Organización de Aviación Civil Internacional

A39-WP/175
EX/64
9/8/16

NOTA DE ESTUDIO

ASAMBLEA — 39º PERÍODO DE SESIONES

COMITÉ EJECUTIVO

Cuestión 16: Seguridad de la aviación — Política

LA CIBERSEGURIDAD EN LA AVIACIÓN CIVIL: POSIBLES MEDIDAS DE LOS ENCARGADOS DE LA REGLAMENTACIÓN Y DE LAS PARTES INTERESADAS

(Nota presentada por Arabia Saudita, Argentina, Bélgica, Emiratos Árabes Unidos, Federación de Rusia, Francia, Guyana, La ex República Yugoslava de Macedonia, Namibia, Nauru, Nepal, Nigeria, Países Bajos, Reino Unido, República de Moldova, República Democrática Popular Lao, Santa Lucía, Senegal, Sierra Leona, Singapur, Sudáfrica, Suiza y Trinidad y Tabago)

RESUMEN

Las ciberamenzas que enfrenta el sistema de la aviación civil son una de las principales preocupaciones de todas las partes interesadas del mundo. Es crucial que la OACI, las autoridades de seguridad de la aviación, la industria de la aviación y otras partes interesadas de este sector colaboren para despertar conciencia acerca de las amenazas y definan políticas, enfoques y medidas prácticos y sostenibles, incluso en el área de la instrucción y la creación de capacidades, para brindar protección contra dichas amenazas y reducir sus repercusiones. En virtud de la interdependencia de las distintas partes que integran el ecosistema de la aviación civil mundial, una coordinación estrecha es esencial para enfrentar estos desafíos.

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

a) tener en cuenta el contenido de esta nota, en especial las posibles medidas de los encargados de la reglamentación y de las partes interesadas para enfrentar las ciberamenazas que pesan sobre las operaciones de la aviación civil;
b) instar a la OACI a establecer un marco mundial de ciberseguridad para las partes interesadas de la aviación civil; y
c) identificar un órgano dentro de la OACI para que trabaje en el desarrollo del marco mundial y lleve a cabo la coordinación con otros órganos pertinentes de la OACI y otras partes interesadas.

Objetivos estratégicos:	Esta nota de estudio se relaciona con los Objetivos estratégicos A – *Seguridad operacional*, B – *Capacidad y eficiencia de la navegación aérea*, y C – *Seguridad de la aviación y facilitación*.
Repercusiones financieras:	No hay repercusiones financieras adicionales.
Referencias:	A39-WP/14, *Estrategia global de la OACI sobre seguridad de la aviación (ICASS)* A39-WP/15, *Establecimiento de un Plan global para la seguridad de la aviación* A39-WP/16, *Declaración consolidada de los criterios permanentes de la OACI relacionados con la seguridad de la aviación* A39-WP/17, *Formas de abordar la ciberseguridad en la aviación civil* Resolución A38-15 de la Asamblea: *Declaración consolidada de los criterios permanentes de la OACI relacionados con la seguridad de la aviación* Informe de la AVSECP/27 (cubierta amarilla) de distribución limita *(en inglés únicamente)*

1. INTRODUCCIÓN

1.1 Se ha reconocido que las ciberamenzas que enfrenta el sistema de la aviación civil han sido una de las principales preocupaciones, al igual que en otros sectores. Existen numerosas vías para los terroristas y las personas que tienen malas intenciones de perpetrar ciberataques contra las partes interesadas de los servicios de aviación civil y su infraestructura. Pueden afectar a las operaciones de la aviación civil, incluso por medio de la intrusión en los sistemas de navegación y control de las aeronaves, interfiriendo con los sistemas de radares y comunicaciones y corrompiendo los diferentes sistemas aeroportuarios. Si bien a la fecha la mayoría de dichos ataques contra el sector de la aviación ha sido de bajo nivel con repercusiones limitadas, un ciberataque contra las operaciones de la aviación civil podría ser catastrófico y tener muchas víctimas, detener los servicios de la aviación civil y/o dañar infraestructura de importancia crítica. Estas preocupaciones se agravan por el hecho de que las líneas aéreas, los aeropuertos y los proveedores de servicios de navegación aérea y otras partes interesadas (es decir, empresas de servicios de escala, proveedores de servicios de mantenimiento, proveedores de servicios de seguridad, empresas proveedoras de combustible, agentes de carga, etc.), dependen cada vez más de la tecnología de la información y las comunicaciones (ICT) para sus operaciones.

