"CIBERDEFENSA AEROESPACIAL"

Aerospace Cyber Defense

Recibido: 21 / 08 / 2019 Aprobado: 31 / 10 / 2019

Comandante
José Igancio Pérez Benítez
España

El autor es comandante del Cuerpo General del Ejército del Aire Español. Actualmente Jefe de la Sección de Defensa del Centro de Apoyo Técnico Avanzado del Ejército del Aire. Oficial especialista en Informática y Controlador de Tránsito Aéreo. Ingeniero Técnico en Informática de Gestión por la Universidad Carlos III de Madrid. Supervisor de Seguridad de Sistemas con formación avanzada en ciberdefensa y específica en sistemas medios. Tiene experiencia en Control de Tránsito Aéreo, gestión de seguridad de las TIC, acreditación y conformidad de Sistemas, gestión INFOSEC/COMSEC, gestión de proyectos de desarrollo de software embarcado, análisis de riesgos y administración de sistemas. Entre sus destinos, el Centro Corporativo de Explotación de Apoyo, el Centro Superior de Estudios de la Defensa Nacional, NATO E-3A Component, el Centro de Informática de Gestión y la Dirección de Ciberdefensa del Ejército del Aire.

RESUMEN

Las amenazas cibernéticas en la aviación civil y militar son una realidad en un ámbito global cada vez más tecnificado. Algunas de ellas son compartidas con otros sectores de la industria, pero otras son específicas de la aviación. Esas amenazas pueden afectar a la seguridad en vuelo creando problemas en el control de tráfico, provocando maniobras anticolisión, distracciones, incremento de la carga de trabajo de pilotos y controladores, desconfianza en el sistema afectado y en las tripulaciones o, en el peor de los casos, un accidente aéreo. Los investigadores han demostrado vulnerabilidades en distintas tecnologías inalámbricas muy usadas por las aeronaves que carecen de los mecanismos básicos de ciberseguridad. Con la disponibilidad creciente de avanzados medios técnicos a bajo coste, surge una nueva amenaza. La necesaria interconectividad de los sistemas incrementa considerablemente el riesgo en un ámbito donde los efectos disruptivos pueden ser devastadores.

Palabras clave:
Amenaza, aeroespacial, malware, análisis de riesgos, impacto, ADS-B, GPWS, TCAS, ILS, seguridad en vuelo.

ABSTRACT

Cyber threats in civil and military aviation represent a reality in a global scope more and more technified. Some of them are shared among different industry sectors but others are specific to aviation. These threats can affect flight safety by creating traffic control problems. These threats can affect flight safety by creating traffic control problems, causing anti-collision maneuvers, distractions, increased workload of pilots and controllers, distrust of the affected system and crews or, in the worst cases, a plane crash. Researchers have demonstrated vulnerabilities in different wireless technologies widely used by aircraft that lack the basic cybersecurity mechanisms. With the increasing availability of advanced technical means at low cost, a new threat has emerged. The necessary interconnectivity of the systems considerably increases the risk in an area where disruptive effects can be devastating.

Keywords:
Threat, aerospace, malware, risk analysis, impact, ADS-B, GPWS, TCAS, ILS, safety.

INTRODUCCIÓN

Todavía parece existir la creencia de que el "Air gap" hace que una aeronave sea inmune a un ciberataque. Nada más lejos de la realidad. Se trata de un entorno en el que el ritmo de adopción tecnológica crece exponencialmente y donde los sistemas en tierra y en vuelo deben en algún momento, estar conectados de forma directa o indirecta y donde las comunicaciones inalámbricas presentan vulnerabilidades evidentes.

