Organización de Aviación Civil Internacional

A40-WP/427
EX/176
2/8/19

NOTA DE ESTUDIO

ASAMBLEA — 40º PERÍODO DE SESIONES

COMITÉ EJECUTIVO

Cuestión 12: Seguridad de la aviación — Política

PROPUESTA PARA LA GOBERNANZA EN LA OACI DE LA CIBERSEGURIDAD Y LA RESILIENCIA

(Nota presentada por Estados Unidos)

RESUMEN

La ciberseguridad y la resiliencia en el ecosistema de la aviación son asuntos multidisciplinarios que afectan o afectarán a casi todos los aspectos de la aviación mundial. Debido a la complejidad y a la dependencia de la información y la comunicación digital compartida, la ciberseguridad y la resiliencia son crecientemente vitales con cada adelanto tecnológico y la modernización continua del ecosistema de la aviación.

Si bien los Estados miembros de la OACI y la industria están trabajando diligentemente para resolver cuestiones de ciberseguridad y resiliencia, el enfoque actual de la OACI carece de una gobernanza apropiada y se centra en sectores individuales y experiencia variada en lugar de reflejar el ecosistema global de la aviación mundial.

Para resolver lo anterior, Estados Unidos recomienda que la OACI establezca un comité técnico del Consejo sobre ciberseguridad y resiliencia, a fin de centralizar la gobernanza y abordar la ciberseguridad y la resiliencia de manera holística. El comité gestionará la política y la integración de las normas de la industria, evaluando al mismo tiempo el desarrollo potencial de normas técnicas y métodos recomendados.

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

a) solicitar que la OACI establezca un nuevo comité técnico del Consejo sobre ciberseguridad y resiliencia como se propone en esta nota;
b) instar a los Estados a que apoyen la estrategia de ciberseguridad de la OACI desarrollada por el Grupo de estudio de la Secretaría sobre ciberseguridad; e
c) instar a los Estados a que respalden el trabajo del Grupo de estudio sobre el marco de confianza.

Objetivos estratégicos:	La presente nota de estudio se relaciona con los Objetivos estratégicos — *Seguridad de la aviación y facilitación*, y *Capacidad y eficiencia de la navegación área*.
Repercusiones financieras:	Ninguna
Referencias:	*Resoluciones vigentes de la Asamblea* (Doc 10075), A39-18 y A39-19 Recomendación 5.4/1 de la decimotercera Conferencia de navegación aérea de la OACI A40-WP/28 — *Estrategia de ciberseguridad de la OACI* *Reglamento interno del Consejo*, Sección III, Artículo 17 a) (Doc 7559/10)

1. INTRODUCCIÓN

1.1 La ciberseguridad y la resiliencia en el ecosistema de la aviación son asuntos multidisciplinarios que afectan o afectarán a casi todos los aspectos de la aviación mundial. Como se reconoció en el 39º período de sesiones de la Asamblea de la OACI en las Resoluciones A39-18 y A39-19, el sistema mundial de aviación es cada vez más complejo y está cada vez más integrado mediante la tecnología de la información y las comunicaciones. Debido a esta complejidad y a la dependencia de la información y la comunicación digital compartida, la ciberseguridad y la resiliencia son crecientemente vitales con cada adelanto tecnológico y la modernización continua del ecosistema de la aviación.

1.2 La importancia de la ciberseguridad y la resiliencia se demuestra además en la Recomendación 5.4/1 resultante de la decimotercera Conferencia de navegación aérea de la OACI, que pide a los Estados y a la OACI que, entre otras cosas, trabajen juntos en coordinación con la industria para elevar el nivel de conciencia sobre las ciberamenazas y se coordinen para mitigar los riesgos. La Segunda Conferencia de alto nivel sobre seguridad de la aviación recomendó también que la OACI formulara una estrategia global de ciberseguridad y realizara un estudio de factibilidad de un grupo de expertos sobre ciberseguridad.

1.3 Si bien la OACI está avanzando en la definición de su estrategia de ciberseguridad (véase A40-WP/28), la gobernanza de la ciberseguridad y la resiliencia en la Organización es todavía insuficiente. La falta de una gobernanza apropiada crea ineficiencias y falta de intercambio de información, lo cual hace imposible abordar debidamente la ciberseguridad y la resiliencia de una manera holística que centralice la gestión de la política, la integración de las normas de la industria y el desarrollo potencial de normas técnicas y métodos recomendados (SARPS).

2. ANÁLISIS

2.1 La actual gobernanza en la OACI de los temas relacionados con ciberseguridad divide las actividades entre la Dirección de transporte aéreo (ATB), que supervisa la ciberseguridad, y la Dirección de navegación aérea (ANB) que supervisa la ciberresiliencia.

