



**Operaciones Cibernéticas en el Ciclo de Vida de Vehículos Aéreos No
Tripulados de Uso Militar - Ciberataques, Contramedidas y Propuesta
de Herramientas Preventivas Aplicadas al Control de Fronteras en
Argentina**

**TRABAJO FINAL DE TESIS
MAESTRÍA EN CIBERDEFENSA y CIBERSEGURIDAD**

Director de Tesis de Maestría: *Brigadier Mayor (R)* Mg. Lic. Alejandro Moresi

Autor: Ing. Pamela Ivana Strusiat

Abstract

Esta investigación se ha enfocado en un estudio de las aeronaves no tripuladas, considerando las características de mayor relevancia, que puedan ser utilizadas para la defensa y seguridad de un país.

Se analizan las potenciales vulnerabilidades y amenazas que pueden sufrir los Vehículos Aéreos no Tripulados (VANTs) de uso militar, entre las que se incluyen los ciberataques.

Los VANT son herramientas de gran potencial para la seguridad del país, pudiendo mejorar la eficiencia de seguridad de las fronteras, disminuyendo costos y evitando poner en riesgo la integridad física de los pilotos militares, frente a otras alternativas de similares características.

Dentro de los aspectos de seguridad se analiza el esquema desde la perspectiva del “Ciclo de Vida” del sistema de vehículos aéreos no tripulados considerando su diseño, fabricación, y operación en misiones de control de fronteras, particularmente la frontera norte argentina.

A partir del mismo, se incluyen contramedidas y se proponen herramientas preventivas para evitar que dichos dispositivos sean blanco de sabotaje.

En resumen, el trabajo pretende demostrar que aplicar VANTs militares para la defensa de la fronteras de un país, es una herramienta que implica baja inversión pero que posee alto impacto en cuanto a la calidad del control fronterizo. A la vez, estos vehículos aéreos no tripulados se encuentran sujetos a ataques cibernéticos que deben ser considerados para lograr éxito en las misiones de control fronterizo.

Palabras clave: VANT-UAV militar-ciberataque-defensa de fronteras.

ÍNDICE

ÍNDICE	3
1.1. Contexto	7
1.2. Justificación	8
1.3. Planteamiento del problema de estudio	10
1.4. Hipótesis	10
1.5. Alcance	11
1.6. Objetivo General	11
1.7. Objetivos Específicos	11
1.8. Metodología de Investigación	11
2. VEHÍCULOS AÉREOS NO TRIPULADOS MILITARES	13
2.1. Estado del Arte en la Tecnología de Defensa	13
2.1.1. Denominación de Vehículos Aéreos no Tripulados	13
2.2. Orígen y Evolución en la Tecnología de VANTs	14
2.3. Caracterización de VANTs Militares	15
2.4. Importancia de VANTs en Seguridad y Defensa	17
2.5. Arquitectura de VANTs	18
2.6. VANTs para la Defensa de la Nación argentina	19
2.7. Ventajas y Desventajas de los VANTs	21
3. MARCO REGULATORIO	23
3.1. Normativa Ciclo de Vida VANTs	23
3.2. Normativa internacional respecto a VANTs	24
3.3. Normativa nacional respecto a VANTs	25
4. ETAPAS DEL CICLO DE VIDA DE LOS VANTs	27
5. CIBERATAQUES EN EL CICLO DE VIDA DE VANTs Y CONTRAMEDIDAS	32
5.1 Ataques no cibernéticos a UAVs-Constramedidas	32
5.2 Ataques cibernéticos a UAVs -Constramedidas	33
7. CONTROL DE FRONTERAS	37
7.1. UAV para control de fronteras - Casos internacionales	37
7.2. Aplicación al control de fronteras en Argentina	38
7.3. Ventajas de utilizar UAV en el control de fronteras argentinas	40
7.4. Empleo de UAVs en ARGENTINA - Antecedentes	40
8. PROPUESTA DE HERRAMIENTAS PREVENTIVAS ANTE AMENAZAS EN CIBERSEGURIDAD DE UAVS	43
9. CONCLUSIONES Y PROPUESTAS PARA FUTURAS INVESTIGACIONES	45

OPERACIONES CIBERNÉTICAS EN EL CICLO DE VIDA DE VANTs DE USO MILITAR, SUS VULNERABILIDADES,
AMENAZAS, CIBERATAQUES, CONTRAMEDIDAS Y PROPUESTA DE HERRAMIENTAS PREVENTIVAS

Maestría en Ciberdefensa y Ciberseguridad UBA-FCE Posgrado

9.1. Conclusiones	45
9.2. Propuestas para futuras investigaciones	48
ANEXO 1	49
ANEXO 2	53
ANEXO 3	73
ANEXO 4	75
10. REFERENCIAS	83

Ing.Pamela Ivana Strusiat.

I. AGRADECIMIENTOS

Agradezco a Dios por permitirme alcanzar una meta más en mi vida, y por Su ayuda y protección constantes cada vez que lo pido y que lo necesito.

Agradezco a mis padres y hermanas por su acompañamiento siempre. Agradezco muy particularmente a mi mamá, Griselda Gomez, líder y heroína, por protegernos, alentarnos a superarnos, guiarnos correctamente con su buen ejemplo, por recomendarnos acertadamente siempre, por escucharnos, y ayudarnos. A mi papá José Strusiat, por su cariño y apoyo; y a mis hermanas Yamina Strusiat y Maia Strusiat quienes de una u otra forma me brindaron su afecto y colaboración en este proceso. Los logros de mi vida son más de mi familia que propios.

Agradezco a mi marido, el Ing. Martín Di Giorgio, por su ayuda a lo largo de toda la maestría y durante la tesis, por su paciencia y contribuciones precisas; porque gracias a su intelecto y amor incondicional me ha brindado la ayuda y el aliento suficientes para la finalización de esta tesis.

Agradezco profundamente a mis inteligentes, hermosas y sanas hijas, Delfina y Evangelina, por cada momento que no estuve con ellas durante este larguísimo tiempo. Espero poder compensar algún día cada segundo que no compartí con ustedes, para culminar este proyecto.

Al director de la maestría en Ciberdefensa y Ciberseguridad de la UBA, el Dr. Roberto Uzal, por su orientación en la organización de las etapas del trabajo, y por todo el conocimiento brindado en lo que refiere al asunto de esta carrera.

Al subdirector de la Maestría, el Ing. Carlos Amaya, por aportar sus valiosas opiniones e ideas para la realización de este trabajo, y por su buena predisposición siempre. Le agradezco por guiarme en la elección de este tema de tesis de maestría, de gran trascendencia.

Agradezco al Brigadier Mayor (R) Mg. Lic. Alejandro Moresi por su constante guía estos años, desde la propuesta, durante el desarrollo y en la finalización de esta Tesis de Maestría. Por su paciencia, en este que fue un aprendizaje que requirió de horas de trabajo y estudio por mi parte, y de horas de correcciones, revisiones y recomendaciones por su parte. Gracias por compartir sus conocimientos conmigo.

Agradezco muy particularmente al ex Jefe del Estado Mayor Conjunto de las Fuerzas Armadas el General de Brigada (R), por su verificación a las herramientas preventivas propuestas en esta tesis, para darle validez a las mismas.

Al Comodoro Ing. Jefe de Proyectos de la DGID de la FAA; al Mayor Jefe del Centro de

Ing. Pamela Ivana Strusiat.

Investigaciones Aplicadas (CIA) de la FAA; al Capitán Salinas de la FAA, y al Comodoro Ponz por el contacto;

Al Jefe del Proyecto RUAS (Rotary-Wing Unmanned Aerial System) Division of Aerospace and Government de INVAP, gracias al Lic. Sagarzazu por el contacto;

A Jorge, Jefe responsable táctico de UAVs a disposición del Ministerio de Seguridad de la Provincia de Buenos Aires, y a Jorge P. por el contacto.

Al Comandante (R), M., al Alférez (R) J. y al operador J. de Gendarmería Nacional, escuadrón norte, y a Mariano por el contacto;

Porque sin sus claras y útiles repuestas sobre VANTs durante las entrevistas, hubiera sido imposible la culminación de este trabajo.

A la Mg. Lic. Adriana Baravalle, por su asesoramiento y por contactarme con mi incomparable director de tesis.

A cada docente de esta maestría, por sus excelentes clases, por su sabiduría compartida, por su asesoría y apoyo en las consultas.

Finalmente, agradezco al jurado de esta tesis, por sus recomendaciones para mejorar y enriquecer la misma:

Prof. Dr. Ingeniero Germán Montejano U. de Vigo - MSc UNSL Lic. UNSL - Máxima categorización como investigador.

Prof. Doctor Ingeniero Daniel Riesco MSc U.Politéc. de Madrid. Lic UNSL Máxima categorización como investigador.

Prof. Ing. Juan José Benítez UBA - UNDef .