Una simple búsqueda en Google arroja resultados preocupantes: exfiltración de datos, multas millonarias a compañías aéreas, investigaciones que demuestran la posibilidad real de un ataque cibernético, accidentes o incidentes indirectamente provocados por malware presente en sistemas, código fuente con vulnerabilidades, hackeo de drones, etc. Todas estas noticias hay que tratarlas con la precaución que merece toda información que llega de medios no contrastados, pensando que hay muchos intereses en juego. Los fabricantes y las aerolíneas querrán mantener su reputación intacta y probablemente harán lo posible por desmentir o negar todo aquello que afecte negativamente al sector. Los gobiernos se preocuparán por mantener la credibilidad de sus capacidades de defensa a toda costa y es posible que no permitan que se conozcan fallos de seguridad en sus sistemas de armas. Por el lado contrario, los investigadores intentarán demostrar que existe un riesgo real y que es necesario actuar. En cualquier caso, a nadie le interesa mantener los riesgos por encima del umbral aceptable, especialmente en el ámbito aeroespacial.

En este ámbito las principales vulnerabilidades provienen de la condición de espacio global común, donde las amenazas pueden venir desde dentro y fuera de los espacios de soberanía. También de la elevada tecnificación y complejidad. Una aeronave moderna implica muchos sistemas embarcados con millones de líneas de código. Este incremento de complejidad supone más dificultad en todas las fases del ciclo de vida e incrementa considerablemente el riesgo de fallo lógico en cualquiera de sus componentes.

En definitiva, estamos ante un entorno complejo altamente tecnificado, interconectado y de ámbito global, donde hay que proteger no solo las aeronaves y sus sistemas embarcados, sino también los sistemas de navegación, las estaciones de control y seguimiento de satélites, los sistemas de control aéreo, los sistemas meteorológicos, las instalaciones aeroportuarias con todos sus sistemas de información asociados, los sistemas de mantenimiento y de gestión logística, los entornos de desarrollo, los canales de distribución del software, los procedimientos de actualización, la organización de la ciberseguridad, las estructuras de mando y control, etc. Se necesita una aproximación integral que permita generar la necesaria confianza a los usuarios, a los gobiernos y a las empresas.

LAS AMENAZAS CIBERNÉTICAS A LA AVIACIÓN MILITAR Y CIVIL

La evolución tecnológica ha hecho que alcanzar ese nivel deseado de ciberseguridad no resulte fácil. Un problema que destaca y que resulta inevitable en el entorno aeronáutico es el de la obsolescencia.

La obsolescencia puede definirse como la pérdida real o inminente de la capacidad de conseguir tecnología de su fabricante original. Afecta al hardware, software, firmware, drivers, interfaces o algoritmos en uso por un sistema CIS[1].

El problema radica en los ciclos de vida de los sistemas de información, es decir, del tiempo que transcurre desde que surge la necesidad del sistema hasta que otro lo sustituye. Hay sistemas aéreos diseñados para estar en servicio 30 años o más, sin embargo, los sistemas que lo soportan especialmente si usan COTS[2], tienen ciclos de vida considerablemente más cortos. Un hardware COTS tiene una vida media de 18 meses y un software COTS de 5 años, lo que puede dar una idea de la dimensión del problema.

Si nos vamos a los tiempos de diseño, podríamos decir que un sistema de armas necesita de unos 10 años en fase de diseño y desarrollo. Un sistema CIS puede necesitar entre 2 y 6 años en dichas fases, lo que significa que en ocasiones, algunos sistemas CIS ya están obsoletos antes de entrar en servicio como parte del sistema de armas que corresponda.

Existen dos tipos de obsolescencia: funcional y tecnológica.

[1]Sistemas de Información y Comunicaciones (en inglés, Communications and Information Systems)
[2]Sistemas comerciales disponibles para el público en general (en inglés, Commercial Off-The-Shelf)

La obsolescencia funcional se produce cuando cualquier elemento de un sistema no realiza la función para la que fue diseñado debido a cambios en otra parte del sistema.

La obsolescencia tecnológica se produce cuando el fabricante no da soporte al elemento por falta de continuidad, el mismo fabricante ya no existe como empresa, no se permite la distribución por guerras tecnológicas, existe falta de disponibilidad en el mercado o aparecen tecnologías disruptivas.

