Afectación de los sistemas de navegación (GNSS) por ataques cibernéticos a los helicópteros de serie H-60.

Mayor (EJC) Julian Andrés Quintero Pérez

Artículo para optar al título profesional:

Magister en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra “General Rafael Reyes Prieto”
Bogotá D.C., Colombia
2024

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

DATOS GENERALES		
Nombre del estudiante	**:**	Mayor (EJC) Julian Andrés Quintero Pérez
Identificación	**:**	1.094.889.345
Programa académico	**:**	Maestría en Ciberseguridad y Defensa
Tutor metodológico	**:**	
Tutor temático	**:**	Teniente Coronel Julian González
Fecha de entrega	**:**	26 de agosto de 2025
Extensión	**:**	7.820 palabras

DECLARACIÓN DE ORIGINALIDAD Y CESIÓN DE DERECHOS

El autor declara que este artículo fue escrito de acuerdo con la normatividad de la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG) y no existe ningún potencial conflicto de interés relacionado con este. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representan la posición oficial ni institucional de la ESDEG, las Fuerzas Militares de Colombia o el Ministerio de Defensa Nacional.

Este artículo es enteramente mi propio trabajo y no ha sido presentado para la obtención de un título en esta u otra Institución de Educación Superior. Se han referenciado todos los trabajos y puntos de vista de otros autores, así como los datos de otras fuentes utilizadas. No se emplearon herramientas de generación de contenido por Inteligencia Artificial para su elaboración.

El autor acepta ceder los derechos de publicación en favor de la ESDEG y su Sello Editorial de acuerdo con los términos de la licencia Creative Commons: Reconocimiento-NoComercial-SinObrasDerivadas.

AUTORIZACIÓN DE PUBLICACIÓN

El autor autoriza / no autoriza que este articulo sea publicado por el Sello Editorial ESDEG en su repositorio institucional y esté disponible bajo una modalidad de acceso restringido.

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

Afectación de los sistemas de navegación (GNSS) por ataques cibernéticos a los helicópteros de serie H-60.

Cyberattacks on H-60 series helicopters disrupt navigation systems (GNSS).

Julian Andrés Quintero Pérez[1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Los sistemas de navegación de las aeronaves son fundamentales para la operación aérea en cualquier parte del mundo, estos nos permiten ir de un lugar a otro de forma precisa y segura; los sistemas GNSS basados en la navegación satelital se han vuelto indispensables en nuestros tiempos para la navegación, no solo por su precisión sino porque retroalimentan varios sistemas adicionales dependiendo del tipo aeronave y su configuración; esta tecnología en nuestro caso local es fundamental para los helicópteros de series H-60, debido a su precisión y su fiabilidad para el desarrollo de operaciones militares, lo que lo convierte en una navegación primaria e indispensable; ahora con ello se genera un problema sustancial como lo es la gran dependencia para la operación de las aeronaves, aperturando una superficie más amplia para un ataque cibernético, en el cual se pueda denegar la disponibilidad del sistema. Es por ello por lo que el objetivo de la investigación se centra en analizar las afectaciones a los sistemas GNSS identificando las principales amenazas, vulnerabilidades y posibles estrategias de mitigación, realizando un estudio bibliográfico sistemático y análisis en simulador de vuelo, que nos permitan identificar riesgos y controles con el fin de evitarlo, reducirlo, mitigarlo, transferirlo o aceptarlo; donde se evidencia que los sistemas de navegación de los helicópteros series H-60 por sus características sistemáticas pueden ser objetos de ataques cibernéticos como el spoofing y el jamming en cualquier fase de vuelo, lo que se convierte en una afectación directa a la seguridad operacional.

Estos hallazgos nos conllevan a la necesidad de mejorar y entender la importancia de la resiliencia en cuanto a guerra electrónica a nivel Aviación del Ejército, incorporando medidas de mitigación iniciando con la concientización, el ajuste y la implementación de procedimientos operacionales y sugiriendo nuevos sistemas redundantes en los H-60 que permitan la disponibilidad, integridad y confidencialidad del sistema.

[1] Mayor del Ejército Nacional de Colombia. Candidato a magíster en ciberseguridad y Ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. https://orcid.org/ 0009-0004-9715-8580- Contacto: julian.quintero@esdeg.edu.co.

Palabras clave: Sistemas de navegación (GNSS); aeronaves Series H-60; Navegación; Spoofing; Jamming.

Abstract: Aircraft navigation systems are essential for air operations anywhere in the world, they allow us to go from one place to another accurately and safely; GNSS systems based on satellite navigation have become indispensable in our times for navigation, not only for their precision but because they provide feedback to several additional systems depending on the type of aircraft and its configuration; This technology in our local case is essential for H-60 series helicopters, due to its precision and reliability for the development of military operations, which makes it a primary and indispensable navigation; now with this, a substantial problem is generated, such as the great dependence for the operation of aircraft, opening a wider surface for a cyber attack, in which the availability of the system can be denied. Therefore, the objective of this research focuses on analyzing the impacts on GNSS systems, identifying the main threats, vulnerabilities, and possible mitigation strategies. This research includes a systematic bibliographic review and flight simulator analysis. This will allow us to identify risks and controls in order to avoid, reduce, mitigate, transfer, or accept them. It is evident that the navigation systems of the H-60 series helicopters, due to their systematic characteristics, can be subject to cyberattacks such as spoofing and jamming at any phase of flight, which directly impacts operational safety.

These findings lead us to the need to improve and understand the importance of resilience in electronic warfare at the Army Aviation level, incorporating mitigation measures starting with awareness, adjustment, and implementation of operational procedures, and suggesting new redundant systems for the H-60s that allow for system availability, integrity, and confidentiality.

Keywords: Navigation Systems (GNSS); H-60 Series Aircraft; Navigation; Spoofing; Jamming.

Introducción

La navegación aérea, está definida por la Aeronáutica Civil Colombiana como el "método que permite operaciones de aeronaves en cualquier curso deseado, al alcance de la cobertura de una estación de referencia con señales de navegación o dentro de los límites de un sistema autocontrolado" (*Aeronautica civil,2025*), esto constituye un elemento esencial para la seguridad operacional. En este contexto, la dependencia de los instrumentos de vuelo es determinante; si estos no proporcionan información confiable de posición, actitud y altitud, es posible que los pilotos en una situación compleja puedan experimentar desorientación espacial, fenómeno responsable de entre el 25 % y el 33 % de los accidentes mortales en la aviación mundial y que en el caso de la aviación del Ejército no es la excepción (FAA Safety Briefing, 2024); (Meeks et al., 2023).

Los sistemas GNSS (Global Navigation Satellite System) se han consolidado como una tecnología primordial para la navegación aérea moderna, tanto en la aviación civil como en la militar, al proporcionar datos precisos y en tiempo real en todas las fases de vuelo (Rignér, 2020; pp.1). En los helicópteros H-60, estos sistemas no solo garantizan el posicionamiento y la altitud, sino que también se integran a subsistemas críticos como el ADS-B, el AHRS (Attitude and Heading Reference System), el AFCS (Auto Flight Control System), el FMS (Flight Manager System) y las unidades EGI, que combinan navegación inercial y satelital (FlightSafety, 2016, pp. 14-3).

Esta creciente dependencia tecnológica plantea una vulnerabilidad estratégica como los ataques cibernéticos contra las señales GNSS mediante técnicas como jamming y spoofing. Estos pueden degradar, interrumpir o manipular la señal satelital, comprometiendo

la seguridad operacional de los helicópteros del Ejército Nacional, en donde la flota H-60 representa cerca del 80% de las operaciones aéreas militares que se realizan a nivel nacional (Estadística; DAVAA).

En consecuencia, es de vital importancia preguntarnos; ¿Cómo afectan los ataques cibernéticos a los sistemas de navegación GNSS de los helicópteros H-60, y qué vulnerabilidades y estrategias de mitigación pueden identificarse?

Este artículo plantea como objetivo general analizar los efectos de los ataques cibernéticos en los sistemas GNSS de los helicópteros H-60, identificando vulnerabilidades y proponiendo estrategias de mitigación para fortalecer la seguridad operacional. Para ello, se plantean tres objetivos específicos, los cuales son: identificar las principales amenazas cibernéticas que pueden afectar dichos sistemas; evaluar los efectos de los ataques en la operación de los GNSS; y proponer lineamientos de mitigación que reduzcan las afectaciones a la seguridad cibernética en la operación de estas aeronaves.

Metodología

La investigación se planteó bajo un enfoque cualitativo, de tipo documental, con un alcance exploratorio y descriptivo (Hernández Sampieri & Fernandez-Collado, 2014), orientado a identificar, comprender y analizar las amenazas cibernéticas que afectan a los sistemas GNSS de los helicópteros H-60.

En una primera fase, se realizaron estudios documentales destinados a recolectar, revisar y analizar información proveniente de fuentes académicas, técnicas y normativas, con el fin de construir un marco interpretativo aplicado al objeto de estudio. La selección de fuentes incluyó manuales técnicos y reglamentos aeronáuticos que permitieron

contextualizar la importancia de la navegación aérea y los efectos de la pérdida de la navegación primaria vinculada con la desorientación espacial.

Posteriormente, se incorporó información estadística que permitió establecer el panorama actual del crecimiento exponencial de las afectaciones a los sistemas GNSS en la aviación a nivel mundial. Este análisis se complementó con pronunciamientos y medidas adoptadas por organismos como la FAA y la OACI, resaltando la relevancia del tema y su impacto en la seguridad operacional.

En una segunda fase, se revisaron documentos técnicos que facilitaron la comprensión de la arquitectura y el funcionamiento general de los sistemas GNSS, aplicándolos posteriormente al contexto específico de los helicópteros H-60. Este análisis permitió identificar subsistemas asociados según la serie de la aeronave y establecer las principales vulnerabilidades documentadas. De manera particular, se abordaron los ataques cibernéticos más relevantes, como el spoofing y el jamming, para proyectar sus efectos sobre el sistema GNSS de estas aeronaves.

Con base en la información recopilada, se procedió a clasificar los datos en tres categorías de análisis: amenazas cibernéticas, vulnerabilidades de los sistemas GNSS de los H-60 y estrategias de mitigación.

Una vez consolidada esta información, la investigación adoptó como referencia metodológica el modelo ISSRM (Information System Security Risk Management) , por su capacidad de representar de manera sistemática la relación entre activos, amenazas, vulnerabilidades y controles, permitiendo un mapeo conceptual detallado de activos críticos (receptores GNSS, antenas y enlaces de datos), mostrando cómo son explotados por técnicas de jamming y spoofing.

Finalmente, se realizó una evaluación cualitativa de riesgos basada en la probabilidad de ocurrencia y en la dificultad de explotación de las vulnerabilidades identificadas. Este ejercicio incluyó la simulación de escenarios en el simulador de vuelo del H-60, con el fin de estimar el impacto de las interferencias GNSS en la percepción y reacción de los pilotos.

Como cierre del proceso metodológico, se identificaron estrategias y lineamientos de mitigación que responden directamente a los objetivos específicos planteados. Entre estas medidas se incluyen la implementación de protocolos de ejecución operativa, inversiones en sistemas redundantes y de respaldo, así como tecnologías anti-jamming que fortalezcan la protección de los receptores GNSS. El propósito final es alcanzar un tratamiento de riesgos transversal que contribuya a dar solución al problema de investigación y fortalezca la resiliencia operacional de la Aviación del Ejército.

Generalidades de los Sistemas GNSS

El sistema GNSS (Global Navegation Satellite System), básicamente es una constelación de satélites que circulan en la órbita de la tierra y triangulan la posición de un GPS, para brindar posición exacta sobre un plano horizontal de cualquier lugar. (Pathak, 2024) "El GPS fue desarrollado por primera vez en 1978 como prototipo por el Departamento de Defensa de Estados Unidos. Se hizo completamente operativo en 1993 con una constelación completa de 24 satélites".

Configuración y funcionamiento

Su funcionamiento radica básicamente en calcular la distancia entre un dispositivo GPS y cada uno de los satélites que orbitan en la tierra de donde obtiene la señal, en un proceso llamado trilateración (Pozo-Ruz et al., s. f.), que básicamente radica en la segmentación de

un lugar en base a la información de cada satélite, es decir el satélite número uno ocupa un perímetro determinado de onda de señal y segundo satélite traslapa el primero, en donde se dan dos posibles opciones de posición en la intersección de círculos concéntricos, el tercer elemento satelital traslapa las señales de los otros dos segmentos y válida la posición correcta de alguna de las dos opciones. Para que este proceso funcione adecuadamente se requieren como mínimo de 3 satélites y así lograr una posición precisa bidimensional (longitud - coordenadas X y latitud - coordenadas Y) (Radoš et al., 2024, p. 4) del receptor GNSS en la superficie de la tierra. En ocasiones los dispositivos utilizan más satélites para determinar altitud y otras opciones de fuente de navegación dependiendo de la tecnología empleada (Humphreys et al., s. f.).

Tecnologías GNSS empleadas en los helicópteros series H-60.

En Colombia se cuenta con dos tipos de serie en helicópteros utilitarios H-60 (UH-60L/S-70I), ambas series de aeronaves son empleadas para las mismas tareas tácticas, como está tipificado en el (*MCE 3-04 AVIACION*, pp. 5-20) "La misión primaria del helicóptero es el transporte táctico de tropas, provisiones y equipo. Las misiones secundarias incluyen adiestramiento, movilización, desarrollo de conceptos nuevos y mejorados, y apoyo de auxilio en caso de desastres".

El UH-60L es la versión mejora de los helicópteros con denominación Alpha, esto traduce mejoras en su planta de potencia , que permiten aumento de potencia y cambios en su gobernación; y los S70i que es la versión civil del UH-60M, en cuanto características de comparación con UH-60L, se presenta un cambio muy significativo en su aviónica, la cual es más avanzada e integra un sistema FMS (Flight Manager System) y un piloto automático,

lo que otorga mejores cualidades de vuelo; y esto es demasiado importante para esta investigación debido a que los sistemas de navegación cambian drásticamente en los dos tipos de aeronaves y genera que las indicaciones y las acciones requeridas sean diferentes según la aeronave, llegado el caso se presente un ataque cibernético a los sistemas GNSS (*Sikorsky S-70A*, s. f.).

