

Artículo Nº 08/2026 LA NAVEGACIÓN AÉREA EN CONFLICTO



*Por Victor Villalobos Collao. Director de Asuntos Aeronáuticos.
12 de junio de 2026. 10 Min. Lectura.*



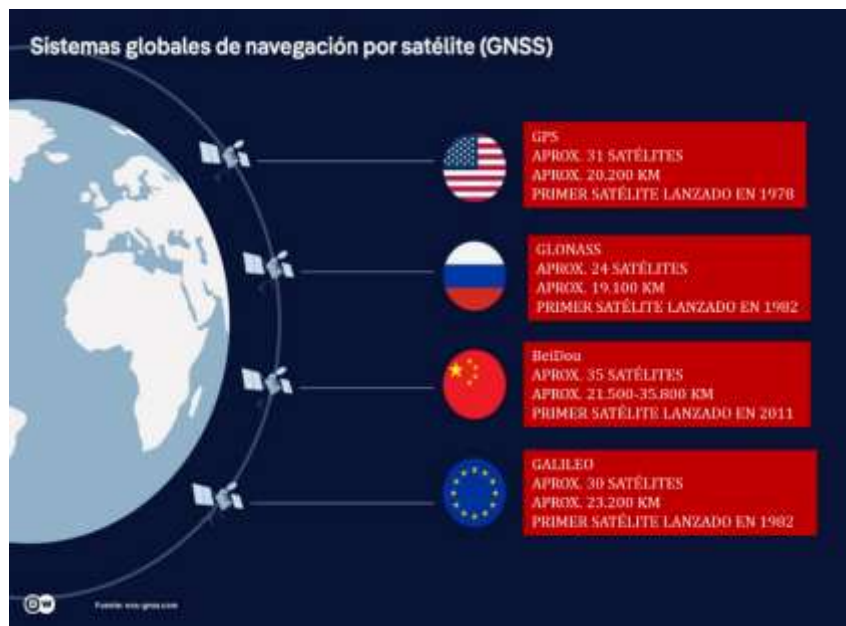
La "guerra invisible del GPS", es un conflicto geopolítico y tecnológico basado en la guerra electrónica para bloquear o falsear las señales satelitales. Su objetivo principal es desarmar la precisión de drones, misiles y tropas enemigas, pero está provocando graves efectos colaterales en la seguridad de la aviación comercial y el transporte marítimo mundial.

Son cuatro las potencias que participan en la navegación global: EE. UU., Rusia, Europa y China. Los dos primeros proporcionan sistemas globales de navegación, los cuales se desarrollaron en la década de 1970, durante la Guerra Fría entre Estados Unidos y la entonces Unión Soviética.

Los Estados Unidos desarrolló el GPS, que se convirtió en la primera red de navegación satelital con cobertura global completa. A la fecha es el sistema más utilizado del mundo.

Al mismo tiempo, la Unión Soviética desarrolló el sistema GLONASS. Más tarde, a comienzos de los años 2000, la Unión Europea decidió que confiar exclusivamente en el GPS la hacía demasiado dependiente de la infraestructura estratégica estadounidense, y comenzó a desarrollar el sistema Galileo.

El sistema chino BeiDou (<https://fach.mil.cl/ceea/documentos/articulos/a7-BEIDOU.pdf>) es el más reciente de los cuatro. Al igual que en Europa, los planificadores militares chinos buscaban reducir su dependencia del GPS estadounidense.



Los diferentes sistemas de navegación por satélite.

Las dos tácticas principales utilizadas.

Los actores estatales utilizan antenas terrestres de alta potencia para manipular el espectro de radiofrecuencias a través de dos métodos:

- Jamming (Bloqueo): Emisión de ruido en la misma frecuencia del GPS. Consiste en saturar el receptor para que pierda la señal por completo. Deja a los sistemas de navegación totalmente a ciegas.
- Spoofing (Suplantación): Envío de señales falsas pero realistas. Engaña al receptor haciéndole creer que está en otra ubicación o huso horario. Es la táctica más peligrosa porque los sistemas automáticos no detectan el engaño de inmediato.