Un sistema obsoleto, sin la capacidad de actualización constante, pasa a ser vulnerable por definición. A partir de aquí, ninguna otra medida de seguridad tiene sentido. Solamente en un esquema de seguridad en profundidad se pueden buscar estrategias para dotar de seguridad capas sobre las que todavía se tiene control tecnológico. La obsolescencia afecta al mantenimiento, a la acreditación o reacreditación de los sistemas, es decir, a su posibilidad legal de manejar o no información clasificada, a las posibles interacciones no contempladas safety/security, etc. Es un problema muy difícil de gestionar, por lo que hay que tratar de evitarla a toda costa.

Otro problema importante es el de la cadena de suministro. Resulta lógico pensar que los fabricantes recurran a otras empresas y países para reducir costes y terminar proyectos más rápidamente. Cualquier sistema formado por subsistemas ensamblados y no fabricados va a presentar este problema. Se trata de conseguir que los canales de distribución sean seguros desde su origen. Los proveedores deberían ser capaces de aplicar las mismas medidas de seguridad a sus sistemas que se aplican en los sistemas propios, así como que la información, clasificada o no, se maneje adecuadamente y con garantías.

Si un subsistema, sistema o producto está comprometido en origen, ya sea por vulnerabilidades no tratadas, por malware, o por cualquier otro motivo, el problema se va a trasladar al producto final. Esto puede hacer que las vulnerabilidades queden latentes durante meses o incluso años esperando ser explotadas. En cualquier caso, si no se toman las medidas adecuadas, es probable que algún punto de la cadena se vea afectado por algún ataque viéndose comprometido el producto final. El problema surge cuando un fabricante de aeronaves actúa como integrador tecnológico que trabaja con proveedores que poseen limitadas capacidades de ciberseguridad, lo cual se traslada al producto final.

Resulta difícil, por no decir imposible, hacer un seguimiento de quien accede a cada sistema en todo momento, los proveedores deberán establecer relaciones de confianza basadas en marcos regulatorios y tecnológicos comunes.

Si nos centramos en el plano técnico existen múltiples vectores de ataque: actualizaciones de software de misión, de las bolsas electrónicas de vuelo, los interfaces de cabina, contenidos infectados en sistemas multimedia, falta de aislamiento efectivo entre sistemas vitales y no vitales para el vuelo, falta de supervisión de puntos de acceso y conexión, etc. Pero si hubiese que elegir uno, sin duda sería el de las comunicaciones inalámbricas.

Resulta chocante descubrir que muchos sistemas de comunicaciones inalámbricas de las aeronaves carecen de mecanismos básicos de seguridad, dejándolos expuestos a ataques. Hay que tener en cuenta que muchos de estos sistemas entran en servicio cuando la seguridad no estaba en la mente de los diseñadores. El auge de las radios definidas software[3] tiene incidencia directa en el incremento de la posibilidad de ataques a este tipo de sistemas a un coste muy bajo.

En concreto, se ha demostrado que en la mayoría de los casos, será suficiente una radio definida software, un ordenador de bajo coste, una antena, un amplificador de señal y software open-source de libre acceso para que un atacante con conocimientos y presupuesto moderados sea capaz de desarrollar ataques remotos a este tipo de tecnologías.

Los ataques pueden ser pasivos o activos. Los pasivos, en principio, no representan una amenaza real, solamente escuchan. Los fines pueden ser observación sin más agregación de datos o vigilancia y como mucho, afectan a la confidencialidad, lo cual en sí no es un riesgo directo para la seguridad ya que no interfieren con el sistema. Sin embargo, no debemos olvidar que todo ataque activo empieza por uno pasivo y puede terminar en un ataque dirigido.

[3]Radio definida por software o SDR (del inglés Software Defined Radio) es un sistema de radiocomunicaciones donde varios de los componentes típicamente implementados en hardware (mezcladores, filtros, moduladores/demoduladores, detectores, etc) son implementados en software, utilizando un ordenador personal u otros dispositivos de computación. De Wikipedia.