Los helicópteros UH-60L, cuentan con diferentes sistemas de navegación GNSS, en los que encontramos el HT9100 GNSS de Honeywell, el GTN 725/750 de Garmin y el Timble 8100, Estos funcionan de forma similar bajo el mismo principio y brindan información de posición, altura, velocidad verdadera, velocidad terrestre que se complementan para navegación en ruta, terminal y aproximación (incluye SIDs, STARs, aproximaciones no precisas), predicción de tiempo estimado de llegada (ETA) y capacidad VNAV para descenso no acoplado. (Sikorky *Manual del Operador para Helicopteros UH-60L*, s. f., pp. 3-1)

Ahora para que estos sistemas obtengan esta información y la procesen de forma automática cuentan con tres elementos claves, en primer lugar con una unidad central de procesamiento llamada NPU, esta recibe las señales de las antenas del GPS, computadoras de datos aéreos de la aeronave, compás heading, sensores internos de la aeronave que le ayudan a determinar cuando la aeronave se encuentra en vuelo o tierra y de los convertidores de datos (SDC), una vez procesa la información es enviada Unidad de control multifunción (MCDU), (Honeywell *GNSS Navegation Mangement System Software Load 07C*, s. f., pp. 2-5) Para ingresar datos, visualizar información del plan de vuelo y ejecutar diagnósticos de mantenimiento; ahora bien la información procesada brinda apoyo y retroalimentación a

subsistemas de la aeronave como lo es HSI/VSI (Heading Situacion Indicate) donde se obtiene información de distancia y dirección en un puntero de demarcación en dirección al destino preseleccionado, la computadora SAS/FPS la cual brindan cualidades básicas de un piloto automático con un sistema de aumento de estabilidad (SAS), el sistema estabilización de trayectoria de vuelo (FPS) y el sistema NGT-9000 (ADS-B) el cual es un sistema de transpondedor transceptor que combina funciones de vigilancia, recepción de tráfico y meteorología, cumpliendo con los estándares de la FAA, OACI, Autoridad Aeronáutica civil y de Aviación Estado, para la modernización del espacio aéreo (*HT9100-007C SYSTEM MAINTENANCE MANUAL*, s. f.).

Los helicópteros de series S-70i, cuentan con aviónica y tecnología avanzada donde se integra un piloto automático mediante un director de vuelo y sistemas que retroalimentan las comunicaciones, el FMS y otro sinnúmero de subsistemas, pero uno de sus principales cambios es la integración a todos estos sistemas de dos unidades idénticas de GPS/Inercial empotrados Honeywell H-764GU (EGI), (Keller, 2023), las cuales son utilizadas por el Sistema de Administración de Vuelo (FMS) para soluciones de navegación y cómputos de actitud de la aeronave, rumbo, presente posición , y datos de régimen de viraje. En adición a las soluciones de navegación del FMS, las EGI´s proveen de información a otros equipos de la aeronave para apoyar la distribución del tiempo, control de vuelo, y las páginas primarias de vuelo. La información de navegación y actitud provista incluye datos de posición, aceleraciones angulares y lineales, velocidad, rumbo magnético y verdadero, actitud (cabeceo y balanceo), regímenes de actitud, tiempo universal coordinado (UTC), hora y fecha. Cada EGI es un conjunto autocontenido de navegación que consiste en el recibidor de

Sistema de Posición Global Empotrado y el conjunto de Navegación Inercial (INS). Cada EGI/INS consiste en un anillo de giróscopos láser y un recibidor de GPS empotrado.

Ahora bien entendiendo cómo funcionan los sistemas GNSS en cada tipo de aeronave, podemos inferir que en caso de un ataque cibernético ya bien sea por denegación o interferencia "Jamming" o una suplantación "Spoofing", las características de vuelo de cada aeronave y el impacto es diferente, en el caso del UH-60 se perdería la capacidad de navegación mediante posicionamiento, distancia y referencias de navegación, perdida del sistema ADS-B y algunas características de cualidades de vuelo del sistema AFCS (AUTOMATIC FLIGHT CONTROL SYSTEM), relacionado con la utilización del FPS (Flight Path Stabilization) integrado con el CISP; cabe resaltar que la pérdida total o parcial del sistema GNSS no tiene indicación en la cabina de manera visual en el panel de avisos y precauciones, lo que dificulta para el piloto tomar una acción apropiada y oportuna al no poder identificar de forma clara la usencia del sistema.

En el S-70i por sus características electrónicas y su tecnología, donde se integran varios sistemas, la perdida parcial o total de una EGI o ambas en la señal del GPS, provocaría un efecto cascada en diferentes sistemas, como el FD (director de vuelo), el piloto automático, el FMS (Sistema de administrador de vuelo), computadora de vuelo asociada a la respectiva EGI, posicionamiento, El Sistema de Alerta de Conciencia del Terreno para Helicópteros (HTAWS) y ADS-B. en pocas palabras se perderían todas las funciones del piloto automático en vuelos recto y nivelado, vuelo estacionario y la capacidad para efectuar de forma automática las aproximaciones de precisión y de no precisión, también el seguimiento y control de tráfico aéreo y el posicionamiento de la aeronave y alertas de

proximidad del terreno; aunque a diferencia del UH-60L esta aeronave integra un sistema inercial que es completamente autónomo a señales externas y utiliza el GPS para complementarse, esto se convertiría en una ayuda de navegación alterna, pero más adelante cuando hablemos de las posibles soluciones al planteamiento del problema trataremos sus ventajas y desventajas.

Marco conceptual

La navegación aérea basada en tecnología GNSS implica el uso simultáneo del espectro electromagnético y del ciberespacio, lo que se traduce como actividades ciberelectromagnéticas (CEMA) (*MCE 3-12 OPERACIONES DEL CIBERESPACIO*, pp. 1-33). Este enfoque busca integrar de manera conjunta la ciberseguridad, la guerra electrónica y las operaciones militares, reconociendo que en los conflictos modernos los dominios cibernético y electromagnético no pueden planearse de manera aislada. Cualquier acción en redes impacta directamente en los sistemas que dependen del espectro electromagnético, como la navegación satelital que es empleada en el entorno de aviación.

En este contexto, las técnicas de denegación (jamming) o suplantación (spoofing) de las señales GNSS afectan de manera directa la operación aérea. La ciberseguridad ofrece las medidas orientadas a proteger la integridad, disponibilidad y confidencialidad de los sistemas de navegación, siendo especialmente relevante frente al spoofing, que busca manipular datos y engañar a los receptores GNSS.

Por su parte, la guerra electrónica constituye el marco doctrinal para comprender el jamming. La Guerra Electrónica, define tres componentes: Apoyo Electrónico (ES), orientado a la detección y análisis de emisiones; Ataque Electrónico (EA) (*MCE 3-36 Guerra*

Electrónica,), que busca degradar, engañar o negar el uso del espectro al adversario; y Protección Electrónica (EP), dirigida a preservar el empleo de los sistemas propios ante interferencias hostiles. Dentro de esta estructura, el jamming se reconoce como una técnica de ataque electrónico, al provocar la denegación de la señal GNSS en el espectro electromagnético.

La articulación de los conceptos ciberseguridad, guerra electrónica y actividades ciberelectromagnéticas constituye el marco teórico que orienta toda la investigación. En este sentido, el spoofing se comprende como un ataque cibernético que afecta la integridad de la información de navegación, mientras que el jamming se interpreta como una acción propia de la guerra electrónica, cuyo objetivo es degradar o bloquear el acceso a las señales satelitales. El CEMA, por su parte, ofrece la visión integradora que permite analizar ambos fenómenos en un escenario híbrido, donde las dimensiones cibernética y electromagnética se entrelazan.

Los ataques de jamming y spoofing a los sistema GNSS deben interpretarse dentro de una zona gris, en razon a que estos ataques no llegan a declararse como guerra abierta en donde se tenga una certeza de los actores, intensiones y sus formas, pero generan efectos estratégicos en la seguridad operacional. Para los helicópteros UH-60, esto implica que la denegación o manipulación de señales GNSS no solo constituye un riesgo técnico, sino también una herramienta híbrida utilizada por actores estatales o no estatales para degradar la capacidad operativa sin necesidad de un enfrentamiento directo, como es descrito en la manera como rusia emplea los ataques ciberneticos y la guerra electronica (*Russia's hybrid war on Europe*, 2025) . De esta manera, el concepto de zona gris complementa el marco doctrinal de la investigación, al evidenciar que la ciberseguridad y la guerra electrónica se

cruzan en un terreno intermedio que demanda preparación, resiliencia tecnológica y conciencia situacional en la tripulación.

Con este fundamento, el marco conceptual no se limita a describir amenazas, sino que orienta la metodología adoptada basada en el modelo ISSRM para identificar activos, identificar vulnerabilidades y valorar riesgos, de manera que los resultados se traduzcan en propuestas de mitigación coherentes tanto con la doctrina nacional como con marcos internacionales.

Identificación de actores y técnicas.

En el panorama actual, los ataques deliberados contra sistemas de navegación satelital (GNSS) pueden provenir de distintos actores con capacidades, intenciones y niveles tecnológicos muy diversos. Identificar y comprender a estos actores es clave para anticipar riesgos y preparar medidas de defensa más efectivas.

Actores estatales

Algunos países con capacidad tecnológica avanzada, como Rusia, Irán o Corea del Norte, han llevado a cabo interferencias deliberadas a los sistemas GNSS de las aeronaves como parte de su estrategia militar en el Oriente Medio y han proporcionado su tecnología a sus aliados (Waterman, 2024). Estos actores utilizan sistemas sofisticados capaces de bloquear señales de navegación o falsificarlas mediante técnicas de spoofing y jamming. Su objetivo suele estar relacionado con el dominio del espacio electromagnético en contextos de tensión o conflicto, y sus acciones pueden afectar tanto a aeronaves militares como a vuelos civiles cercanos, como se ha visto en zonas como Ucrania, el Mar Báltico y el Medio Oriente (Perez, 2024). Ahora bien aunque en Colombia no tiene actualmente conflicto con otros estados, si

han existido tensiones con los países vecinos, un ejemplo de esto es Venezuela y las supuestas influencias y financiamiento de los grupos armados organizados al otro lado de la frontera, así mismo tensiones por diferendos fronterizos no definidos en el mar territorial; ejemplo de ello es la crisis en los años ochenta con la fragata Caldas; esta clase de tensiones y relaciones volátiles nos hacen pensar en las capacidades y los equipos que han adquirido otras naciones para su defensa o el ataque, en el caso particular de Venezuela es sabido de la compra de equipos, a el Gobierno Ruso y el Chino como lo es el sistema CHL-906 de guerra electrónica y de igual manera del equipamiento varios a buques y aviones con tal fin . Por otro lado, y no menos importante es la disputa constante con Nicaragua por las islas de San Andrés, Providencia y Santa Catalina; adicional el aumento de la capacidad de los grupos ilegales en el Ecuador con injerencias en ambas fronteras que podría generar un problema diplomático. Esto nos lleva a pensar de que debemos estar preparados como Fuerzas Militares en todo momento, y esto incluye las capacidades estratégicas estando a la vanguardia de las nuevas tecnologías de guerras cibernéticas y electrónicas que se presentan en el dominio ciberespacial.

Grupos armados organizados

Colombia es un país que durante más de 60 años ha persistido su conflicto interno, y en nuestra actualidad los principales grupos armados organizados como él (ELN, las disidencias de las FARC y el Clan de golfo) tiene un gran financiamiento y un alto músculo económico proveniente de las economías ilícitas como lo son el narcotráfico, la minería ilegal y la extorsión entre otros. Estos actores cuentan con influencia de grandes zonas donde ejercen el control para las actividades ilícitas, y ejecutan constantemente actos hostiles para frenar el

actuar de la Fuerza Pública, realizando atentados, instrumentalización del personal civil, ataques armados y en el último año, han implementado el uso de la tecnología con drones para realizar ataques; un ejemplo es "en el último año se registraron 85 ataques con drones contra la Fuerza Pública en el departamento del Cauca, principalmente por disidencias de las FARC" (Cuesta, 2024).

Ahora de aquí podemos inferir varias situaciones particulares; la primera, estos grupos armados cuentan con el músculo financiero para adquirir cualquier tipo de equipo que genere jamming, que por sus características son de muy bajo costo, con el fin de denegar el servicio de GNSS o llegado el caso, utilizar técnicas avanzadas de spoofing implementando tecnología basada en amplificadores y simuladores de señales GNSS que generen un ambiente degradado en un área de interés, causando efectos como la cancelación de una operación militar o que afecte a una tripulación de una aeronave que podría conducir a una eventual desorientación espacial. En segunda medida, la utilización de drones para el transporte de cargas explosivas lleva a la necesidad de crear sistemas que inhibida la señal mediante técnicas y dispositivos de jamming. Estos dispositivos, de acuerdo a su capacidad de generación de ruido, también inhibida la señal GNSS de las aeronaves, y si esto es potencializado, serviría de arma con triple propósito: el primero, defenderse de ataques, inteligencia y observación de los drones de la fuerza pública; segundo, resguardar zonas de interés y tercero, ser utilizado contra aeronaves sobre avenidas de aproximación para generar confusión en las misiones de alta complejidad.

Técnicas y tipos de ataque

Las guerras hibridas contemporáneas nos han ensayado nuevas técnicas, táctica y procedimientos que los actores estatales y no estatales utilizan en entornos completamente

cambiantes, ya bien sea para la ofensiva o defensiva en búsqueda de la ventaja militar y la desestabilización, esto induce al desarrollo de nuevas dinámicas donde la tecnología y el ciberespacio juegan papales importantes y fundamentales, ejemplos claros de esto es la utilización de UAS y misiles dirigidos de alta precisión contra los adversarios, que incorporan tecnologías GNSS para poder dirigirse a objetivos específicos con un margen mínimo de error, esto intrínsicamente genera eventualmente que también se busquen técnicas para minimizar estos efectos; es en este punto donde se comienza a abordar los términos spoofing y el Jamming. Estas técnicas no solo son empleadas para minimizar efectos y daños con el uso de drones y misiles, sino que también se ha evolucionado en la teoría y práctica para ser empleados en la parte de la aviación y la marina, es así como lo explica (Álvarez, 2017) "Todd Humphreys, investigador de la Universidad de Texas en Austin, ha investigado el uso del spoofing desde 2013, demostrado que el buque con el más avanzado de los receptores GPS puede ser sacado de su curso y ocasionar caos de una forma relativamente sencilla". Y sostienen:

> "Desde hace años se está experimentando con este nuevo formato de guerra electrónica. En Moscú reportaron que sus smartphones estaban fallando al mostrar una ubicación errónea; el fallo se centraba en la zona aledaña al Kremlin, trasladando a cualquier persona al aeropuerto de Vnukovo, a 32 km de distancia". Se cree que esta falsificación en la localización estuvo activada por motivos de seguridad, ya que la mayoría de las bombas, misiles, drones y ataques aéreos dependen de la navegación GPS, por lo que el uso de un dispositivo de spoofing alejaría cualquier amenaza lejos del Kremlin".

En la arquitectura de los helicópteros H-60M para el caso del ARMY de los Estados Unidos, suelen estar equipados con receptores GPS de grado táctico que incluyen módulos de anti-falsificación SAASM (Selective Availability Anti-Spoofing Module) (*Army Aviation Reaches Navigation Milestone*, 2024), El SAASM permite a los receptores utilizar las señales criptografiadas de GPS militar (P(Y) code) en bandas de frecuencias L2, las cuales ofrecen mayor seguridad frente a spoofing al requerir contraseñas para su decodificación, aunque cabe resaltar que no son del 100% efectivos ante un ataque.

