Organización de Aviación Civil Internacional

A40-WP/197
TE/79
1/8/19

NOTA DE ESTUDIO

ASAMBLEA — 40º PERÍODO DE SESIONES

COMISIÓN TÉCNICA

Cuestión 30: Otros asuntos que habrá de considerar la Comisión Técnica

MARCO DE CONFIANZA EN UN ENTORNO DIGITAL

(Nota presentada por Brasil)

RESUMEN

El crecimiento de las infraestructuras y servicios digitales de aviación ha facilitado mucho el aumento de la capacidad y la optimización del espacio aéreo pero, al mismo tiempo, ha planteado desafíos en relación con la interoperabilidad y la ciberresiliencia. Es preciso establecer un marco de confianza para que la aviación opere sin discontinuidades entre las fronteras internacionales.

Decisión de la Asamblea: Se invita a la Asamblea a:

a) pedir que la OACI promueva el concepto de marco de confianza y una red de confianza a escala mundial para evitar divergencias en las iniciativas de los Estados y regiones;
b) recomendar que la OACI siga adelante con las medidas formuladas por la 13ª Conferencia de navegación aérea con respecto al marco de confianza y una red de confianza para el intercambio de información crítica de seguridad operacional;
c) pedir que la OACI incluya en el marco de confianza métodos para aislar a la comunidad de la aviación de la Internet pública;
d) pedir que la OACI, con el apoyo del sector de la aviación y sectores ajenos a la aviación, defina la arquitectura y los requisitos de una red de confianza, en apoyo del intercambio de información en un entorno digitalmente conectado; y
e) recomendar que los Estados respalden con los recursos necesarios el desarrollo del marco de confianza.

Objetivos estratégicos:	Esta nota de estudio se relaciona con los Objetivos estratégicos: *Seguridad operacional*, *Capacidad y eficiencia de la navegación aérea* y *Seguridad de la aviación y facilitación.*
Repercusiones financieras:	Capacitación de personal, instalación de equipo y sistemas tanto terrestres como de a bordo.
Referencias:	Anexo 17 — *Seguridad — Protección de la aviación civil internacional contra los actos de interferencia ilícita* *Resoluciones vigentes de la Asamblea (al 6 de octubre de 2016)* (Doc 10075) *Manual para implantar la red de telecomunicaciones aeronáuticas (ATN) utilizando normas y protocolos de la familia de protocolos de Internet (IPS)* (Doc 9896) *Plan mundial de navegación aérea* (Doc 9750)

1. INTRODUCCIÓN

1.1 Vivimos en la era informática. Los aparatos y las máquinas están cada día más interconectados mediante una compleja red de datos que reduce las distancias y aumenta la velocidad de intercambio de los mensajes. El mundo se vuelve más pequeño. Sin embargo, con estas instalaciones también aumentan considerablemente las amenazas que, a diferencia de lo que ocurría en el pasado, vienen de todas partes del mundo y son invisibles.

1.2 Enfrentar estas amenazas representa uno de los desafíos más grandes en este momento ya que son distintas, están en todas partes y pueden causar grandes pérdidas en términos de vidas y gastos financieros.

1.3 En un mundo cada día más interconectado, la aviación no puede mantenerse al margen. A pesar de que existe un gran número de sistemas analógicos y aislados, están implementándose nuevas tecnologías que usan información digital que viaja a través de redes de datos. Conceptos tales como el sistema mundial de navegación por satélite (GNSS), la vigilancia dependiente automática — radiodifusión (ADS-B), las comunicaciones por enlace de datos controlador-piloto (CPDLC), las comunicaciones de datos entre instalaciones ATS [servicios de tránsito aéreo] (AIDC), la red de telecomunicaciones aeronáuticas (ATN), la gestión de la información de todo el sistema (SWIM), los sistemas de aeronaves pilotadas a distancia (RPAS) y otros, aportan beneficios enormes a la aviación, pero generan nuevos desafíos en lo que se refiere a garantizar la disponibilidad, integridad, confidencialidad y autenticidad de la información proporcionada por los servicios.

1.4 Solamente con una sólida gobernanza pueden conocerse, controlarse y mitigarse los riesgos inherentes de los nuevos conceptos que se han implantado. Para esto, el punto de partida es el desarrollo de un marco de confianza que permita normalizar los procedimientos y los protocolos para la gestión y la integración de las infraestructuras de la red y los servicios, y que sirva de protección contra los ciberataques.

