Organización de Aviación Civil Internacional

HLCAS/2-WP/18
16/10/18

NOTA DE ESTUDIO

SEGUNDA CONFERENCIA DE ALTO NIVEL SOBRE SEGURIDAD DE LA AVIACIÓN (HLCAS/2)

Montreal, 29 – 30 de noviembre de 2018

Cuestión 2: Futuros enfoques de gestión de riesgos en el ámbito de la seguridad de la aviación

ELABORACIÓN DE UNA ESTRATEGIA MUNDIAL DE CIBERSEGURIDAD

(Nota presentada por Rumania)

RESUMEN

En esta nota se presentan recomendaciones a los Estados y la industria, que deberían apoyar activamente la elaboración de una estrategia mundial de ciberseguridad en la aviación civil.

Las medidas propuestas a la Conferencia de alto nivel sobre seguridad de la aviación figuran en el párrafo 4.

1. INTRODUCCIÓN

1.1 La Cumbre sobre ciberseguridad en la aviación civil para Europa, Oriente Medio y África se celebró en Bucarest (Rumania), del 7 al 9 de mayo de 2018. Concurrieron a esa cumbre 416 delegados de 55 Estados y 19 organizaciones internacionales. En la cumbre se debatió la manera de armonizar y promover marcos de ciberseguridad.

1.2 La cumbre recordó la *Declaración de Dubai sobre ciberseguridad en la aviación civil*, presentada inicialmente en Dubai el 5 de abril de 2015. Asimismo, reconoció la labor del Grupo de estudio de la Secretaría de la OACI sobre ciberseguridad (SSGC) y su labor continua con miras a considerar todos los elementos del marco de la aviación internacional que puedan verse afectados por ciberincidentes.

2. ANÁLISIS

2.1 Hace un decenio, la ciberseguridad recibía poca atención como problema internacional en la industria de la aviación. Desde el comienzo de la década actual, los expertos en aviación han advertido que un ciberataque malicioso a las operaciones de aviación civil podría resultar catastrófico. Como la tecnología transforma radicalmente el diseño, la producción, la operación y el mantenimiento, se deben adaptar los modelos de seguridad de la aviación y seguridad operacional.

2.2 El ciberespacio se ha convertido en un sustrato esencial para las interacciones económicas, sociales y políticas. Sin embargo, con el aumento de la interdependencia y las oportunidades económicas llegaron también la vulnerabilidad y la inseguridad. Con los macrodatos, el aprendizaje de computadora y la Internet de las cosas, algunos expertos prevén que la cantidad de conexiones a Internet aumentará hasta llegar a casi un billón para 2035. La cantidad de posibles blancos de ataque, tanto de los actores privados como del estado, aumentará considerablemente e incluirá desde sistemas de controles industriales hasta marcapasos, automóviles sin conductor, drones y, por último pero no por eso menos importante, la aviación civil.

2.3 Al igual que otras industrias que adoptaron la “revolución digital”, la aviación debe mantener la confianza de las partes interesadas percibiendo correctamente las vulnerabilidades y oportunidades y entendiendo las amenazas de los adversarios. A continuación figuran las amenazas que enfrenta una aviación civil conectada y digitalizada:

2.3.1 A medida que la industria de la aviación conecta cada vez más a los sistemas y servicios, la superficie de ataque posible de los sistemas con los que podría interactuar un adversario es de un tamaño y complejidad crecientes, lo que la convierte en un blanco más grande.

2.3.2 Como la industria de la aviación depende en gran medida de la tecnología, cada vez más en el entorno cibernético, entender y superar las diferencias culturales entre las dos industrias requerirá una reforma mundial. El desarrollo de una cultura compartida, donde se consideren las dificultades y posibles soluciones en conjunto, requerirá una cooperación multidisciplinar.

2.3.3 La percepción de la amenaza que representa la potencia digital será fundamental para entender y gestionar los riesgos. Es necesario que todos los que forman parte de la industria alcancen el mismo nivel de percepción y comprensión para abordar el posible riesgo y promover un diálogo en colaboración en que se valoren múltiples perspectivas.

2.3.4 La industria de la aviación tiene décadas de experiencia en materia de enfrentar problemas de seguridad de la aviación y seguridad operacional, pero el desafío que plantea la ciberseguridad es comparativamente nuevo. Tal vez desarrollar y remplazar los sistemas de aviación lleve más tiempo que el que insume para los perpetradores el desarrollo de capacidades, lo que genera un problema para la correcta evaluación de riesgos y los modelos de amenazas.

2.3.5 Las inversiones en gestión del tránsito aéreo (ATM) ya están rindiendo frutos, pero el uso de tecnologías de avanzada como los sistemas mundiales de determinación de la posición (GPS), las comunicaciones digitales y la vigilancia dependiente automática — radiodifusión (ADS-B) significa que debemos gestionar las vulnerabilidades que surgen de esas tecnologías y alentar la ciberresiliencia.

2.3.6 Los aeropuertos son federaciones de varias organizaciones distintas con enfoques posiblemente diferentes, y la vulnerabilidad cibernética de una puede afectar a todas las demás. Una protección adecuada de los sistemas de seguridad física de las ciberamenazas en los aeropuertos es fundamental.