Magister Juan Carlos Guerra, Teniente Coronel de Comunicaciones - Oficial de Estado Mayor (Italia) y Magíster (TFM Calificado SOBRESALIENTE) en Ciberdefensa / Ciberseguridad) UBA.

1. INTRODUCCIÓN

Los avances tecnológicos en el campo de los vehículos aéreos no tripulados (UAV-por sus siglas en inglés) han revolucionado las operaciones militares, ofreciendo una mayor flexibilidad y eficacia en una amplia gama de aplicaciones (Bressano et al., 2014). Sin embargo, con la creciente dependencia de los UAV militares en operaciones críticas, también ha surgido una preocupación significativa en torno a la seguridad cibernética de estos sistemas. En el contexto del control de fronteras de Argentina, donde la integridad y la eficacia de las operaciones fronterizas son de suma importancia, la protección contra ciberataques se vuelve esencial. (de Vergara & Trama, 2016)

Esta tesis se centra en explorar las operaciones cibernéticas en el ciclo de vida de los UAV militares utilizados en el control de la frontera norte de Argentina, abordando cuestiones como los ciberataques, las vulnerabilidades existentes, las amenazas potenciales y las contramedidas necesarias para proteger estos sistemas críticos. Además, se propone una serie de herramientas preventivas diseñadas para fortalecer la seguridad cibernética de los UAV y prevenir posibles ataques.

A través del análisis detallado de las vulnerabilidades existentes, entrevistas a personal de la Fuerza Aérea y Ejército Argentino, la identificación de amenazas potenciales y la exploración de contramedidas efectivas, esta investigación tiene como objetivo proporcionar recomendaciones prácticas y aplicables para mejorar la ciberresiliencia del ciclo de vida los UAV militares en el contexto específico del control de frontera norte argentina. La implementación de estas medidas preventivas no solo protegerá la integridad de las operaciones fronterizas, sino que también contribuirá a fortalecer la seguridad nacional y la defensa del país ante posibles ataques cibernéticos.

A lo largo de esta tesis, se abordarán aspectos clave relacionados con la seguridad cibernética en los UAV militares, destacando la importancia de la protección contra ciberamenazas en un entorno operativo cada vez más digitalizado y conectado. Este estudio busca ser un aporte significativo en la comprensión y mejora de la ciberseguridad en las operaciones de UAV militares, con un enfoque específico en el control de la frontera norte en Argentina¹.

¹ Cabe aclarar que un análisis similar, respecto del control de la frontera argentina para la zona marítima por medio de uav militares se encuentra en la tesis: Determinación y conocimiento de la capacidad de los vehículos aéreos no tripulados para su empleo en la vigilancia y control de los espacios marítimos. Instituto universitario naval. (mazza, 2023)

1.1. Contexto

En la era moderna de la tecnología militar, los vehículos aéreos no tripulados (UAV) han emergido como una herramienta estratégica fundamental en operaciones militares, proporcionando capacidades avanzadas de vigilancia, reconocimiento y ataque en una variedad de entornos operativos (Mary, 2024). En el ámbito de la defensa y la seguridad nacional, los UAV desempeñan un papel cada vez más importante en la protección de las fronteras y en la implementación de medidas de control y vigilancia efectivas. (Hochauser, 2023)

Sin embargo, el aumento en la dependencia de tecnologías UAV en operaciones militares también ha puesto de manifiesto la vulnerabilidad de estos sistemas a los ciberataques. Con el avance de las capacidades cibernéticas de actores maliciosos, los UAV militares se enfrentan a una creciente amenaza de ataques cibernéticos que pueden comprometer su integridad y seguridad operativa (Martinez, 2023).

1.2. Justificación

Cuando las fronteras de un país son muy extensas, ya sea, que se encuentren sobre un cordón montañoso prolongado, con altos picos, altas temperaturas de día y bajas temperaturas de noche; fronteras con selva, monte, ríos, ambientes desérticos, y violencia impulsada por el crimen organizado; o fronteras con amplias superficies de costa y mar, con altas profundidades, y peligrosas corrientes; requieren, para su control, generar diversas estrategias, que nivelen diferentes variables que permitan obtener resultados de control aceptables a costos razonables. Argentina es un país con fronteras de este tipo (Frederic, 2020).

Dicho control parece una tarea difícil de conseguir. En la práctica se pueden observar presupuestos altos para la defensa de fronteras, o controles de poca eficiencia (Vicejefatura de Gabinete del Interior, 2021). Si se consideran las herramientas tradicionales, se requiere de varias estrategias para cada tipo de frontera, y probablemente, cada estrategia requiera su propia administración, gran inversión en infraestructura, entrenamiento diferente para cada tipo de estrategia, y una importante nómina de personal dedicada a las tareas. Ello es sinónimo de gran cantidad de recursos económicos para hacer la tarea de forma correcta y aceptable.

Los VANTs son sistemas que poseen potencial para transformarse en una solución de control de fronteras para países como la Argentina. Pueden realizar inteligencia, seguimiento, y ataque en cualquier punto del país, en poco tiempo. Controlar diversos tipos de fronteras con una sola estrategia, permitiría bajar los costos de forma significativa. (Ministerio de Gobierno – Policía de Misiones, 2024)

En el contexto específico del control de fronteras en Argentina, donde la protección y vigilancia efectiva de los límites territoriales es una prioridad en términos de seguridad nacional, la seguridad cibernética de los UAV utilizados en estas operaciones se convierte en un aspecto crítico a considerar. La capacidad de prevenir, detectar y mitigar ciberataques contra los UAV militares es esencial para garantizar la eficacia y la integridad de las operaciones de control fronterizo en el país (*Drones y Seguridad Nacional*, 2023).

El perímetro de fronteras argentino en la porción continental americana, se extiende a lo largo de aproximadamente 15.000 km. De este total, 5.117 km corresponden al litoral fluvial del Río de la Plata y el Mar Argentino, y 9.376 km a los límites territoriales con los cinco países, distribuidos de este modo (Rhi Sausi & Oddone, 2013, p.169):

- Brasil: 1.132 km.
- Bolivia: 742 km.
- Chile: 5.308 km.
- Paraguay: 1.699 km.
- Uruguay: 887 km.

En los límites norte, Argentina limita con Bolivia, Paraguay y Brasil, como se observa en la Figura I.

Figura I: Límites al norte de Argentina



Fuente: Ministerios del Interior y de Seguridad de la Nación-La Gaceta

Ing.Pamela Ivana Strusiat.

Argentina-Bolivia comparten **742 kilómetros** de frontera, a lo largo de los cuales se ubican 5 pasos internacionales legales, tres de ellos en Salta y uno en Jujuy -El Condado-La Mánora, Aguas Blancas-Bermejo, Salvador Mazza-Yacuiba y La Quiaca-Villazón- y cuentan con un amplio marco institucional de integración física bilateral y multilateral. (Integración Territorial Internacional, 2011)

La frontera **Paraguay-Argentina** comprende, para el caso argentino, las provincias del Chaco, Corrientes, Formosa, Misiones y Salta. Para el territorio paraguayo, los departamentos de Alto de Paraná, Asunción, Boquerón, Itapúa, Ñeembucú, Misiones y Presidente Hayes. La misma tiene una extensión de 1.345 km de límite fluvial y 345 km de frontera seca, totalizando **1.699 km** en toda su extensión, la segunda mayor después del límite con Chile. Fue delimitada a través del “Tratado de Límites” del 3 de febrero de 1876 (Machain-Yrigoyen), y el “Tratado Complementario” del 5 de julio de 1939 (Arbo-Cantilo). Esta frontera cuenta con 36 pasos internacionales legales, y otros ilegales. (Rodríguez, n.d.)

Argentina-Brasil, con 17 pasos fronterizos legales, Brasil limita con Argentina en 1.132 km, y bordea las provincias de Corrientes y Misiones, y los estados de Río Grande do Sul y Paraná (*Límites Territorio Argentino*, n.d.).

Dada la extensa frontera norte argentina, esta tesis analiza las complejidades de las operaciones cibernéticas en el ciclo de vida de los UAV de uso militar en el contexto del control de la frontera norte argentina. A través del análisis de vulnerabilidades, amenazas, ciberataques, y contramedidas para estos sistemas, se busca proporcionar recomendaciones prácticas y herramientas preventivas operaciones y garantizar la protección de las fronteras del país. Diseñadas para fortalecer la seguridad cibernética de los UAV, evitar el sabotaje de sus

El estudio de la ciberseguridad en los UAV militares en el control de la frontera norte de Argentina pretende contribuir a la protección y defensa del territorio nacional.

1.3. Planteamiento del problema de estudio

A partir de un análisis cualitativo de amenazas y debilidades cibernéticas en vehículos aéreos no tripulados, se realiza un estudio de métodos para proponer herramientas a aplicar en las distintas etapas del ciclo de vida (proceso de desarrollo, producción y operación) de VANTs militares.

A raíz de lo cual surge el siguiente cuestionamiento ¿un análisis de ciclo de vida de los drones desde la perspectiva de la resiliencia cibernética incrementa su probabilidad de supervivencia y/o de éxito de las misiones en países de extensas y diferentes fronteras como las de la Argentina?

