Organización de Aviación Civil Internacional

A40-WP/172[1]
EX/70
1/8/19

NOTA DE ESTUDIO

ASAMBLEA — 40º PERÍODO DE SESIONES

COMITÉ EJECUTIVO

Cuestión 12: Seguridad de la aviación — Política

CIBERRESILIENCIA

[Nota presentada por la Organización de servicios de navegación aérea civil (CANSO)]

RESUMEN

La ciberseguridad constituye un tema cada vez más importante en aviación, por lo que varias iniciativas, tales como la Gestión de información de todo el sistema (SWIM), generan sistemas que se vuelven cada vez más interoperables y transparentes. Actualmente, el examen de qué medidas debe tomar la OACI para garantizar la ciberresiliencia es evaluado por su Grupo de estudio de la Secretaría sobre ciberseguridad (SSGC). El mando lo asume la Oficina de Transporte Aéreo (ATB) de la OACI y está respaldado por su propia Oficina de Navegación Aérea (ANB).

Esto significa poca gobernabilidad para los estados, la Comisión de Navegación Aérea (ANC) y el Consejo de la OACI. El SSGC está actualmente compuesto por unos cincuenta participantes. El proceso parece carecer de celeridad, debido al hecho de que el Grupo de estudio de la Secretaría (SSG) no es capaz de proponer Normas y métodos recomendados (SARP), ni tiene competencias para coordinar la actividad de todos los paneles o grupos de trabajo relacionados con la ciberseguridad. El SSGC se estableció para proporcionar asesoramiento, mientras que el seguimiento se somete a examen por parte de la Secretaría General.

Dada la importancia de la ciberresiliencia y la necesidad de aplicar medidas rápidas, surge la urgencia de una forma más efectiva de abordar el tema. Para obtener la mejor gobernabilidad y acelerar el proceso de introducción de material orientativo y, en caso necesario, SARP, el SSGC actual debería transformarse en un Panel de la OACI dependiente del propio Consejo de la OACI. El recientemente formado "Grupo de estudio del marco de confianza" *(*TFSG) debería enmarcarse en este nuevo panel como un grupo de trabajo (WG).

Un nuevo Panel de ciberresiliencia, seguridad y protección (CRSSP) debería tratar y proponer SARP y materiales de orientación nuevos o adaptados para garantizar la consistencia y coherencia de todas las actividades relacionadas con la cibernética en aviación dentro de los paneles de la OACI y sus diferentes grupos de expertos.

[1] Las versiones en español, árabe, chino, francés e inglés fueron proporcionadas por CANSO.

Decisión de la Asamblea: Se invita a la Asamblea a: a) Reconocer la necesidad de un enfoque multidisciplinar, bien administrado y diligente para la ciberseguridad; b) Instar al Consejo de la OACI a crear un Panel de ciberresiliencia, seguridad y protección (CRSSP, por sus siglas en inglés) directamente dependiente del Consejo de la OACI y el Comité de Transporte Aéreo (ATC); y c) Instar al Consejo de la OACI a crear un grupo de trabajo (WG) bajo el recientemente formado CRSSP para el establecimiento de un marco orientado a un Marco de Confianza (*Trust Framework*) en la aviación.	
Objetivos estratégicos:	Esta nota de estudio se relaciona con los Objetivos estratégicos: Seguridad operacional; Capacidad y eficiencia de la navegación aérea; Seguridad y Facilitación.
Repercusiones financieras:	
Referencias:	

1. INTRODUCCIÓN

1.1 De forma similar a otros sectores que acogieron “la revolución digital”, la aviación tiene que mantener la confianza de las partes interesadas mediante la percepción precisa de oportunidades y vulnerabilidades, junto con el entendimiento de las amenazas del adversario. A continuación se indican los retos a los que se enfrenta una aviación civil digitalizada y conectada:

1.2 Dado que el sector de la aviación cada vez conecta más sistemas y servicios, los potenciales ataques a sistemas que el adversario puede realizar aumentan y se vuelven más complejos, lo que genera amenazas y objetivos mayores.

1.3 Debido a que el sector de la aviación confía en gran medida en la tecnología y cada vez se sumerge más en el entorno cibernético, será necesaria una reforma global para el entendimiento y la superación de las diferencias culturales entre ambos ámbitos. El desarrollo de una cultura compartida, observando juntos los retos y las potenciales soluciones, necesitará de una cooperación multidisciplinar.

1.4 La percepción de la amenaza planteada por un entorno digital se está volviendo esencial a la hora de entender y gestionar el riesgo. Resulta necesario que todos, dentro del sector de la aviación, adquiramos el mismo nivel de percepción y entendimiento a fin de abordar el riesgo potencial y fomentar un diálogo colaborativo que valore la multiplicidad de perspectivas.

1.5 El sector de la aviación cuenta con décadas de experiencia abordando temas sobre seguridad y protección; sin embargo, el reto de la ciberseguridad es comparativamente nuevo. Desarrollar y reemplazar los sistemas de aviación puede llevar más tiempo que el que tengan los autores materiales de los ataques para adquirir capacidades, lo cual genera un reto en la evaluación precisa del riesgo y los modelos de amenaza.

