



DECIMOTERCERA CONFERENCIA DE NAVEGACIÓN AÉREA

Montreal, Canadá, 9 al 19 de octubre de 2018

COMITÉ A

Cuestión 5 del orden del día:

5.4:

Cuestiones emergentes
Ciberresiliencia

NOCION DE SISTEMA-DE-SISTEMAS EN LA CIBERSEGURIDAD EN AVIACION

(Presentado por Canadá, por Austria en nombre de la Unión Europea y sus Estados Miembros², y los otros Estados Miembros de la Conferencia Europea de Aviación Civil³, por EUROCONTROL y por Singapur. Co-esponsorizado por Australia y Nueva Zelanda)

RESUMEN

Esta nota introduce brevemente el concepto de sistema-de-sistemas, y describe por qué este enfoque sería adecuado con el fin de abordar las consideraciones de ciberseguridad en la aviación civil. Esta nota también introduce la noción de seguridad-por-diseño, y cómo la integración de este concepto en el sistema de aviación mejorará su resiliencia.

Medidas propuestas a la Conferencia:

Se invita a la Conferencia a acordar con las recomendaciones del párrafo 3.

1. INTRODUCCIÓN

1.1 La disponibilidad de información precisa y el funcionamiento correcto de los sistemas de seguridad críticos son un pre-requisitos para un sistema de aviación civil seguro y protegido en un momento en el que el sector se encuentra ante una progresiva digitalización. El sistema de aviación está altamente integrado y la información se difunde globalmente. Por lo tanto, las iniciativas de ciberseguridad en el sector de la aviación deben tomar un enfoque holístico y de punta-a-punta.

1.2 Un enfoque holístico y de punta-a-punta solo puede tener éxito si la aviación es entendida como un “sistema-de-sistemas”, en el que todos los miembros de la comunidad aeronáutica compartan la responsabilidad. El sistema de aviación está compuesto por una variedad de redes y aparatos que cada vez son más interdependientes y están más interconectados para el intercambio de datos e información digital.

¹ La versión en chino fue proporcionada por Singapur.

² Alemania, Austria, Bélgica, Bulgaria, Chipre, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, Rumanía y Suecia.

³ Albania, Antigua República Yugoslava de Macedonia, Armenia, Azerbaiyán, Bosnia y Herzegovina, Georgia, Islandia, Mónaco, Montenegro, Noruega, República de Moldavia, San Marino, Serbia, Suiza, Turquía y Ucrania.

Al mismo tiempo, las partes interesadas tal como Estados, operadores de aeronaves y aeropuertos, proveedores de servicios de navegación aérea (ANSPs) y otros, cada vez dependen más para su operación diaria de sistemas con tecnología de comunicaciones e información altamente interconectada e inter-operativa (ICT).

1.3 Desarrollos tales como la Gestión de Información de Todo el Sistema (SWIM), la introducción de aeronaves a control remoto (RPAS) y la futura aparición de usuarios del espacio aéreo que todavía no están operacionales, ha incrementado esta interdependencia. El sistema de aviación del futuro por lo tanto requiere un diseño más concertado y una menor evolución individualizada para poder mantener su resiliencia contra interferencias cibernéticas.

1.4 La evolución hacia los sistemas de información interconectados e inter-operativos mencionados anteriormente también crea nuevas vulnerabilidades. Los eventos cibernéticos pueden impactar a la aviación a diferentes niveles y pueden poner en peligro el funcionamiento del sistema de navegación aérea y la seguridad global del sector. Estos eventos pueden influir en los intercambios de información entre las partes interesadas, directamente afectando a la seguridad, protección, capacidad y eficiencia, y con repercusiones potencialmente severas.

2. ANÁLISIS

2.1 **La aviación como un sistema-de-sistemas (SoS)** – en el sector aeronáutico, muchas partes interesadas juegan, directa o indirectamente, un papel en el funcionamiento y mantenimiento tanto de los sub-sistemas individuales como del sistema global – siempre entendiendo que un sistema puede abarcar tanto a productos, personas y procesos. Cada uno de estos sub-sistemas depende directamente de otros sub-sistemas para poder funcionar correcta y eficientemente; a su vez, cada uno de estos sub-sistemas también tiene un impacto importante en los otros sistemas cuando no funciona correctamente.

