del gobierno ucraniano. Los ciberatacantes utilizaron técnicas de sabotaje para interrumpir los módems conectados a la red satelital. El impacto fue tan profundo que algunos terminales quedaron completamente inservibles.

- Spoofing en GPS: Ataques a buques (2020).
  En 2020, se detectaron varios incidentes de spoofing en señales GPS que afectaron a buques en las costas de China y el Mar Negro. Estos ataques alteraron las ubicaciones mostradas en los sistemas de navegación, poniendo en peligro a embarcaciones comerciales. Los atacantes lograron enviar señales falsas a los receptores GPS, desviando a las embarcaciones de su curso sin que los operadores se dieran cuenta. Estos incidentes subrayaron el riesgo creciente para los satélites de navegación y la urgencia de mejorar la ciberseguridad en el espacio.

- Hackeo a satélites comerciales en India (2021).
  En 2021, un grupo de hackers conocidos como "DragonFly" lanzó un ataque contra satélites comerciales utilizados por India para servicios de comunicación. Aunque, el ataque no tuvo éxito en tomar control total de los satélites, los hackers lograron penetrar en las redes terrestres, destacando la vulnerabilidad de las estaciones de control en tierra y la posibilidad de futuros ataques más devastadores.

- Ataque de DoS a sistemas de vigilancia espacial de EE. UU. (2023).
  En mayo de 2023, un ataque de denegación de servicio (DoS) dirigido a los sistemas de vigilancia espacial del Comando Espacial de EE. UU. interrumpió temporalmente las operaciones de monitoreo de satélites.
  Este incidente subrayó la importancia de proteger tanto los activos en órbita como las infraestructuras terrestres críticas.
  El ataque, aunque temporal, creó preocupaciones sobre la seguridad nacional y la capacidad de monitorear el espacio en tiempo real.

Estrategias de defensa en ciberseguridad espacial.

Para proteger los satélites de estas crecientes amenazas, la ciberseguridad espacial ha desarrollado una serie de técnicas avanzadas:

- Cifrado de comunicaciones robusto.
  La información transmitida y almacenada en los satélites se protege mediante algoritmos de cifrados avanzados, dificultando el acceso no autorizado.
- Sistema de Detección de intrusiones.
  Se implementan sistemas de monitoreo continuo para detectar y responder rápidamente a cualquier actividad sospechosa en los satélites.
- Aislamiento de redes.
  La separación de las redes satelitales de otras redes reduce el riesgo de propagación de malware y otros ataques cibernéticos.
- Actualizaciones de software continuas.
  Se mantienen actualizados los sistemas operativos y aplicaciones de los satélites, corrigiendo vulnerabilidades antes de que puedan ser explotadas.
- Capacitación del personal.
  Se forma continuamente al personal que opera los satélites en las mejores prácticas de ciberseguridad, asegurando una defensa proactiva.

- Inteligencia Artificial (IA).
  La IA se utiliza para analizar grandes volúmenes de datos en busca de patrones de amenazas, mejorando la capacidad de respuesta ante ataques emergentes.

Casi todos los conflictos bélicos modernos dependen de la información que entrega los satélites, por lo que las vulnerabilidades cibernéticas socavan la confianza en el rendimiento de los sistemas estratégicos, aumentando la incertidumbre en la información y el análisis, afectando la credibilidad de la disuasión y la estabilidad estratégica.

Además, la pérdida de confianza en la tecnología, también tiene implicaciones para determinar la fuente de un ataque malicioso (atribución), el cálculo estratégico en la toma de decisiones en crisis y puede aumentar el riesgo de percepción errónea.

El funcionamiento de todos los satélites depende de la tecnología cibernética, incluidos los programas informáticos, el hardware y otros componentes digitales, y cualquier amenaza que pudiera afectar los controles, la confiabilidad o la disponibilidad de ancho de banda de un satélite, plantearía un desafío directo a los activos críticos nacionales.

Si las ciberamenazas no se abordan de manera eficaz, las vulnerabilidades en la infraestructura estratégica podrían tener graves consecuencias para la seguridad, ya que las vulnerabilidades cibernéticas golpean el corazón de las tecnologías claves en todos los ámbitos.

Los sistemas militares estratégicos dependen en gran medida de los activos espaciales para la navegación y la selección de objetivos, la sincronización, el posicionamiento, el mando y el control, la supervisión operativa, la recopilación de inteligencia y el reconocimiento, entre otras funciones. Sin embargo, la creciente vulnerabilidad de los bienes basados en el espacio, las estaciones terrestres, los sistemas de mando y control conexos y el personal que gestiona los sistemas aún no ha recibido la atención que merece.

Invertir en medidas de mitigación y en la resiliencia de los sistemas espaciales para los diferentes fines ya sean civiles o militares, son clave para lograr la protección en todos los ámbitos.

AAW, información de fuentes abiertas, internet, Cybersecurity of NATO's Space-based Strategic Assets | Chatham House – International Affairs Think Tank.