Se podría decir que actualmente hemos pasado de ataques de denegación tipo "jamming"[4], a ataques de falsificación tipo "spoofing"[5] mucho más peligrosos y complicados de detectar, por ejemplo, en sistemas de navegación como el GPS.

En cualquier caso, vamos a repasar algunos de estos sistemas, empezando por el ADS-B (Automatic Dependent Surveillance Broadcast).

El ADS-B es un sistema que determina la posición de la aeronave mediante navegación vía satélite y periódicamente la emite de forma inalámbrica, permitiendo que pueda usarse por otras aeronaves o por el control de tránsito aéreo y visualizar su posición y altitud en las pantallas sin necesidad de radar.

Este sistema ofrece numerosas ventajas, mejor control de tránsito aéreo, menor coste que el radar primario y secundario, mejor visualización, mejor cobertura, más precisión, etc. Es un sistema que se usa en un alto porcentaje de los aviones comerciales y con previsión de seguir haciéndolo. De hecho, un mandato de la FAA[6] requiere la instalación de un transpondedor "ADS-B Out" no más tarde del 1 de enero del 2020. Otro mandato similar de la Unión Europea entraría en vigor algo más tarde, el 7 de junio de 2020.

Este sistema emite mucha información, identificación del vuelo, identificación del avión, posición (latitud/longitud), altitudes, régimen de ascenso/descenso, ángulos y velocidad sobre el terreno, indicaciones de emergencia (cuando se selecciona algún código), etc., todo ello sobre enlaces sin cifrar, sin ningún tipo de autenticación o integridad, lo que permite manipularla o hacer spoofing [7] anto de aeronaves como de las estaciones de control en tierra.

Los ataques pasivos al ADS-B pueden hacerse, además de con los medios descritos anteriormente, adquiriendo un receptor ADS-B o acudiendo a uno de los múltiples servicios en internet que proporcionan datos ADS-B en tiempo real. Sin embargo, no son estos ataques los que preocupan.

Un ataque activo tipo sería la generación de un avión fantasma. Mediante la emisión de nuevos mensajes ADS-B de un avión inexistente (fantasma), los sistemas los van a interpretar como una aeronave real, lo cual puede llegar a forzar a realizar maniobras innecesarias para evitar una colisión.

Otro ataque sería la denegación de servicio. Usando la técnica anterior, inundar los sistemas con múltiples aviones fantasma con la intención de que los sistemas de vigilancia, de los aeropuertos o de las propias aeronaves no se puedan utilizar.

Existen otras posibilidades de ataque activo como modificación de trayectorias, generación de falsas alarmas, aeronaves desaparecidas o spoofing de aeronaves, siempre generando, eliminando o manipulando mensajes de forma aislada o en combinación con otras técnicas como manipulando transpondedores en cabina para modificar la dirección ICAO[8] y simular ser otra aeronave distinta.

Otro sistema vulnerable es el ACARS (Aircraft Communications Addressing and Reporting System), ampliamente utilizado. Se trata de un sistema del año 1978. Existe un cifrado estándar para este sistema, pero no se ha implantado de forma generalizada. Se utiliza para la transmisión de mensajes cortos entre el avión y las estaciones de tierra con distintos fines como informes de rendimiento, comunicaciones interactivas con la tripulación, planes de vuelo antes del despegue, incidencias técnicas o de otro tipo, etc.

Los ataques activos al sistema ACARS consisten en la inyección, modificación o borrado de mensajes, que puede usarse para provocar, por ejemplo, actualizaciones falsas de planes de vuelo, información meteorológica falsa, alertas innecesarias, etc.