2.2 **La aviación como un sistema-de-sistemas (SoS)** – en el sector aeronáutico, muchas partes interesadas juegan, directa o indirectamente, un papel en el funcionamiento y mantenimiento tanto de los sub-sistemas individuales como del sistema global – siempre entendiendo que un sistema puede abarcar tanto a productos, personas y procesos. Cada uno de estos sub-sistemas depende directamente de otros sub-sistemas para poder funcionar correcta y eficientemente; a su vez, cada uno de estos sub-sistemas también tiene un impacto importante en los otros sistemas cuando no funciona correctamente.

2.3 Dado que estos sub-sistemas tienen funciones individuales que están enlazadas unas a otras para conseguir unos objetivos comunes (por ejemplo, las comunicaciones entre el control de tráfico aéreo y los pilotos, o los datos de seguimiento de localización entre los centros de control de operaciones y la aeronave), el comprometer uno de estos sub-sistemas podría afectar adversamente el funcionamiento global de la cadena completa de sub-sistemas. Es por ello que la gestión de los riesgos de ciberseguridad ha de hacerse mediante un enfoque holístico, con el fin de reducir el alcance de las amenazas a las funcionalidades centrales del sistema.

2.4 **Ciberseguridad: un asunto en continuo progreso evolutivo** – dado el carácter evolutivo del SoS descrito anteriormente, la ciberseguridad debe ser igualmente un asunto en continuo progreso dentro de las distintas partes interesadas del SoS de la aviación. Es igualmente imperativo que el SoS de la aviación mantenga las condiciones de ciberseguridad necesarias a través de una suficiente flexibilidad y adaptabilidad, dado que sus componentes interaccionan permanentemente y de diferentes modos entre ellos (por ejemplo, aeronaves interaccionando con diferentes proveedores de servicios de navegación aérea cuando transitan a través de diferentes regiones de información de vuelo).

2.5 Por lo tanto, el desarrollo y mantenimiento de dicha ciberresiliencia a través del SoS requiere una continua coordinación entre las partes interesadas (ver el párrafo 2.2), con el fin de mantener la flexibilidad y adaptabilidad necesaria para que el SoS de aviación funcione correctamente.

2.6 Un reto importante para alcanzar este objetivo es el concepto de “componibilidad” – la posibilidad de integrar de modo seguro múltiples elementos (componentes en el caso de sistemas, o sub-sistemas en el caso del SoS) dentro de entidades más grandes. El reto principal es la desviación que esto implica con respecto al paradigma de seguridad, por el cual la integración de elementos se ha enfocado principalmente basándose en su funcionalidad e interacciones a través de su interfaz. Desde una perspectiva de ciberseguridad, la integración de elementos individuales también requiere considerar cuidadosamente como los aspectos de ciberseguridad de cada elemento contribuyen al estado global de ciberseguridad. Una pregunta fundamental para lograr esto es cómo se puede apoyar a los Estados y regiones (y a otras partes interesadas) en su proceso de desarrollo, de forma que el SoS pueda ser protegido efectivamente de los ciber-ataques a pesar de las inevitables variaciones existentes entre los sub-sistemas.

2.7 Para alcanzar dicha meta, la integración de los sub-sistemas individuales requerirá considerar e integrar cuidadosamente los entornos de seguridad nativos de cada sub-sistema, de forma que emerja un entorno holístico y ciberresiliente. Los enfoques descoordinados hacia la ciberseguridad pueden desembocar en vulnerabilidades no detectadas. Los solapes de las defensas percibidas en los sistemas pueden ser igualmente peligrosas, dado que dicho escenario podría resultar potencialmente en una superficie viable de ataque al SoS de aviación.

2.8 Por lo tanto, es esencial tomar un enfoque global coordinado hacia la gestión de las interacciones de los sistemas, y algo fundamental para ello es una visión común sobre cómo estos sistemas y sub-sistemas interactúan.

2.9 **Integración de la seguridad-por-diseño de los sistemas de aviación** – para lograr que el SoS de la aviación alcance el nivel deseado de ciberresiliencia, es importante que las consideraciones de ciberseguridad sean incorporadas desde el inicio del desarrollo del sistema, en contraposición a considerarlas de forma retroactiva. Esto permitiría una mejor consideración de los interfaces entre los sub-sistemas, de forma que estas interacciones tengan lugar de un modo seguro y eficiente.