Los helicópteros S-70i, del Ejército Nacional, representan una de las series más avanzadas tecnológicamente disponibles en las Fuerzas Militares. Esto le permite tener acceso a algunos sistemas redundantes como las EGI, pero, como se mencionó anteriormente, esta es la versión civil del H-60M, lo que conlleva que no se tenga acceso a tecnologías militares como El SAASM exclusivas de la Fuerza Aeroespacial de los Estados Unidos, quienes gestionan la red de constelaciones del sistema GNSS.

Sin embargo, incluso con SAASM, los receptores siguen siendo vulnerables a interferencia de jamming, ya que la señal GPS, aunque esté cifrada, es débil al llegar a la Tierra, que es una de las principales razones por las que se produce la interferencia (*Global Navigation Space Systems*, 2011, p. 13).

Ahora, una de las consideraciones más importantes que se debe tener en cuenta en esta investigación radica en que la mayoría de H-60 (cerca del 90% de toda la flota H-60); en servicio son modelos antiguos (UH-60L), cuyos receptores GNSS no cuentan con mejoras de seguridad, así como la falta de sistemas inerciales de respaldo, por lo que entender las vulnerabilidades actuales del GNSS en los H-60 es crítico para mitigar riesgos mientras se

implementan dichas mejoras o, como en el caso de esta investigación, se propongan alternativas viables para administrar y gestionar el riesgo.

Jamming (Interferencia)

Este ataque cibernético afecta la disponibilidad y la integridad de los sistemas GNSS de las aeronaves, que en cierta forma lo podríamos catalogar como una denegación de servicio (DoS) electromagnético; básicamente consiste en la interferencia de las señales de satélites mediante la emisión deliberada de ondas de radiofrecuencia en su misma banda con mayor frecuencia, esto colapsa el espectro en bandas de frecuencias que para nuestros casos nos aplicaría (L1) entre 1 GHz y 1,6 GHz aproximadamente, bloqueando las señales reales de cada satélite. Esto se da en cierta parte por varios factores como la interferencia ionosférica y la distancia entre los satélites y el receptor como lo argumenta (Morales-Ferre et al., 2020) "una consecuencia de la baja potencia de los sistemas de navegación por satélite, y en particular de las señales GNSS utilizadas en la navegación basada en GNSS, es su vulnerabilidad a las interferencias. Por ejemplo, una interferencia de baja potencia (10 dBm) emitida por un inhibidor de bajo costo (10 euros) puede bloquear cualquier señal GNSS en un radio de 100 m alrededor del inhibidor, provocando la pérdida de la navegación GNSS"; esto quiere decir que con una buena inversión y con equipos un poco más potentes, un atacante puede alcanzar grandes distancias, tanto verticales como horizontales, que se ve mucho más agudizado en el vuelo de aeronaves de ala rotatoria como es el caso de las aeronaves H-60, que por sus misiones y características vuelan a bajo nivel (por debajo de 200 Ft), al estar aproximadamente a 10 millas fuera de los objetivos.

Los helicópteros H-60 tienen la particularidad de contar con diversos sistemas de navegación, como lo son VOR-ILS-ADF adicionales a los sistemas GNSS, y los S-70i cuentan con la adición de los sistemas inerciales, que son sin lugar a dudas alternativas validadas para la ejecución de vuelos, pero esto depende en gran medida del tipo de vuelo que se realice, ya bien sea vuelos administrativos o tácticos, debido a que la complejidad de la misión determina en cierta medida las acciones subsiguientes a un ataque cibernético. En el contexto de las operaciones tácticas, el H-60 emplea el GPS no solo para la navegación primaria de punto "A" a punto "B", sino también para la orientación de rutas planificadas. Sin embargo, es fundamental tener en cuenta que ningún receptor GNSS es inmune a las interferencias de radiofrecuencia y bajo estos contextos es imposible acceder a otros medios alternativos de navegación en el caso de UH-60L, las aeronaves S-70i tendrían la posibilidad de acceder al sistema inercial, pero aun así las EGI perderían capacidad de precisión por acumulación de errores dependiendo del tiempo y la distancia de exposición a la interferencia y sin GPS se pierde funciones como la capacidad de alinearse rápidamente en vuelo o de recalibrar errores generando acumulaciones que un momento de alta tensión el piloto no podría identificar y no daría tiempo para tomar una medida que contrarreste la interferencia sino cuenta con un buen criterio, análisis y entrenamiento en entornos VICA (volátiles-inciertos-complejos-ambiguos).

Un ataque de interferencia bien planeado contra un H-60 podría aprovechar sus puntos débiles. Lo ideal sería saturar la banda GPS cuando el helicóptero se encuentra en una fase de vuelo delicada, como baja altitud, vuelo de formación con múltiples aeronaves o condiciones meteorológicas adversas, para causar la máxima incertidumbre con un alto

impacto. Por ejemplo, si un H-60 está realizando una misión especial en condiciones LVN, un dispositivo de interferencia que interrumpa la señal a mitad de ruta podría generar que la tripulación falle en la ubicación del objetivo o el punto de inserción, comprometiendo la misión y la integridad de la aeronave y del personal que transporta, abriendo la posibilidad de entrar en una desorientación espacial o realizar un desembarco en un área preparada. En un escenario aún más desfavorable, una suplantación dirigida podría hacerles creer que han llegado al punto correcto cuando en realidad se encuentran a kilómetros de distancia, causando errores operativos graves. En ejercicios, se ha demostrado que las tripulaciones poco entrenadas pueden tardar varios minutos en percatarse de que el GPS les proporciona información errónea, especialmente si las indicaciones en cabina parecen poco obvias.

Spoofing (suplantación)

La suplantación de GPS constituye un método mediante el cual una persona altera intencionalmente las señales difundidas por el Sistema de Posicionamiento Global (GPS). El objetivo de esta interrupción del GPS/GNSS es proporcionar información espacial o temporal errónea a los receptores del GPS, lo que da lugar a la presentación de datos de ubicación engañosos, lo que puede tener consecuencias adversas para los sistemas de navegación, los dispositivos y las aplicaciones basadas en satélites (*Aviations GPS Spoofing & How to Avoid It | APG*, s. f.). A diferencia del jamming (interferencia que bloquea o degrada la señal y resulta evidente por la pérdida de señal), el spoofing engaña silenciosamente al sistema, haciendo que las tripulaciones y sistemas automáticos confíen en datos de navegación falsos.

Ahora bien, como lo explicamos anteriormente, los sistemas GNSS con los que se cuentan actualmente, no integran la tecnología suficientes para hacer frente a un ataque

cibernético de estas características y esto es debido en gran medida a la dependencia de señales satelitales en las bandas de frecuencia L1 (1575.42 Mhz) que son extremadamente bajas, las cuales carecen de sistemas de autenticidad de señales como el sistema SAASM (Selective Availability Anti-Spoofing Module), (Cole, s. f.)

Los dispositivos de suplantación de identidad no solo están disponibles con mayor facilidad, sino que también son significativamente menos costosos. Un dispositivo de suplantación utilizado anteriormente para redirigir una embarcación, que tenía un precio aproximado de 3000 USD en 2013, ahora puede adquirirse por menos de 250 USD (Tech & Liu, s. f., p. 4). Estos dispositivos no solo han demostrado su eficacia, sino que también están diseñados para un uso discreto; sus dimensiones son similares a las de un teléfono, integrado en muchas ocasiones con unos amplificadores de frecuencias y un simulador de GNSS, (Westbrook, 2023).

Ahora bien, este ataque es considerado como uno de los más peligrosos y esto radica en la incapacidad del piloto para determinar si está ante un eventual ataque de suplantación, ocasionando que una aeronave se desvíe del curso y de su objetivo real, y en cuanto a la complejidad de las operaciones que realizan las aeronaves, esto sería crítico, porque se podría presentar un aterrizaje en un área preparada o entrar en condiciones meteorológicas adversas con niveles mínimos de visibilidad, lo que conllevaría a desorientación espacial que terminaría en un eventual accidente.

Tabla 1. Técnicas de ataque.

Criterio	Jamming	Spoofing
Definición	Emisión intencional de radiofrecuencia en la misma banda del sistema GNSS, con el fin de saturar el receptor y bloquear la señal legítima.	Generación y transmisión de señales falsas GNSS que imitan a las originales, logrando que el receptor procese información de posición, velocidad y tiempo incorrecta.
Mecanismo de acción	Incrementa el nivel de ruido térmico en el canal, reduciendo la relación señal/ruido por debajo del umbral mínimo requerido (–30 a –33 dB-Hz en GPS L1 C/A), imposibilitando la adquisición o el tracking de la señal.	Manipula la estructura de los códigos de espectro ensanchado (ejemplo. C/A Code en L1, P(Y) Code en L1/L2) generando réplicas sincronizadas que desplazan gradualmente la solución de navegación.
Impacto en aeronaves	Pérdida de capacidad de GNSS; la tripulación recibe indicaciones de cabina. Se requiere recurrir a sistemas alternativos (INS-DME-VOR/VHF).	Engaña al receptor manteniendo la disponibilidad del GPS, pero con datos falsos; mayor riesgo porque no se detecta de inmediato y puede inducir trayectorias erróneas en fases críticas (aproximación, inserción, misiones complejas).
Clasificación doctrinal	Se clasifican como guerra electrónica se trata de interferencia electromagnética deliberada	Constituye una "línea gris": puede ser guerra electrónica (emisión engañosa) y también ciberataque porque compromete la integridad de los datos. OACI y la doctrina colombiana (RACAE 91) lo reconocen como interferencia ilícita.
Nivel de detección	En relación con la aeronave, una pérdida total de señal es rápidamente identificada por los sistemas de monitoreo, especialmente en aquellos que incorporan tecnología con retroalimentación integrada a las señales, permitiendo detectar inconsistencias de manera eficiente.	Difícil de detectar: el receptor sigue funcionando. Se requiere detección avanzada (antenas multibanda, verificación por ángulo de llegada, autenticación criptográfica, correlación cruzada).
Ejemplos documentados	Interferencias en Siria y Ucrania (uso de jammers militares de alta potencia), reportes de STRIKE3 con 73.000 eventos de gran impacto .	Incidentes marítimos en el Mar Negro (buques desviados), drones desviados en conflictos, ensayos en laboratorios (Univ. Texas 2013) y en ejercicios OTAN NAVWAR.

Riesgo operacional en UH-60L	Puede afectar la fase IFR o aproximación, despegue en zonas sin ayudas terrestres, misiones de alta complejidad.	Riesgo crítico: en operaciones tácticas: infiltración, CSAR, aproximaciones en condiciones meteorológicas adversa, puede comprometer la misión sin que la tripulación note el engaño, incrementando la probabilidad de accidente o ingreso zonas preparadas.

Fuente: Elaboración propia

Análisis de resultados.

En los últimos años se ha evidenciado notablemente la interrupción de recepción o transmisión de datos erróneos en los sistemas de navegación de las aeronaves que utilizan como fuentes primarias los sistemas GNSS; un ejemplo de esto es el caso documentado por OpsGroup (GPS-Spoofing-Final-Report-OPSGROUP-WG-OG24), Destacan la desviación de un avión comercial el 09 de septiembre del 2024 que volaba en la ruta Turquía-Irak; cuando se acercaban a la frontera de Irak, tuvieron algunas indicaciones en los sistemas que suponían una eventual pérdida del GPS, la tripulación continuó con el vuelo con apoyo de la navegación de respaldo en el IRS (navegación inercial). Al norte de Bagdad, la tripulación de vuelo perdió todos los sistemas de navegación, y el IRS indicó que se habían desviado entre 70 y 90 millas de la ruta, próximos a ingresar a espacio aéreo no autorizado.

Estos casos siguen aumentando de una forma exponencial y gran parte se debe a la necesidad de las naciones en conflicto de mantener su supremacía en el dominio ciberespacial, afectando todo tipo de aeronaves, tanto civiles como militares, en razón de que un ataque de tipo spoofing o jamming no discrimina una cosa de la otra, y en otros casos se

debe a personas o piratas informáticos que utilizan software o dispositivos de interferencia; esto es afirmado por (Westbrook, 2023). Es también de suma importancia reseñar el despliegue que ha tenido la Unión Europea para analizar estas situaciones particulares en donde "se captaron y analizaron 450.000 señales de interferencia del GNSS, de las cuales 73.000 se clasificaron como de gran impacto en el GNSS, y 59.000 de ellas se identificaron como señales de interferencia".

Otros datos estadísticos que debemos analizar son los recopilados por Eurocontrol que desde el año 2017 al 2019 logran identificar un aumento del 2.000% en interferencias a los sistemas GNSS (*eurocontrol-think-paper-9-radio-frequency-intereference-satellite-navigation.pdf*, s. f.).

En el año 2019, entre julio y agosto, la OACI reportó más de 50 informes de interferencias en las señales de estos sistemas cerca de aeropuertos internacionales con alto flujo aéreo, en la mayoría de los casos, estás afectaciones ocurren de forma sistemática, mas no aislada. En el año 2024, en la Vigésima segunda Reunión del Grupo Regional de Planificación y Ejecución del Caribe y Sudamérica (*GRP22NI14.pdf*, s. f.), se comienzan a tratar las posibles formas de mitigación del jamming y spoofing en las operaciones aéreas, donde lo catalogan como una amenaza significativa para la segurida operacional mundial (OACI, s. f.).

Ahora bien, dentro de los ejercicios conjuntos de entrenamiento realizado por la OTAN, sobre el sector cabo blanco en las isla Mallorga sobre el mediterráneo, se han utilizado técnicas de jamming y spoofing mediante pruebas diseñadas para demostrar la efectividad de un sistema denominado LOKI, implementado por Centro Universitario de la

Defensa en la Escuela Naval Militar de España, (Ortuño et al., 2024) y se demuestra la facilidad de crear un dispositivo capaz de generar degradación en los sistemas GNSS de buques y aeronaves utilizando un computador portátil, un simulador GNSS, un amplificado de señal en las bandas de frecuencia L1 y una antena de tipo helicoidal, donde han obtenido resultados de jamming y spoofing a una distancia de diez millas desviando la trayectoria de aproximadamente 15 buques navales (MARSEC, MINEX, NEMO, GNEX) y varias aeronaves tanto de ala fija como ala rotatoria de forma exitosa; esto se efectúa utilizando los dos tipos de ataques de forma casi simultánea.

De acuerdo con lo anterior, la posibilidad de ocurrencia, como se analiza a nivel mundial, es exponencial y las capacidades de los actores en varios ambientes operacionales han aumentado probablemente por la evolución de la tecnología y el carácter de la guerra que muta atreves del tiempo; es por ello, por lo que es necesario observar las características de respuesta de las tripulaciones ante un ataque cibernético en cuanto a la suplantación o denegación de los sistemas GNSS.

Para estos casos se plantean dos escenarios particulares: uno de ambientes de alta complejidad y otro de baja complejidad, y esto se basa en el análisis de riesgo de la misión (amenaza, supervisión, planeamiento, frecuencia en operaciones, experiencia, condiciones meteorológicas, complejidad de misión, factores geográficos, factores de LVN) = MUY ALTO-ALTO-MEDIO-BAJO.