Algunas aeronaves tienen el sistema ACARS conectado al FMS[9] lo cual incrementa considerablemente el riesgo. En concreto, en la conferencia "Hack in the Box 2013" en Amsterdam se demostró que con equipos comprados en ebay se pueden ver y manipular los mensajes y enviar código malicioso al FMS. En primer lugar, se

[4]Creando interferencias o altos niveles de ruido.
[5] Uso de técnicas a través de las cuales un atacante, se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.
[6] La Administración Federal de Aviación (en inglés, Federal Aviation Administration, FAA) es la entidad gubernamental responsable de la regulación de todos los aspectos de la aviación civil en los Estados Unidos.
[7]Uso de técnicas a través de las cuales un atacante, se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.
[8]Código de 24-bits que identifica de forma unívoca a la aeronave.
[9] Sistema de gestión de vuelo (del inglés, Flight Management System)

localiza el avión con ADS-B, luego se usan mensajes ACARS para subir malware al FMS y posteriormente manipular el sistema cambiando planes de vuelo, predicciones meteorológicas, información del avión, o incluso controlar el avión si el piloto automático está conectado.

ADS-B y ACARS son los sistemas que parecen acumular más literatura en relación con comunicaciones inalámbricas no protegidas, pero no son los únicos. El GPWS (Ground Proximity Warning System) es otro ejemplo a considerar.

El GPWS es un sistema que alerta a los pilotos sobre la proximidad del terreno, que comenzó su vida a finales de los años 60. Usa un radioaltímetro para calcular la distancia al terreno que sigue patrones estándar de frecuencia de emisión y barrido. Se usa el cambio de frecuencia y el tiempo de ida y vuelta de la señal emitida para calcular la altura sobre el terreno.

Un posible ataque consistiría en emitir una ráfaga de frecuencias simulando la señal de vuelta en el rango y momento adecuados. De esta forma se puede simular que el terreno se aproxima rápidamente. Con este tipo de ataque no se espera provocar un accidente, sino más bien una maniobra para evitar una colisión. También se podría anular el sistema mediante una denegación de servicio, que el sistema no es capaz de detectar y con ello, aumentar la posibilidad de un accidente.

Para materializar este ataque será necesario utilizar antenas direccionales que se situarían bajo la trayectoria de aproximación para transmitir las señales al radioaltímetro de la aeronave. La capacidad de despliegue dependerá de la seguridad física del aeródromo/aeropuerto y su perímetro.

Algo similar ocurre con el TCAS (Traffic Collision Avoidance System). Un Sistema de los años 80 que, con independencia de equipos en tierra, proporciona resolución de conflictos y alertas ante una amenaza de colisión aérea entre aeronaves.

El TCAS también utiliza canales de comunicación sin autenticación. En este caso, un requisito a resolver para un potencial atacante sería el alcance, ya que la velocidad de una aeronave hace que rápidamente quede fuera del mismo. Esto puede solucionarse desplegando múltiples antenas con la separación física adecuada.

En cualquier caso, la intención del atacante es emitir señales de alerta de proximidad de una aeronave inexistente para provocar maniobras innecesarias.

Un último ejemplo de comunicaciones no protegidas sería el ILS (Instrument Landing System). El ILS es un sistema de aterrizaje por instrumentos que permite que un avión sea guiado y aterrizado con precisión durante la aproximación a la pista de aterrizaje, incluso en condiciones de baja visibilidad.

El ILS se compone de equipos en tierra, que emiten las señales y equipos a bordo del avión, que las procesa y permite guiar al piloto horizontal (localizador) y verticalmente (senda de planeo) hasta la pista de aterrizaje.

Un atacante pretenderá generar lóbulos de señal falsos que repliquen los legítimos del sistema con la intención de desencadenar múltiples aproximaciones frustradas, causar que el avión toque la pista antes de lo previsto o que la sobrevuele por completo.

Lo que más dificulta este posible ataque serían las limitaciones físicas, ya que habría que situar el equipamiento próximo a la pista de aterrizaje. Es algo difícil, pero no imposible. No obstante, una vez que el avión está en el localizador, se puede generar una senda de planeo falsa, emitiendo un lóbulo con más potencia y a cierta distancia del aeropuerto, lo que es más sencillo ya que estaría fuera de la zona de protección física.