La suplantación GNSS implica la generación y transmisión deliberada de señales GNSS falsas. Estas señales imitan las señales GNSS reales, pero están diseñadas para ser ligeramente más fuertes y abrumar gradualmente las señales reales recibidas por el dispositivo objetivo.

El objetivo es engañar al dispositivo objetivo para que acepte las señales falsas como legítimas, dando como resultado datos de posición o de tiempo falsos.

A diferencia de la interferencia, en la que simplemente se interfieren las señales GNSS, la suplantación es una forma de ataque más sofisticada. Requiere un conocimiento exhaustivo del sistema y de su estructura de señales. Los suplantadores deben generar señales que no sólo sean similares en

estructura a las señales GNSS reales, sino que además estén sincronizadas con precisión para mezclarse perfectamente con ellas. Esta complejidad requiere hardware y software avanzados, así como conocimientos técnicos sobre la tecnología GNSS.

Los riesgos de la falsificación son significativos. Pueden engañar a los sistemas de navegación, alterar los sellos de tiempo en las transacciones financieras o interrumpir infraestructuras críticas que dependen de datos precisos de tiempo y localización. Reconocer y mitigar los ataques de suplantación es, por tanto, de gran importancia para la seguridad y la fiabilidad de los sistemas que dependen de los datos GNSS.

El alcance total de estos efectos secundarios y en cascada sigue siendo incierto, lo que subraya la necesidad de una mayor vigilancia operativa y una toma de decisiones conservadora siempre que se sospeche de anomalías en el GNSS.

Notificar sin demora las sospechas de interferencias en el GNSS al control aéreo y a los sistemas internos de notificación de seguridad. Y realizar un reinicio en tierra después de cada vuelo en el que se sospeche que ha habido interferencias de radiofrecuencia, borrando todas las señales GNSS corruptas de todos los sistemas de la aeronave.

Dado que las señales de los satélites llegan a la Tierra con una potencia relativamente baja, un transmisor terrestre puede emitir señales falsas de mayor intensidad que sean captadas por los sistemas de navegación, incluidos los de las aeronaves. Por ello, la suplantación de señales (*spoofing*) suele ser utilizada principalmente por fuerzas armadas que buscan reducir la precisión de las armas enemigas que dependen del GPS para su navegación, como misiles de largo alcance y drones de pequeño tamaño. Para ello, muchas fuerzas militares cuentan con unidades especializadas encargadas de desarrollar y operar estos transmisores, ya sea desde instalaciones fijas o mediante plataformas móviles montadas en vehículos.

Para hacer frente a la guerra electrónica, la industria de la aviación y las agencias de defensa implementan tanto tecnologías de blindaje en los aviones actuales como sistemas de navegación alternativa (APNT) que prescinden por completo de los satélites.

Zonas rojas del conflicto.

Este fenómeno se concentra en regiones con tensiones militares activas y se extiende a lo largo de miles de kilómetros:

- El Mar Báltico: Epicentro global de las interferencias. Afecta gravemente a Polonia, Suecia y los países bálticos debido a emisores en el enclave ruso de Kaliningrado.
- Medio Oriente: El conflicto entre Israel, Irán y otras potencias regionales mantiene bajo constante estrés al Golfo Pérsico y el espacio aéreo contiguo.
- Frontera de Ucrania: Toda la periferia del conflicto armado sufre alteraciones masivas para neutralizar ataques con drones.



Mapa actividad aérea en la zona del mar Báltico. Captura de pantalla del monitor Flightradar24.com

Impacto en el transporte civil comercial.