Ahora bien, las tendencias de las tripulaciones observadas en simulador de vuelo son extraídas de los dos escenarios anteriores y juegan un papel muy importante en la parte cognitiva de las acciones instintivas e inmediatas a realizar por parte de las tripulaciones,

basado básicamente en el tiempo para identificar y responder ante el evento y las situaciones de vuelo donde se presentan; así podemos identificar las siguientes tendencias comunes; así:

- Una de las principales dificultades que enfrentan las tripulaciones es la falta de identificación oportuna del ataque, ya que suelen depender exclusivamente de las indicaciones de cabina o de la navegación visual. Esto se debe, principalmente, a la ausencia de un adecuado planeamiento y al desconocimiento del área de operación. En consecuencia, la incapacidad para reconocer de inmediato el evento compromete la toma de decisiones y aumenta el riesgo durante la operación.
- Las reacciones instintivas se reducen por falta de conocimiento de procedimientos y de la problemática. (No hay enlaces neuronales) que permitan acciones inmediatas; en consecuencia, el piloto tiende a efectuar un procedimiento dependiendo de sus creencias o experiencias, que pueden ser buenas o malas, con vacíos procedimentales y secuencias lógicas.
- Desorientación espacial; la tripulación pierde la percepción de la ubicación de los puntos cardinales, sin saber bajo una toma de decisiones acertadas hacia qué sector proceder, debido a la pérdida de navegación primaria y secundaria.
- Los pilotos con acceso pleno de los controles de vuelo tienen la tendencia de virar hacia la derecha, desacelerar la aeronave, a velocidades extremadamente bajas y peligrosas, que generan falta de control positivo de la aeronave.
- Coordinación de la tripulación mínima; esto genera confusión e incertidumbre y en la administración de la cabina tiene tendencias de fijación por parte de la

tripulación, adicional de una característica marcada por parte del piloto al manado de solucionar de forma autónoma la contingencia, generando cargas autoimpuestas.

- En condiciones de baja visibilidad, hay tendencias de entrar en condiciones meteorológicas imprevistas con un bajo juicio y resolución de la situación.

Riesgos asociados a las tecnologías GNSS aplicados a los H-60.

Como se analizó anteriormente, la navegación aérea y la utilización de los sistemas GNSS en las aeronaves H-60, son indispensables para llevar a cabo todo tipo de misiones. Ahora bien hemos identificado algunos actores y técnicas que pueden ser utilizadas en contra de nuestros sistemas y su arquitectura, que nos lleva en este momento a analizar el entorno operacional donde se identifican las amenazas relevantes y el desarrollo de vulnerabilidades, los activos potencialmente afectados, y se propone un tratamiento de riesgos que incluye algunas medidas de reducción del impacto.

Tabla 2. Identificación de la amenaza "1" ISO/IEC 27005/2022 – Gestión de Riesgos en Seguridad de la Información.

Principios de seguridad		**Disponibilidad**	**Integridad**	**Confidencialidad**
Amenaza	**Pérdida de integridad de navegación**	x	x	x
Descripción	Se generan señales falsas que simulan ser auténticas, induciendo al sistema GNSS a calcular una posición errónea.			
Vulnerabilidades	• Falta de autenticación en señales GNSS civiles (L1 C/A) • Ausencia de filtros anti-spoofing • Receptores sin verificación cruzada con INS (sistema inercial) • Falta de entrenamiento de tripulaciones • No hay procedimientos de emergencias			
TTP	• **Táctica:** Impedir acceso a áreas de alto interés, ejes de acceso, en vuelos ejecutados de baja altitud, busca redirigir a zonas preparadas.			

	• **Técnica:** Spoofing • **Procedimientos:** Observación de áreas recurrentes , con inicio del ataque y prolongación sobre estas rutas.

Fuente: Elaboración propia

Tabla 3. Identificación de la amenaza "2" ISO/IEC 27005/2022 – Gestión de riesgos en seguridad de la Información.

Principios de seguridad		Disponibilidad	Integridad	Confidencialidad
Amenaza	**Pérdida total de señal GNSS**	x	x	
Descripción	Saturación de ruido de las bandas de frecuencias L1.			
Vulnerabilidades	• Falta de protección de las antenas receptoras de la señal • Receptores sin función hold/freeze en misión crítica • No integración con INS o sensores redundantes • Falta de entrenamiento tripulaciones • No hay procedimientos de emergencia			
TTP	• **Táctica:** Denegar el servicio del sistema GNSS, inhabilitando todas sus funciones. • **Técnica:** Jamming • **Procedimientos:** Zonas constantemente preparadas de alto flujo y movilidad operacional, utilización de dispositivos de generación de ruido en bandas de frecuencia entre 1 GHz y 1,6 GHz.			

Fuente: Elaboración propia

Tabla 4. Identificación de la amenaza "3" ISO/IEC 27005/2022 – Gestión de Riesgos en Seguridad de la Información.

Principios de seguridad		Disponibilidad	Integridad	Confidencialidad
Amenaza	**Pérdida de GNSS en situaciones de maniobras críticas.**	x	x	
Descripción	Debido a interferencia se pierde varios subsistemas que utilizan GNSS.			
Vulnerabilidades	• Sistema de alertas en cabina. • No interpretación de las alertas asociado a la perdida de sistemas. • Falta de entrenamiento tripulaciones • No hay procedimientos de emergencia			
TTP	• **Táctica:** Generar reacción en cadena a los sistemas de la aeronave induciendo perdidas de control y percepción cognitiva. • **Técnica:** Jamming • **Procedimientos:** Zonas constantemente preparadas de alto flujo y movilidad operacional , se ubican de forma permanente en sectores altos, entradas de cañones y se tiene más de un dispositivo.			

Fuente: Elaboración propia

Tabla 5. Identificación de la amenaza "4"- ISO/IEC 27005/2022 – Gestión de Riesgos en Seguridad de la Información.

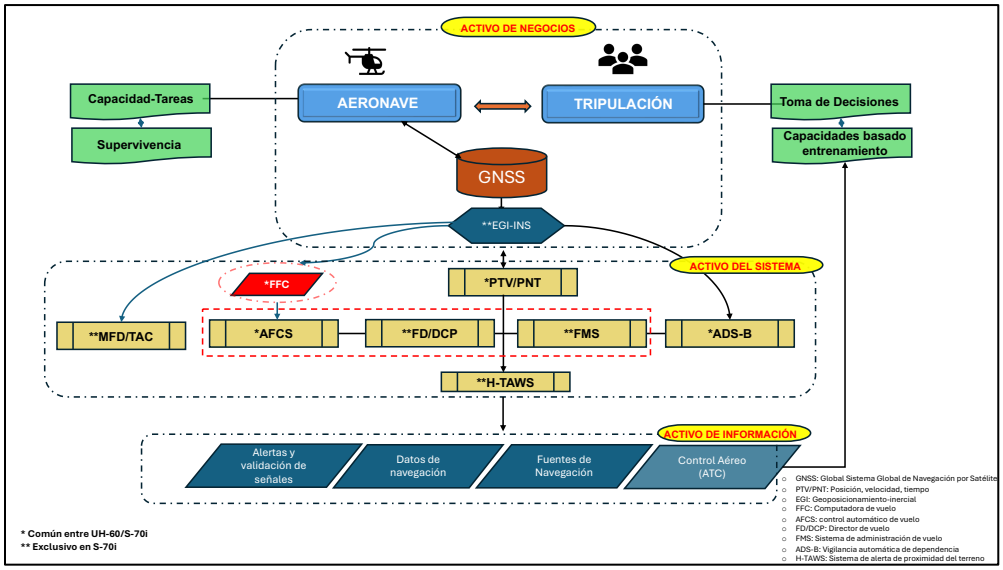
Principios de seguridad		Disponibilidad	Integridad	Confidencialidad
Amenaza	**Manipulación de trayectoria de vuelo**	x	x	
Descripción	Ataque deliberado que causa los cambios de rumbos y modifica el segmento de trayectoria durante un lapso.			
Vulnerabilidades	• Falta de autenticación en señales GNSS civiles (L1 C/A) • Ausencia de filtros anti-spoofing • Receptores sin verificación cruzada con INS (sistema inercial) • Falta de entrenamiento tripulaciones • No hay procedimientos de emergencia			
TTP	• **Táctica:** Desorientar a la aeronave o llevarla a un punto falso de destino, de forma constante, buscando alejarla de un área de interés especifica, evitando acceso preciso a una área de interés. • **Técnica:** Spoofing • **Procedimientos:** Configuración de escenario falso, interferencia de señales reales y emisión de señales falsas desde un punto geográfico controlado.			

Fuente: Elaboración propia

Identificación de activos.

Los activos de negocios los representamos básicamente en 3 grandes grupos (Figura 1), que trabajan de forma sincronizada para lograr un vuelo seguro en el cumplimiento de una misión y estos se relacionan de la siguiente forma:

Figura 1. Identificación de activos "arquitectura básica de los sistemas"



Fuente: elaboración propia con base a los manuales del operador Uh-60l/S70i (capitulo 3).

Como foco central encontramos la **aeronave** la cual es una capacidad institucional que nos permite el cumplimiento de la misión de una forma razonable y segura independientemente del contexto operacional o variables que puedan existir en espacio, tiempo o condición determinada, es por ello que se requiere **tripulaciones** entrenadas con la suficiente capacidad y experticia que le permitan tener una adecuada toma de decisiones en momentos críticos, pero para llevar a cabo un vuelo seguro en cualquier contexto operacional es requerido de la precisión y sincronización de la navegación en ruta y objetivos, mediante la disponibilidad del sistema **GNSS en los depósitos GPS/INS** (EGI) el cual retroalimenta otras subsistemas de la aeronave que completan funciones básicas de comportamiento de vuelo, navegación precisa y otras de grado terciario en cuanto a seguimiento y control de ruta.

Ahora la relación interseca existente con los activos del sistema impactan directamente el vuelo y la controlabilidad de la aeronave en razón a que las señales recibidas

desde las EGI a las FCC1/2 son procesadas y enviadas al sistema AFCS, que están integrado por 4 componentes principales los cuales serán degradados de forma parcial como lo es el sistema de aumento de estabilidad (SAS), sistema de trayectoria de vuelo (FPS) entrelazado con el director de vuelo en funciones como el HOVER POS/ACLL/DESC (posicionamiento en vuelo estacionario) y deshabilitando la función recuperación inusual impidiendo la desaceleración de la aeronave para mantener la posición deseada al momento de realizar el PUSH en el cíclico, en adición a lo anterior se perdería el ADS-B impidiendo la observación de posicionamiento del control del tráfico aéreo con la dependencia de control y con otras aeronaves y esto es completamente delicado y crucial en un ambiente de control de tráfico aéreo con alto flujo de aeronaves.

Propuesta de tratamiento de riesgos

Inicialmente, vamos a definir los riesgos de acuerdo con el análisis de amenazas, vulnerabilidades y la categorización de sus activos y sus relaciones, para realizar una evaluación y poder efectuar un tratamiento en donde vamos a categorizar la acción entre (evitarlo, reducirlo, transferirlo o aceptarlo).

Tabla 6. Identificación de riesgo Nº1

Riesgo Nº1	**Componentes de riesgo específicos**
Activos del sistema	• MFD/TAC • ADS-B • FMS
Vulnerabilidad	1. Métodos de autenticación del sistema con encriptación. 2. Falta de capacidad de detección por parte de la tripulación. 3. No hay redundancia en el sistema (UH-60L).
Agente de amenaza	1. **Agente:** Estados, GAO, GDO

	2. **Capacidad:** Acceso a dispositivos y capacidad de guerra electrónica obtenida de experiencias en guerras mundiales actuales; Ejemplo. Utilización de drones; debido al alto grado de recursos económicos con que se cuenta. 3. **Motivación:** Guerra prolongada en búsqueda de minimizar la capacidad aérea de movilidad y desarrollo de operaciones quirúrgicas de alta precisión.
Método de ataque	• Spoofing.
Impacto y sus daños	• Colisión con otras aeronaves en un espacio aéreo controlado con alta afluencia de aeronaves. • Accidentes aéreos en condiciones de vuelo de baja visibilidad, donde el vuelo VMC es completamente limitado.
Definición del riesgo	Un atacante, mediante un simulador GNSS, retarda y altera la hora con respecto al generador principal de tiempo atómico, inyectando nuevos parámetros de tiempo, generando en tiempo y espacio disparidad, con navegación errónea y desvió de trayectoria de la aeronave.

Fuente: elaboración propia

Tabla 7. Identificación de riesgo Nº2

Riesgo Nº2	**Componentes de riesgo específicos**
Activos del sistema	• MFD/TAC • H-TAWS • FFC • ADS-B • PTV/PNT • AFCS
Vulnerabilidad	1. Sistemas de protección robustos de anti-jamming. 2. Falta de capacitación por parte de las tripulaciones al reaccionar de forma oportuna e inmediata. 3. No hay redundancia en el sistema (UH-60L). 4. Dependencia del ADS-B para el control de tráfico aéreo.
Agente de amenaza	1. **Agente:** Estados, GAO, GDO.

	2. **Capacidad:** Acceso a dispositivos comerciales y algunos más avanzados, financiados por otros estados o de adquisición propia, con alcances perimetrales de 10 MN alrededor de una zona de interés. 3. **Motivación:** Afectación de las aeronaves con el fin de denegar el acceso a zonas de alta influencia criminal con intereses particulares.
Método de ataque	• Jamming.
Impacto y sus daños	• Estos impactos varían de acuerdo con la condición de vuelo y las tareas que se realicen en un entorno operacional. En vuelos que por sus características son controlados, tanto sus espacios aéreos, como en el tipo de misión, donde por la configuración de la misión, la altura, velocidades y condiciones meteorológicas logran que el impacto y daño sea menor, en razón de la posibilidad de tener tiempo, medios y radio de acción, se puede responder a un ataque de forma controlada, buscando sistemas alternos de navegación. Ahora bien, estas condiciones varían en un entorno mucho más complicado que integra vuelos a bajo nivel, baja velocidad, condiciones meteorológicas y visuales degradadas, múltiples aeronaves en zonas con características del terreno adverso con topografía variable y confinada; estos factores son sumamente importantes en el desarrollo de tareas y es el ambiente operacional común donde las aeronaves operan. Con este contexto presente, un ataque en un entorno complicado sería crítico en razón de la confluencia de muchos factores que pueden llevar a una desorientación espacial en zonas con difícil oportunidad de maniobra que conllevarían un accidente aéreo, si no se cuenta con el suficiente entrenamiento y capacidad de reacción.
Definición del riesgo	Un atacante, mediante el uso de varios dispositivos de bajo costo y de fácil acceso comercial, ubicados de forma estratégica en un área determinada, genera ruido a las señales de banda a las aeronaves que vuelan a baja altitud y velocidad, denegando el servicio en su disponibilidad e integridad, buscando degradar la capacidad de movilidad y ejecución de operaciones militares.