2. ANÁLISIS

2.1 Aunque el ciclo de evolución tecnológica de la aviación es más lento, el mundo digital pasa cada día más a formar parte de los distintos sistemas de comunicaciones, navegación, vigilancia, meteorología, gestión del tránsito aéreo (ATM), gestión de la información aeronáutica (AIM), entre otros. La digitalización de la información, las interconexiones de la red y la automatización de los servicios requieren una gobernanza altamente eficaz para garantizar la interoperabilidad y la seguridad de las operaciones.

2.2 Para la introducción del concepto SWIM en la aviación, por ejemplo, se requerirán las normas, la infraestructura y la gobernanza necesarias para la gestión de la información ATM y su intercambio entre participantes cualificados mediante servicios interoperables.

2.3 No obstante, para lograr este objetivo, las distintas redes de telecomunicaciones aeronáuticas de los Estados deben estar interconectadas a fin de garantizar la circulación de la información. Cada Estado es responsable del despliegue y el funcionamiento de su infraestructura de red y de velar por su seguridad pero, para mantener la continuidad de las operaciones a través de las fronteras, se requiere ajustarse a normas.

2.4 Estas normas deben elaborarse conforme a los principios del Convenio de Chicago, para establecer un marco de confianza que pueda garantizar la seguridad de todos los que participan en el intercambio de información en un entorno digitalmente conectado.

2.5 Otro aspecto que es preciso considerar es la necesidad de que todos los que usan los servicios y redes tengan un certificado digital que garantice su identificación en todo el mundo.

2.6 La comunidad aeronáutica siempre ha procurado aislarse físicamente de las redes externas, pero ahora esto resulta difícil porque los datos siguen numerosos caminos distintos alrededor del mundo. No obstante, la OACI cuenta con un medio que le permite salvaguardar su infraestructura si considera que se trata de un problema que no es local o regional. Es el sistema de todo el mundo el que debe ser seguro y resiliente.

2.7 Asimismo, como el sistema global usa la infraestructura actual de la Internet para fines diferentes, es necesario que esta industria participe con la OACI para garantizar el aislamiento lógico que se requiere para aumentar el nivel de protección de las redes del sistema de la aviación.

2.8 El aislamiento lógico puede lograrse de diferentes maneras, siempre que se garantice que si alguien decide actuar malintencionadamente y hacer algo en contra de la aviación en el ciberespacio, se reconozca que no pertenece al ecosistema de la aviación y se le niegue el acceso. De este modo se reforzarán los niveles de protección del sistema que serán compatibles con los niveles acordados de seguridad operacional de la comunidad de la aviación.

2.9 Debe reconocerse que ningún sistema puede estar totalmente protegido pero, si se cuenta con aislamiento lógico, cualquier persona malintencionada tendrá que trabajar más duro para introducirse en el sistema de aviación. Contar con un marco de confianza conjuntamente con una red aislada lógicamente no implica que se puede confiar absolutamente en todos los que están en la red. Significa que toda la comunidad tiene conocimiento de quiénes son los participantes y cuál es la función que deberían desempeñar dentro de la red. Además del aislamiento lógico, otra capa de protección es contar con un sistema de identificación con base en una entidad reguladora, lo que resulta más eficaz que contar con un gran número de sistemas de identificación dispersos en todo el sector.

2.10 En la 13º Conferencia de navegación aérea se consideró y se convino en que era necesario elaborar un marco de confianza global y disposiciones relativas a la gobernanza y las políticas de una red de confianza. Ahora llegó el momento de que la OACI trabaje con los Estados y la industria para adelantar la labor y crear conciencia con respecto a las ciberamenazas para la seguridad operacional y la resiliencia de las operaciones.

3. CONCLUSIÓN

3.1 El intercambio de información en formato digital está creciendo rápidamente y todos los que en él participan están aplicando medidas para proteger sus sistemas digitalmente conectados contra las ciberamenazas y garantizar la resiliencia de los sistemas de navegación aérea.

3.2 Los que recién se integran al sistema de aviación están innovando rápidamente y necesitan un marco de confianza y una red de confianza globales para reforzar la seguridad operacional y la eficiencia de sus operaciones y evitar así que la seguridad operacional se vea negativamente afectada. Los proveedores de servicios de navegación aérea deben estar preparados para satisfacer estos requisitos.

3.3 Además, la OACI debe dar apoyo a los Estados en su labor de integración, lo cual puede requerir la participación de entidades ajenas a la aviación que se encargan de redes privadas. Asimismo, se necesita orientación de la OACI acerca de la manera de abordar estos asuntos para la armonización a escala mundial de los procedimientos y la interoperabilidad de los sistemas.

— FIN —