2.3.7 Se han acordado y se comprenden las políticas y reglamentos nacionales e internacionales para la seguridad operacional y la seguridad física, pero todavía no está claro de qué manera la ciberseguridad de la aviación puede alcanzar la misma madurez y

claridad. Es por eso que la OACI, la AESA, EUROCONTROL, la CEAC y otras entidades multilaterales deben seguir trabajando codo a codo para elaborar políticas y reglamentos, sistemas de pensamiento coherentes, gobernanza y rendición de cuentas, confianza resiliente y proceso seguro y humano de toma de decisiones en un entorno cibernético compartido, multifuncional y transfronterizo.

2.3.8 La OACI se encuentra en condiciones de reunir las numerosas iniciativas de ciberseguridad de la aviación mundial, ofrecer coherencia y liderazgo y establecer normas. Para promover la coherencia en la elaboración de normas de ciberseguridad entre las naciones y fomentar el diálogo y la colaboración entre partes interesadas dispares, es necesario efectuar una evaluación crítica de los Anexos (8, 10, 17, 18, etc.) del Convenio de Chicago, que deberán ser enmendados en consecuencia desde el punto de vista de la ciberseguridad. Es verdaderamente necesario reconocer que la interferencia ilícita a través de medios cibernéticos ya es una realidad e incorporar perspectivas cibernéticas con numerosos paralelos con el actual enfoque físico.

2.3.9 El desarrollo de capacidades en materia de ciberseguridad –la sinergia entre las personas, la tecnología y los procesos– mediante un enfoque operativo basado en una red de información y la capacidad de detectar, proteger, defender, analizar, decidir y reaccionar, además de restaurar, garantizará la resiliencia de la aviación civil en el futuro cercano.

2.3.10 El intercambio de información amplio y oportuno reducirá los riesgos al mínimo, y el valor agregado de esa labor en colaboración es una mejor gestión de la ciberseguridad para las partes interesadas. El recientemente establecido Centro Europeo de Ciberseguridad en la Aviación con vínculos con CERT UE, el Centro de intercambio y análisis de información sobre la aviación o centros de operaciones de seguridad de la aviación son multiplicadores de la fuerza de la ciberseguridad para los Estados miembros.

2.3.11 También es importante el intercambio de información cívico-militar. Tal vez la aviación civil pueda aprender una lección a partir de la manera en que las fuerzas armadas perciben y abordan el desafío de asegurar las aeronaves y sistemas dentro de entornos que enfrentan interferencia deliberada y por simulación de señales en la radiofrecuencia y ciberamenazas.

2.3.12 La AESA elaboró la “Declaración de Bucarest sobre iniciativas de alto nivel en la ciberseguridad de la aviación civil” que se centra en varios objetivos, como la coordinación a nivel europeo, cooperación internacional, evaluaciones de riesgos, incremento de la concientización, intercambio de información e investigación y desarrollo. También se deseaba que los reglamentos se armonizaran a nivel internacional dado que estos desafíos requieren un abordaje integral y más amplio.

3. CONCLUSIÓN

3.1 Considerando que para desarrollar un ciclo de vida de la ciberseguridad, la gestión de riesgos cibernéticos comprende desde el concepto, diseño, aseguramiento, suministro, construcción, entrega, operaciones y mantenimiento; por lo tanto es necesario contar con un enfoque abarcador, amplio e integrador. Para salvar la brecha entre la situación actual y el resultado deseado es necesario actuar cuanto antes para enfrentar los riesgos y amenazas del nuevo entorno cibernético.

3.2 Los funcionarios y representantes de los Estados, las organizaciones regionales e internacionales y las industrias que participamos en la Cumbre de la OACI sobre ciberseguridad en la aviación civil para Europa, Oriente Medio y África, celebrada en Bucarest (Rumania), del 7 al 9 de mayo de 2018 para abordar los desafíos de las ciberamenazas a la aviación civil internacional.

3.3 Conscientes de la necesidad de garantizar la seguridad operacional, la seguridad de la aviación y la continuidad de la aviación civil de manera ordenada, recomendamos que:

3.3.1 Se elaboren marcos de ciberseguridad de los Estados y la industria de manera armonizada en la máxima medida posible;

3.3.2 Los Estados y la industria fomenten la cooperación regional en la definición de estrategias comunes, intercambio de información y mejores prácticas, siguiendo el ejemplo de las iniciativas ya existentes;

3.3.3 Se promuevan marcos de confianza para permitir el intercambio seguro de información cuando corresponda;

3.3.4 Los Estados y la industria colaboren para identificar las necesidades de recursos humanos a largo plazo y establezcan estrategias para atraer, educar y retener a la próxima generación de profesionales de la aviación; y

3.3.5 Los Estados y la industria apoyen activamente la elaboración de una estrategia mundial de ciberseguridad bajo los auspicios de la Organización de Aviación Civil Internacional.

4. MEDIDAS PROPUESTAS A LA CONFERENCIA DE ALTO NIVEL

4.1 Se invita a la Conferencia de alto nivel sobre seguridad de la aviación a respaldar las conclusiones y apoyar la necesidad de un enfoque abarcador, amplio e integrador en la esfera de la ciberseguridad.

— FIN —