EDITORIAL ESDEG

Revista
Ciberespacio, Tecnología e Innovación
Volumen 1, número 1, enero-junio 2022
Bogotá, D.C, Colombia
ISSN: 2955-0270
Página web: https://esdegrevistas.edu.co/index.php/rcit

Riesgos cibernéticos para la aviación regular "el 11 de septiembre cibernético"

Cyber risks for regular aviation "cyber 9/11"

Germán Darío Ramón Bonilla

CITACIÓN APA:

Ramón Bonilla, G. D. (2022). Riesgos cibernéticos para la aviación regular "el 11 de septiembre cibernético". *Ciberespacio, Tecnología e Innovación, 1*(1), 93-98. https://doi.org/10.25062/2955-0270.4775

Publicado en línea: **Junio 30 de 2022**

Enviar un artículo a la Revista

Revista Ciberespacio, Tecnología e Innovación
Volumen 1, número 1, enero-junio 2022 (pp. 93-98)
Bogotá, D.C, Colombia

EDITORIAL ESDEG

Riesgos cibernéticos para la aviación regular "el 11 de septiembre cibernético"

Cyber risks for regular aviation "cyber 9/11"

DOI: https://doi.org/10.25062/2955-0270.4775

Germán Darío Ramón Bonilla
Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D. C., Colombia

Resumen

Durante los últimos años, en particular a partir de año 2020, se ha evidenciado un incremento considerable de ataques cibernéticos a la aviación, en particular a las aerolíneas, y en menor proporción a las entidades encargadas de liderar y controlar los servicios de tránsito aéreo o Civil Aviation Authorities (CAA). Tal como le sucedió a la Administración Federal de Aviación (FAA) que en un lapso menor a tres meses fue víctima de dos ataques a la disponibilidad de sus sistemas de información, afectaciones que colocan en evidencia que Estados Unidos a pesar de ser uno de los países con mayor madurez cibernética, aún presenta vulnerabilidades que se deben contrarrestar. Por tal motivo, este articulo explora los riesgos cibernéticos para la aviación regular.

Palabras Clave: Aviación; Riesgos cibernéticos; Seguridad

Abstract

During recent years, particularly since 2020, there has been a considerable increase in cyber attacks on aviation, particularly on airlines, and to a lesser extent on the entities in charge of leading and controlling air traffic services or Civil Aviation Authorities (CAA). Just as it happened to the Federal Aviation Administration (FAA), which in a period of less than three months was the victim of two attacks on the availability of its information systems, attacks that show that the United States, despite being one of the Countries with greater cyber maturity still present vulnerabilities that must be counteracted. For this reason, this article explores cyber risks for regular aviation.

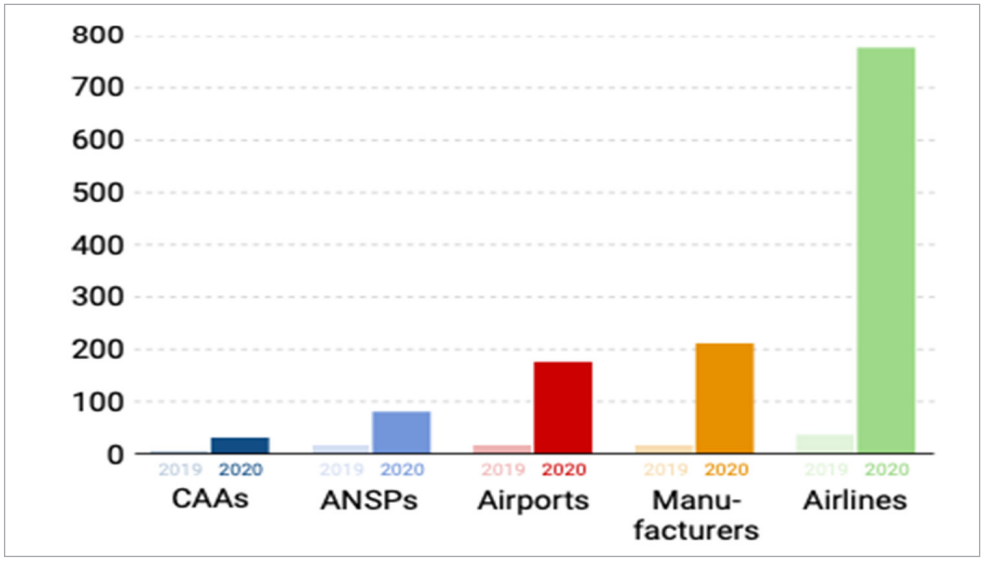
Key words: Aviation; Cyber risks; Security