En este artículo sólo se han tratado posibles ataques a sistemas específicos. Un escenario más complejo y efectivo para un potencial hacker consistiría en combinar ataques simultáneos a distintas tecnologías.

Hemos visto que, en el plano técnico y de forma relativamente sencilla, se pueden utilizar medios accesibles para materializar distintos tipos de ataques.

Entonces, ¿qué se puede hacer para resolver o mitigar estas amenazas? ¿se puede hacer algo? La respuesta no es sencilla.

Podríamos pensar inicialmente que con aplicar medidas técnicas adecuadas ya sería suficiente. Por ejemplo, podríamos dar seguridad a las comunicaciones inalámbricas, incorporando autenti-

cación y cifrado, también podríamos pensar en utilizar siempre sistemas redundantes, es decir, duplicando sistemas para que en caso de fallo siempre haya otro disponible; resistentes, que soporten condiciones de temperatura y presión extremas, pero que también sean capaces de resistir ataques físicos o eléctricos y resilientes, que utilicen distintas tecnologías para realizar la misma función y, de esta forma minimizar los efectos de ataques dirigidos a tecnologías concretas.

Todas estas medidas técnicas aportan seguridad, pero ¿qué ocurre si el jefe de mantenimiento no registra los incidentes mecánicos? ¿Y si se actualiza el software embarcado siguiendo un procedimiento no escrito? ¿O si un técnico utiliza la memoria USB de su ordenador particular infectado para trasferir datos de misión a un sistema embarcado? ¿Y si un contrato de mantenimiento no cubre la posible incorporación de nuevas funcionalidades, o se alcanza obsolescencia funcional porque el mantenimiento no contempla la posibilidad de adaptarse a un nuevo entorno actualizado?

Podríamos empezar por mejorar los contratos de mantenimiento de los sistemas. Tradicionalmente el mantenimiento podía ser: preventivo, con revisiones periódicas se pretende identificar y detectar fallos latentes y correctivo, identificando y eliminando defectos o corrigiendo errores reales. Sin embargo, es necesario pensar en un mantenimiento adaptativo, que permita adaptar un entorno determinado a las actualizaciones de sistemas que le puedan afectar, predictivo, que permita evaluar el flujo de ejecución para anticiparse a posibles fallos y estudiar la situación actual para programar el siguiente mantenimiento en función de la situación, perfectivo, que permita incorporar nuevas funcionalidades o capacidades, mejoras de rendimiento, dependencias o mantenibilidad y evolutivo, para estar actualizado y no permitir la obsolescencia.

Vemos que además de las medidas técnicas, la revisión de los contratos también aporta seguridad. Aunque hay muchas otras áreas de mejora. En cualquier caso, lo que está claro es que hay que actuar desde distintos frentes buscando una aproximación integral. Las medidas técnicas no lo son todo, hay que pensar en normativa, organización, procedimientos, acuerdos comerciales, canales de distribución, concienciación, etc.

En este punto podríamos hacernos varias preguntas: ¿no estamos ante un problema demasiado complejo? ¿no hay una forma de tratar todos los problemas de manera holística? ¿por dónde empezamos?…

La respuesta a gran parte de todas estas preguntas la encontramos en la gestión y el análisis de riesgos.

Pero ¿qué es el riesgo? El riesgo es una estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos, causando daños o perjuicios a la organización. Es decir, es una combinación del impacto que supone la pérdida total o parcial del activo y la probabilidad de que esto ocurra.

RIESGO = PROBABILIDAD * IMPACTO

Esta fórmula es importante ya que el riesgo será alto si el impacto es alto, si la probabilidad de que ocurra es alta, o si la combinación de ambos factores es alta. Por ejemplo, la probabilidad de que un sistema crítico del avión sea hackeado por personal de mantenimiento utilizando una bolsa electrónica de vuelo puede ser baja, sin embargo, el impacto producido si se materializa esta amenaza sería muy alto, por lo tanto, el riesgo será alto.