1.4. Hipótesis

A partir de la recopilación de información disponible en fuentes abiertas y entrevistas a personal militar de la fuerza aérea, un análisis cualitativo permitiría producir herramientas holísticas que logren un mejor entendimiento y abordaje de las vulnerabilidades del ciclo de vida de los VANTs militares en relación con los efectos que pueden producir las operaciones cibernéticas.

La implementación de contramedidas y herramientas preventivas efectivas, contribuye a fortalecer la ciberresiliencia de estos sistemas en operaciones de control de fronteras en Argentina, reduciendo el riesgo de ciberataques y garantizando su adecuado funcionamiento.

1.5. Alcance

El alcance incluirá un análisis de las operaciones cibernéticas en los VANTs de uso militar, centradas en sus vulnerabilidades, amenazas y ciberataques potenciales. Se mencionarán contramedidas y se propondrán herramientas preventivas diseñadas para proteger los VANTs contra posibles riesgos cibernéticos, durante su ciclo de vida, y en el contexto específico de estudio de control de frontera norte en Argentina.

1.6. Objetivo General

Proponer herramientas preventivas tendientes a fortalecer el ciclo de vida de vehículos aéreos no tripulados militares ante ataques cibernéticos permitiendo optimizar su operación a lo largo de extensas y diferentes fronteras.

1.7. Objetivos Específicos

1. Investigar y analizar las etapas del ciclo de vida de los UAV militares, centrándose en la importancia de la seguridad cibernética en este ámbito específico.
2. Identificar los diferentes tipos de ciberataques a los que están expuestos los UAV militares, describiendo sus contramedidas.
3. Evaluar los beneficios y desafíos asociados de implementar UAV militares para control de la frontera norte argentina.

4. Proponer herramientas preventivas que puedan ser implementadas para mitigar los riesgos de ciberataques en los UAV militares utilizados en el control de la frontera norte Argentina, con el objetivo de fortalecer la seguridad cibernética en esa área.

1.8. Metodología de Investigación

1. Revisión de la literatura existente sobre operaciones cibernéticas en UAV militares, ciberataques, vulnerabilidades, y medidas de seguridad cibernética.
2. Estudio de casos sobre aplicación de UAV militares para control de fronteras.
3. Investigación de campo, entrevistando a expertos en diseño, fabricación y/u operaciones de VANTs militares.
4. Recopilación y análisis de datos relevantes sobre ciberataques a UAV militares, vulnerabilidades, y contramedidas aplicadas en el contexto militar y de seguridad fronteriza.
5. Basado en la revisión de la literatura, el estudio de caso, la investigación de campo y el análisis de datos, se desarrolla una propuesta de herramientas preventivas para fortalecer la seguridad cibernética de los UAV militares en el control de la frontera norte en Argentina.
6. Se hace una validación, sometiendo la propuesta a la revisión de expertos en seguridad cibernética y operaciones militares para validar su viabilidad y efectividad en la prevención de ciberataques.

2. VEHÍCULOS AÉREOS NO TRIPULADOS MILITARES

Los UAV militares, conocidos también como VANTs militares o vehículos aéreos no tripulados, son aeronaves que operan sin la necesidad de un piloto a bordo. Estos sistemas son utilizados por las fuerzas armadas en una variedad de roles y misiones debido a su versatilidad y capacidad para realizar tareas de manera autónoma o controlada remotamente. (*Sistemas de Aeronaves no Tripuladas (UAS)* Cir 328 AN/190, 2011)

2.1. Estado del Arte en la Tecnología de Defensa

La tecnología es la que determina cómo realiza un ejército sus funciones y es la que acaba marcando el perfil y las capacidades que debe poseer un militar. Los cambios tecnológicos dejan anticuadas ciertas actividades, las transforman o crean otras nuevas. (Martí Sampere, 2018)

Tanto en sus orígenes como en su evolución y actualidad, la cibernética es igualmente aplicable a los sistemas físicos y sociales. En términos técnicos, se centra en funciones de control y comunicación: ambos fenómenos externos e internos del/al sistema. (*Noción De Sistemas: Cibernética Y Dinámica.*, 2016)

Para el caso particular de la fabricación de un Vehículo Aéreo No Tripulado (VANT) es necesario manejar un conjunto de tecnologías relevantes como: Grupo motopropulsor (motor), forma aerodinámica, forma anti radares, diversos sensores (transductores), sistemas de telecomunicación, el piloto automático, CPUs, memorias, software/firmware y desarrollo de materiales y aleaciones. Estas tecnologías están en constante evolución, por lo que los VANTs son actualizados para no quedar obsoletos. (Aleo, 2021)

A su vez, aparecen nuevas tecnologías a las clásicas ya citadas, como: inteligencia artificial que afectan a los nuevos sistemas de piloto automático, Sistemas Optoelectrónicos de Reconocimiento, modelos atmosféricos que mejoren el plan de misión, motores alternativos que no sean a explosión, por ejemplo eléctricos o a hidrógeno, almacenamiento de energía por ejemplo en baterías o almacenamiento de hidrógeno, energía solar, GPUs, protocolos de comunicación y sistemas de encriptado. Muchas de ellas actúan en el espectro electromagnético y/o emplean el ciberespacio como medio de transferencia de información y por ende es necesario focalizar las cuestiones de ciberdefensa que afectan su ciclo de vida. El desarrollo de estas tecnologías es una tesis en sí misma, pero se mostrará un resumen de algunas de estas tecnologías y su evolución en la aplicación de VANTs (*Nuevas Tecnologías en la Seguridad Transfronteriza*, 2010).

2.1.1. Denominación de Vehículos Aéreos no Tripulados

Antes de continuar, será de utilidad proponer una diferenciación entre las diferentes terminologías que se refieren a los vehículos aéreos no tripulados.

El término drone, es utilizado con mayor frecuencia para referirse a estos vehículos, desde los de uso militar y alta tecnología, a los comerciales para recreación. Pero también ocurre que diferentes palabras se utilizan para describir el mismo aparato o su sistema completo, entre ellos se encuentran:

- **VANT:** Vehículo Aéreo No Tripulado;
- **RPA:** *Remotely Piloted Aircraft* (Aeronave pilotada a distancia - por sus siglas en español);
- **RPAS:** *Remotely Piloted Aircraft System* (Sistemas de aeronaves pilotadas a distancia - por sus siglas en español);
- **UAS:** Unmanned Aerial System (Sistemas de aeronaves no tripuladas- por sus siglas en español). Hace referencia tanto al vehículo aéreo, como a su estación de control, los RRHH , y el adiestramiento entre otros;
- **VACNT:** Vehículos Aéreos de Combate No Tripulados;
- **UCAV:** *Unmanned Combat Air Vehicle* (Vehículo aéreo de combate no tripulado- por sus siglas en español), también conocido a nivel popular como “drone de combate”;
- **UAV:** *Unmanned Aerial Vehicle* (Vehículo aéreo no tripulado- por sus siglas en español), comúnmente conocido como **Drone**. Puede comprender todos los elementos relacionados con la concepción, el diseño, la fabricación, la operación, el mantenimiento, y la disposición final, de los VANT; o puede corresponder únicamente al aparato volador no tripulado.

En la presente investigación se emplearán indistintamente los términos VANT y UAV para hacer mención a los vehículos aéreos no tripulados de gran envergadura de uso militar o de seguridad.

2.2. Orígen y Evolución en la Tecnología de VANTs

Tras el fin de la I Guerra Mundial, la necesidad de entrenar a las dotaciones del ejército aéreo llevó a la industria a proponer los llamados drones o pequeñas plataformas no tripuladas teledirigidas desde tierra que reemplazaron a los antiguos cilindros de lona arrastrados con un cable por un avión, usados para la práctica del tiro aire-aire o tierra-aire. Los drones pronto despertaron un nuevo interés entre los operadores. La posibilidad de ampliar sus funciones, dio lugar a los UAVs. (Escuela Superior de Guerra Aérea, n.d., cap. UAVs y UCAVs).

El UAV no necesitaba un terreno particular para su operación pues podía ser lanzado desde un punto en tierra, desde un vehículo o desde la mano de un operador, según el modelo. Su recuperación también era simple, pues podía aterrizar como un aeromodelo, o ser recogido por una red. El UAV primitivo, dotado con sensores de observación, podía volar pocas decenas

de kilómetros sobre territorio adversario con bajas probabilidades de ser detectado por su tamaño, recogía la información que se le ordenaba mediante un control remoto, y retornaba a su lugar de despegue. Si era descubierto y destruido, podía ser sustituido con unos pocos miles de dólares. Lo que más preocupaba era la pérdida de la información no entregada, dado que la finalidad principal de los UAVs es reunir información y transmitirla sin demora. (Escuela Superior de Guerra Aérea, n.d., cap. UAVs Y UCAVs).

