Hasta el momento no se han notificado accidentes, pero sí problemas en vuelo:

Preocupación por incremento de ataques con señales de GPS falsas que afectan a aviones

Desde abril se pasó de una docena de reportes de aeronaves interferidas al día a más de 1.000. Las zonas perjudicadas son cercanas a un conflicto bélico, como el Medio Oriente o la frontera rusa, entre otras.

ALEXIS IBARRA O.

En el mundo de la aviación hay preocupación tras el incremento de un peligroso ataque cibernético que afecta a la aeronavegación de aviones. Se trata de la suplantación de GPS o *GPS Spoofing*, en inglés.

"Es una técnica que permite interferir en las señales que reciben los sistemas de navegación y poner en riesgo la seguridad de vuelo", resume Osvaldo Bahamondes, jefe de capacitación, extensión y posgrado del departamento de Aeronáutica de la U. Técnica Federico Santa María.

Esta forma de ataque "consiste en manipular las señales GPS para que los receptores abordo reciban señales erróneas, las que interpretan como que se encuentran en lugares geográficos distintos y alejados de la ubicación que efectivamente están sobrevolando. Esto se hace mediante la transmisión de señales falsas que simulan provenir de los satélites GPS legítimos", explica Bahamondes.

El OPS Group —una comunidad internacional de pilotos, controladores de vuelo y otros profesionales de la aviación— ha reportado un alarmante incremento de este tipo de interferencias a la aviación.

En un informe dado a conocer hace pocas semanas, se detalla que durante este año se experimentó un alza de 500%, reportándose en algunos momentos cerca de 1.500 casos diarios en el mundo. Ellos se concentran en zonas afectadas por conflicto bélico, como Oriente Medio y la frontera rusa.

El sitio SkAI-data-services.com —creado con el apoyo del Centro de Aviación de la U. de Ciencias Aplicadas de Zúrich— lleva un registro en tiempo real tanto de la suplantación como de la interferencia de GPS o *jamming* (ver infografía y recuadro).

"El aumento más significativo comenzó en abril, cuando el número de aeronaves afectadas se incrementó de docenas por día hasta llegar a 2.000 en mayo. Actualmente, estamos viendo cerca de 1.000 aeronaves afectadas diariamente, y las cifras se han mantenido estables desde este verano boreal", dice a "El Mercurio", Benoit Figuet, cofundador de SkAI Data Services.

"Los ataques GPS representan una amenaza importante para la seguridad de la aviación. También tienen un impacto en la eficiencia operativa, los pilotos deben confiar en otros sistemas de navegación que no son tan precisos como el GPS y, por lo tanto, deben volar de manera menos eficiente", añade.

Forbes dio el ejemplo de un Bombardier Challenger 604 (avión de negocios de tamaño medio) con destino a Qatar que fue afectado por suplantación avanzada de GPS al norte de Bagdad. El sistema de navegación les decía que se habían desviado de su rumbo por cerca de 150 kilómetros y el Sistema de Gestión de Datos de Vuelo daba datos erróneos. Los pilotos se vieron obligados a contactar al centro de control de tránsito aéreo para consultar su posición y recibir nuevas indicaciones de rumbo.

"Es difícil identificar a los responsables, pero generalmente se trata de grupos con conocimientos avanzados en telecomunicaciones y ciberseguridad", agrega Palacios.

"Si uno ve los reportes, se da cuenta de que estos ataques están concentrados en zonas del mundo donde hay conflictos bélicos", apunta Hugo Durney, doctor en Teoría de Señal y Telecomunicaciones y académico de la U. Tecnológica Metropolitana. Allí se les usa con fines militares, por ejemplo, para alterar los sistemas de navegación automatizados de drones y misiles.

Hasta el momento no se han reportado accidentes causados por este ataque. "Los aviones afectados logran corregir su trayectoria sin causar incidentes graves, gracias a la intervención de los controladores aéreos. Sin embargo, el riesgo de accidentes aumenta si los ataques se hacen más sofisticados, con potencial de causar desviaciones peligrosas en vuelos comerciales", dice J. Alberto Palacios, CEO de Globalsat Group.