El primer paso sería hacer un análisis, ver cómo estamos para poder tomar decisiones que supondrán un coste. Esto es lo que proporciona el análisis de riesgos. Es decir, es una actividad básica cuyo resultado es un mapa de riesgos que da una idea de lo que se puede perder si se materializa cualquier amenaza.

Una vez se tiene el análisis, hay que pasar por una evaluación, para que la dirección coteje el riesgo estimado contra los criterios de la organización y priorizar las medidas que deberán adoptarse para mantener dicho riesgo bajo umbrales aceptables. Esto derivará en el correspondiente “plan de seguridad” que llevará a la práctica todo lo decidido en forma de proyectos, desarrollos y contrataciones y, como cualquier otro proyecto deberá tratar tareas, tiempos y recursos.

Algunos ejemplos de salvaguardas a aplicar podrían ser:

- Aislar funciones críticas desde la fase de diseño.
- Sistemas redundantes, resistentes y resilientes.

- Refinar los contratos con los proveedores, con respecto a:
  - Responsabilidades bien definidas.
  - Habilitaciones de seguridad[10].
  - Incorporar todos los tipos de mantenimiento.
- Realizar inspecciones de calidad.
- Elaborar un plan de concienciación.
- Incorporar autenticación y cifrado en las comunicaciones inalámbricas.
- Incorporar infraestructura de clave pública en la entrada de datos a sistemas críticos.
- Etc.

Entonces ¿ya está? ¿tenemos la solución en nuestras manos? ¿hemos encontrado la forma de abordar de forma holística la amenaza ciber en el entorno aeronáutico? De nuevo la respuesta no es sencilla.

En primer lugar, siempre conviene acudir a metodologías internacionalmente reconocidas. Entre ellas podemos citar MAGERIT, OCTAVE, CRAMM, MEHARI o SP800-30 entre otras.

Será necesario contar con herramientas que faciliten el trabajo. El análisis de riesgos es una actividad compleja, metódica y cíclica. El análisis debe hacerse tanto en la fase de especificación, como en la de desarrollo y, por supuesto, durante la operación del sistema. El problema es que no hay herramientas que traten los riesgos aeronáuticos de forma específica, o al menos el autor de este artículo no las ha encontrado. ENISA (European Union Agency for Cybersecurity) publica un inventario de metodologías[11] y herramientas[12] con plantillas de atributos que describen en detalle dichas metodologías y herramientas.

Lo cierto es que el entorno aeronáutico se enfrenta a riesgos específicos, por ejemplo, actividades interrumpidas por dependencias SAFETY/SECURITY no previstas, datos radares corruptos, saturación de procesamiento por obsolescencia de sistemas, sistemas de mantenimiento comprometidos, falta de resiliencia, resistencia o redundancia en los sistemas, uso de COTS, etc. Estos factores deben ser incorporados a herramientas específicas.

CONCLUSIÓN

Estamos ante un escenario complejo y cada vez más tecnificado donde muchos actores e intereses entran en juego. La amenaza cibernética es una realidad y representa un riesgo importante en el entorno aeronáutico.

Es de esperar que los sistemas en este ámbito sufran fallos y ataques cibernéticos. Es necesario conseguir detectar intrusiones e implementar una adecuada defensa activa y en profundidad.

Los ciberataques vienen sin aviso previo y pueden afectar a múltiples sistemas simultáneamente. Una adecuada concienciación y entrenamiento del personal implicado resulta fundamental.

Las medidas técnicas aportan seguridad, pero es necesario seguir una aproximación integral que cubra otras áreas de actuación.

Los análisis de riesgos se presentan como una herramienta básica de apoyo a la decisión. Es un primer punto de partida que permite saber que salvaguardas habría que aplicar, ya sean organizativas, procedimentales o técnicas. Es importante usar una metodología reconocida para evitar arbitrariedades.