Sin embargo, el estudio de las tecnologías que desembocaron en los VANTs actuales, pueden ser analizados teniendo como punto de partida el “campo de batalla electrónico” de la guerra de Vietnam (1 de noviembre de 1955 a 30 de abril de 1975). Ello permitiría entender el desarrollo del avión de guerra no tripulado contemporáneo, o drone, precursor a su vez de los modelos para uso civil (de Vergara & Trama, 2016).

En 1970 la Fuerza Aérea Norteamericana puso en marcha un programa para aumentar las capacidades de alcance y de vigilancia electrónica de los VANTs. El programa consistió en la financiación de las compañías Boeing y Ryan para desarrollar aviones no tripulados resistentes que volaran a gran altitud. Estos prototipos fueron los más ambiciosos aviones teledirigidos de vigilancia no tripulados en la historia de la Fuerza Aérea, capaces de volar más de 24 horas, siendo pilotados desde el suelo. Al mismo tiempo que los aviones no tripulados, se desarrollaron una serie de «mini-VANT» como los prototipos Praeire, que eran capaces de llevar láser y cámaras de video. Además de aviones no tripulados de vigilancia, la Fuerza Aérea comenzó a experimentar con Firebees² armados. (Delgado, 2016)

El próximo salto relevante en la tecnología de VANTs fue en 1972 donde los aviones teledirigidos de vigilancia fueron equipados con tecnología LORAN (Long Range Navigation o navegación de largo alcance) que mejoraron drásticamente la capacidad operacional de estas aeronaves no tripuladas gracias a un sistema de ayuda a la navegación electrónico que utiliza el intervalo transcurrido entre la recepción de señales de radio transmitidas desde tres o más transmisores para determinar la posición del receptor (algo parecido a la triangulación que utilizan los GPS). (Paucas, 2021)

El empleo de drones en el Valle de la Bekaa en 1982 fue un hito importante en la decisión de impulsar esta capacidad; no solo para reconocimiento, ayudando a descubrir la posición exacta de las baterías antiaéreas enemigas, sino para engañar a los sistemas de radar sirios, haciéndolos pensar que eran aviones tripulados. (Jordán, 2012)

El profundo desarrollo en computación y sistemas de control electrónico durante los años 80 y 90 dieron lugar a los VANTs del presente. Pero no sería hasta finales de los 90 que las fuerzas aéreas americanas comenzaron a tratar los aspectos técnicos que llevaron a dotar

² Ryan Firebee es una serie de blancos aéreos no tripulados desarrollada por la Ryan Aeronautical Company, comenzando en 1951. Fue uno de los primeros drones a reacción, y sigue siendo uno de los blancos aéreos más utilizados jamás construidos.

a estos VANTs de misiles. (Historia De Los Drones, n.d.)

2.3. Caracterización de VANTs Militares

Los VANTs o UAV militares, son utilizados por las fuerzas armadas en una variedad de roles y misiones debido a su versatilidad y capacidad para realizar tareas de manera autónoma o controlada remotamente.

Algunos conceptos clave asociados con los UAV militares incluyen:

1. **Carga útil - Payload:** Refiere al equipo o instrumentación que transporta el UAV para llevar a cabo sus funciones, como cámaras, sensores, armamento, entre otros (*Tecnologías Asociadas a Sistemas De Enjambres De UAVs-La Carga Útil*, 2010);
2. **Carga Paga:** Cantidad de kilogramos de carga que la aeronave puede destinar para sensores u otros dispositivos destinados al cumplimiento de las tareas operacionales del sistema (*Los Sistemas No Tripulados*, 2012);
3. **Alcance operativo:** La distancia máxima que un UAV puede volar desde su punto de origen y regresar, o la distancia que puede cubrir durante una misión específica (Observatorio Aeroespacial, 2020);
4. **Altitud máxima de vuelo:** La altura máxima a la que un UAV puede operar de manera segura y efectiva;
5. **Techo Operativo -Handheld:** Nivel de Vuelo o altitud medida en metros o pies sobre el nivel del mar en que se realizan las operaciones normales asignadas al vehículo (Duarte, 2019);
6. **Autonomía en estación:** tiempo de vuelo en horas en que el móvil puede realizar la tarea operativa (Marquez, 2024);
7. **Tiempo de vuelo:** La duración máxima que un UAV puede permanecer en el aire antes de necesitar recargar combustible o baterías(Sistemas de Aeronaves no Tripuladas (UAS) Cir 328 AN/190, 2011);
8. **Sistema de control:** La infraestructura de comunicaciones y control utilizada para guiar y operar el UAV de forma remota(Sistemas de Aeronaves no Tripuladas (UAS) Cir 328 AN/190, 2011);
9. **Radio de Acción-radio de combate:** distancia en Millas Náuticas que puede recorrer la aeronave en un perfil de vuelo especificado (*Reglas de Vuelo y Operación General*, 2022);
10. **Furtividad (Stealth):** La capacidad de un UAV para evadir la detección por radares enemigos al reducir su firma radar (*Los Sistemas No Tripulados*, 2012);
11. **Peso Máxima de Despegue (MTOW):** es el peso máximo de despegue que soporta el móvil medido en kilogramos. (Moresi, 2009, p. 1).
12. **Auto-Pilot** o autonomía de conducción: capacidad que posee un VANT para realizar tareas de modo independiente, sin control del piloto en tierra. (Piloto Automático, n.d.).
Cuanto mayor sea el número de decisiones que pueda tomar el VANT sin control del

Ing.Pamela Ivana Strusiat.

piloto en tierra, más óptimo será el autopilot, y mientras más complejas sean esas decisiones, más capacidad autónoma posee. Ante VANTs diferentes de características similares, cuanto mejor sea el auto-pilot, mejor será el VANT. Ejemplos de auto-pilots que pueden efectuar los VANTs sin el control del piloto en tierra son: aero-navegar de un punto a otro³; despegar y aterrizar; realizar el seguimiento de un objetivo⁴; detectar que está siendo atacado; y aplicar protocolos de autodefensa cuando sus sensores registran ataques; entre otros.

Estos conceptos son fundamentales para comprender el diseño, implementación y operación efectiva de los UAV militares en entornos de seguridad y defensa.

2.4. Importancia de VANTs en Seguridad y Defensa

Las operaciones cibernéticas en los vehículos aéreos no tripulados (UAV) de uso militar juegan un papel fundamental en la seguridad y defensa nacional por varias razones destacadas:

1. **Vigilancia y Reconocimiento:** Los UAV proporcionan capacidades de vigilancia aérea sin exponer directamente a tripulaciones humanas, lo que los hace ideales para recopilar información sobre las actividades enemigas y áreas de interés (Julio Herrero Isla, 2003).
2. **Apoyo en misiones de combate:** Los UAV pueden llevar a cabo misiones de ataque, reconocimiento y apoyo aéreo cercano, lo que ayuda a reducir el riesgo para el personal militar y aumenta la precisión y efectividad de las operaciones (Mazza, 2023).
3. **Operaciones de Inteligencia:** La información recolectada por los UAV puede ser vital para la toma de decisiones estratégicas y tácticas, proporcionando inteligencia en tiempo real sobre amenazas potenciales (Varela Sabando, 2014).
4. **Reducción de costos:** En comparación con aeronaves tripuladas, los UAV suelen ser más económicos de construir, operar y mantener, lo que permite una mayor disponibilidad para realizar misiones críticas de seguridad y defensa (Jorquera, 2023).
5. **Capacidad de respuesta rápida:** Los UAV pueden desplegarse con rapidez en situaciones de emergencia o crisis, lo que permite una respuesta ágil y efectiva ante amenazas inesperadas (*Uso De Drones En Emergencias*, n.d.).

³ En la presente tesis, se entenderá como Comando al conjunto de instrucciones en el software que tienen como objetivo cumplir un fin determinado en el VANT.

⁴ Existen variados comandos de seguimiento, ya sea que el objetivo sea un blanco fijo en tierra, un blanco móvil en tierra o un blanco móvil en el espacio. Estos ejemplos de comando que se detallaron no son requisitos obligatorios que deba tener el VANT, sino son ejemplo de en qué puede consistir la programación del auto-pilot. Algunos ejemplos de los mencionados son algoritmos simples, otros solo son posibles gracias a los avances en IA.

6. **Seguridad Nacional:** Los UAV desempeñan un papel crítico en la seguridad nacional al proporcionar capacidades de vigilancia, reconocimiento y, eventualmente, ataque (Serruya, 2013).

En resumen, los UAV militares son una herramienta invaluable que aumenta la capacidad de las fuerzas armadas para proteger la seguridad nacional, proporcionando una ventaja estratégica y táctica significativa en diversas situaciones operativas.

Por otra parte, son esenciales para garantizar la seguridad y defensa de un país, al permitir proteger las Infraestructuras Críticas, protegiendo así activos críticos, manteniendo la integridad de los datos y asegurando la eficacia operativa de estos sistemas clave en entornos militares y de control fronterizo.