2.10 La mayoría de los estándares de seguridad actuales se centran en medidas mitigadoras tomadas e implementadas *dentro* del contexto de la organización. Sin embargo, hay una necesidad imperiosa de ajustar el enfoque de dichas medidas con el fin de incluir medidas que tengan asimismo en cuenta la perspectiva inter-organizativa. Esto permitiría asegurar la seguridad global del SoS, más allá de crear seguridad a través una amalgama de sub-sistemas que sean individualmente seguros.

2.11 Sin una gestión adecuada, las estrategias descoordinadas en relación a la ciberseguridad de sub-sistemas de aviación puede implicar un riesgo para el sistema como un todo. Esta falta de coordinación viene potencialmente originada por una comunicación insuficiente entre los gestores de los sub-sistemas y otras partes interesadas durante el desarrollo y diseño de estrategias de ciberseguridad.

2.12 A través de niveles múltiples de coordinación (por ejemplo, entre los Estados como gestores de los sistemas de aviación domésticos, los gestores de sub-sistemas dentro de los sistemas de aviación domésticos, etc.) entre distintos niveles de sub-sistemas, así como asegurando que los sub-sistemas individuales están de por sí adecuadamente protegidos, los Estados estarían contribuyendo a un SoS de aviación que mantenga una defensa en profundidad como el resultado natural de dicho trabajo.

2.13 **Trabajo futuro** – Ese trabajo de incorporar la seguridad-por-diseño como parte del diseño inicial de sistemas no debería sustituir las buenas prácticas perfeccionadas por la comunidad

aeronáutica a lo largo de muchas décadas de experiencia en el desarrollo de sistemas de aviación y de trabajo en los retos de la ciberseguridad. Incorporando dichos principios de seguridad-por-diseño en paralelo al enfoque tradicional de redundancia de sistemas, así como el énfasis en maximizar la facilidad de acceso a datos y sistemas operacionales, las partes interesadas contribuirán a reforzar el SoS de aviación en sus políticas de ciberresiliencia, a la vez que mantienen la efectividad operacional.

2.14 Como parte de la variedad de conceptos y soluciones operacionales discutidos en la actualidad en los diferentes foros aeronáuticos, es importante que los Estados y la industria tomen en cuenta las consideraciones anteriormente mencionadas durante el proceso de desarrollo y diseño. Por extensión, la comunidad podría también evolucionar su trabajo colectivo hacia la mejor identificación de sub-sistemas representativos e investigar en qué medida sus resultados – basados en las medidas tomadas y las prácticas utilizadas – pueden ser transferidos a otros sub-sistemas con el fin de mejorar la ciberresiliencia en todo el espectro de sistemas.

2.15 De forma similar, y una vez asegurado el éxito en dicha tarea, la comunidad aeronáutica podría considerar trabajar en el progresivo desarrollo de sub-sistemas más grandes, de forma que tengan en consideración la seguridad de la información durante la fase inicial de diseño. Conforme dicho trabajo progrese y madure, las partes interesadas podrían comenzar a explorar colectivamente si existen candidatos adecuados y de confianza que puedan ser encargados con la responsabilidad de desarrollar y mantener dichos sistemas, que sean seguros-por-diseño, y si dicho proceso es posible para el sistema global de aviación en el futuro.

2.16 A través de la continua dedicación de esfuerzos en el área de la ciberresiliencia de sistemas, la comunidad aeronáutica contribuirá de modo efectivo a una operación segura y eficiente del ecosistema aeronáutico (SoS) hasta bien entrado el futuro.

3. CONCLUSIÓN

3.1 Se invita a la Conferencia a acordar con las siguientes recomendaciones:

Que la Conferencia:

- a) Urja a ICAO y a los Estados a reconocer que la ciberresiliencia del sistema de aviación depende de la continua coordinación entre todas las partes interesadas;
- b) solicite a ICAO reconocer el concepto de sistema-de-sistemas (SoS), requiriendo la necesidad de colaboración y coordinación entre los gestores de los sub-sistemas, en particular durante el desarrollo, integración, operación y mantenimiento de sub-sistemas que sean “seguros-por-diseño”;
- c) urja a ICAO a desarrollar un marco que requiera y guíe a los Estados en la implementación de medidas que mitiguen los riesgos y amenazas de ciberseguridad sobre los sistemas de aviación civil. Esto podría resultar en el desarrollo de SARP’s relativas a diversos Anexos de ICAO; y
- d) Reconozca los conceptos contenidos en la Nota Informativa “*Consideraciones sobre la Ciberseguridad en Aviación*”.