Fuente: Elaboración propia

Tabla 8. Identificación de riesgo Nº3

Riesgo Nº3	**Componentes de riesgo específicos**
Activos del sistema	• Sistema de misión asistida (MFD, FMS). • Director de vuelo (FD/DCP). • PTV/PNT

	• AFCS
Vulnerabilidad	1. Dependencia funcional de los sistemas GNSS para realizar maniobras críticas sin un entrenamiento robusto en modos manuales o de respaldo. 2. Falta de redundancia, como INS (Inertial Navigation System) no calibrado o no disponible.
Agente de amenaza	1. **Agente:** Estados, GAO, GDO 2. **Capacidad:** Acceso a dispositivos y capacidad de guerra electrónica obtenida de experiencias en guerras mundiales actuales; ejemplo. Utilización de drones; debido al alto grado de recursos económicos con que se cuenta. 3. **Motivación:** degradar la capacidad operativa, generar confusión o evitar la presencia militar en operaciones.
Método de ataque	• Jamming-Spoofing
Impacto y sus daños	• Pérdida del control automatizado de la aeronave en maniobras de bajo nivel o vuelo estacionario. • Degradación en la precisión de maniobras críticas como asaltos aéreos o misiones especiales. • Mayor exposición al error humano bajo estrés debido a eventos inesperados en situaciones críticas, como inserción de tropas mediante técnicas especiales, aterrizajes o despegues y tramos finales de las aproximaciones. • Abortar la misión o incurrir en errores tácticos graves como aterrizajes o desembarcos en zonas preparadas.
Definición del riesgo	Un atacante, utilizando diferentes técnicas (jamming-spoofing), logra degradar o inhabilitar los sistemas GNSS de la aeronave, generando un fallo funcional de los sistemas de navegación, guiado y misión durante maniobras críticas debido a interferencias GNSS.

Fuente: elaboración propia

Tabla 9. Identificación de riesgo Nº4

Riesgo Nº4	**Componentes de riesgo específicos**
Activos del sistema	• PTV/PNT • Sistema de misión asistida (MFD, FMS).

Vulnerabilidad	1. Métodos de autenticación del sistema con encriptación. 2. Pérdida de la conciencia situacional por falta de referencias visuales y fuentes óptimas de navegación. 3. Falta de capacidad de detección por parte de la tripulación. 4. No hay redundancia en el sistema (UH-60L).
Agente de amenaza	1. **Agente:** Estados, GAO, GDO 2. **Capacidad:** Acceso a dispositivos y capacidad de guerra electrónica por su alta capacidad financiera, obtenida por las diferentes economías ilícitas. 3. **Motivación:** Causar un gran daño e impacto a las aeronaves de asalto, afectando las misiones y disminuyendo la capacidad de la Fuerza.
Método de ataque	• Jamming-spoofing.
Impacto y sus daños	• Este impacto es altamente peligroso, debido a que un campo preparado conlleva a la destrucción total de la aeronave y afectación a los ocupantes y las tripulaciones.
Definición del riesgo	Un atacante, mediante el uso de simuladores GNSS, logra que una aeronave ingrese de forma intencionada a zonas preparadas, hostiles o peligrosas debido a alteraciones y falsificación en la navegación satelital.

Fuente: elaboración propia

Tabla 10. Identificación de riesgo Nº5

Riesgo Nº5	Componentes de riesgo específicos
Activos del sistema	• MFD/TAC • H-TAWS • FFC • ADS-B • PTV/PNT • AFCS
Vulnerabilidad	1. Entrenamiento de las tripulaciones ante escenarios de guerra electrónica. 2. Alta dependencia de los sistemas GNSS 3. No hay redundancia en el sistema (UH-60L).
Agente de amenaza	1. **Agente:** Estados, GAO, GDO

	2. **Capacidad:** Para lograr un ataque más efectivo, se utilizan los métodos de ataque de forma sincrónica, de manera que inicialmente se efectué un jamming con el fin de denegar la disponibilidad del sistema y posteriormente inyectar mediante el spoofing nuevas indicaciones falsas. 3. **Motivación:** Causar un gran daño, destrucción e impacto a las aeronaves de asalto y las tripulaciones, impactando las misiones y disminuyendo la capacidad de la Fuerza.
Método de ataque	• Jamming-spoofing.
Impacto y sus daños	• El impacto es completamente abrumador, debido a que los sistemas, aunque son afectados, no van a lograr causar un daño visible si no se afecta cognitivamente a las tripulaciones, que identifican, procesan y responden al ataque, y este es el objetivo final que tiene como resultado aprovechar la falta de capacidad de entrenamiento en análisis y respuesta, y lograr el efecto de cancelar una misión estratégica hasta generar un accidente aéreo, alimentado por las condiciones y entornos complejos.
Definición del riesgo	Un atacante utilizando métodos simultáneos, denegando el servicio y posteriormente inyectando información falsa, logrando desorientación espacial en pilotos por pérdida de referencias GNSS en condiciones operativas adversas.

Fuente: Elaboración propia

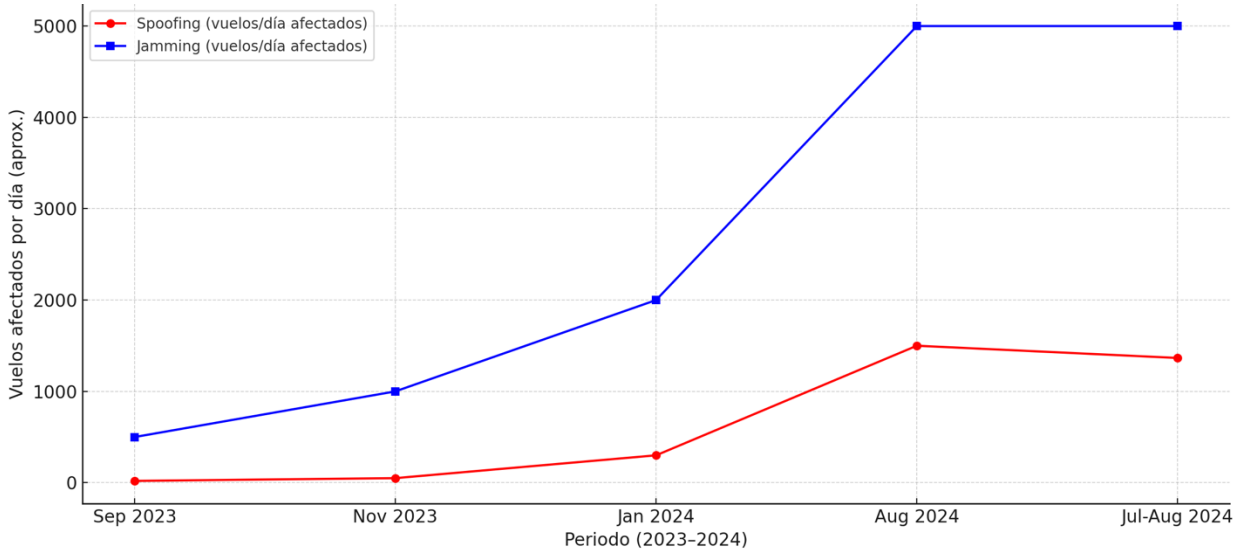
Evaluación de riesgo.

Durante este proceso de evaluación para determinar la amenaza se realiza un cruce de probabilidad Vs impacto. En primer lugar se determinó la probabilidad basada en dos variables que incluye la frecuencia histórica y la capacidad técnica para el desarrollo del ataque.

Como primer criterio a nivel mundial se documenta un aumento vertiginoso de esta problemática documentada desde el año 2022 por la agencia de seguridad de aviación de la Unión Europea (*Safety Information Bulletin Operations – ATM/ANS – Airworthiness*), de la misma forma en Europa en abril del 2024 se reportan cerca de 46.000 ataques de jamming

(Topham & correspondent, 2024), estos datos también son respaldos por (*GPS-Spoofing-Final-Report-OPSGROUP-WG-OG24*, s. f.) en sus informes donde detallan el crecimiento exponencial de 41.000 vuelos afectados en un mes (julio-agosto del 2024), un promedio que pasa de 300 a 1.500 vuelos al día durante 2024.

Figura 2. Tala comparativa Jamming Vs Spoofing



Fuente: OPSGROUP, GPSJam, EASA.

Ahora como lo observamos en la tabla comparativa podemos analizar que los ataques de jamming son más frecuentes que los spoofing y esto se debe básicamente a las capacidades técnicas para el desarrollo y el bajo costo en la adquisición, construcción o implementación.

Como segundo criterio, analizamos un ejercicio activo de simulación de un ataque real de spoonfing y jamming a una plataforma TECNAM P-92, donde se reafirma la teoría de las vulnerabilidades e impacto a los sistemas de navegación de las aeronaves en las bandas de frecuencia L1 y L5, (Iudice et al., 2024), esto es de suma importancia porque nos permite analizar la complejidad técnica que existe para ejecutar un ataque spoonfing para sincronizar tiempo, fase y potencia, pero esto no quiere decir que no se pueda realizar de forma sencilla

con cierto nivel intermedio de conocimientos, y con un dispositivos con SDR (Software Defined Radio) (Kožović & Đurđević, 2021), a diferencia de jamming que requiere menos sincronización y puede lograrse con suficiente potencia saturando de ruido.

Ahora bien, basado en el análisis vamos a determinar los riesgos sumados con la características de ataque añadiéndole peso a los factores de probabilidad basado en la frecuencia de los factores. En este orden de días determino darle un 60% (0,6) a la frecuencia basado en las estadísticas de aumento de los factores y en segunda medida 40% (0,4) basado a los aspectos técnicos cualitativos de la investigación.

Tabla 11. Medición de la probabilidad.

Riesgo	Tipo	Vuelos Promedio afectados a nivel mundial	Frecuencia (F)/(1–5)	Capacidad (C)/(1–5)	Índice compuesto (IP) 0.6 x F + 0.4 x C	Probabilidad
R1	**Spoofing**	18%	2	3	2,4	2
R2	**Jamming**	81%	5	5	5	5
R3	**Jamming**	81%	5	5	5	5
R4	**Spoofing**	18%	2	2	2	2
R5	**Jamming**	81%	5	5	5	5

Fuente: Elaboración propia

En cuanto al impacto se analizó el comportamiento de los pilotos en simulador de H-60, desde el abril hasta septiembre con 23 pilotos y 04 instructores, trabajando dos escenarios completamente diferentes que se basan en las dos premisas que guía nuestra investigación (Escenarios de baja complejidad y alta complejidad), con un total de 49,5 horas donde se extrajo el 0,2 por hora para analizar impactos, amenazas y vulnerabilidades en los efectos

de los riesgos R1-R2-R3-R5; le riesgo R4 por la naturaleza del mismo se pondero con la puntuación más alta.

Figura 3. Mapa de calor de evaluación de riesgos

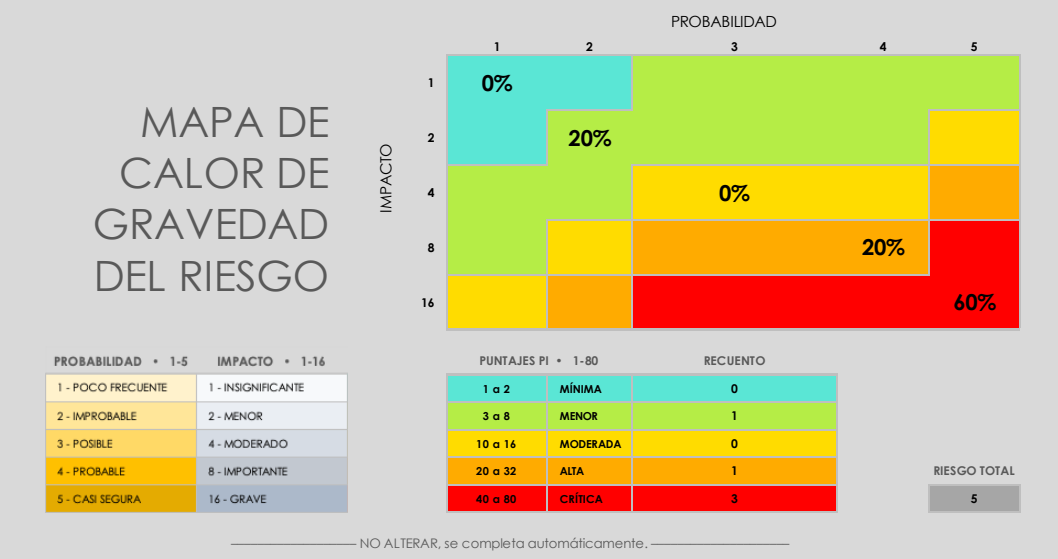


TABLA DE DATOS DE LA EVALUACIÓN DE RIESGOS

ID DE REF.	FECHA DE PRESENTACIÓN	DESCRIPCIÓN DEL RIESGO	PROBABILIDAD 1-5	IMPACTO 1-16	PUNTAJE DE GRAVEDAD DE RIESGO Probabilidad x Impacto	NOTAS
R1	00/00/00	Navegación errónea o desviación de trayectoria.	2	4	8	
R2	00/00/01	Perdida total de la señal GNSS en un área crítica	5	16	80	
R3	00/00/02	Fallo funcional de los sistemas de navegación, guiado y misión durante maniobras críticas debido a interferencias GNSS intencionadas.	5	16	80	
R4	00/00/03	Ingreso a zonas preparadas	2	16	32	
R5	00/00/04	Generación de desorientación espacial en pilotos por pérdida de referencias GNSS en condiciones operativas adversas	5	16	80	

***Fuente*:** ISO/IEC 27005:2022 – Gestión de riesgos de seguridad de la información

Teniendo en cuenta que, de acuerdo con la relación entre impacto y probabilidad, el riesgo R2/R3/R5 es crítico, el riesgo R4 es alto y el riesgo R1 es moderado; se procederá a tratarlos conforme a los siguientes criterios:

- Reducir: El riesgo no se puede evitar, pero sí disminuir su impacto o probabilidad con controles técnicos, humanos o procedimentales viables. El costo de mitigación es menor al impacto potencial.

- Aceptar: El riesgo es de bajo impacto y probabilidad (riesgo residual). El costo de mitigación supera el beneficio, no afecta objetivos críticos. Está dentro del apetito de riesgo de la organización.
- Transferir: Para este caso no se utilizará en razón debido de que los riesgos son directamente controlados por la organización.
- Evitar: El riesgo tiene impacto catastrófico o no es tolerable; adicionalmente no existen controles y se tiene que modificar o evitar completamente la operación o las actividades.