2. INICIATIVAS PARA HACER FRENTE A LAS CIBERAMENAZAS

2.1 En los últimos años, las partes interesadas de la aviación civil han venido prestando más atención a las ciberamenazas. En 2014, la OACI, la Asociación del Transporte Aéreo Internacional (IATA), el Consejo Internacional de Aeropuertos (ACI), la Organización de servicios de navegación aérea civil (CANSO) y el Consejo Coordinador Internacional de Asociaciones de Industrias Aeroespaciales (ICCAIA) emitieron un plan de acción conjunto para hacer frente a estos desafíos. La IATA también desarrolló un conjunto de información sobre ciberseguridad para las líneas aéreas, en tanto que muchos aeropuertos, proveedores de servicios de navegación aérea y fabricantes de aeronaves emprendieron diversas medidas para reforzar la seguridad de sus operaciones contra las ciberamenazas.

2.2 A nivel internacional, los encargados de la reglamentación de la seguridad de la aviación civil ya han abordado cuestiones de ciberseguridad en el Grupo de expertos sobre seguridad de la aviación (AVSECP) de la OACI. El Grupo de trabajo sobre amenazas y riesgos (WGTR) del AVSECP ha presentado una serie de evaluaciones y dado asesoramiento al grupo de expertos con respecto al riesgo de ciberataques, y se inició la coordinación entre el AVSECP y los grupos de expertos de la OACI que se ocupan de la seguridad operacional a fin de simplificar las iniciativas sobre este tema común.

2.3 A pesar de estas medidas, muchas partes interesadas siguen intentando combatir estos desafíos. Crear conciencia y promover el diálogo entre las partes interesadas acerca de las ciberamenazas sería de utilidad como medida para ayudar a entender mejor esta cuestión. Realizar evaluaciones de riesgos detalladas permitirá a las partes interesadas identificar las lagunas de seguridad de la aviación, de manera que puedan tomarse las medidas necesarias para llenarlas. En julio de 2015, Singapur organizó una conferencia sobre ciberseguridad en asociación con la OACI y la IATA, que fue apoyada por varios Estados y partes interesadas de la industria, en la cual participaron expertos de todo el ecosistema de la aviación civil para analizar la cuestión de las ciberamenazas. Entre los participantes figuraron explotadores de aeropuertos, líneas aéreas, fabricantes de motores de aeronaves, proveedores de servicios de escala, de servicios de seguridad y de equipo de seguridad, organizaciones internacionales relacionadas con la aviación civil y encargados de la reglamentación. Las siguientes son algunas de las cuestiones que se debatieron:

a) las amenazas y los riesgos que plantean los ciberataques para el sistema mundial de la aviación civil: la OACI y las partes interesadas pueden aprovechar las evaluaciones periódicas que ha realizado el WGTR de estas amenazas y riesgos para desarrollar medidas preventivas y de respuesta que resulten eficaces;

b) consideraciones respecto a medidas preventivas y de respuesta, así como medidas de contingencia y de recuperación en caso de un ciberataque contra operaciones de la aviación civil;

c) medidas que algunas partes interesadas han emprendido para enfrentar las ciberamenazas;

d) el hecho de que el sector de la aviación civil se encuentra particularmente en riesgo, ya que es más probable que los ciberataques tengan éxito en un sector cuyas partes componentes son altamente interdependientes y, también, porque los mecanismos de ciberdefensa con los que el sector de la aviación civil cuenta actualmente aún no son adecuados para enfrentar esta amenaza que evoluciona rápido; y

e) la necesidad de un enfoque horizontal que incluya a todo el sector de la aviación para garantizar una aplicación coordinada, proporcionada y eficaz.