Artículo de reflexión
Recibido: 23 de enero de 2022 • **Aceptado:** 14 de marzo de 2022
Contacto: Germán Darío Ramón Bonilla germanr@esdeg.edu.co

Introducción

Durante los últimos años, en particular a partir de año 2020, se ha evidenciado un incremento considerable de ataques cibernéticos a la aviación, en particular a las aerolíneas, y en menor proporción a las entidades encargadas de liderar y controlar los servicios de tránsito aéreo o Civil Aviation Athoroties (CAA), tal como le sucedió a la Administración Federal de Aviación (FAA[1],por sus siglas en inglés), una entidad norteamericana que en un lapso menor a tres meses fue víctima de dos ataques a la disponibilidad de sus sistemas de información, afectaciones que colocan en evidencia que Estados Unidos a pesar de ser uno de los países con mayor madurez cibernética, aún presenta vulnerabilidades que se deben contrarrestar.

Figura 1. Ciber Ataques Reportados en Aviación 2019 vs. 2020



Fuente: Elaboración propia a partir de EUROCONTROL EATM-CERT Services

Es importante reconocer que los aeropuertos, como infraestructura crítica de cualquier nación, son objetivos de alto valor estratégico para actores que buscan extorsionar, interrumpir o dañar la reputación de un estado; afectando directamente su economía, por supuesto, a las aerolíneas y a sus usuarios.

Con la aparición de nuevas tecnologías en aviación, sobre todo por la integración del Internet de las cosas (IoT) a sistemas de control y apoyo a la Gestión de Tránsito Aéreo (ATM), hay mayor probabilidad de sufrir ataques cibernéticos procedentes de actores que

1 FAA, Federal Aviation Administration

buscan las vulnerabilidades de la tecnología con la que operan ciertos aeropuertos, ocasionando pérdidas económicas reflejadas en retrasos, cancelaciones de vuelos e incluso llegando afectar la seguridad operacional.

La Agencia Europea de Seguridad Aérea (EASA[2] por sus siglas en inglés) afirma que la cantidad de ataques a los sistemas de información al servicio de la aviación crecerá de manera exponencial por el aumento de aplicaciones, dispositivos tecnológicos y el uso del internet de las cosas (IoT[3] por sus siglas en inglés) en la industria aeronáutica.

Si bien los ataques y fallas de software pueden causar retrasos, cancelaciones y restricciones de acceso a la información; las autoridades de aviación civil (CAA) como entes reguladores tienen la responsabilidad de identificar las nuevas amenazas y adoptar estrategias para mejorar la resiliencia cibernética: "capacidad de una organización para prevenir, resistir y recuperarse de incidentes de ciberseguridad" (IBM, 2020, párrafo 3).

A pesar de que los ataques de denegación de acceso a la información, DDoS, son considerados complejidad media y baja criticidad, la aplicación de estos a sistemas de información aeronáutica para el desarrollo de vuelos, genera un efecto cascada con afectaciones significativas al normal desarrollo de las operaciones aéreas, dos casos recientes de afectación por denegación de acceso a los servicios de información aeronáutica en Estados Unidos, serán expuestos con el propósito de dilucidar la magnitud de un ataque cibernético a los sistemas de información aeronáutica:

El pasado 11 de enero de 2023, a las 07:20 horas, la FAA debió ordenar a todas las aerolíneas estadounidenses pausar las salidas de sus vuelos nacionales mientras restauraban la base de datos del sistema de aviso de información de vuelo (NOTAMs[4] por sus siglas en inglés); información obligatoria para consulta de pilotos y despachadores, previo al desarrollo del vuelo.

