



NOTA DE ESTUDIO

DECIMOTERCERA CONFERENCIA DE NAVEGACIÓN AÉREA

Montreal, Canadá, 9 al 19 de octubre de 2018

COMITÉ A

Cuestión 5 del
orden del día: Cuestiones emergentes
5.4: Ciberresiliencia

CONSIDERACIONES ACERCA DE LA CIBERSEGURIDAD EN LA AVIACIÓN

[Nota presentada por la Organización de servicios de navegación aérea civil (CANSO), el Consejo Coordinador Internacional de Asociaciones de Industrias Aeroespaciales (ICCAIA), la Federación Internacional de Asociaciones de controladores del tráfico aéreo (IFATCA) y la Federación Internacional de Asociaciones de Pilotos de Línea Aérea (IFALPA)]

RESUMEN

En esta nota de estudio se presentan las posturas de CANSO, ICCAIA, IFATCA e IFALPA con respecto a la necesidad de desarrollar un marco mundial armonizado entre todos los interesados en la aviación civil, para un intercambio de información digital seguro y confiable (un Marco de confiabilidad en la aviación), para apoyar la modernización de la aviación mundial. En esta nota se apoyan en particular, los principios estratégicos propuestos en la nota de la Secretaría AN-Conf/13-WP/27, así como la necesidad de crear los requisitos de políticas y de gobernanza para permitir una implementación segura, capaz y económica. Queda entendido que los detalles técnicos de dicha implementación se concretarán una vez que se establezca un foro formal de la OACI.

Medidas propuestas a la Conferencia: Se invita a la Conferencia a avalar la recomendación presentada en el párrafo 3.

1. INTRODUCCIÓN

1.1. El sector de la aviación civil en su conjunto está cambiando rápidamente mediante la adopción de nuevos conceptos operacionales basados en la extensa conectividad y en las nuevas tecnologías para mejorar la operación ordenada y segura del tráfico aéreo. Estos esfuerzos de modernización cuyo objeto es mejorar las operaciones en la aviación auguran importantes beneficios a través de la optimización del espacio aéreo. A medida que aumenta la demanda de un intercambio de datos confiable, interconectado y dinámico, los beneficios también conllevan riesgos de ciberseguridad y la posibilidad de recibir ataques cibernéticos contra la seguridad, la capacidad de la navegación aérea, la eficiencia y las capacidades operacionales.

¹ Las versiones en español, árabe, chino, francés, inglés y ruso fueron proporcionadas por el ICCAIA.

1.2. En respuesta a estos cambios, debe desarrollarse un nuevo enfoque armonizado de extremo a extremo para apoyar la necesidad de aumentar la ciberresiliencia del sistema de aviación civil. Este sistema debe establecerse de manera que apoye a todos los interesados de la aviación civil. Este enfoque debe considerar aspectos técnicos y de gobernanza y debe aprovechar la tecnología comercialmente disponible así como los métodos para satisfacer las demandas de la velocidad y la asequibilidad para la industria. A medida que los futuros sistemas de aviación se vuelvan complejos, se necesitarán métodos y estrategias modernos para operar como un entorno global integrando todas las especificaciones locales y regionales. Este desafío no puede dividirse en los elementos clásicos aeronave/servicios de navegación aérea (ANS)/aeródromo, sino que debe tratarse como una solución integrada de extremo a extremo. Deben considerarse las capacidades horizontales y verticales, así como los riesgos de ciberseguridad.

1.3. La aviación civil debe adoptar, entre otros elementos, un marco mundial armonizado en acuerdo con todos los interesados de la aviación, para obtener un intercambio de información digital seguro en la aviación (un Marco de confiabilidad en la aviación) que considere las áreas sensibles (geopolíticas y financieras) de la comunidad de la aviación.

2. ANÁLISIS

2.1. Dentro del contexto de la extensa conectividad entre los actores de la aviación civil, el objetivo de la resiliencia identificado en el Plan global para la seguridad de la aviación (GASEP) e identificado en la nota de la Secretaría sobre el tema, no se confirmará sin la creación de un marco de confianza que identifique los principios clave para confiar en la infraestructura de la aviación y la información que se intercambia a través de infraestructura (identidad, integridad, confidencialidad y disponibilidad). Un marco de confianza es una herramienta clave para establecer una solución integrada eficiente y efectiva de extremo a extremo para todas las partes. Actualmente las partes dedican recursos y tiempo considerables para gestionar las interfaces externas y, en muchos casos, es limitado su conocimiento del riesgo que representa cada conexión externa. Las siguientes consideraciones destacan la importancia de la confianza y la interoperabilidad que se deben examinar y adoptar, para obtener los beneficios y a la vez manejar los riesgos:

Consideraciones acerca de la gobernanza:

- a) Establecer los requisitos mínimos para el cumplimiento de la ciberseguridad.

Identificar el nivel mínimo aceptable de requisitos de ciberseguridad y las normas comunes para asegurar una mayor integridad. El sistema de gestión de riesgos debe ser la parte principal del enfoque. Necesita completarse con normas abiertas de la industria y un enfoque de cumplimiento para lograr un marco de trabajo fiable.

- b) Establecer métodos de inspección o validación.