3. POSIBLES MEDIDAS DE LOS ENCARGADOS DE LA REGLAMENTACIÓN Y DE LAS PARTES INTERESADAS

3.1 Se identificaron varias posibles medidas de los encargados de la reglamentación y de las partes interesadas, por ejemplo:

a) La asignación urgente de la responsabilidad de la cuestión, comenzando a **nivel mundial**, para lo cual sería de utilidad que la **OACI estableciera un marco mundial para que las partes interesadas de la aviación civil hagan frente a las ciberamenazas**. Este marco, que debería basarse en las mejores prácticas actuales en materia de seguridad de la información y desarrollarse en estrecha consulta con expertos en seguridad de la aviación y seguridad operacional, podría contener un conjunto de principios, directrices y enfoques para los encargados de la reglamentación y la industria.

b) **A nivel estatal, es importante que las autoridades de seguridad de la aviación (en coordinación con otras autoridades responsables de la ciberseguridad a nivel nacional) creen un mecanismo de supervisión normativa y proporcionen dicha supervisión para hacer frente a las ciberamenazas**. El régimen de supervisión normativa debería abarcar el sector de la aviación civil y todas las partes que intervienen en el ecosistema de aviación civil, desde un punto de vista holístico, en virtud de su interdependencia.

c) **A nivel de cada parte interesada, cada interesado necesita establecer su propio conjunto de medidas para proteger sus operaciones contra las ciberamenazas, especialmente con respecto a sistemas importantes para la seguridad operacional y la seguridad de la aviación**.

d) Las partes interesadas deben responder a las ciberamenazas lo antes posible. Por lo tanto, es importante que el sector de la aviación civil **desarrolle medidas de pronta detección, coordinación y corrección.** La notificación de incidentes de ciberseguridad a equipos de respuesta a emergencias informáticas (CERT) o a centros de intercambio y análisis de información (ISAC) proporcionaría un aviso oportuno a otras partes interesadas, la cual debería promoverse a nivel nacional con la coordinación internacional dirigida por la OACI.

e) Dado que la evolución de las amenazas y las nuevas tendencias tecnológicas impulsan la ciberseguridad, **es necesario integrar todos los elementos, como son la gente, el proceso, la tecnología y los sistemas, a fin de garantizar que en cada uno de esos elementos haya capacidad funcional para identificar y mitigar las amenazas**.

f) **Es esencial compartir entre los organismos información y mejores prácticas sobre la ciberseguridad de la aviación civil**. Esto ayudará a los Estados y a las partes interesadas a, en forma conjunta y de manera colectiva, detectar las tendencias, identificar las amenazas y desarrollar contramedidas eficaces. También es importante que los organismos encargados de los servicios de información y otros organismos pertinentes sigan esforzándose por mejorar la comprensión de las ciberamenazas que pesan sobre la aviación civil.

g) Dada la naturaleza interconectada de los sistemas de información de la aviación civil, **es necesaria una idea común sobre qué sistemas y datos son críticos o esenciales para la seguridad operacional, la seguridad de la aviación y el funcionamiento continuo del sistema de la aviación civil**. Los encargados de la reglamentación de la aviación deberían definir conjuntamente criterios para los sistemas que se consideran críticos (a escala mundial, regional y/o nacional), para que sirvan de guía en el proceso de implantación.

h) **Es importante que se imparta instrucción al personal de la aviación civil en todo el ecosistema de este sector para que adquiera consciencia de las amenazas y los riesgos que plantean los ciberataques y para que responda rápido y en forma adecuada**. Detectar anomalías y dar temprano la alerta sobre toda novedad o actividad sospechosa podría impedir o contener un ciberataque y reducir al mínimo la alteración de las operaciones. Es importante incluir en los programas de instrucción en seguridad de la aviación los desafíos que plantea la ciberseguridad, así como contratar especialistas y auditores en seguridad de la aviación que estén familiarizados con la ciberseguridad.

i) **También será importante intensificar la cultura de seguridad de la aviación para que haya una mejor comprensión de las ciberamenazas**. Si el personal directivo superior hace suya la necesidad de ocuparse de estas amenazas y apoya firmemente la instrucción del personal y la inversión en recursos para hacer frente a las mismas, el sector de la aviación civil será capaz de hacer frente a ellas con mayor eficacia.

— FIN —