La responsabilidad de esta interrupción aún es materia de investigación, no obstante, se indicó por la FAA que esta base de datos fue afectada por un archivo dañado, según lo manifestó comunicado de la misma organización por medio de Twitter.

Esta interrupción del servicio de información generó que, sobre el medio día, se cancelaran 1.100 vuelos y se retrasaran otros 7.300. El secretario de transporte de los estados Unidos, Pete Buttigieg, indicó el mismo día que la FAA identificará las causas para evitar que esto vuelva a suceder, por tratarse de una situación similar a la ocurrida el pasado 10 de octubre de 2022, en la que los sitios web de cinco aeropuertos estadounidenses se vieran afectados por un ataque de denegación de distribución de servicio

2 EASA, European Aviation Safety Agency

3 IoT, Internet of Things

4 NOTAMs, Notice for Air Missions

de información (DDoS[5] por sus siglas en inglés) a pasajeros; hechos atribuidos al grupo Pro-Ruso *Killnet*.

Si bien el evento más reciente se encuentra en investigación, es de notar que las afectaciones han sido progresivas en términos de contundencia y acercamiento a los sistemas operativos de información aeronáutica, situación que aumenta la preocupación por parte de las autoridades estadounidenses, por la incertidumbre de no saber cuál será el próximo ataque a enfrentar (Mundo Posgrado, 2021).

Respecto el evento del 10 de octubre de 2022, a pesar de no haber afectado de manera considerable el cumplimiento de los vuelos programados, es un ejemplo de ataque trascendental, utilizando el concepto de operaciones de zona gris (Hoffman et al., 2007, como se citó en Dziwisz, 2020), se hacen importante considerar acciones defensivas y ofensivas en el desarrollo de las operaciones cibernéticas, lo cual puede emplear tácticas convencionales. La misma Dziwisz (2020) argumenta que:

> La zona gris es cada vez más poblada, porque países como China o Rusia utilizan cada vez más herramientas cibernéticas y no cibernéticas para superar las fortalezas de EE. UU. en diplomacia, leyes y comercio global. No sorprende que esta nueva competencia de zona gris sea dura e inquietante para Estados Unidos (Dziwisz, 2020, p. 23).

Es así como los riesgos cibernéticos para los sistemas de apoyo a la aviación regular, podrán ser potencializados debido al desconocimiento de las vulnerabilidades de los sistemas del apoyo a la aviación, aumentando la probabilidad de materialización de ataques exitosos que buscan afectar la confidencialidad, disponibilidad e integridad de los sistemas de apoyo a la Gestión de Tránsito Aéreo, siendo esta la joya de la corona, por afectar a la seguridad operacional.

Expertos en ciberseguridad para la aviación, han identificado cuatro propósitos a lograr con el empleo efectivo de amenazas cibernéticas para la aviación: "el espionaje comercial, la ciberdelincuencia, la interrupción y los fines Político-Militares" (Safe Skies, 2018, párrafo), el último propósito coincidente con lo sucedido el pasado 10 de octubre de 2022 en EE.UU.

De igual manera, se ha identificado que las Amenazas Persistentes Avanzadas (APT[6] por sus siglas en inglés); son ejecutadas la principal amenaza para la aviación, ya que son desarrolladas por organismos militares o entidades de inteligencia extranjeras que buscan obtener alguna ventaja militar, política o estratégica trasnacional, mediante "Un conjunto de tácticas, técnicas y procedimientos que hacen compleja la detección de una intrusión cibernética en varios sistemas informáticos" (Parra, 2019, p. 32).

