INTERNATIONAL CIVIL AVIATION ORGANIZATION (ICAO)
ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL (OACI)

COMISIÓN LATINOAMERICANA DE AVIACIÓN CIVIL (CLAC)
LATIN AMERICAN CIVIL AVIATION COMMISSION (LACAC)

CUARTA REUNIÓN DEL GRUPO REGIONAL SOBRE SEGURIDAD DE LA AVIACIÓN Y FACILITACIÓN (AVSEC/FAL/RG/4)

Oficina Regional NACC de la OACI, Ciudad de México, México, 3 al 5 de junio de 2014

AVSEC/FAL/RG/4 — NE/14
06/05/14

Cuestión 9 del Orden del Día: **Otros asuntos**
9.1 Interferencias a los Sistemas de Gestión de Tránsito Aéreo

INTERFERENCIAS A LOS SISTEMAS DE GESTIÓN DE TRÁNSITO AÉREO

(Presentada por Argentina)

RESUMEN EJECUTIVO

La presente Nota de Estudio aborda la posibilidad de producir engaños a los Sistemas de Gestión del Tránsito Aéreo (ATM), y la importancia del estudio del caso a los fines de prevenir esta modalidad para la comisión de un acto de interferencia ilícita.

Acción:	La acción sugerida se presenta en la Sección 4.
Objetivos Estratégicos:	• Seguridad de la aviación y facilitación
Referencias:	• Convenio de Chicago • Anexo 17 – *Seguridad* • Doc. 8973/8 • Doc. 9924 • Doc. 9985 • *Reporte Final* AVSECP/25

1. Introducción

1.1 Además de las posibilidades de interferencia ilícita en el procesamiento de los sistemas de Gestión de Tránsito Aéreo (ATM) y del equipamiento de a bordo que se encuentran en las aeronaves, que se pueden ver perjudicados induciendo errores a los segmentos de comunicaciones, navegación y vigilancia a través de la vulneración a la "ciberseguridad", existen otras posibilidades de vulnerar a los sistemas CNS/ATM sin la imperiosa necesidad de atacar a las redes informáticas de estos sistemas.

1.2 Cabe destacar que la preocupación por el tema referido fue oportunamente debatido en el 25° Panel AVSEC de la OACI en Montreal entre el 17 al 21 de marzo de 2014, habiéndoselo abordado únicamente en el marco de los ataques relacionados con terrorismo, es decir, actos deliberados y maliciosos con la intención de causar pérdida de vidas y/o perturbaciones importantes y daño en la actividad económica del sector de la aviación. La evaluación se concentra en ataques a los sistemas de gestión del tránsito aéreo (ATM) basados en tecnología de la información (IT) y no incluye específicamente ataques más amplios y menos específicos que pueden afectar inadvertidamente a la aviación.

2. Desarrollo

2.1 En este sentido, existen otras posibilidades se basan en el engaño producido por sistemas de prueba de radares secundarios (PARROT's) que son operacionalmente válidos ***siempre y cuando*** las autoridades de la Administraciones de Aviación Civil los informen adecuadamente a la comunidad aeronáutica a través de las Publicaciones de Información Aeronáutica (AIP) o hasta su formalización en la AIP utilizando los mensajes de NOTAM (notice to airmen).

2.2 Estos equipos de prueba pueden ser programados remotamente para indicar una posición, altitud o nivel de vuelo y una clave de identificación. El efecto que producirían estos equipos operacionalmente traen una sucesión de hechos que pueden enumerarse en:

a) Confusión en el personal de controladores de tránsito aéreo;
b) Avisos de alerta y en el peor de los casos avisos de resolución en los sistemas anticolisión de a bordo.

2.3 Como consecuencia de esto se alteraría la situación aérea, especialmente en zonas de alta densidad de tránsito aéreo, que desencadenaría un efecto dominó entre las posiciones de las aeronaves controladas. Todo lo expuesto hasta ahora sería el resultado de un error u omisión sobre la indicación de estos equipos de prueba que son y deben ser usados para garantizar el funcionamiento normal de un sistema de vigilancia como es el radar secundario.

2.4 Hoy día los PARROTS se logran partiendo de un respondedor de radar secundario utilizado por las aeronaves ya sea en los modos convencionales (A y C) como también en modo S y se les adicionada un módulo de interface con la capacidad de programar los parámetros antes mencionados de posición, nivel de vuelo y clave de identificación.

2.5 Como la adquisición de estos equipos (transponders) está a un alcance inmediato de cualquier persona con conocimientos básicos de aviación, la posibilidad de la utilización mal intencionada de los mismos podría provocar de manera deliberada, afectando directamente la seguridad operacional. Esto desataría una situación de alto riesgo entre aeronaves en vuelo, que podría provocar desde tan solo un control caótico de la situación aérea reinante en el entorno de dos ó más aeronaves próximas en vuelo, hasta la posibilidad de ocasionar un grave incidente aéreo o en el peor de los casos en una colisión entre aeronaves en vuelo.

2.6 También hay que destacar que públicamente se pueden seguir los vuelos en el mundo a través de diversas páginas de internet, brindando éstas información certera como indicativos de vuelo y sus claves de identificación.

2.7 La conjunción de estas alternativas de equipamientos y de datos de las aeronaves casi en tiempo real podrían ser la mezcla necesaria para que individuos u organizaciones delictivas puedan usar todo esto para generar un escenario difícil de dominar, ya que una vez disparado, llevar a la situación de normalidad se tornaría con dificultad acentuada mientras se vuelva a establecer la conciencia situacional, tanto en los centros de control de tránsito aéreo, como en la cabina de mando de las aeronaves, las coordinaciones entre las distintas dependencias de los servicios de tránsito aéreo y éstas con las aeronaves bajo las respectivas jurisdicciones y la determinación de la falsa información producida intencionalmente.

3. Conclusión

3.1 Sintéticamente, el resultado de esta acción, aunque todavía nunca fue puesta en práctica, afectaría a los sistemas automatizados de gestión de tránsito aéreo interfiriendo básicamente en las claves de identificación de radar secundario, ADS- B, sistemas ACAS y congestión de comunicaciones orales y de datos.

4. Acción Sugerida

4.1 Se invita a la Reunión a:

a) analizar la Nota de Estudio presentada, intercambiar criterios y sugerir las medidas que sean pertinentes; y
b) solicitar a los Estados que hayan analizado este tipo de amenazas, o estén interesados en hacerlo, que contribuyan a este trabajo.

— FIN —