2.5. Arquitectura de VANTs

Por lo general, la arquitectura de UAVs consta de tres elementos principales: aeronave no tripulada, estación de control terrestre y enlace de datos de comunicación. Estos componentes se describen brevemente a continuación:

1. Controlador de vuelo: se clasifica como la unidad central de procesamiento del vehículo aéreo no tripulado. (Jacob et al., 2020)
2. Estación de Control Terrestre (GCS): se basa en una Instalación en Tierra (OLF, por sus siglas en inglés), que proporciona a los operadores humanos las capacidades necesarias para controlar y/o monitorear los UAV durante sus operaciones a distancia. Las GCS difieren según el tamaño, el tipo y las misiones de los drones. (Jacob et al., 2020)
3. Enlaces de datos: son enlaces inalámbricos que se utilizan para controlar el flujo de información entre el dron y el GCS. Esto depende del alcance operativo de los UAV. (Jacob et al., 2020)

El control de los VANTs se puede clasificar según su distancia del GCS:

- Distancia de línea de visión visual (VLOS): permite enviar y recibir señales de control mediante el uso de ondas de radio directas.
- Distancia más allá de la línea de visión visual (BVLOS): permite controlar los drones a través de comunicaciones por satélite. (Jacob et al., 2020)

2.6. VANTs para la Defensa de la Nación argentina

Fuerza Aérea Argentina

A continuación, en la **Tabla I -2.6**, se menciona la dotación asignada de VANTs militares de la FAA, para los años 2015-2023 (*Libro Blanco de la Defensa*, 2023, p. 92) utilizados para la defensa de nuestro país.

Tabla I-2.6: Dotación asignada de VANTs militares de la FAA para los años 2015-2023

DENOMINACIÓN	DESCRIPCIÓN
TEHUELCHÉ 350B	3 unidades, incorporado como UAV de instrucción.
AR-1 F BÚHO	4 unidades, designado para adiestramiento y adaptación de operadores.
AR-1A AUKAN	1 unidad, con la función de instrucción y formación de controladores.

Fuente: elaboración propia

Por otra parte, el Ministerio de Defensa, el 11 septiembre de 2022, dio a conocer el estado actual de los proyectos de Sistemas Aéreos no Tripulados que desarrolla el Ministerio de Defensa Argentino, y que fue publicado en el Informe 133 de la Honorable. Cámara de Diputados de la Nación, pregunta N°1117 (*Informe 133. Jefatura De Gabinete De Ministros*, 2022), lo cual se resume la **Tabla II- 2.6**.

Tabla II- 2.6: Sistemas Aéreos No Tripulados Argentinos en desarrollo por el Ministerio de Defensa Argentino⁵.

DENOMINACIÓN	DESCRIPCIÓN
Clase I small de ala fija - Búho y Aukán	Desarrollo de la Dirección General de Investigación y Desarrollo de Fuerza Aérea, en etapa de producción de series cortas.
Vehículo Aéreo No Tripulado Clase I de Propulsión Eléctrica - AR 1 F Búho	Corresponde a la categoría ", diseñado para el adiestramiento y adaptación de los operadores en tareas básicas como despegue, aterrizaje, empleo de sensores aerotransportados y navegación acotada. Lo desarrolla la Dirección General de Investigación y Desarrollo de la

⁵ Cabe aclarar que los Vehículos Clase II y III cuentan con antecedentes, tanto de parte de la FAA como de INVAP. En el caso de la Fuerza Aérea, fue el proyecto de un VANT MALE (Medium-Altitude Long-Endurance / Altitud Media Largo Alcance) Clase III denominado Vigía 2B; y en el caso de INVAP, hubo un intento de contrato en 2015, pero se frenó totalmente en 2016.

DENOMINACIÓN	DESCRIPCIÓN
	Fuerza Aérea Argentina.
Vehículo Clase I Plus - Aukán	Con un peso máximo de despegue aproximado a 100 kilogramos puede operar en modo comando y control en tiempo real hasta los 150 kilómetros. Su configuración y capacidad de recibir diversas cargas, permite ejecutar operaciones tácticas diurnas o nocturnas, brindando apoyo a fuerzas terrestres o en el marco de operaciones en apoyo a la comunidad. Lo desarrolla el Centro de Investigaciones Aplicadas (CIA) ubicado en la provincia de Córdoba.
Clase I de ala rotativa y despegue vertical (VTOL)	Desarrollo de un prototipo pre-serie. Son dos proyectos, uno a iniciar en 2022 a través de la Fábrica Argentina de Aviones (FAdA S.A); y otro proyecto del Ejército Argentino para el desarrollo de una serie corta, a través de la Fábrica Argentina de Aviones (FAdA) a iniciar en 2024.
Clase I de ala rotativa y despegue vertical (RUAS)	Contrato en ejecución entre la Armada Argentina e INVAP para el desarrollo de un prototipo navalizado. A futuro el proyecto propone una serie corta de 4 unidades. Para actividades de defensa y seguridad, INVAP ofrece equipar al RUAS con una plataforma giroestabilizada con sensores EO/IR, LIDAR y radar SAR en banda X, otorgando la capacidad de detectar, reconocer e identificar objetos móviles y estacionarios tanto en tierra como en el mar ⁶ .
Clase II de ala fija - Vigía	Desarrollo de la Dirección General de Investigación y Desarrollo de Fuerza Aérea. Con un peso máximo de despegue del orden de los 350 kg. tendrá una capacidad para portar un sensor multiespectral con una amplia gama de aplicaciones en el campo táctico . Lo desarrolla la Dirección General de Investigación y Desarrollo de la Fuerza Aérea.
Clase II de ala fija	Desarrollo de un prototipo operativo, Proyecto a iniciar en 2022 con INVAP y la Fábrica Argentina de Aviones (FAdA S.A) ⁷ .
Clase III de ala fija	Desarrollo de un prototipo operativo. Proyecto en formulación para iniciar en 2024. Lo desarrolla la Dirección General de Investigación y Desarrollo de la Fuerza Aérea.

Fuente: elaboración propia

⁶ Este proyecto guarda similitudes con el VTOL, pero son proyectos ejecutados con diferentes objetivos, diferentes equipos de trabajo y diferentes presupuestos.

⁷ Este proyecto guarda similitudes con el VIGIA, pero son proyectos ejecutados con diferentes objetivos, diferentes equipos de trabajo y diferentes presupuestos.

Ejército Argentino

El Ejército Argentino comenzó en 1996 el desarrollo de la familia de los UAV's "Lipán" (I, II y IIB), desarrollado por técnicos propios. A mediados de 2006 se presentó el Lipán M3 (con 10 unidades producidas en total). (Amorelli, 2021) Posteriormente desarrolló el UAV "Carancho" para misiones ISR y de reducidas dimensiones; y en 2012 se anunció el desarrollo del Lipán XM4 y del remolcador de blancos móviles Tehuelche 320. En la actualidad se encuentran operativos 4 Lipan M3. (Díaz, 2023)

Armada Argentina

Se pudo determinar que los mismos poseen un UAV llamado "Guardián" Aeronave No Tripulada para búsqueda, reconocimiento, detección e identificación de blancos en tiempo real, operando desde buques de superficie y apoyo anfibio de la Infantería de Marina de la Armada Argentina. El Guardián es un UAV de reconocimiento que se utiliza desde buques de superficie para brindar información en tiempo real a la marina. (Borches, 2011)

2.7. Ventajas y Desventajas de los VANTs

Las ventajas y desventajas de los VANTs respecto de los aviones convencionales surgen como resumen de todos los conceptos que se desarrollaron a lo largo de este documento. Los conceptos desarrollados y sus referencias se encuentran a lo largo del trabajo.

Ventajas

- Una de las mayores ventajas que poseen estos tipos de plataformas o vehículos aéreos frente a los sistemas tripulados radican básicamente en evitar riesgos a las personas en situaciones complicadas, como pueden ser vuelos en entornos hostiles o con situaciones climatológicas adversas (Mazza, 2023).
- Algunos VANT tienen gran autonomía, por lo general, de muchas horas, pudiendo llegar a volar por poco más de 24 horas (Observatorio Aeroespacial, 2020).
- Al estar la estación de control en tierra, la operación se puede repartir en varios equipos humanos, en varias jornadas de trabajo (Sistemas de Aeronaves no Tripuladas (UAS) Cir 328 AN/190, 2011).
- El costo de adquisición es muy inferior al de un avión convencional utilizado para las mismas funciones/o dotado con el mismo payload⁸ (Sistemas de Aeronaves no Tripuladas (UAS) Cir 328 AN/190, 2011).

Desventajas

⁸ Carga útil que transporta el vehículo aéreo.