5 DDoS, Distributed Denial of Service

6 APT, Advanced Persistent Threat

Con mayor preocupación se debe considerar que amenazas emergentes seguirán en desarrollo; más aún cuando el avance de la tecnología y la modernización de aeropuertos y de aeronaves es proporcional a nuevas variables, la afectación podría pasar de eventos en tierra a situaciones en vuelo; como por ejemplo la manipulación de la señal satelital utilizada por las aeronaves para navegar y reportar posición a otras aeronaves y al ATC[7] siendo esta una preocupación reciente de la OACI[8] por el lanzamiento de la tecnología celular 5G, con recientes investigaciones por su incidencia con los sistemas de navegación de las aeronaves, (Federal Aviation Administration, 2023), situación que podría llegar a cambiar el concepto de secuestro físico de un avión, vulnerabilidad manifestada por Munro (2020):

> Estás conectando un avión que tradicionalmente no ha estado tan bien conectado y gran parte de la conectividad está empezando a romper muchos de los modelos de seguridad tradicionales que tenemos en torno al hecho de que el hacker puede saltar a una bahía de aviónica y empezar a jugar con un avión. (p. 16).

Podríamos listar muchas más amenazas, no obstante, lo importante es reconocer que ningún sector está lo suficientemente preparado para contrarrestarlas, siempre habrá algo más por hacer, pues cada paso que da la tecnología es una puerta que se abre a las amenazas cibernéticas; de esta manera es de reconocer que no se trata solo de adaptarnos a nuevas tecnologías, es también conocer su alcance.

Conclusiones

A pesar de que el sector aeronáutico está utilizando cada vez más tecnologías para mejorar las operaciones y los servicios que proporcionan a sus usuarios, hay un gran desafío en detectar cuáles son las ventajas y desventajas de estas tecnologías.

De igual manera, es apremiante recalcar a los entes reguladores de aviación, la importancia de diferenciar las redes de información (IT[9]) y (OT[10]), ya que, por practicidad y economía, algunas autoridades aeronáuticas y aerolíneas combinan sus portales operacionales, con temas administrativos e informativos de acceso público, siendo más vulnerables a que un solo ataque afecte ambos sistemas.

Finalmente, con urgencia se debe prestar atención a la interferencia de la tecnología celular 5G con los sistemas de navegación de las aeronaves, pues no existe manera de detectar si una perturbación a una señal satelital sea identificable oportunamente, sobre

7 ATC. Air Traffic Control

8 OACI, Organización de Aviación Civil Internacional

9 IT, Information Technology

10 OT, Operation Technology

todo en las fases cercanas al terreno (despegue y aterrizaje), y así evitar que se repita un 11 de septiembre, cibernético, mediante alteración, inserción e inhibición de señales a los sistemas de navegación a bordo de las aeronaves.

Declaración de divulgación

El autor declara que no existe ningún potencial conflicto de interés relacionado con este artículo.

Autor

Germán Darío Ramón Bonilla. Mayor de la Fuerza Aérea Colombiana. Candidato a magíster en ciberseguridad y ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Administración Aeronáutica, Escuela Militar de Aviación "Marco Fidel Suarez", Colombia.

ORCID: https://orcid.org/0009-0000-8444-9187
Contacto: germanr@esdeg.edu.co

Referencias

Dziwisz, D. (2022). "Cyber Pearl Harbor Is Not Coming: US Politics Between War and Peace". *Politeja* 19 (4), 95-109. https://doi.org/10.12797/Politeja.19.2022.79.07.

Federal Aviation Administration. (2023). *FAA. 5G and Aviation Safety.* https://www.faa.gov/5g

IBM. (2020). *IBM.COM. ¿Qué es la resiliencia cibernética?* https://www.ibm.com/co-es/topics/cyber-resilience

Munro, K. (23 de Abril de 2020). *Airport-Technology. Roundtable: Are airports prepared for cyber threats?* https://www.airport-technology.com/features/cybersecurity-in-airports/

Mundo Posgrado. (2021). *Estos son los 7 tipos de amenazas cibernéticas más frecuentes*. https://www.mundoposgrado.com/amenazas-ciberneticas-mas-frecuentes/

Parra, J. (2019). *Amenazas persistentes avanzadas y su impacto en Latinoamérica ¿cómo estar preparados?* [Trabajo de grado]. Universidad Piloto de Colombia. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6285/00005219.pdf?sequence=1&isAllowed=y

Safe Skies. (2018). *Sskies.org. PARAS -Program for Applied Research in Airport Security* https://www.sskies.org/images/uploads/subpage/PARAS_0007.CybersecurityQuickGuide.FinalReport.pdf