Tabla 12. Tratamiento de los riesgos

I/R	Valor	Clasificación	Tratamiento	Justificación	Control
R1	12	**Moderado**	• Reducir (UH-60). • Aceptar (S70i)	• En el caso del UH-60 se debe reducir con protocolos e inversión en tecnología, y en el caso del S-70i se acepta por su capacidad de redundancia.	• Protocolo de ejecución. (Anexo A) • Mejoras tecnológicas. (Integración sistema INS) • llaves criptográficas GPS de tipo SAASM o M-Code
R2	80	**Crítico**	Evitar	• Este riesgo es inaceptable. Deben evitarse zonas geográficas con interferencia. Se requiere uso obligatorio de sistemas de respaldo (INS, mapas digitales, navegación alterna) y sistemas anti-jamming	• Protocolo de ejecución. (Anexo A) • UH-60L. (Actualización de la cabina) • Antenas anti-jamming

				e integrar protocolos de contingencia y respuesta.	
R3	20	**Crítico**	Evitar	• Este riesgo no es permisible, basado en la cercanía del terreno durante vuelos de bajo nivel, despegues y aproximaciones IFR.	• Protocolo de ejecución (Anexo A) • UH-60L. (Integración sistemas INL) • Antenas anti-jamming • llaves criptográficas GPS de tipo SAASM o M-Code
R4	32	**Alto**	Reducir	• Genera un alto grado de complejidad para su ejecución lo cual hace que su probabilidad sea baja aunque su impacto sea alto.	• Protocolo de Ejecución (Anexo A) abarca el procedimiento antes del vuelo.
R5	64	**Crítico**	Evitar	• Este riesgo puede generar pérdida total de control situacional y es subsiguiente a los demás riesgos de forma secuencial. Se requiere entrenamiento para vuelo en condiciones degradadas, redundancia de instrumentos y sensores inerciales activos. Evitar misiones en condiciones adversas sin preparación.	• Llaves criptográficas GPS de tipo SAASM (Módulo Anti-Spoofing de Disponibilidad Selectivo) M-Code. • Antenas anti-jamming • En este sentido se debe aplicar el protocolo en todo su alcance, debido a que es transversal a los demás riesgos.

Fuente: elaboración propia

* Nota: Cuando se utilizan los protocolos de entrenamiento, se abarcan (concientización, entrenamiento y diseño operacional).

Propuestas de controles para mitigación de riesgos.

El factor humano juega un papel crucial en la gestión de riesgos ante ataques de guerra electrónica, siendo la última capa de defensa frente a su impacto. Aunque las técnicas de interferencia o suplantación de sistemas GNSS no implican necesariamente el derribamiento de una aeronave, afectan la navegación de forma exponencial y la capacidad cognitiva del piloto, especialmente en situaciones de alta tensión. Casos recientes, como la colisión de un UH-60M en Washington D.C., ponen en reflexión si este tipo de ataque puede causar efectos devastadores.

Ahora bien, debemos tener claro que el entrenamiento, es transversal a todos los riesgos, es la medida esencial para preparar a las tripulaciones y desarrollar su capacidad de respuesta en condiciones críticas, y esto debe estar complementado con la implementación de tecnologías resilientes, lo cual es clave para afrontar estos desafíos.

Entrenamiento continuado y de misión.

Se diseña un protocolo con el fin de preparar a las tripulaciones para la guerra electrónica en diferentes fases de vuelo y entornos de diversas dificultades, adquiriendo habilidades, que les ayuden a identificar y responder ante una emergencia de forma oportuna y rápida de acuerdo con la situación, donde, de acuerdo con la emergencia, se requieren unas acciones instintivas y se priorice la consideración primordial, la cual radica en el control de la aeronave. Este protocolo estará en el **"ANEXO A"**, basado en tres fases claves (La concientización, entrenamiento y procedimientos operacionales).

Restructuración de la aviónica.

Uno de los grandes retos actuales con los que cuenta la Aviación del Ejército es la antigüedad y retraso de tecnología en las aeronaves UH-60L que son el gran grueso con que se cuenta para el desarrollo de operaciones de todo tipo; estas aeronaves a diferencia de los S70I, no cuenta con sistemas de navegación redundantes, y la aviónica en cuanto a los radios de comunicación VHF/UHF/HF/AM/FM están teniendo diversos problemas relacionados con su potencia de transmisión, que en consecuencia abren una brecha a la capacidad de enfrentar amenazas relacionadas con guerra electrónica y al mismo tiempo impacta la seguridad operacional al no completar requisitos mínimos de operación siendo desactualizados u obsoletos lo que dificulta la forma de administración de cabina por parte de las tripulaciones; Ahora bien, dentro este proceso de actualización se contaría con ciertas ventajas y capacidades (Trevithick, 2017), así:

1. La interoperabilidad con estándares de operación con OTAN en guerra electrónica al incorporar sistemas de comunicación y navegación compatibles y estandarizados, con capacidad de autogestión y resiliencia.
2. Reemplazo de instrumentos (comportamiento, navegación y sistemas) de análogo a digital, integrando la siguiente tecnología; así:

Tabla 13. Aviónica incluida en la modificación de la cabina.

Comunicaciones		
Elemento	**Cantidad**	**Función**
AN/ARC-231 UHF/VHF/AM/FM	02	Proporciona comunicaciones de voz y datos bidireccionales y multimodo en un rango de frecuencia de 30 a 512 MHz, esto permite comunicación de amplificación de banda con las

		dependencias de tránsito aéreo, con capacidad adicional de comunicación vía satelital y con seguridad antijamming. (*Multiband Comunications and Crypto Systems*, s. f., p. 4)
AN/ARC-201D VHF/FM	02	Radio táctico compatible con el sistema SINCGARS (Single Channel Ground and Airborne Radio System), proporciona comunicaciones de voz y datos seguras y anti-interferencia. (Harris, 2020)
AN/ARC-220 HF	01	Equipo de comunicación de alta frecuencia diseñado específicamente para aeronaves de ala rotatoria que efectúan vuelos de bajo nivel o ras de tierra. (*An Arc 220 Hf Airborne Communication System*, s. f.)
Navegación		
H-764GU EGI	02	Sistema de navegación integrado INS/GPS, reemplaza la analogía en giróscopos actitud (balanceo, cabeceo, resbalamiento) velocidades laterales/ horizontales y rumbo. (*Embedded GPS/INS (EGI) Navigation System With Advanced*, s. f.)

Fuente: elaboración propia en base a las referencias.

3. La digitalización permite la eliminación de fricción, resistencia e interferencia de los giróscopos de cabeceo, balanceo y guiñada, en adición a que mejora la comunicación, precisión de navegación, estandarización de procedimientos, la reducción de costos de mantenimiento y entrenamiento común para todas las flotas de aeronaves series H-60 aumentando los estándares de seguridad; también reduce el peso de la aeronave en aproximadamente 100 libras, lo que mejora su rendimiento.

Ahora bien, esta actualización de aviónica en cuanto a comunicación y navegación, viene acompañada de una restructuración de la cabina al utilizar enlaces de estándares mundiales de intercomunicación entre sistemas y una actualización de algunos sistemas, como el eléctrico, en razón del aumento de carga electrónica que conllevan las nuevas aviónicas e instalación de pantallas (MFD) y FMS, integrando convertidores de corriente con capacidad de 400 amp, nuevas baterías DC , trayendo consigo un cambio drástico en el esquema de la generación de corriente convertida de alterna a continua. También pueden hacerse modificaciones importantes en la aeronave, como en el sistema de propulsión, generación y transferencia de potencia mediante el tren de potencia, así como asegurar los requisitos mínimos necesarios para incorporar tecnología.

Figura 4. Fases de actualización de cabina UH-60L.

Fuente: elaboración propia en base al Program Executive Office, Aviation U.S ARMY 2023.

Estas modificaciones son importantes visualizarlas en razón de entender los precios asociados a la implementación de esta tecnología, donde actualizar las cabinas es más rentable que adquirir nuevas aeronaves y donde es una necesidad primordial para la operación

segura, donde la actualización oscila entre 4 a 6 millones de dólares por helicóptero en comparación al valor de adquirir helicópteros UH-60M o S-70I donde su precio oscila entre 16 a 20 millones de dólares. (Michael Maya, 2022)

Tecnología anti-jamming (interferencia).

Uno de los factores más críticos, como lo analizamos dentro de los riesgo es la alta probabilidad de interferencia en los sistemas GNSS, y así mismo sus impactos, es por ello que, adicional a la implementación de sistemas inerciales u otros que permitan la redundancia de los sistemas, es necesario contar con dispositivos que brinden una protección integral a la recepción de los sistemas, esto se puede conseguir con antenas anti-jamming, que actualmente en Colombia ninguna aeronave de ala rotatoria tiene instalada.

Básicamente, estas antenas tienen como finalidad comparar amplitudes y fases de señal con un software, lo que permite verificar la señal de cada satélite y comparar la dirección, determinar y filtrar en descarte señales horizontales Vs verticales. Una vez realiza este proceso, genera nulos de bloqueos en dirección del atacante con patrones de ruido de mayor decibel. Estos sistemas son demasiado efectivos y, en el caso de los helicópteros H-60M del Army, han sido instalados y probados con éxito e integrados al sistema EAGLE-M los cuales brindan códigos de encriptación de señales a las EGI del sistema de GNSS (David Hylton, 2023), esto quiere decir que ambos sistemas pueden ser integrados a la aviónica de los S-70i.

Ahora bien, esta clase de antenas tiene una particularidad y es la capacidad de ser integradas a las aviónicas de las aeronaves sin modificaciones grandes, lo que es ventajoso al poder ser instaladas de forma sencilla en cualquier tipo de aeronave de serie H-60, (*GAJT-710ML Anti-*

Jam Antenna - LOW OEM PRICING - NovAtel - Borealis Precision - Industry Leading Representative, s. f.).

Ahora bien, actualmente Mayflower Communications Company, Inc. ofrece un producto llamado NavGuard 710 que puede adquirirse y exportarse a países que forman parte de la Autorización de Comercio Estratégico de EE. UU. También puede adquirirse y exportarse a otros países que no forman parte de la STA **(**Strategic Trade Authorization) y que mantienen una buena relación con EE. UU. El NavGuard 710 ya está aprobado para exportación y puede adquirirse y exportarse. Los productos militares de Mayflower, como el MAGNA-F o el MAGNA-I, aún están sujetos a la ITAR (International Traffic in Arms Regulations) así como la tecnología SAASM (Módulo Anti-Spoofing de Disponibilidad Selectivo) M-Code; sin embargo, el Departamento de Estado planea modificar la ITAR de USML en septiembre de este año. Se prevé que la ITAR se eliminará de los productos MAGNA. *(Joseph P. Thomas; Senior director, Government Programs Mayflower Communications Company).*

Tabla 14. Costos de la implementación del sistema.

Number of Units Lot	**NavGuard 710 ROM Cost NavGuard 710 Per unit w/ TSO**
1-9	$104.013
10-19	$97.784
20-49	$90.024
50-99	$72.956

Fuente: *Mayflower Communications Company*

Conclusiones.

La afectación de los sistemas de navegación (GNSS) por ataques cibernéticos a los helicópteros de serie H-60 es una realidad que genera múltiples peligros y riesgos para la

seguridad operacional y, en el nuevo entorno de la guerra electrónica, ha evolucionado de tal manera que los casos a nivel mundial de ataques a diferentes aeronaves han aumentado de forma exponencial, de la misma forma que la capacidad de diferentes actores con nuevas tácticas, técnicas y procedimientos.

Respondiendo ahora a nuestro gran interrogante: ¿Cómo afectan los ataques cibernéticos en los sistemas de navegación GNSS de los helicópteros H-60?, el análisis de riesgos realizado demuestra que dichos ataques impactan directamente los activos críticos de la operación (tripulación, aeronave y sistemas), explotando vulnerabilidades de la infraestructura GNSS. En primer lugar, afectan la capacidad cognitiva del piloto en ambientes operacionales complejos, al retrasar sus reacciones instintivas por ausencia de procedimientos estandarizados, lo que conlleva a un incremento de la carga de trabajo y puede derivar en desorientación espacial, ante la imposibilidad de determinar la posición, la altitud y la actitud respecto al eje de referencia terrestre.

En segundo lugar, la pérdida de referencias GNSS provoca una reacción en cadena sobre los subsistemas dependientes, degradando el funcionamiento del AFCS, el piloto automático acoplado al director de vuelo, el FMS, el H-TAWS, entre otros, lo cual resulta especialmente crítico según el perfil de vuelo y el nivel de conciencia situacional del piloto. Finalmente, se identificó la limitada capacidad de detección en cabina por parte de las tripulaciones, ya que las indicaciones en instrumentos como el EICAS o el CDU pueden presentarse de manera errónea, retrasando la reacción de los pilotos ante un ataque cibernético y dificultando la toma de decisiones oportunas.

Una vez abordado los efectos, en cuanto a su evaluación resultaron críticos los riesgos (R2-R3-R5) los cuales en razón a su naturaleza y al apetito del riesgo no pueden ser aceptados por la organización en razón a su impacto en cada uno de los activos (negocio, sistema e información). También logramos identificar las principales vulnerabilidades de los sistemas que radican principalmente en la gran dependencia para la navegación y que es potencializada por la falta de resiliencia del sistema, por ausencia de medios que permitan la redundancia, la autenticación de señales y los medios de protección de los activos de negocio y sistemas en cuanto a la parte técnica; ahora cuanto hablamos de estos activos de negocios apartándonos de la parte técnica tenemos que hablar necesariamente del factor humano, donde una de las principales vulnerabilidades que es trasversal a todas las amenazas y que explota todos los riesgos identificados es el entrenamiento de las tripulaciones donde hay carencia de protocolos, técnicas de identificación, medidas de mitigación, políticas y directrices claras en la organización para enfrentar cada uno de los riesgos que conlleva en estar expuestos en ambientes de guerra electrónica.

En cuanto la identificación de amenazas se pudo establecer, la pérdida total de señal GNSS y su ausencia en maniobras críticas, provocadas por vulnerabilidades en la arquitectura explotadas con técnicas de jamming. Este tipo de ataque, por su fácil acceso en el mercado, la baja capacidad técnica requerida para su implementación y su impacto directo en la disponibilidad e integridad del servicio, se convierte en un factor que se materializa en tres riesgos dentro del proceso de gestión. En segundo lugar, se identificaron amenazas como la pérdida de integridad de navegación y la manipulación de la trayectoria de vuelo, asociadas a técnicas de spoofing. Aunque su probabilidad es menor debido al mayor costo y

complejidad técnica, no es menos peligroso, ya que la evolución de los dispositivos SDR y la difusión de guías públicas han reducido de forma significativa su barrera de entrada. Esto coincide con la tendencia actual de la guerra, que ha evolucionado hacia el campo cibernético y electrónico, impulsado por el financiamiento de los actores en cuestión. En consecuencia, estas amenazas se traducen en dos riesgos adicionales en el proceso de gestión.

En el análisis del artículo y la aplicación del modelo ISSRM (Information System Security Risk Management), se identificaron vulnerabilidades y amenazas que representan riesgos relevantes. A partir de esto, se proponen medidas de mitigación, comenzando por la adopción de un protocolo de ejecución que permita a la organización implementar políticas claras ante los desafíos existentes. Este protocolo integra tres elementos esenciales: concientización, capacitación y establecimiento de procedimientos estándar que contribuyen a gestionar el apetito de riesgo organizacional.