Durney agrega que los sistemas de control de trayectoria y posición de los aviones no son tan fáciles de engañar. "Usan otros sistemas adicionales e independientes a los GNSS (Sistema global de navegación por satélite, por sus siglas en inglés) para controlar las trayectorias de rutas aéreas y la radio ayuda para las maniobras de aterrizaje". Estos sistemas son el VOR —una antena en tierra que emite señales para la navegación aérea por instrumentos— y el ILS (Sistema de aterrizaje instrumental).

También en barcos

Durney agrega que el *spoofing* no solo afecta a aeronaves sino también a navíos.

"En el ámbito marítimo el *spoofing* podría usarse para terrorismo, por ejemplo, para que un crucero en una zona de poca visibilidad sea llevado a aguas que no son seguras", dice Marco Arellano, académico de la carrera de Ingeniería en Marina Mercante, en UNAB Concepción.

Arellano agrega que los barcos mercantes y, con mayor razón los de guerra, tienen múltiples sistemas de navegación. "De hecho, nosotros entrenamos a nuestros alumnos simulando errores en el GPS y también apagones completos de electricidad para que ellos resuelvan el problema", agrega.

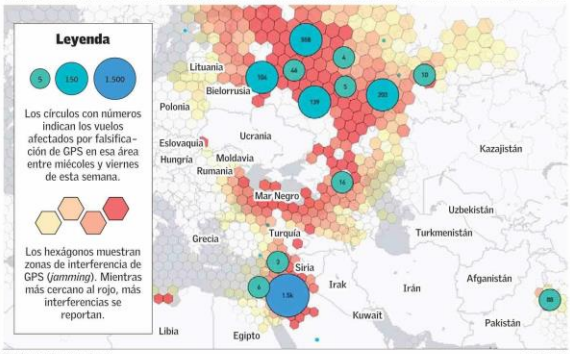
En ese sentido, Arellano, explica que el mayor tamaño de los barcos les permite tener más sistemas de información que los aviones. "El ámbito marino está menos expuesto al *spoofing* por la diversidad de equipamiento y señales independientes de los que se dispone en el puente de mando, como, por ejemplo, Inmarsat C (otro tipo de sistemas de navegación por satélite)".

Según Palacios este tipo de ataques seguirían en aumento. "La facilidad para obtener equipamiento necesario hace que estos ataques sean cada vez más comunes. Mientras no se implementen mejores defensas en los sistemas de navegación, la tendencia es que los incidentes sigan aumentando".

En ese sentido, Durney dice que Galileo, otro sistema satelital, está en etapas de pruebas para aumentar su nivel de seguridad. "Es a prueba de falsificaciones entre satélites y receptores".

Mapa de falsificación e interferencia de GPS en aeronaves

SkAI Data Services y el Centro de Aviación de la U. de Ciencias Aplicadas de Zúrich mantienen un sitio que muestra en tiempo real los vuelos afectados por manipulación de la señal de GPS. La información la obtienen de OpenSky Network.



Fuente opensky-network.org EL MERCURIO

Así funciona el engaño

Un transmisor es usado para generar una señal falsa de GPS que, por su mayor potencia, es captada por los aviones. Esa señal GPS entrega una ubicación distinta a la real, pudiendo alterar los planes de aeronavegación.

Dos amenazas

Spoofing (falsificación) no es lo mismo que el *jamming* (interferencia radioeléctrica) que es otro tipo de ataque electrónico, pero que lleva más tiempo ocurriendo. "En este último una o varias señales de gran potencia son generadas deliberadamente para interrumpir o contaminar las señales de tipo GPS, impidiendo así que los receptores tengan las condiciones mínimas de calidad de señal para poder procesar la información y determinar la ubicación esperada", dice Durney.

Y añade: "Para ambos tipos de ataque electrónico existen técnicas de prevención y protección".