Organización de Aviación Civil Internacional

A40-WP/105
TE/33
30/7/19

NOTA DE ESTUDIO

ASAMBLEA — 40º PERÍODO DE SESIONES

COMISIÓN TÉCNICA

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

HABILITANDO LA AVIACIÓN DIGITAL A TRAVÉS DEL DESARROLLO CIBERNÉTICO DEL PERSONAL DE ELECTRÓNICA DE SEGURIDAD DEL TRÁNSITO AÉREO (ATSEP)

[Nota presentada por la Federación Internacional de Asociaciones de Especialistas en Sistemas Electrónicos para la Seguridad Operacional del Tránsito Aéreo (IFATSEA)]

RESUMEN

La próxima generación de personal operativo, de tripulaciones aéreas y de controladores de tráfico aéreo (ATCO) dependerá cada vez más de la capacidad técnica y de gestión de los ATSEP para resistir las amenazas cibernéticas a los sistemas de información y a las infraestructuras CNS que protegen a los viajeros civiles. La obligación de los Estados de identificar infraestructuras críticas y establecer un Equipo de Respuesta a Emergencias Informáticas se superpone con la responsabilidad personal de los ATCO y ATSEP. También hay superposiciones entre infraestructuras críticas. Si hay un ataque en las infraestructuras más amplias que soportan los sistemas ATM, el ATSEP de Seguridad tiene un papel claro que desempeñar en la coordinación de la recuperación, al tiempo que debe garantizar que las operaciones de ATM se mantengan seguras.

Decisión de la Asamblea: Se invita a la Asamblea a considerar la información contenida en esta nota de estudio y solicitar al Consejo que tome las medidas necesarias para desarrollar un nuevo rol de ATSEP de seguridad física, seguridad operacional y ciberseguridad, así como la capacitación correspondiente asociada a esta nueva figura.

Objetivos estratégicos:	Esta nota de estudio se relaciona con los Objetivos estratégicos: Seguridad operacional, Capacidad y eficiencia de la navegación y Seguridad de la aviación y facilitación.
Repercusiones financieras:	Se espera que el coste asociado a la implementación del nuevo rol de ATSEP sea mínimo, ya que simplemente amplía la implementación actual de la instrucción y capacitación basada en competencias descrita en el Doc 10057.
Referencias:	Anexo 10 — Telecomunicaciones Aeronáuticas, Volúmenes I, II, III y IV Doc 8071, *Manual sobre ensayo de radioayudas para la navegación* Doc 9683, *Manual de instrucción sobre factores humanos* Doc 9868, *Procedimientos para los servicios de navegación aérea — Instrucción* (PANS-TRG) Doc 10057, *Manual sobre capacitación y evaluación basadas en competencias del personal de electrónica de seguridad del tráfico aéreo*

1. INTRODUCCIÓN

1.1 En todo el mundo existen planes para desarrollar nuevas infraestructuras que admitan la gestión del tráfico aéreo, por ejemplo: el Sistema de transporte aéreo de la próxima generación (NextGen) y Programa de investigación ATM en el marco del cielo único europeo (SESAR). Todas estas visiones se basan en metodologías muy fiables de comunicación y procesamiento digital. El desarrollo seguro y con éxito de estas grandes y complejas infraestructuras plantea múltiples desafíos, incluyendo la necesidad de integrar nuevas tecnologías con sistemas preexistentes. Estos sistemas ATM digitales, punteros e interoperables necesitan que la ciberseguridad esté plenamente integrada en su seno a fin de poder garantizar la integridad y la seguridad de las operaciones de tránsito aéreo. A su vez, esto requiere que el personal especialista en sistemas electrónicos para la seguridad operacional del tránsito aéreo (ATSEP) disponga de todo un nuevo conjunto de capacidades dinámicas. Es evidente que la naturaleza de las amenazas cibernéticas a la aviación cambiará con el tiempo. Esta presentación propone un enfoque práctico y sistemático del desarrollo de la formación, la pedagogía y la instrucción basada en competencias que permita habilitar a una nueva generación de personal capaz de llevar a cabo nuestra visión de la aviación digital.

2. EXPOSICIÓN

Seguridad física y operacional en ATM/ANS

2.1 Los nuevos reglamentos (US PPD-21, EU 2016/1148) requieren cada vez más que los Estados definan sus infraestructuras críticas e identifiquen las crecientes interdependencias que aparecen entre ellas, por ejemplo, entre telecomunicaciones digitales y sistemas de gestión del tránsito aéreo.