Una segunda medida clave es la necesidad de adaptarse continuamente al carácter cambiante de las amenazas, especialmente en contextos bélicos o cibernéticos. Para lograrlo, es fundamental invertir en tecnología que refuerce la resiliencia frente a ataques cibernéticos o guerra electrónica que puedan afectar los sistemas GNSS. Esto implica actualizar la cabina de las aeronaves para incorporar sistemas de comunicaciones modernas adecuados al entorno de contaminación electromagnética, así como integrar tecnologías de navegación inercial y geoposicionamiento que fortalezcan la resiliencia de los helicópteros UH-60 L ante eventuales ataques.

Por último, una alternativa más económica consiste en la implementación de sistemas integrales anti-jamming, los cuales han sido implementados por el Ejercito de los Estados

Unidos en sus aeronaves tripuladas y no tripuladas que por sus características no generan modificaciones sustanciales en la arquitectura de aviónica de las aeronaves, brindando protección integral a los receptores de navegación.

En síntesis, la investigación confirma que los ataques de jamming y spoofing representan una amenaza real y creciente para las aeronaves H-60 , con impactos directos en la operación, la seguridad de la tripulación y la disponibilidad de los sistemas. Si bien existen medidas de mitigación organizacionales, tecnológicas y específicas que pueden fortalecer la resiliencia, la complejidad del entorno ciber-electromagnético exige avanzar hacia un modelo de mejora continua, integrando entrenamiento, inversión tecnológica y cooperación interinstitucional; solo así será posible garantizar la seguridad operacional y ser resilientes en estos escenarios.

Referencias Bibliográficas.

Aeronautica civil,2025. (s. f.). Recuperado 20 de abril de 2025, de https://www.aerocivil.gov.co/atencion/transparencia/glosario

Álvarez, R. (2017, agosto 11). *Se presenta el primer caso de falsificación de GPS: Una nueva forma de ataque electrónico*. Xataka. https://www.xataka.com/seguridad/se-presenta-el-primer-caso-de-falsificacion-de-gps-una-nueva-forma-de-ataque-electronico

An Arc 220 Hf Airborne Communication System. (s. f.). Recuperado 25 de junio de 2025, de https://www.collinsaerospace.com/what-we-do/industries/military-and-defense/communications/airborne-communications/hf-communications/an-arc-220-hf-airborne-communication-system

Army Aviation Reaches Navigation Milestone. (2024, mayo 6). Www.Army.Mil. https://www.army.mil/article/276031/army_aviation_reaches_navigation_milestone

Aviations GPS Spoofing & How to Avoid It | APG. (s. f.). Recuperado 12 de mayo de 2025, de https://flyapg.com/blog/what-is-gps-spoofing

Centro de excelencia aviación Ejercito Estados Unidos. (01-mar-25). H-60 Series Aircrew Training Manual. *DA Form 2028*.

Cole, S. (s. f.). *Securing military GPS from spoofing and jamming vulnerabilities—Military Embedded Systems*. Recuperado 12 de mayo de 2025, de https://militaryembedded.com/comms/encryption/securing-military-gps-spoofing-jamming-vulnerabilities

Cuesta, A. M. (2024, diciembre 27). *Entregan primeros inhibidores de drones en el Cauca para enfrentar ataques de grupos armados*. El Tiempo. https://www.eltiempo.com/justicia/conflicto-y-narcotrafico/entregan-primeros-inhibidores-de-drones-en-el-cauca-para-enfrentar-ataques-de-grupos-armados-3412737

David Hylton. (2023, enero 18). *Peo Aviation Conducts First Flight Of Critical Army Aviation Modernized Navigation Equipment*. Www.Army.Mil. https://www.army.mil/article/263326/peo_aviation_conducts_first_flight_of_critical_army_aviation_modernized_navigation_equipment

Embedded GPS/INS (EGI) Navigation System With Advanced. (s. f.).

Eurocontrol-think-paper-9-radio-frequency-intereference-satellite-navigation.pdf. (s. f.). Recuperado 6 de febrero de 2025, de https://www.eurocontrol.int/sites/default/files/2021-03/eurocontrol-think-paper-9-radio-frequency-intereference-satellite-navigation.pdf

FAA Safety Briefing. (2024, mayo 9). It's a Confusing World Up There. *Cleared for Takeoff*. https://medium.com/faa/its-a-confusing-world-up-there-5070c1e5806b

FlightSafety. (2016). *Sikorsky S-70i Pilot Training Manual*. *Versión 0.0*.

GAJT-710ML Anti-Jam Antenna—LOW OEM PRICING - NovAtel—Borealis Precision—Industry Leading Representative. (s. f.). Recuperado 26 de junio de 2025, de https://www.gnss.ca/novatel/84-gajt-710ml-anti-jam-antenna

Global navigation space systems: Reliance and vulnerabilities. (2011). Royal Academy of Engineering.

GNSS Navegation Mangement System Software Load 07C. (s. f.).

GPS-Spoofing-Final-Report-OPSGROUP-WG-OG24. (s. f.).

GRP22NI14.pdf. (s. f.). Recuperado 5 de mayo de 2025, de https://www.icao.int/NACC/Documents/Meetings/2024/GRP22/GRP22NI14.pdf

Harris. (2020). *AN/ARC-201D SINCGARS AIRBORNE RADIO*.

Hernández Sampieri, R., & Fernandez-Collado, C. F. (2014). *Metodología de la investigación* (P. Baptista Lucio, Ed.; Sexta edición). McGraw-Hill Education.

HT9100-007C SYSTEM MAINTENANCE MANUAL. (s. f.).

Humphreys, T. E., Ledvina, B. M., Tech, V., Psiaki, M. L., O'Hanlon, B. W., & Kintner, P. M. (s. f.). *Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer*.

Introduction of the Emergency Response Methodology. (s. f.).

Iudice, I., Pascarella, D., Corraro, G., & Cuciniello, G. (2024). A real/fast-time simulator for impact assessment of spoofing & jamming attacks on GNSS receivers. *2024 11th International Workshop on Metrology for AeroSpace (MetroAeroSpace)*, 309-314. https://doi.org/10.1109/MetroAeroSpace61015.2024.10591529

Keller, J. (2023, febrero). *Sikorsky to build UH-60M utility helicopters, avionics, and navigation systems for Australian military*. Military Aerospace. https://www.militaryaerospace.com/sensors/article/14290077/helicopters-avionics-navigation

Kožović, D., & Đurđević, D. (2021). Spoofing in aviation: Security threats on GPS and ADS-B systems. *Vojnotehnicki Glasnik*, *69*(2), 461-485. https://doi.org/10.5937/vojtehg69-30119

Manual del Operador para Helicopteros UH-60L. (s. f.).

MCE 3-12 OPERACIONES DEL CIBERESPACIO. (s. f.).

MCE 3-36 Guerra Electrónica. (s. f.).

Meeks, R. K., Anderson, J., & Bell, P. M. (2023). Physiology Of Spatial Orientation. En *StatPearls [Internet]*. StatPearls Publishing. https://www.ncbi.nlm.nih.gov/books/NBK518976/

Michael Maya. (2022). Cabina de Genesys. *Vertical Mag*. https://verticalmag.com/features/what-is-it-like-to-fly-an-eh-60-black-hawk-with-the-new-genesys-cockpit/

Morales-Ferre, R., Richter, P., Falletti, E., De La Fuente, A., & Lohan, E. S. (2020). A Survey on Coping With Intentional Interference in Satellite Navigation for Manned and Unmanned Aircraft. *IEEE Communications Surveys & Tutorials*, *22*(1), 249-291. https://doi.org/10.1109/COMST.2019.2949178

Multiband Comunications and Crypto Systems. (s. f.).

Ortuño, N., María, J., & Pastoriza, T. (2024). *Sistema de perturbación (spoofing) para receptores GPS embarcados*.

Pathak, A. (2024). Tecnología GNSS vs GPS: Explicación de las principales diferencias. *geekflare*. https://geekflare.com/es/gnss-vs-gps-technology/

Perez, E. (2024, marzo). *La guerra electrónica se intensifica.* https://www.xataka.com/transporte/guerra-electronica-se-intensifica-1-600-aviones-europa-dos-dias-han-tenido-problemas-gps

Pozo-Ruz, A., Ribeiro, A., García-Alegre, M. C., García, L., Guinea, D., & Sandoval, F. (s. f.). *SISTEMA DE POSICIONAMIENTO GLOBAL (GPS): DESCRIPCIÓN, ANÁLISIS DE ERRORES, APLICACIONES Y FUTURO*.

Radoš, K., Brkić, M., & Begušić, D. (2024). Recent Advances on Jamming and Spoofing Detection in GNSS. *Sensors*, *24*(13), 4210. https://doi.org/10.3390/s24134210

Rignér, J. (2020). *Adapting to increased automation in the aviation industry through performance measurement and training*. 1.

Russia's hybrid war on Europe: Jamming and spoofing in the «grey zone». (2025, septiembre 5). euronews. http://www.euronews.com/2025/09/05/tackling-russias-hybrid-war-on-europe-jamming-and-spoofing-in-the-grey-zone

Safety Information Bulletin Operations – ATM/ANS – Airworthiness. (s. f.).

Sikorsky S-70A: Familia UH-60M Black Hawk – Archivos Históricos Igor I Sikorsky. (s. f.). Recuperado 28 de abril de 2025, de https://sikorskyarchives.com/home/sikorsky-product-history/helicopter-innovation-era/sikorsky-s-70a-uh-60m-black-hawk-family/

Tech, V., & Liu, S. (s. f.). *All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems*.

Topham, G., & correspondent, G. T. T. (2024, abril 22). Thousands of flights to and from Europe affected by suspected Russian jamming. *The Guardian*. https://www.theguardian.com/business/2024/apr/22/thousands-of-flights-to-and-from-europe-affected-by-suspected-russian-jamming

Trevithick, J. (2017, abril 3). The U.S. Army's UH-60V Brings Older Black Hawks Into the Digital Age. *The War Zone*. https://www.twz.com/8880/the-u-s-armys-uh-60v-brings-older-black-hawks-into-the-digital-age

UNITED STATES ARMY AVIATION CENTER OF EXCELLENCE. (s. f.). *H-60 Series Aircrew Training Manual*.

Waterman, S. (2024, julio 10). Russian Jamming Wreaks Havoc on GPS. Is It Hybrid Warfare? *Air & Space Forces Magazine*. https://www.airandspaceforces.com/russian-gps-jamming-nato-ukraine/

Westbrook, T. (2023). A Taxonomy of Radiofrequency Jamming and Spoofing Strategies and Criminal Motives. *Journal of Strategic Security*, *16*(2), 68-80. https://doi.org/10.5038/1944-0472.16.2.2081

ANEXO "A"

PROTOCOLO DE EJECUCIÓN

1. Alcance.

Sera aplicado a los programas de entrenamiento de tripulaciones de las aeronaves H-60 series de la División de Aviación de Asalto Aéreo, y la cual será implementada en la T2 de la semana de la excelencia en dos componentes de teoría y práctica.

2. Ejecución.

El proceso de implementación está dividido en cuatro fases, que tienen como finalidad seguir una secuencia lógica y sistemática que brindará herramientas necesarias para la acertada toma de decisiones de las tripulaciones en el momento de presentarse un ataque cibernético debido a spoofing o jamming, así: **(concientización, entrenamiento, procedimientos operacionales).**

2.1. Concientización.

Inicialmente se debe tener un periodo de difusión de los riesgos de exposición de una tripulación ante un ataque cibernético en desarrollo de operaciones de vuelo y su impacto a los cumplimientos de la misión, esto requiere una visión general a nivel organización del problema y sus consecuencias, donde se debe integrar la parte gerencial de la Aviación del Ejercito e incluso mismo Ejercito Nacional en razón a que estas aeronaves son un activo estratégico de la nación y se debe entender el problema y mitigar con la protección de los sistemas de navegación con nuevas tecnologías y modernización que estén a la vanguardia

del contexto mundial y nacional, adicional la implementación políticas claras que sean adoptados a nivel operacional y táctico durante el planeamiento y ejecución de operaciones conjuntas acompañado por una serie de capacitaciones que tienen como fin estudiar la amenaza latente durante el desarrollo de operaciones militares.

Dentro de la parte operativa se deben comenzar a realizar planeamientos más detallados donde se tengan contempladas contingencias con respecto a este problema y, dentro de los análisis realizados en la recolección de información por parte de los organismos de inteligencia, se debe tener claridad de la capacidad del enemigo con respecto a la guerra electrónica, donde se puedan identificar áereas específicas.

Las tripulaciones tienen como responsabilidad entender las amenazas, vulnerabilidades y riesgos que conllevan la degradación o denegación de los sistemas GNSS, para poder entender la raíz del problema al momento de presentarse y adoptar un entrenamiento diferencial.

- Entrenamiento.

Los procedimientos y técnicas iniciadas en el proceso de concientización deben ser integradas a los programas de entrenamientos de tripulaciones, y los Sumarios de Órdenes Permanentes, en sus anexos "Tareas 3000", adicionales basadas en la misión, en el siguiente orden, así:

2.2.1. **Entrenamiento continuado:** Este entrenamiento se basa en dos fases, la primera es la parte académica/teórica, su fin primordial es identificar mediante indicadores de cabina las características de vuelo de la ocurrencia del ataque mediante cualquiera de las dos técnicas (spoofing-jamming), se analizan generalidades,

casualidades, indicaciones y procedimientos. La segunda fase recolecta la teoría y se coloca en práctica en un simulador de vuelo o, si hay posibilidad, se practica en vuelo real, donde la intención del entrenamiento es observar las acciones instintivas por parte del piloto y corregir novedades que vayan en contra de los procedimientos estandarizados.

2.2.2. Dentro de la **integración al programa de entrenamiento de tripulaciones**, en la semana de la excelencia que se efectúa anualmente y es requisito para ejercer funciones de vuelo, cada tripulación realizará un repaso de la concientización, factores críticos, indicaciones y procedimientos, de igual manera, será asignado dentro de las tareas obligatorias a ejecutar en el simulador de vuelo, integrado a la tarea 1166 "Responder a condiciones meteorológicas imprevistas".

2.2.3. **Evaluación de vuelo:** Se realizará anualmente en el tiempo de evaluación (T2), integrado al (PAPNIP) prueba anual de pericia y nivel de preparación, y será evaluado por cada piloto instructor con una estandarización del procedimiento.

3.3. Procedimientos operacionales.

Este diseño se basa en las reacciones instintivas de los pilotos en ejercicios de simulador de vuelo en dos entornos particulares, el primero en vuelo cruceros controlados y el segundo se basa en zonas confinadas con degradaciones visuales, simulando las condiciones más difíciles de operación con algunos complementos particulares dependiendo de las configuraciones de la misión. Este procedimiento se divide en dos partes (antes del vuelo, durante el vuelo) y se tratará la aproximación y el despegue como complemento del segundo punto.

3.3.1. **Antes del vuelo:** Se basa en alistamiento previo a la misión, dependiendo de las condiciones en que se realiza, se siguen los parámetros de normas y procedimientos sugeridos en la tarea (1004-1006) de los manuales de entrenamiento de tripulaciones (UNITED STATES ARMY AVIATION CENTER OF EXCELLENCE, s. f., pp. 3-2), más estas adiciones relacionadas con guerra cibernética.