- Actúan mecánicamente y por lo tanto requieren estímulos u órdenes externas. (Sistemas de Aeronaves no Tripuladas (UAS) Cir 328 AN/190, 2011).
- Están sujetos a los problemas técnicos propios de toda máquina portadora de equipos sensibles y complejos (payload). (Sistemas de Aeronaves no Tripuladas (UAS) Cir 328 AN/190, 2011).
- Dependencia de las estaciones de Tierra (conforme su grado de autonomía) (Sistemas de Aeronaves no Tripuladas (UAS) Cir 328 AN/190, 2011).
- Delay entre el piloto y la aeronave. En una aeronave convencional el tiempo en que un piloto realiza una observación, de los instrumentos y del entorno, analiza la información, toma una decisión y ejecuta un movimiento es casi imperceptible en comparación a un VANT (Mazza, 2023).
- En general su velocidades son bajas por lo tanto son más fáciles de interceptar que una aeronave convencional (Mazza, 2023).
- Cuando operan en terrenos o situaciones que los diseñadores no imaginaron, es probable que puedan sufrir daños que una aeronave convencional, con un piloto experimentado pueda solucionar (Sistemas de Aeronaves no Tripuladas (UAS) Cir 328 AN/190, 2011).
- Capacidad de vuelo limitada por el tamaño, alcance y su sistema de enlace y navegación (Mazza, 2023).

A continuación se enmarca normativamente la situación argentina respecto de UAVs.

3. MARCO REGULATORIO

Cada vez son más los Estados que desarrollan y/o invierten en la tecnología de VANTs. En la mayoría de los países, dicho desarrollo tiene generalmente propósitos de inteligencia y vigilancia, aunque hay Estados que los desarrollan para fines ofensivos (Rojo, 2022). El crecimiento de la demanda y la oferta de VANTs abre un debate sobre las reglas y limitaciones en el uso de los mismos.

Aparecen entonces cuestiones jurídicas particulares para este tipo de aeronaves. Prácticamente todas las autoridades y sectores involucrados en la regulación del tráfico aéreo de los VANTs, concuerdan en el criterio que deben cumplir con procedimientos y requisitos de infraestructura de aplicación similares a la aviación tripulada, aunque el concepto de operación sea sustancialmente diferente.

A continuación se citan normas referidas al ciclo de vida del VANT, y normas referidas al uso de VANTs en territorio nacional y en territorio internacional.

3.1. Normativa Ciclo de Vida VANTs

Es de interés señalar que, por el Derecho Aeronáutico, la plataforma que forma parte del UAS no puede ser enteramente asimilable a las aeronaves, dado que el concepto jurídico de aeronave, resulta análogo, más bien, al UAS en su conjunto. (Revista de la Escuela Superior de Guerra Aérea, n.d., pp 136-138). La razón de ello es que el artículo 79, referido al Personal aeronáutico, del Código Aeronáutico Argentino (Decreto 1.954/77) establece que toda aeronave debe tener a bordo un piloto habilitado para conducirla, con las funciones de comandante, y que cuando no exista persona específicamente designada, el piloto al mando será el comandante de la aeronave. (*Parte 135- Requerimientos de Operación: Operaciones no Regulares Internas e Internacionales*, 2012)

Las normas STANAG (STANdardization AGreement) emitidas por la OTAN (Organización del Tratado del Atlántico Norte - NATO "North Atlantic Treaty Organization", por sus siglas en inglés), que se aplican durante el Ciclo de Vida de los VANTs, son las más evolucionadas. Previo a estas regulaciones, los VANTs militares sólo podían operar bajo certificaciones emitidas por su propia autoridad aeronáutica militar. Por ello, la OTAN, para evitar exigir normativas vigentes de aeronaves tripuladas y que se deban interpretar o incluso modificar para encuadrar a los VANTs militares, emitió una serie de Acuerdos de Normalización (STANAG desde 2007) para certificar los VANTs. Así la OTAN, con esta normativa, intenta estandarizar los requisitos regulatorios de los VANTs militares de los países miembros y a la vez que los mismos cuenten con autorización legal por parte de la autoridad correspondiente para operar en el espacio aéreo. (Elaskar et al., 2019, p.46)

3.2. Normativa internacional respecto a VANTs

Algunos instrumentos internacionales respecto al marco regulatorio de VANTs se incluyen en la Tabla 3.2-1.

Tabla 3.2-1: Normativa Internacional VANTs

INSTRUMENTO	DESCRIPCIÓN
Doc 10.019 AN/507- Manual sobre sistemas de aeronaves pilotadas a distancia - Manual on Remotely Piloted Aircraft Systems (RPAS) - OACI - 2015	Contribuye al establecimiento a nivel internacional de un marco regulatorio único para sistemas de aeronave pilotada remotamente, basado en estándares técnicos y prácticas operacionales comunes. Busca integrar de forma segura la operación de ART ⁹ con la aviación convencional, cubriendo así la totalidad del sector, incluye autoridades nacionales e internacionales, fabricantes, operadores, pilotos e inspectores. Para ello, OACI presentó un calendario a corto y largo plazo, con diferentes etapas, para el desarrollo normativo y la implementación de medidas necesarias. (<i>Manual on Remotely Piloted Aircraft Systems (RPAS)</i> , 2015)
Circular 328 AN/190 - Sistemas de aeronaves no tripuladas (UAS) - OACI - 2011	Provee información sobre los Sistemas de aeronaves no tripuladas (UAS), ya que la aviación civil se ha basado hasta ahora en la noción de que un piloto dirige la aeronave desde el interior de ella misma y, con mucha frecuencia, con pasajeros a bordo. Retirar el piloto de la aeronave plantea importantes problemas técnicos y operacionales. (Sistemas de Aeronaves no Tripuladas (UAS) Cir 328 AN/190, 2011)
Doc 7.300 - Convenio sobre Aviación Civil Internacional - Convenio de Chicago - 1944	Las aeronaves tripuladas a distancia son un tipo de aeronave no tripulada. Todas las aeronaves no tripuladas, ya sean pilotadas a distancia, completamente autónomas, o una combinación de ambas, están sujetas a las disposiciones del Artículo 8 del Convenio Internacional sobre Aviación Civil titulado Aeronaves sin piloto. El Artículo 8 exige que las aeronaves no tripuladas que planean operar sobre el territorio de otro Estado obtengan una autorización de ese Estado. (<i>Convention on International Civil Aviation-Doc 7300</i> , 1944)
Artículo 3 (c) y (d) de la Circular 330 AN 189 (OACI, 2011)	Ninguna aeronave de Estado de un Estado contratante podrá volar sobre el territorio de otro Estado contratante o aterrizar en el mismo sin haber obtenido autorización para ello y de conformidad con las condiciones de la autorización. (<i>Cir 330 AN/189 Cooperación Cívico-Militar Para La Gestión Del Tránsito aéreo</i> , 2011, p. 1)
Anexo 11, del Convenio sobre	Permite a los Estados delegar la responsabilidad de la provisión de ATS (Air Traffic Service) en otro Estado, manteniendo la soberanía sobre el espacio

⁹ Sistema o dispositivo autónomo que se utiliza en aeronaves para fines específicos, como sistemas de control de vuelo autónomos, sistemas de navegación autónomos, o cualquier otra tecnología autónoma implementada en aeronaves para mejorar la eficiencia, seguridad o funcionalidad.

INSTRUMENTO	DESCRIPCIÓN
Aviación Civil Internacional	aéreo delegado. (Anexo 11 Al Convenio Sobre Aviación Civil Internacional, 2016)

Fuente: elaboración propia

3.3. Normativa nacional respecto a VANTs

En Argentina la regulación legal sobre el tema se encuentra en plena evolución. Actualmente el marco jurídico está dado por la Resolución N° 880/19 de la Administración Nacional de Aviación Civil (ANAC) que aprueba el texto definitivo del Reglamento de VANT y de SVANT. A nivel constitucional, los artículos 18 y 19 aplican a los derechos a la intimidad y a la privacidad. Además, en la **Tabla 3.3-1**, se destacan otros instrumentos.

Tabla 3.3-1: Normativa aplicada a nivel nacional respecto de VANTs

INSTRUMENTO	DESCRIPCIÓN
Código Aeronáutico (Ley N° 17.285)	Se encuentran legisladas en el Título VII y siguientes, la Responsabilidad del Transportista Aéreo, la Responsabilidad por Daños a Terceros Superficiales y la Responsabilidad por Abordaje. No incluye normas sobre soberanía de nuestro espacio aéreo, por lo que rigen las antiguas normas de Política Aérea que hasta el presente no han sido derogadas. ("Régimen Legal De Las Aeronaves Sin Piloto," n.d., cap. 2)
Ley N° 25.326 y la Disposición N° 20/15 de la Dirección Nacional de Protección de Datos Personales	Reglamentan la captura y el tratamiento de datos personales mediante estas aeronaves
Ley N° 11.723 Ley de Propiedad Intelectual	Alude al derecho de la persona retratada sobre su imagen.
Res. MD N°639 del 24 de mayo de 2007	El RAM, Reglamento de Aeronavegabilidad Militar, junto con las Directivas (DIRAM- <i>Directiva</i> del Reglamento de Aeronavegabilidad Militar), fijan los criterios rectores y pautas generales para asegurar las condiciones de aeronavegabilidad de las aeronaves militares en Argentina. Un aspecto central en la certificación de aeronaves militares, se sustenta en que la Res.