La Federación Internacional de Asociaciones de Pilotos de Líneas Aéreas (IFALPA por sus siglas en inglés) ha denunciado un importante aumento de “los incidentes de interferencia de radiofrecuencia, es decir, interferencias y suplantaciones intencionadas que degradan o manipulan la información de posición, navegación y sincronización basada en satélites”

Estas interferencias se producen sin aviso, en todo el mundo “con un inicio, una duración y un alcance impredecibles. Además, se ha observado que cada vez son más los sistemas aeronáuticos y terrestres afectados, incluidos sistemas que antes no se consideraban dependientes del GNSS”, alertan, además de recordar que “suponen un riesgo para la seguridad”.

Destacan que: “Estos impactos desconocidos y emergentes aumentan la preocupación de que las interferencias de radiofrecuencia puedan propagarse a través de interacciones complejas e insuficientemente documentadas dentro del sistema”.

Hasta ahora estos problemas de interferencias y suplantación de señales se daban en zonas bastante concretas, y muchos pilotos ya sabían de este problema y cómo asegurar la navegación de la aeronave utilizando otros equipos sin depender de las señales procedentes de los satélites de los diferentes sistemas de navegación existentes.



Desde IFALPA señalan como sistemas y equipos que pueden verse afectados al depender de estas señales para su correcto funcionamiento, así como qué puede ocurrirles. Estos son:

- El sistema de gestión de vuelo (FMS por sus siglas en inglés) y sistemas de referencia inercial (IRS): Los datos GNSS erróneos o perdidos pueden desviar la navegación o anular sensores más robustos.
- La funcionalidad del receptor ILS puede verse afectada, lo que degrada la capacidad de aproximación.
- El sistema de alerta y reconocimiento del terreno (TAWS) y sistema de alerta y reconocimiento de salida de pista (ROAAS): Alertas falsas o señales de terreno/aterrizaje degradadas.
- Las interferencias de radiofrecuencia en el GNSS, en particular el ‘spoofing’, también pueden dar lugar a entradas erróneas en las funciones de vigilancia y seguimiento del sistema de prevención de colisiones en el aire (ACAS/TCAS), ya que estos sistemas se basan en la posición precisa de la propia aeronave y de los intrusos y utilizan funciones de prueba internas que pueden inutilizar el sistema en determinadas condiciones de interferencias.
- El radar meteorológico puede verse afectado por las interferencias de radiofrecuencia.
- Los sistemas de vigilancia dependiente automática (ADS-B/ADS-C), y de comunicaciones CPDLC, pueden transmitir transmisiones de posición incorrectas o perdidas que afectan al control aéreo y al conocimiento del tráfico.
- Y además, las entradas de sincronización del sistema y los problemas de sincronización pueden afectar a la aviónica, las comunicaciones y la coordinación con los sistemas terrestres.
- Ahora también, según se ha detectado “las interferencias de radiofrecuencia del GNSS, también, pueden afectar a otras aeronaves, sistemas terrestres o de apoyo a través de mecanismos que aún no se comprenden del todo ni se han documentado formalmente.

Casos Mediáticos.

Caso 1.

Uno de los casos más mediáticos de posibles interferencias fue el del avión en el que volaba Ursula Von der Leyen, el 31 de agosto de 2025.



En efecto, este fue un episodio de gran repercusión. El avión en el que viajaba la presidenta de la Comisión Europea, Ursula von der Leyen, sufrió una grave interferencia en su sistema de navegación por satélite (GPS) mientras volaba sobre Bulgaria.

El incidente ocurrió cuando la aeronave se aproximaba al aeropuerto de Plovdiv, en Bulgaria. De repente, los sistemas electrónicos de navegación fallaron y el GPS de toda la zona quedó inoperante. Ante la emergencia y tras sobrevolar la terminal durante un tiempo, el piloto tuvo que realizar el aterrizaje de forma manual, utilizando mapas analógicos en papel.