1.6 Las inversiones en la Gestión del tráfico aéreo (ATM) están ya proporcionando beneficios importantes, aunque utilizar tecnologías avanzadas, tales como los sistemas globales de posicionamiento (GPS), la comunicación digital y la Transmisión – vigilancia dependiente automática (ADS-B), significa que tenemos que gestionar las vulnerabilidades que surgen de estas tecnologías, además de fomentar su ciberresiliencia.

2. ANÁLISIS

2.1 Durante los últimos años, la OACI ha tratado tanto la ciberseguridad como la ciberresiliencia en diferentes foros. El Panel sobre Seguridad en la Aviación (AVSECP) se ha estado fijando en las vulnerabilidades del sistema de la aviación descubiertas a causa de interferencias ilícitas. El Grupo de trabajo WG sobre amenazas y riesgos del AVSECP ha indicado varias veces lo bajo que es el riesgo de actos cibernéticos de interferencia ilícita.

2.2 Para investigar la posibilidad de una red de confianza en la aviación, la Secretaría de la OACI fundó el equipo de detección "INNOVA". Este grupo de expertos creó un Concepto de operaciones (CONOPS) para una red interoperable y resiliente en la aviación a escala global. Desde mayo de 2019, el grupo INNOVA se ha transformado en el Grupo de estudio del marco de confianza (TFSG). Este grupo expande su trabajo en diferentes grupos de trabajo, que definen los requisitos de identificación y las necesidades actuales y futuras para la mencionada red. Otro grupo de trabajo dependiente del TFSG está desarrollando una visión sobre un marco de confianza digital común, al tiempo que tiene la tarea de guiar la evolución con objeto de facilitar un intercambio integral, resiliente y seguro de información en un entorno digitalmente conectado en favor de operaciones actuales y futuras.

2.3 La OACI estableció el Grupo de estudio de la Secretaría sobre cibernética (SSGC) bajo el mando del director adjunto, Facilitación y seguridad en aviación (DD/ASF). El SSGC está supervisado por el Grupo superior de gestión de la Secretaría en asuntos comunes de seguridad y protección, y presidido por el secretario general de la OACI.

2.4 El enfoque actual dentro de la OACI no permite un punto de vista eficiente y holístico. Un Grupo de estudio de la Secretaría tiene que enviar sus resultados a paneles independientes de la OACI, quienes evaluarán y decidirán si es necesario crear unas SARP sobre ese tema. Además, toda la tecnología de la información (TI) relacionada con las SARP se distribuye entre casi el total de los 19 anexos de la OACI. Sería más eficiente establecer un Panel de ciberresiliencia, seguridad y protección (CRSSP) que informe a través del Comité de Transporte Aéreo (ATC) y del Comité de Interferencia Ilícita (UIC) directamente al Consejo de la OACI. Este nuevo Panel crearía un enfoque holístico y multidisciplinar en toda la OACI y consolidaría todo el trabajo dentro de la misma en referencia a temas relacionados con la cibernética.

2.5 El CRSSP debería considerar y aconsejar sobre el desarrollo de un anexo exclusivo sobre temas relacionados con la ciberresiliencia, la seguridad y la protección dentro del sector de la aviación. El beneficio de un anexo exclusivo sería que todos los temas relacionados con la cibernética se aglutinarían igual que hace el Anexo 19 en relación con la gestión de la seguridad. Otro beneficio sería que los estados podrían enviar directamente todas las SARP y cambios en los mismos a los expertos en TI. Esto también mostraría la importancia de la ciberresiliencia, la seguridad y la protección en la posterior digitalización del mundo de la aviación.

2.6 El TFSG actual trabajaría directamente de acuerdo con el CRSSP como un grupo de trabajo aparte.

3. CONCLUSIÓN

3.1 El método actual de trabajo de la OACI para tratar los asuntos relacionados con la ciberresiliencia, la seguridad y la protección no resulta suficientemente coordinado ni es eficiente.

3.2 Al crear un panel multidisciplinar sobre toda ciberresiliencia, ciberseguridad y ciberprotección, se mejorarían la coordinación y eficiencia para investigar y contrarrestar los asuntos

sobre ciberresiliencia, seguridad y protección dentro del sistema de la aviación. Para asegurarse de que se da un enfoque multidisciplinar y dotado de una supervisión eficiente, el Panel debe depender directamente del Consejo de la OACI, el ATC y el UIC. Los resultados del Panel deben debatirse durante las reuniones conjuntas entre el ATC y el UIC para alcanzar una coordinación holística.

3.3 La creación de un anexo separado para los asuntos relacionados con la ciberresiliencia, la seguridad y la protección dará cuenta de la importancia de estos tres aspectos en la digitalización del sistema de aviación y creará una vigilancia integral de las SARP en referencia a estos mismos aspectos a través de los anexos de la OACI.

3.4 Se invita a la Asamblea a respaldar las decisiones que figuran en este resumen.

— FIN —