Figura 5. Lista de verificación antes del vuelo.

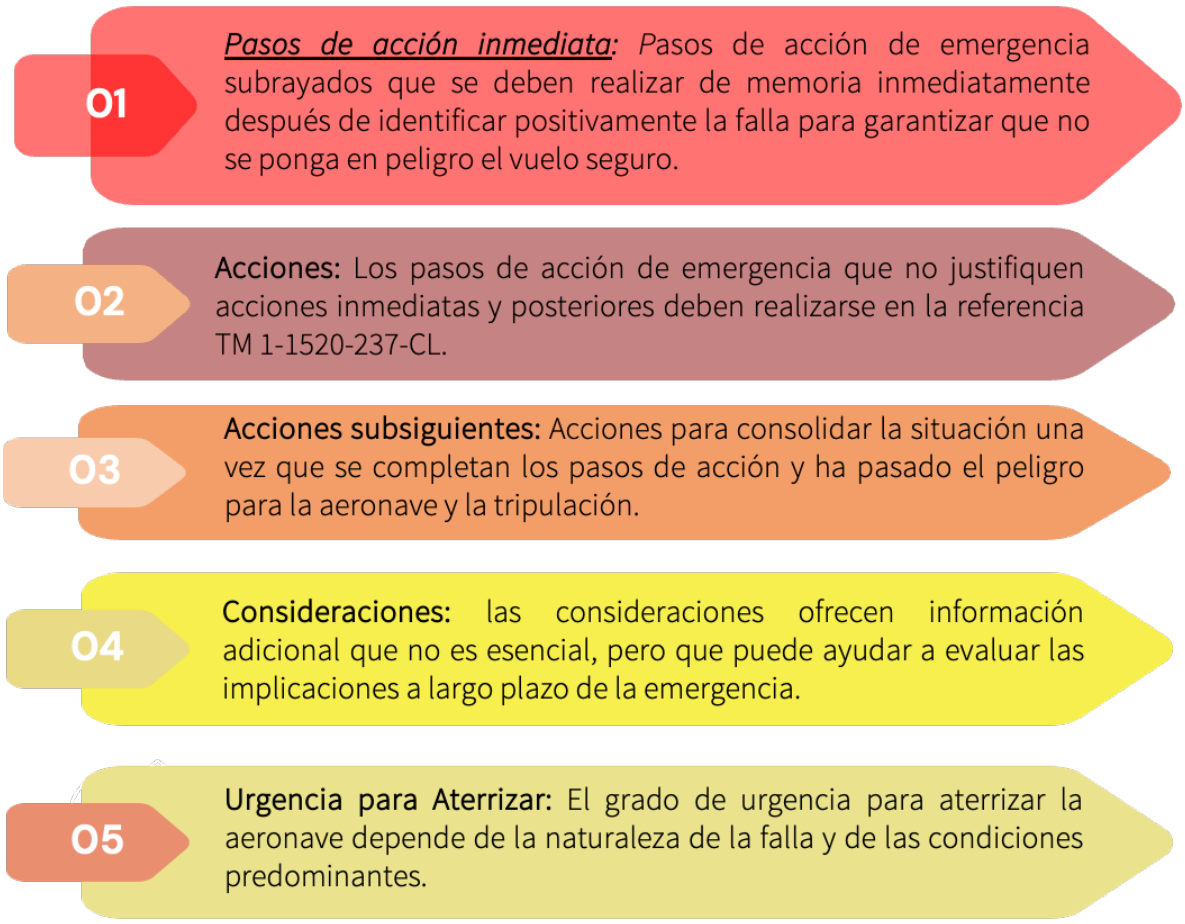
1	2	3	4	5
TIPO DE MISIÓN	**INTELIGENCIA**	**RUTAS DE VUELO**	**ENSAYOS**	**ORIENTACIÓN DE LA TRIPULACIÓN**
• **Alta complejidad.** • **Baja complejidad** **DETERMINACIÓN DE LA CAPACIDAD DE LA AERONAVE**	• **Conocimiento de la amenaza.** • **Ambiente operacional.** • **Variables de la misión.**	• **Características de la ruta basado en la misión .**	• **Ensayos y supervisión.**	• **Implementación de la administración de recursos de cabina.**
1. Se basa en el análisis de riesgo de la misión (amenaza, supervisión, planeamiento frecuencia en operaciones, experiencia, condiciones meteorológicas, complejidad de misión , factores geográficos, factores de LVN)= MUY ALTO-ALTO-MEDIO-BAJO 2. Orientación local de los sectores.	1. Se debe determinar las capacidades de afectación del enemigo en cuanto a guerra cibernética. 2. Así mismo las características que convergen factores, PEMSII Y METTT-P	1. Altimetría de las zonas. 2. Condiciones de vuelo y visibilidad. 3. Ayudas de navegación en ruta. 4. Cartas visuales.	1. Su finalidad radica en el ensayo de procedimientos estandarizados para misiones de alta complejidad y se verifica las acciones de acción inmediata	1. Tratamiento en todas las misiones durante la orientación de misión para la tripulación.

Fuente: elaboración propia basado en las tareas (1004-1006)

3.3.2. **Durante el vuelo:** Es importante tener claridad inicialmente de la secuencia con que se desarrollará la emergencia, en donde se implementará una lógica de pasos ordenados que le permiten al piloto responder de forma lógica y coherente a la situación. Inicialmente, se analizarán las indicaciones de un ataque con las características de un jamming o spoofing, las consideraciones, advertencias, acciones

de respuestas inmediatas, acciones, acciones subsiguientes y la necesidad de urgencias para aterrizar si es aplicable; basado en los procedimientos de respuesta de emergencia FADEC (*Introduction of the Emergency Response Methodology*, s. f.). Aquí las definiciones para cada caso; así:

Figura 6. Metodología de respuesta a emergencias

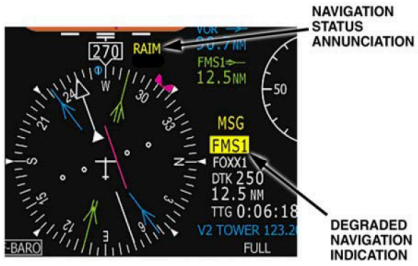


Fuente: elaboración propia con base (Centro de excelencia aviación Ejército Estados Unidos, 01-mar-25)

a) Indicaciones y características de vuelo.

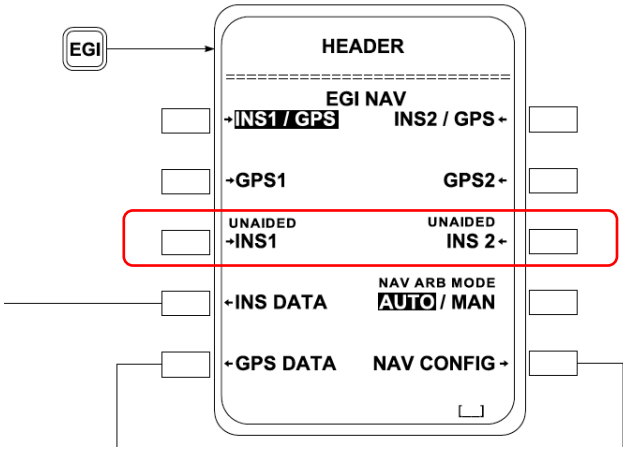
Antes de realizar cualquier procedimiento, si el tiempo y la situación lo permiten, se deben analizar las indicaciones ante cualquier eventual ataque, así:

Tabla 15. Indicaciones de cabina en Spoofing-Jamming

INDICACIONES JAMMING		
MFD (MULTIFUNCTION DISPLAYS) Modo Tactical/Mission. (S-70i)	• Congelamiento del indicador digital de la aeronave en el mapa táctico.	
MFD (MULTIFUNCTION DISPLAYS) modo Primary Flight Display. (S-70i)	• Indicaciones en pérdida de fuente de la navegación (GPS). RAIM FMS 1/2	
FD (FLIGHT DIRECTOR). (S-70i)	• Incapacidad de acoplamiento • Indicación de verde/magenta • PRECAUCIÓN: FLT DIR FAIL	

FMS (FLIGHT MANAGEMENT SYSTEM). (S-70i)

- Fuente de navegación INS1/2
- Demás fuentes de navegación inactivas

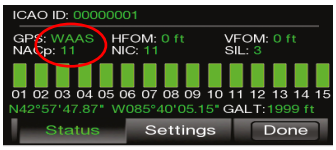


AFCS (AUTO FLIGHT CONTROL SYSTEM). (S-70i)

- Afectación de las EGI y pérdida del director de vuelo puede causar la degradación FCC1/FCC2

ADS-B (Automatic Dependent Surveillance – Broadcast). (S-70i/UH60L)

- "**No Pos**" - unknown or DR (Insufficient Satellites to compute a position)



HTAWS (Helicopter Terrain Awarreness Warning System). (S-70i)

- Congelamiento del indicador digital de la aeronave en el mapa táctico.
- Indicaciones de Warning/ Cautio/Pull up

HSI (Horizontal situation indicator). (UH-60L)	• Fluctuación puntero de demarcación Nº1. • Aparece banderola NAV	

INDICACIONES SPOOFING

Con indicaciones de cabina es difícil detectar un spoofing por parte de las tripulaciones, en el caso del UH-60, solo se podría intuir comparando rumbos con la brújula de la aeronave o si se está con navegación por radioayudas, debido a la carencia de tecnología con que cuenta la aeronave. En el caso del S70i se podría presentar una disparidad entre el sistema inercial y el GPS que podría darle alguna información al piloto en el FMS, pero si el ataque es constante, combinado y preciso sería imperceptible.

- Disparidad en ruta observada durante la navegación visual Vs navegación electrónica, con accidentes geográficos o áreas de interés con los estudios realizados de ruta y durante navegación a la estima.
- Disparidad entre los punteros de marcación Nº1 o Nº2 (UH-60L).

Fuente: elaboración propia en base a (*Manual del Operador para Helicopteros UH-60L*, s. f.)

b) <u>Consideraciones.</u>

El jamming en un entorno de ambientes complejos dificulta la identificación de las indicaciones, debido al tiempo reducido para analizar y tomar una acción pertinente en el momento en que se pierde las señales de los sistemas GNSS, ya bien sea con indicaciones en los punteros de demarcación Nº1 (UH-60L) o en el FMS en el S70i.

Una situación de spoofing puede que no sea detectable bajo estas condiciones en un UH-60L y más si las distancias de los puntos de llegada están por debajo de las 5 millas, en donde no habrá capacidad de análisis y de reacción, mientras en el S70i dependiendo de la calidad del ataque, se podrá identificar en la Primary Fly Display o en el FMS y en cierto modo y

momento, la precisión será suplida por el sistema inercial de acuerdo con la acumulación de errores del sistema. Esta variable, así como en el anterior caso, depende en gran medida de la distancia hacia el punto de llegada u objetivo.

c) Advertencias.

Se describirán cuatro consideraciones en donde no es permisible un ataque cibernético a las aeronaves y, por ende, los definiremos como criterios básicos para abortar la misión; así:

- Vuelos de formación con múltiples aeronaves. Esto podría conllevar desorientación espacial, entrada en condiciones meteorológicas imprevistas o colisión entre aeronaves.
- Incapacidad o dudas de ubicación del objetivo o lugar de destino planeado, sin puntos de referencia o capacidad de realizar navegación visual, que conllevaría a desorientación espacial.
- Condiciones meteorológicas y referencias visuales degradadas, en donde haya la posibilidad de entrar en condiciones meteorológicas inadvertidas.
- Cuando se están realizando vuelos bajo reglas de vuelo por instrumentos.

d) Procedimientos de acción inmediata.

Basado en ambientes y entornos complejos y despegues durante un ataque y siguiendo los siguientes procedimientos así:

Tabla 16. Responder a emergencia metodología FADEC-F

Ítem	Metodología	Descripción	Procedimientos
I.	**F: Vuele la aeronave**	Consideración primordial es el control de la aeronave	• Actitud: Desaceleración • Altitud: Ascenso inmediato por encima de los obstáculos más altos.

			• Velocidad: Se debe mantener entre 80 Kias y 60 Kias, nunca por debajo. • Rumbo: Nivelada si las condiciones lo permiten; si no vire con régimen no mayor a 30º grados o de acuerdo con la situación y los obstáculos presentes. • Rpm R: dentro de lìmites
II.	**A: Alerte a la tripulación.**	Requisito de la coordinación de la tripulación.	• Anuncie el evento • Anunciar obstáculos y posibles condiciones meteorológicas.
III.	**D: Diagnosticar la emergencia.**	Efectos a subsistemas.	• Identifique la condición de acuerdo con indicadores de cabina. • Verificación de recuperación de navegación a medida que se asciende a una altura segura o donde se pueden obtener señales de radionavegación (VOR-ADF).
IV.	**E: Ejecute procedimiento de emergencia.**	Segunda consideración primordial, obtener o recuperar las fuentes de navegación.	• Verifique altura para librar obstáculos y ascienda lo más alto posible, tratando de salir del ruido de interferencia. • Sintonice radioayuda más cercana. • Ejecute procedimiento por instrumentos si hay disponible. • Ejecute plan durante orientación y vire hacia la zona más baja para recuperar la señal o por donde se llegó. • Verificar el retorno de la señal a medida que se aleja del área afectada.

V.	**C: Comunicar plan de acción.**	Requisito de la coordinación de la tripulación y apoyo del ATC	• Informar a la tripulación intenciones para apoyo a la navegación • Tomar contacto con ATC para vectorización y control radar, si es posible, mediante transpondedor.
VI.	**F: Vuele la aeronave**	Condición primordial	• Verifique condición de los subsistemas y mantenga los sistemas entre los límites durante todo el vuelo después del mal funcionamiento.

Fuente: elaboración propia en base (Centro de excelencia aviación Ejército Estados Unidos, 01-mar-25)

e) Acciones.

Basados en ambientes controlados de baja complejidad donde se realicen misiones de carácter administrativo o movimientos aéreos los cuales, durante la evaluación del riesgo obtengan un valor de bajo o medio.

Ítem	Procedimientos
I.	• Sintonice, identifique y monitoree la estación más cercana.
II.	• Determine su posición con respecto a la estación.
III.	• Reinicie las EGI de forma separada (para el caso del S-70i). se deben desacoplar todas las funciones del piloto automático, mientras se realiza el procedimiento e intentar una alineación en vuelo. **Advertencia:** El procedimiento se debe realizar de forma individual, debido a que la perdida de una EGI no solo restablecerá el sistema GPS/INS, sino que también en la posición del piloto en particular al que corresponda la información se perderán las indicaciones de (actitud, balanceo y cabecero)
IV.	• Saque y entre el cortacircuito asociado al GPS.

V.	• Tome contacto con el control de tráfico aéreo si no puede determinar su posición para poder ser vectorizado y ser anunciado de tráficos aéreos sobre el sector.