La Comisión Europea y las autoridades de inteligencia apuntaron a una presunta guerra electrónica orquestada por Rusia. Esta zona del este de Europa ha registrado un aumento masivo de bloqueos (jamming) y suplantaciones de señales (spoofing) desde 2022.

Caso 2.

Durante tres horas, el avión en el que viajaba el jueves 21 de mayo, el ministro de Defensa británico, John Healey, fue blanco de un masivo ataque de guerra electrónica. El GPS dejó de funcionar. Los dispositivos electrónicos no se conectaron a Internet. El tablero de instrumentos registró fallas. El piloto del avión tuvo que dirigir el vuelo por navegación inercial, como se hacía hace varias décadas. El hecho se produjo cuando el avión sobrevolaba Estonia, cerca de la frontera con Rusia. Según los datos de vuelo examinados por el servicio global de la BBC, el transpondedor del avión comenzó de repente a indicar que se encontraba en pleno territorio ruso, a 300 kilómetros de donde había estado segundos antes. Supuestamente volaba a solo 11 kilómetros sobre un lago cerca de San Petersburgo. Nada de esto era real. El sistema de navegación del avión se confundió debido a una suplantación de GPS.

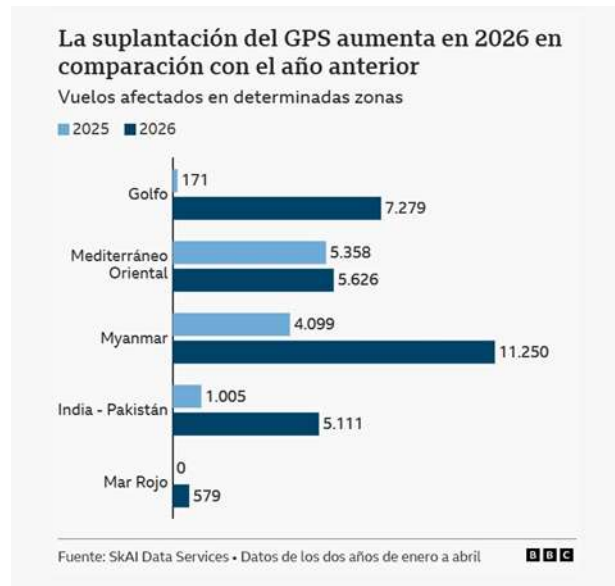
No fue un accidente, sino un ataque de guerra electrónica. Así lo cree el Gobierno británico, que ha calificado la acción de "temeraria", y la ha atribuido a Rusia, un país con un amplio historial de interferencias en los espacios aéreos de sus vecinos del Oeste, incluyendo a las Repúblicas Bálticas - de las que Estonia forma parte- y Polonia.



Secretario de Defensa del Reino Unido, John Healey

Resumen de casos.

Los datos compartidos con la BBC por la consultora de aviación SkAI Data Services muestran que más de 100 aviones de pasajeros transmitían ubicaciones incorrectas como consecuencia de la suplantación.



Los mismos datos indican que la suplantación y el bloqueo, están cada vez más extendidos en áreas cercanas a zonas de guerra o donde hay mucha actividad militar, como la región del Báltico, el Golfo, el Mar Rojo, India y Pakistán, y los alrededores de Myanmar.

En el Golfo, por ejemplo, se produjo un aumento de los vuelos que notificaron suplantación de GPS tras el inicio de la guerra de Estados Unidos e Israel contra Irán el 28 de febrero.

En el mes de enero se informaron 14 casos, en febrero 99 casos y en marzo, 5.381 vuelos notificaron suplantación, según SkAI Data Services.

Los casos en la región del Báltico se dispararon de 17.243 en 2024 a 59.447 en 2025, según muestran las cifras de SkAI Data Services.

Este incremento coincide con el uso creciente de ataques con drones en la guerra entre Rusia y Ucrania.

Otras rutas aéreas muy transitadas de Europa, Medio Oriente y Asia también han sufrido suplantaciones o interferencias, con una media de más de 800 vuelos afectados al día en todo el mundo este año.