[10]Permisos otorgados por la autoridad nacional cuando se requiera manejar, almacenar o generar información clasificada en las instalaciones del proveedor.
[11]https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods
[12]https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools

REFERENCIAS

Air Line Pilots Association. (2017). *Aircraft cybersecurity: the pilot's perspective.* Recuperado de http://www.alpa.org/-/media/ALPA/Files/pdfs/news-events/white-papers/white-paper-cybersecurity.pdf?la=en

Berges, P. M. (2019). *Exploring the vulnerabilities of traffic collision avoidance systems (TCAS) through software defined radio (SDR) exploitation.* (Tesis inédita de maestría). Faculty of the Virginia Polytechnic Institute and State University, Virginia, Estados Unidos. Recuperado de https://vtechworks.lib.vt.edu/handle/10919/90165

Cohen, N. (2019). *When an aircraft landing system is made to enter the spoofing zone.* Recuperado de https://techxplore.com/news/2019-05-aircraft-spoofing-zone.html

Costin, A. y Francillon, A. (2012). *Ghost in the air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices.* Recuperado de https://www.researchgate.net/publication/267557712_Ghost_in_the_AirTraffic_On_insecurity_of_ADS-B_protocol_and_practical_attacks_on_ADS-B_devices

EASA. (2018). *Impact assessment of cybersecurity threats (IACT) (proyecto de investigación).* Recuperado de https://www.easa.europa.eu/document-library/research-projects/easarepresea20161

Geister, R., Buch, J-P., Niedermeier, D., Gamba, G., Canzian, L. y Pozzobon, O. (2018). *Impact study on cyber threats to GNSS and FMS systems.* Recuperado de https://www.icas.org/ICAS_ARCHIVE/ICAS2018/data/papers/ICAS2018_0249_paper.pdf

LTG Wyche, L. y Pieratt, G. (2017). *Securing the Army's weapon systems and supply chain against cyber attack. association of the United States Army.* Recuperado de https://www.ausa.org/publications/securing-armys-weapon-systems-and-supply-chain-against-cyber-attack

Mandelbaum, J., Patterson, C., Brown, R. (2017). *The evolution of DMSMS management in DOD – there's still room for improvement.* Recuperado de https://www.ida.org/research-and-publications/publications/all/t/th/the-evolution-of-dmsms-management-in-dod-theres-still-room-for-improvement

Ro, S. (2013). *Boeing's 787 dreamliner is made of parts from all over the world.* Recuperado de https://www.insider.com/boeing-787-dreamliner-structure-suppliers-2013-10

Sathaye, H., Schepers, D., Ranganathan, A. and Noubir, G., Northeastern University. (2019). *Wireless attacks on aircraft instrument landing systems.* Recuperado de https://www.usenix.org/system/files/sec19-sathaye.pdf

Schäfer, M., Lenders, V., Martinovic, I. (2013). *Experimental analysis of attacks on next generation air traffic communication.* Recuperado de https://link.springer.com/chapter/10.1007/978-3-642-38980-1_16

Smith, M., Strohmeier, M., Harman J., Lenders, V. y Martinovic, I. (2019). *Safety vs. security: Attacking avionic systems with humans in the loop.* (Department of computer science, University of Oxford). Recuperado de https://arxiv.org/pdf/1905.08039.pdf

Strohmeier, M., Smith, M., Schäfer, M., Lenders, V. y Martinovic, I. (2016). *Assessing the impact of aviation security on cyber power.* 2016 8th International Conference on Cyber Conflict (CyCon). Recuperado de https://ieeexplore.ieee.org/abstract/document/7529437

Wolf, M., Minzlaff, M. y Moser, M. (2014). *Information technology security threats to modern e-enabled aircraft: a cautionary note.* Recuperado de https://doi.org/10.2514/1.I010156