Ing.Pamela Ivana Strusiat.

INSTRUMENTO	DESCRIPCIÓN
	MD N°639, establece que el RAM debe aplicarse de forma análoga a las normativas civiles. (Elaskar et al., 2019, p. 48)
Decreto-Ley 9358/45, art. 2º, y Decreto-ley 12.507/56 art. 2º	El artículo 2º del Decreto-Ley No 9358/45, dispone que “la Nación ejercerá soberanía completa y exclusiva sobre el espacio existente sobre su territorio y aguas territoriales adyacentes al mismo”. Este precepto es reiterado por el Decreto-ley N° 12.507/56 en su artículo 2º. (<i>Decreto/Ley 9358, 1945</i>)
Disposición N° 20/2015 - Boletín Oficial	Protección de Datos Personales referida a las condiciones de licitud para la recolección de datos personales a través de vehículos aéreos no tripulados. Esta nueva norma se encuentra en línea Red de Seguridad y Defensa de América Latina con la anterior disposición sobre aspectos relativos a la privacidad en el uso de dispositivos de video vigilancia (Regulación sobre video vigilancia del 13 de marzo de 2015).
Documentación del Estado Mayor Conjunto de las Fuerzas Armadas (DGAMC), “CAM 4-1” Sistemas de Aeronaves No Tripuladas (SANT) del 23 enero 2014,	Establecen los conceptos básicos relacionados con la aeronavegabilidad y operación de aeronaves no tripuladas militares y los sistemas que ésta integra. Indica, entre otras cosas, que todos los VANTs, ya sea en espacio aéreo controlado o no controlado, deberán volar dentro de áreas restringidas y aprobadas por autoridad de tránsito aéreo. (<i>CAM 4-1 Sistemas De Aeronaves No Tripuladas (SANT)</i> , 2016).
Resoluciones N° 40.250/16 y N° 378/21 de la Superintendencia de Seguros de la Nación	Referidas a las condiciones contractuales del seguro de responsabilidad civil para VANT y SVANT. (Santa, 2022, p. 8)
Normativa, Disposición 1/2015, de la Oficina Nacional de Tecnologías de Información	Se encuentran aspectos relacionados a normas de seguridad para empleados en tecnología complejas. (<i>normativa disposición 1/2015, 2015</i>) un extracto de las mismas se aplican en el Ciclo de Vida de los VANTs.

Fuente: elaboración propia

El aumento de las operaciones militares multinacionales transfronterizas exige coordinación y planificación complejas para evitar la segregación o restricciones innecesarias y obtener el nivel requerido de seguridad operacional. (*Cir 330 AN/189 Cooperación Cívico-Militar Para La Gestión Del Tránsito aéreo*, 2011, p. 2)

Ing.Pamela Ivana Strusiat.

4. ETAPAS DEL CICLO DE VIDA DE LOS VANTs

Las etapas del Ciclo de Vida de un UAV, deben seguir normas específicas, las mismas incluyen:

4.1. Diseño y Desarrollo: En esta etapa se planifica y diseña el UAV, considerando sus requerimientos y funcionalidades específicas. Dicha etapa comienza con un contrato de requerimiento operativo¹⁰ en el que el usuario detalla lo que debe incluir el producto (prototipo), características, payload, además del número de unidades a producir. (Centro Argentino de Ingenieros, n.d.)

Para el caso particular del ámbito militar, se pueden seguir las normas de diseño detalladas en:

- MIL STD 468: Estándar Militar para Desarrollo de Software y Documentación. El propósito de este estándar es establecer requisitos uniformes para el desarrollo y la documentación del software (según entrevista al Capitán S.¹¹ de la Fuerza Aérea Argentina (FAA));
- Norma STD MIL-810g para diseño de aviónica y comunicación (según Mayor D. S., Jefe del Centro de Investigaciones Aplicadas (CIA) de la FAA);
- DO-254: Design Assurance Guidance for Airborne Electronic Hardware (ex Jefe Del Comando Conjunto de la Ciberdefensa);
- STANAG 4586: interoperabilidad de sistemas VANT para la NATO (ex Jefe Del Comando Conjunto de la Ciberdefensa);
- ISO 27001: Gestión de seguridad de la información, aplicable para la protección de datos de VANTs (ex Jefe Del Comando Conjunto de la Ciberdefensa);
- DO-160G: Environmental Conditions and Test Procedures for Airborne Equipment (ex Jefe Del Comando Conjunto de la Ciberdefensa);
- STANAG 4671: UAV system airworthiness requirements (ex Jefe Del Comando Conjunto de la Ciberdefensa);
- La DOD-STD 2167/2168¹² - Defense Systems Software Development. Estándar de defensa de los Estados Unidos, publicado en 1988 (según entrevista Brigadier Mayor (R) M. de la FAA).

4.2. Producción: Consiste en la fabricación y ensamblaje del UAV de acuerdo con el diseño establecido. En esta etapa se establece el espacio físico dónde se van a realizar las tareas de control de calidad, de ensamblado, de almacenamiento de materia prima y del producto.

¹⁰ El requerimiento operativo es un documento detallado de las capacidades, características, operaciones y todo otro aspecto que se considere de interés para que el sistema sea diseñado en relación a las necesidades del cliente.

¹¹ No se incluyen nombres propios a pedido de los entrevistados.

¹² MIL-STD-2167 y MIL-STD-2168, son los números de especificación oficiales para los estándares militares del Departamento de Defensa de EE. UU. que describen los documentos y procedimientos necesarios para desarrollar sistemas informáticos militares. (Estas especificaciones fueron reemplazadas por MIL-STD-498 en 1994).

(Centro Argentino de Ingenieros, n.d.)

Se definen las normas de calidad del proceso productivo y de elecciones de materias primas, ya que esto determinará el proceso de certificación.

Cada fuerza armada posee su propia Doctrina de Empleo, en la cual se desarrolla la estrategia para la utilización de cualquier medio militar, en este caso UAV, pero estos documentos son en general de carácter reservado (según entrevista al Comodoro L. FAA).

Por ejemplo, las normas utilizadas serán:

- Para el control de calidad en el firmware: se aplica la normativa de testeo para software, y las ISO 25.000 (Systems and software engineering), ISO 9.126 (estándar internacional para la evaluación de la calidad del software), e ISO 15.504 (Software Process Improvement Capability Determination) (según entrevista al Comodoro L. Jefe de Proyectos de la DGID de la FAA);
- Lista de verificación de cumplimiento: FAA Order 8230.34D, ASTM F38.01, ASTM F38.02, MIL-HDBK-516C, RTCA DO-160 y MIL-STD-461 EMI/EMC (Jefe del Proyecto RUAS-INVAP);
- Guías de Producción: ASTM F2911, y F3003-14 (Jefe del Proyecto RUAS-INVAP).

Se debe tener en cuenta que el hardware empleado en los vehículos debe ser sometido a un análisis y control de ciberseguridad, que aseguran la CID (Confidencialidad, Integridad y Disponibilidad), a nivel de: los módulos de hardware, los procesos de arranque (boot) seguros, y la lógica de la firmware (recomendación Ing. Benítez)

4.3. Pruebas y Validación: Se realizan pruebas exhaustivas para verificar el correcto funcionamiento y la seguridad del UAV.

- La MIL STD 810F: normas para ensayos ambientales de carácter militar (MIL STD), aplicable también a UAV y sus equipos (según entrevista al Comodoro L. Jefe de Proyectos de la DGID de la FAA);
- STANAG 4671, Controles de calidad a la aeronave terminada aplicable a los Sistemas con Aeronave de ala fija y con un MTOW (Peso máximo de despegue) entre los 150 y 20.000 kg (según entrevista al Comodoro Larrosa Jefe de Proyectos de la DGID de la FAA y al Capitán S. FAA);
- STANAG 4702, Controles de calidad a la aeronave terminada, aplicable a Sistemas con aeronaves de ala rotatoria y MTOW entre 150 y 3.175 kg (según entrevista al Capitán S. FAA);

- STANAG 4746, Controles de calidad a la aeronave terminada, aplicable a sistemas con aeronaves de ala rotatoria y con MTOW igual o inferior a los 150 kg (según entrevista al Capitán S. FAA);
- Normas de Calidad: SAE AS-9100 (Jefe del Proyecto RUAS -INVAP).

4.4. Certificación: Obtención de la certificación de las autoridades reguladoras que aseguren que el VANT es seguro para operar.

- La FAR 23 (Federal Aviation Regulations, Parte 23¹³) para sustanciar algunos puntos endebles que la STANAG no logra completar (Mayor S. de FAA).
- STANAG 4703: indica los requerimientos necesarios a realizar en procesos de “certificación” para el diseño de un UAV bajo normativa militar, la cual abarca a las aeronaves de menos de 150 kg. (coinciden entrevistas al Comodoro L. Jefe de Proyectos de la DGID de la FAA, al Mayor S. de FAAY al Capitán S. FAA);
- DO-178C: Software Considerations in Airborne Systems and Equipment Certification (ex Jefe del Estado Mayor Conjunto de la Ciberdefensa EA);
- Certificado de Aeronavegabilidad (Experimental para I+D): conformidad militar con DIGAMC CAM 4-1 y Conformidad civil con: ANAC RS885 (según Jefe del Proyecto RUAS-INVAP).