Protección inmediata: ¿Cómo se defienden los aviones actuales?

Las aerolíneas y los fabricantes modifican el hardware y el software a bordo para filtrar y desacreditar las señales falsas:

- Antenas CRPA (Controlled Reception Pattern Antennas): Son antenas inteligentes compuestas por múltiples receptores. Cuando detectan una señal de *jamming* o *spoofing*, "apagan" digitalmente la

recepción en esa dirección específica para ignorar el ataque y mantener el enlace con los satélites legítimos.

- **Receptores Multifrecuencia y Multiconstelación:** Los aviones modernos ya no dependen solo del GPS estadounidense. Validan la posición cruzando datos en tiempo real con Galileo (Europa), GLONASS (Rusia) y BeiDou (China), usando bandas de frecuencia distintas. Si una frecuencia muestra anomalías de potencia, el sistema la descarta.
- **Filtros por algoritmos criptográficos:** Se aplican sistemas de autenticación de señal (como los desarrollados para la red europea Galileo). El software del avión exige una "firma digital" cifrada del satélite; si los datos carecen de ella o la hora de llegada no concuerda de forma exacta, la señal se bloquea por considerarse *spoofing*.

El futuro: Tecnologías de navegación sin satélites.

Para romper la dependencia absoluta del espacio, se despliegan arquitecturas como el *HANA (Alternative Navigation Architecture)* de empresas líderes como Honeywell. Estas tecnologías utilizan el propio entorno físico terrestre y espacial:

Tecnología	¿Cómo funciona?	Estado actual
Sistemas Inerciales (INS)	Usan giroscopios y acelerómetros internos para calcular la posición según el movimiento físico del avión desde el despegue, completamente aislados del exterior.	Principal respaldo actual en vuelos comerciales.
Navegación Cuántica (Quantum INS)	Evolución del INS que utiliza átomos ultrafríos para medir el movimiento físico. Reduce a cero el margen de error por desviación que afecta a los sistemas inerciales tradicionales.	En fase avanzada de pruebas militares y laboratorios aeroespaciales.
Navegación Magnética (MagNav)	Sensores miden las anomalías del campo magnético de la Tierra. Una Inteligencia Artificial compara la lectura con un mapa magnético global (como una huella dactilar del terreno).	Probado con éxito por la Fuerza Aérea de EE. UU. mediante soluciones de firmas como Sandbox AQ.
Navegación Óptica y Estelar	Cámaras de alta definición escanean el terreno (comparándolo con mapas digitales) o rastrean la posición de las estrellas de día y de noche.	Integrado en drones avanzados y bombarderos estratégicos.

El blindaje contra la guerra electrónica está transformando los costos de la aviación comercial, generando un impacto financiero inmediato en combustible y desvíos, además de una millonaria inversión obligatoria a largo plazo para actualizar las flotas de las aerolíneas.

El impacto económico se divide en pérdidas operativas del día a día y costos de capital para implementar la nueva tecnología.

1. Costos operativos inmediatos.

Cuando un avión comercial sufre *spoofing* o *jamming*, la pérdida de rutas optimizadas por satélite destruye la eficiencia del vuelo:

- Aumento en el consumo de combustible: Al perder la guía satelital exacta, las aeronaves deben recurrir a rutas e instrucciones tradicionales de control de tráfico aéreo más largas. El consumo de combustible puede incrementarse hasta en un 25%.
- El costo por trayecto: En rutas de larga distancia (como un vuelo trasatlántico en un Boeing 777), este desvío de ruta representa más de 9.000 kg (20.000 lbs) extras de combustible, lo que equivale a un gasto adicional superior a los \$15.000 USD por vuelo afectado.
- Desvíos imprevistos: Si un avión no carga combustible extra suficiente para mitigar estas ineficiencias o si los sistemas de aterrizaje instrumental basados en GPS fallan en aeropuertos con mal clima, el avión debe desviarse a un aeropuerto alternativo. Cada desvío cuesta a la aerolínea más de \$100.000 USD entre tasas, logística y compensación a pasajeros.