2.2 La ATB se encarga de formular SARPS y enmendar el Anexo 17 – *Seguridad*. También presta apoyo al trabajo del Grupo de expertos sobre seguridad de la aviación y al Comité sobre Interferencia ilícita (UIC), incluida la constitución del Grupo de estudio de la Secretaría sobre ciberseguridad (SSGC). Este grupo actúa como coordinador del trabajo de ciberseguridad; estudia los Anexos de la OACI para consolidar los SARPS relacionados con la ciberseguridad y promueve en general el intercambio de información en toda la comunidad de la aviación.

2.3 El enfoque de la ATB funciona bien cuando la ciberseguridad se considera como un solo tema centrado en proteger los sistemas críticos contra interferencia ilícita, tal como se define en la Sección 4.9 del Anexo 17. No obstante, la aviación mundial es un ecosistema holístico que incluye muchos sistemas interconectados que afectan directamente las operaciones, y que no están bajo la responsabilidad del ATC ni del UIC en términos de ciberseguridad.

2.4 La ANB se encarga de formular y enmendar SARPS relativos a la seguridad operacional y a la capacidad y eficiencia de la navegación aérea contenidos en 17 anexos. También presta apoyo al trabajo de la Comisión de Aeronavegación y de sus grupos de expertos técnicos, incluida la constitución del Grupo de trabajo INNOVA y del Grupo de estudio sobre el marco de confianza. Este último coordina el desarrollo de interconexiones ciberresilientes en la red a través de un marco de confianza que permite la transferencia de datos e información aeronáutica vitales para las operaciones.

2.5 El enfoque de la ANB funciona bien cuando se consideran únicamente los datos operacionales y la transferencia de información. Sin embargo, no tiene en cuenta los sistemas de seguridad que no están conectados a la red operacional, y que pueden tener un impacto en otras áreas que afectan la seguridad operacional o la eficiencia.

2.6 Si bien es claro que la OACI está ocupándose tanto de la ciberseguridad como de la resiliencia, la actual estructura de gobernanza crea una división entre la seguridad y la resiliencia, que afecta negativamente el ecosistema holístico de la aviación. Los Estados miembros y la industria han reconocido este problema y han recomendado establecer un nuevo grupo de expertos sobre ciberseguridad y resiliencia. No obstante, los grupos de expertos de la OACI tienen como misión específica buscar soluciones a problemas especializados o elaborar SARPS (véanse las *Instrucciones relativas a los grupos de expertos de la Comisión de Aerona*vegación, Doc 7984). La ciberseguridad y la resiliencia son más multidisciplinarias y globales que un ´problema especializado´ y en este momento deberían utilizarse normas de la industria para ciber en lugar de elaborar SARPS nuevos o un nuevo anexo de la OACI.

2.7 Teniendo esto en mente, la ciberseguridad y la resiliencia deberían reconocerse por su impacto en todo el ecosistema de la aviación y por ende elevarse y gestionarse centralmente en el Consejo de la OACI bajo un comité técnico establecido para ese fin.

2.8 Conforme a la Sección III, Artículo 17 a) del Doc 7559/10, *Reglamento interno del Consejo*, Estados Unidos propone que se constituya un comité técnico del Consejo sobre ciberseguridad y resiliencia. El Doc 7559/10 especifica que el Consejo puede crear otras comisiones, comités o grupos de trabajo permanentes o temporales. Puede establecerse un nuevo comité del Consejo para tratar problemas relacionados con aspectos técnicos, económicos, sociales y jurídicos de la aviación civil internacional que, para su resolución, requieren conocimientos expertos de los que no dispone el Consejo por otros medios.

2.9 El comité técnico propuesto trabajará bajo el control directo del Consejo, órgano que también formulará las atribuciones del comité y establecerá su membresía de acuerdo con las "*Instrucciones para el Comité sobre ciberseguridad y resiliencia*". El SSGC y el grupo de estudio sobre el marco de confianza se reorganizarán bajo el nuevo comité técnico, considerando plenamente las tareas, trabajo y costos necesarios para asegurar la debida gestión del nuevo comité. De esta manera, el comité utilizará debidamente a expertos en diversas disciplinas, incluyendo expertos que están dentro de la estructura de trabajo de la OACI, evitando ineficiencias y problemas de comunicación generados por la distribución de asuntos complejos e interrelacionados entre varias direcciones y oficinas con distintas prioridades.

3. CONCLUSIÓN

3.1 La ciberseguridad y la resiliencia inciden considerablemente en todo el ecosistema global de la aviación. El enfoque propuesto en esta nota de estudio elevará este aspecto crítico a nivel de un comité técnico del Consejo que puede trabajar en medidas multidisciplinarias y valerse de la experiencia y conocimientos de distintas direcciones de la OACI y de toda la comunidad de la aviación, manteniendo al mismo tiempo el ritmo de innovación frente a las siempre crecientes amenazas.

3.2 Se invita a la Asamblea a respaldar las medidas que se presentan en el resumen.

— FIN —