2.2 Actualmente muchos proveedores de servicios de navegación aérea (ANSP) carecen de experiencia cibernética; esto es natural, ya que en el pasado los niveles de amenaza eran muy bajos. A menudo también carecen de personal bien cualificado. Muchos ANSPs han afrontado esta limitación contratando consultorías externas de ciberseguridad. A menudo se firman contratos con compañías que no pertenecen al sector de la aviación sin tener en cuenta que estas carecen del conocimiento suficiente del sector que es necesario a fin de mantener la seguridad y el éxito de las operaciones. Puede ser difícil para los consultores externos convencer a los ATCO de la amenaza potencial para las operaciones que puede derivarse del *malware* que consigue atravesar la “cámara de aire” que mantiene a sus sistemas aislados de la Internet pública. Por ello, es frecuente que las compañías externas tengan un efecto muy limitado sobre la capacidad de adaptación de muchos estados miembros. Además, el desarrollo de una cultura de seguridad fuerte, como en el campo de la seguridad operacional, es más efectivo cuando se desarrolla de forma interna. Dentro de la estructura de los proveedores ATS, las compañías externas carecen de la influencia necesaria sobre los ATSEP, que son responsables de los sistemas técnicos, y sobre los ATCO, que dependen de los sistemas para proporcionar los servicios de tránsito aéreo.

2.3 Los ATSEP desempeñan un rol cada vez más importante en la protección de todas esas interfaces críticas (ICAO A39.WP17 EX / 5). Por ejemplo, la mayoría de los países han desarrollado o están empezando a desarrollar un equipo de intervención en caso de emergencia informática (Computer Emergency Response Team, CERT), que recaen bajo la responsabilidad de los ATCO y los ATSEP. Sin embargo, el tratamiento de la ciberseguridad en la formación de los ATSEP es inconsistente, en el mejor de los casos, y, en el peor, se realiza meramente *ad hoc*.

Contexto Político y Legislativo

2.4 La importancia de estos problemas ha sido reconocida y recogida en toda una serie de documentos. Entre ellos se encuentran determinados aspectos de los servicios de la Administración Federal de Aviación (FAA), Enterprise Network Services (ENS), así como el Reglamento (EC) núm. 300/2008 del Parlamento Europeo y de la Comisión, de 11 de marzo de 2008, sobre normas comunes para la seguridad de la aviación civil. En otras regiones del mundo existe el peligro de que algunos países puedan quedarse aún más retrasados en cuanto respecta a la ciberseguridad. Existe la necesidad de una orientación más clara respecto a las medidas apropiadas para proteger nuestro futuro común en las infraestructuras de la aviación digital, especialmente teniendo en cuenta que el Reglamento (EU) Nº 1254/2009 permite a los Estados Miembros derogar parte de los estándares comunes básicos de seguridad operacional en la aviación civil y adoptar medidas de seguridad alternativas. La Secretaria General de la OACI, la Dra. Fang Liu, también subrayó la importancia de una visión tan clara como esta durante el Fórum OACI-EASA el 21 de septiembre de 2018.

3. CONCLUSIÓN

3.1 Propuesta de desarrollo de un nuevo rol de ATSEP de seguridad física, seguridad operacional y ciberseguridad, así como de la capacitación correspondiente asociada a esta nueva figura.

3.2 Sugerimos que se cree, para el personal ATSEP, una nueva cadena de seguridad operacional, seguridad física y ciberseguridad que complemente sus actuales conocimientos relativos a las infraestructuras de la aviación con unas bases sólidas en cuanto se refiere tanto a las amenazas que afrontan dichas infraestructuras como a los medios para defenderlas. Concebimos una competencia que se extienda a áreas anexas en otras infraestructuras críticas; esto ampliaría la capacidad de adaptación al cambio de la aviación, que a su vez se basa en extensas cadenas de suministro que utilizan tecnologías digitales de mercado de amplia difusión y que son bien conocidas por hackers y por agencias estatales.

3.3 Llamamos la atención sobre este asunto porque los diversos estados miembros están aplicando estrategias radicalmente diferentes en cuanto a la ingeniería de la ciberseguridad en las operaciones ATM, aun cuando todos confiamos en las capacidades de nuestros vecinos para mantener las redes de transporte.

3.4 Además, IFATSEA propone que se establezca una nueva rama de formación en ciberseguridad en la que las cualificaciones de acceso estén definidas en cooperación con los Estados o con los Proveedores de Servicios de Navegación Aérea, pero siempre con el objetivo común de aumentar la confianza en la resiliencia de las infraestructuras de aviación de nuestros vecinos, puesto que de este modo todas ellas estarán protegidas por ATSEP con alta cualificación.

3.5 Asimismo, IFATSEA le ofrece asistencia a la OACI en las cuestiones relativas a la formación de los ATSEP, en la implementación y en la operación de sistemas técnicos y funciones.

— FIN —