2. El costo del blindaje (Inversión en Hardware).

Modificar aeronaves civiles que originalmente no fueron diseñadas para resistir ataques de guerra electrónica militar exige inversiones masivas:

- Instalación de Antenas Inteligentes (CRPA): Las antenas de recepción controlada (anti-bloqueo) de nivel premium aptas para la aviación cuestan entre \$6.000 y \$15.000 USD por unidad solo en hardware.
- Mano de obra y certificación: La instalación de aviónica en aviación comercial es altamente compleja. El costo de cableado, la perforación del fuselaje y las rigurosas certificaciones de seguridad aérea suelen sumar entre \$5.000 y \$10.000 USD adicionales por avión en mano de obra. Un kit completo de actualización de protección satelital puede superar fácilmente los \$25.000 USD por aeronave.
- Integración de sistemas alternativos: Configurar sistemas de respaldo con Inteligencia Artificial (como el mapeo magnético *MagNav* o nuevos sensores inerciales avanzados) requiere renovar los ordenadores de vuelo primarios, un negocio que está disparando el valor de mercado de los proveedores aeroespaciales.

Comparativa de Costos: ¿Es rentable blindar la flota?

Los analistas del sector estiman que la inacción es exponencialmente más cara que la prevención:

Concepto	Costo de Mitigación (Blindaje)	Costo de la Inacción (Sufrir ataques)
Inversión por Avión	~\$25.000 USD (Antenas CRPA e instalación).	\$0 USD en el taller.
Impacto por Vuelo Afectado	Mínimo. El avión ignora la interferencia y mantiene la ruta óptima.	+\$15.000 USD en combustible extra por trayecto.
Riesgo de Cancelación/Crisis	Bajo. Continuidad total del servicio.	+\$100.000 USD por desvío. Caos logístico en aeropuertos principales.

El balance final.

Debido a que los incidentes globales de interferencia aérea han escalado de unos 300 vuelos diarios a más de 1.500 vuelos diarios, el costo de las cancelaciones, retrasos y desvíos acumulados en un solo día en un nodo aeroportuario clave (como Frankfurt o Londres), ya supera el valor total de actualizar tecnológicamente la flota entera de una aerolínea. Por ello, el blindaje pasó de ser un gasto militar a una prioridad de supervivencia financiera comercial.

Medidas o Recomendaciones.

Ante ello, la Federación Internacional de Asociaciones de Pilotos de Líneas Aéreas, recomienda una serie de medidas inmediatas, algunas de las cuales ya se adoptan en muchos casos.

Informar a las tripulaciones de vuelo y a los equipos de operaciones sobre los riesgos de interferencias de radiofrecuencia y 'spoofing'.

Informar a las tripulaciones de vuelo y a los equipos de operaciones sobre los procedimientos operativos estándar para mitigar las interferencias de radiofrecuencia.

Aclarar la descripción de los sistemas técnicos disponibles para las tripulaciones de vuelo con el fin de facilitar la comprensión del uso de las señales GNSS en los distintos sistemas de la aeronave que puedan verse afectados por las interferencias de radiofrecuencia.

Planificar las rutas para minimizar la exposición a regiones conocidas de alto riesgo de interferencias de radiofrecuencia siempre que sea posible.

Garantizar que se disponga de procedimientos de navegación alternativos, actualizados y documentados.

Garantizar que la formación periódica de la tripulación de vuelo esté actualizada y cubra los efectos conocidos y las medidas necesarias.

Mantener las ayudas de radionavegación convencionales (VOR, DME, ILS) como medida de redundancia.



Bibliografía:

- Información de fuentes abiertas, internet, Global, BBC, Aerospace, Spacenews, Spirent, International finance, Flynews.