La ciberseguridad requiere un enfoque complementario a las evaluaciones físicas de cumplimiento de seguridad que se realizan en la actualidad. Los riesgos de ciberseguridad evolucionan constantemente, por lo que será necesaria la validación continua del cumplimiento de las normas operacionales de ciberseguridad. A medida que las partes interesadas estén más integradas se requerirá la cooperación mutua entre las partes relacionadas para validar y gestionar tanto el riesgo individual como el riesgo conjunto de extremo a extremo.

c) Políticas jurídicas

Actualmente, la industria sigue normas de seguridad física. La evaluación de los riesgos de ciberseguridad y la validación del cumplimiento deben añadirse a los procesos existentes. Además, las organizaciones deben mantener un cumplimiento aceptable en ciberseguridad.

Consideraciones técnicas:

Todas las partes deberán construir y operar su sistema de la manera más efectiva y eficiente para ellas. A medida que la comunidad se vuelva más integrada, las soluciones pueden volverse complejas y costosas. La modernización de la estructura técnica y las normas establecidas por las partes deben adaptarse a cada entorno operacional individual, mediante la normalización para permitir la interoperabilidad y la conectividad entre las partes.

El marco debe:

- a) Apoyar la demanda creciente de interconectividad con el uso de tecnología nueva, promover métodos técnicos comunes, como certificados digitales y atributos acordados mutuamente para establecer una confianza recíproca.
- b) Promover una base de confianza entre las partes interesadas conforme a un marco común de normas modernas, protocolos y tecnologías comerciales.
- c) Apoyar el establecimiento de un entorno operacional común para la interconectividad y el intercambio de información digital. Aprovechar conceptos como la red de la Sociedad para las Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT) que utilizan los bancos en todo el mundo, así como las lecciones aprendidas de la industria financiera.
- d) Disminuir los costos de operación de muchas partes interesadas de la comunidad mundial y crear oportunidades para otros mercados.
- e) Considerar la adaptabilidad y modularidad de las capacidades como una manera de actualizar y de adaptar el marco rápidamente conforme a la evolución de la tecnología, para responder a los ataques cibernéticos.

2.2. La normalización crea un grado de confianza común en las operaciones de la aeronave y de los servicios de tránsito aéreo en todo el mundo. La comunidad de la aviación civil no cuenta actualmente con las normas necesarias para asegurar la confianza mutua y la protección para el intercambio de información digital, los métodos de interconectividad ni el proceso para protegerse contra los riesgos mutuos. Establecer un marco común para el intercambio de información utilizando normas válidas para todas las partes permitirá asegurar la gestión de los riesgos y proporcionará el grado de confianza necesario.

2.3. Con un marco de confianza común, las iniciativas clave de la aviación civil identificadas en el Plan mundial de navegación aérea (GANP, Doc 9750) de la OACI se podrán lograr más rápido, con menor complejidad y la vez permitir las capacidades necesarias del futuro de:

- a) la integración mundial (es decir, SWIM, FF-ICE, etc.) de comunicación digital segura y confiable entre los actores de la aviación civil;
- b) la modernización de marcos confiables existentes para interoperar con marcos tradicionales;

- c) el control de los nuevos participantes con infraestructuras tradicionales costosas; y
- d) el aprovechamiento de la identidad, integridad y confidencialidad para otras capacidades (es decir, datos operacionales y de misión que respalden una mayor eficiencia).

2.4. El marco de confianza debe considerar a todas las partes, que podrían tener diferentes grados de madurez en su estructura de gobernanza o capacidades técnicas. Al implantarse, las partes podrían hacer gradual y fácilmente la transición sin dificultades de los elementos tradicionales, mientras que los nuevos participantes en el mercado tendrán que hacerlo de manera rápida y asequible con objetivos operacionales y comerciales específicos. El método de transición debe proporcionar una base común que pueda aprovechar todas las partes para implantar en etapas y disminuir el impacto con base en la madurez de la organización. Todos deben apoyar la integración segura y sin interrupciones dentro del espacio aéreo.

3. CONCLUSIÓN

3.1. La Organización de servicios de navegación aérea civil (CANSO), el Consejo Coordinador Internacional de Asociaciones de Industrias Aeroespaciales (ICCAIA), la Federación Internacional de Asociaciones de controladores del tráfico aéreo (IFATCA) y la Federación Internacional de Asociaciones de Pilotos de Línea Aérea (IFALPA) fomentan la necesidad de desarrollar un marco de confianza mundial coordinado de la aviación para el intercambio de la información digital como una herramienta clave para la creación de un futuro ecosistema ciberresiliente de la aviación civil. Este desafío no puede dividirse en los elementos clásicos aeronave/ANS/aeródromo, sino que debe crearse una solución integrada de extremo a extremo y tomar en consideración las capacidades horizontales y verticales, así como los riesgos de ciberseguridad.

3.2. Se invita a la conferencia a convenir en la siguiente recomendación:

Recomendación 5.4/x – ciberresiliencia

Que la conferencia:

- a) solicite a la OACI establecer un proyecto formal que incluya a los Estados y las organizaciones internacionales para la creación de un marco de confianza armonizado y aceptado para abordar los objetivos descritos en la presente nota; y
- b) solicite a la OACI crear una hoja de ruta con el compromiso de la industria y se incluya dentro del GANP para el desarrollo de elementos tecnológicos clave para abordar las necesidades cambiantes en ciberseguridad de la aviación civil (es decir, cadenas de bloques -blockchain-, servicios en la nube y otras tecnologías cambiantes).