4.5. Logística: Abarca todos los aspectos de logística relacionados con los recursos humanos, materiales, conservación y transporte de VANTs hasta ser entregados a los responsables de la operación. (Centro Argentino de Ingenieros, n.d.)

Se considera logística en la fase de construcción a todo el proceso de almacenamiento de los VANTs terminados y de entrega de los mismos a las fuerzas de seguridad, es decir, a los operadores, de forma segura, sin que se vea vulnerada la seguridad de los VANTs en ningún momento.

¹³ es un conjunto de normas establecidas por la Administración Federal de Aviación (FAA) de los Estados Unidos, que regula los requisitos de aeronavegabilidad para aviones de aviación general.

4.6. Despliegue y Operación: El UAV es implementado para llevar a cabo las tareas para las cuales fue diseñado, operando de manera rutinaria. La operación es el tiempo en que el sistema es empleado en la función específica para la cual fue diseñado¹⁴, donde los operadores de VANTs lo operan de manera remota. Posteriormente su efectividad puede comenzar a declinar, por lo que puede ser modernizado o pasar a disposición final.

Se utilizan las siguiente normas:

- STANAG-4670 (ED-3): Acuerdo De Normalización: Guía para la Formación de Operadores de Sistemas de Aeronaves no Tripuladas (UAS) (22-Abr-2014);
- Licencias de personal: Tripulación remota: Circular 381 de la OACI y ANAC RS885 (Jefe del Proyecto RUAS (Rotary-Wing Unmanned Aerial System)-INVAP);
- Seguridad Operacional: Evaluación de riesgos de operación específica SORA, de JARUS, con directrices de la autoridad suiza Oficina Federal de Aviación Civil (FOCA), y Evaluación de seguridad del sistema conforme a SAE ARP 4761 y MIL-STD-882E (Jefe del Proyecto RUAS-INVAP)
- Entrenamiento de la tripulación: Militar EMCO DHAM PC 13-04 (militar), además por medio del Simulador y entrenador de la Crew: Piloto remoto y operador de carga útil.(Jefe del Proyecto RUAS (Rotary-Wing Unmanned Aerial System)-INVAP).

La etapa operación se subdivide en las subetapas: mando, control, comunicación y cálculo.

4.6.1. Mando: Desarrollo y planificación de la misión. Dicha tarea es realizada por altos mandos de las fuerzas. Los datos que se generen para desarrollar la misión, pueden ser útiles para la planificación futura de otras misiones.¹⁵

4.6.2. Control: Hace referencia al control de misión y su correcto desarrollo en tiempo real. Una forma es sabotear las comunicaciones entre el control y el VANT.

4.6.3.Comunicación: Cuando se está desarrollando la misión en tiempo real, puede compartir la información o parte de la información que se está generando, con diferentes agentes externos, por fuera de la sala de control propiamente dicha.

4.6.4. Cálculo: Hace referencia al procesamiento de datos durante la misión para

¹⁴ Los Operadores son entendidos como clientes para los Desarrolladores y/o Fabricantes. Los recursos humanos de los Operadores son en su mayoría del rubro militar. Generalmente, las fases que no son Operación están constituidas en su mayoría por civiles. En el organigrama, la fase de Operación debe depender de forma directa del poder Ejecutivo, y esto es así ya que la fase de Operación pertenece al área de Defensa del país y el Presidente de la nación es el Jefe de las Fuerzas Armadas.

¹⁵ Se puede observar que cada misión genera un volumen elevado de datos. De dichos datos, va a existir información que se genere fácilmente, observando estos datos de forma directa, con métricas estadísticas, con gráficos o una combinación de estas; pero va a existir otra información que deberá ser extraída de los datos aplicando técnicas más complejas, por eso se deberá recurrir a un área de ciencia de datos.

generar información que vaya modificando la misma en tiempo real, pero no al objetivo de la misión en sí misma. Para lograr esto se debe contar con sistemas desarrollados a medida, y hardware de alta complejidad para soportar los mismos. El equipo de trabajo que desarrolla esto debe ser el mismo que desarrolla las herramientas y realice la ciencia de datos para la base de datos histórica de Mando.

4.7. Mantenimiento y Soporte: Se brinda mantenimiento regular al UAV para garantizar su correcto desempeño, así como soporte técnico en caso de ser necesario.

Por ejemplo, se puede seguir las normas:

- STANAG 3609: Normas para el Mantenimiento de Sistemas Fijos de Recepción, Almacenamiento y Suministros de Combustible de Aviación: El propósito de este acuerdo es establecer estándares mínimos de mantenimiento para las instalaciones fijas de almacenamiento de combustible para aviones (JFSI) utilizadas por las naciones de la OTAN. (STANAG 3609 - Ed: 6, 2019);
- Mantenimiento, guías: ASTM F2909-19 y - ASTM F3366-19 (Jefe del Proyecto RUAS -INVAP)

4.8. Retirada y Eliminación: Cuando el UAV llega al final de su vida útil, se retira de servicio de manera segura y se procede con su eliminación o desmantelamiento adecuado. Un VANT puede ser dado de baja por obsoleto, por fallas insalvables, por haber sufrido sabotaje, por haber cumplido las horas de vida del fabricante o por rotura tras un ataque que sean irreparables. La baja de un VANT debe cumplir ciertos requisitos para no exponer la tecnología. Es importante destacar que no puede bajo ninguna circunstancia ser entregado a terceros, ya que incluso un VANT que fue dado de baja por roturas insalvables tras un ataque contiene información de sus vulnerabilidades. (*Soluciones C4ISR Para Sistemas De Aeronaves No Tripuladas (UAS)*, 2021)

En el ANEXO 4, se presenta una propuesta de normas STANAG que podrían ser utilizadas para certificar los VANTs de uso militar.

A los efectos de la presente investigación, se describirán las etapas: **diseño, construcción y logística, mantenimiento y operación**. En el ANEXO 1 se propone emplear la llamada "Curva de Davies" o "Curva de la Bañera" como medio para establecer el ciclo de vida de los VANTs militares.

5. CIBERATAQUES EN EL CICLO DE VIDA DE VANTs Y CONTRAMEDIDAS

Los vehículos aéreos no tripulados (UAV) militares son propensos a una serie de ataques y ciberataques que pueden comprometer su integridad y seguridad operativa (de Vergara & Trama, 2016).

En operación, los VANTs pueden ser atacados tanto en la parte física (el aparato), el ciberespacio (durante la operación) o en aspectos virtuales como la comunicación, o como al operador (amenaza o soborno). Los sistemas de comunicación utilizados para controlar y operar los UAV pueden ser vulnerables a interceptación, spoofing (suplantación) o jamming (interferencia), lo que podría permitir a un atacante tomar el control del UAV. Debido a la casi completa dependencia de las operaciones de los UAV en varios insumos del entorno externo, la mayoría de los ataques comienzan con modificaciones externas maliciosas de estos insumos. (Jeler & Alexandrescu, 2020)

5.1 Ataques no cibernéticos a UAVs-Contramedidas

Entre los ataques no cibernéticos a UAVs, y a modo de ejemplo, podemos mencionar los listados en la Tabla 5.1-1:

Tabla 5.1-1: Ataques no cibernéticos a UAVs y Contramedida

ETAPA	CIBERATAQUE	CONTRAMEDIDAS
Diseño	Ingeniería Social: Actores malintencionados intentando obtener información sensible mediante la manipulación de empleados (phishing, pretexting, etc.) (de Vergara & Trama, 2016)	Capacitación en riesgos de ingeniería social; y aplicación de protocolos de verificación de identidades (de Vergara & Trama, 2016).
	Inserción de Vulnerabilidades: Actores internos o infiltrados que introducen errores o fallos de seguridad deliberadamente en el diseño (entrevistas).	Auditorías de diseño y código, y Seguridad y control de acceso rigurosos (Fernández Provecho, 2016).
Construcción	Manipulación de Hardware: Interferencia física con los componentes del UAV para debilitar su operatividad (de Vergara & Trama, 2016).	Supervisión y vigilancia durante la fabricación, y uso de componentes de proveedores confiables (entrevistas).
Operación	Soborno o extorsión: en el momento de realizar la operación, la misma se ve	En operaciones con VANTs, el anonimato de los operadores resulta de vital

ETAPA	CIBERATAQUE	CONTRAMEDIDAS
	entorpecida porque el operador se encuentra distraído o persuadido en alguna forma, o un operador retirado puede ser extorsionado en alguna forma para entregar información relevante(entrevistas).	importancia, dado que pueden ser víctimas de persuasión por métodos no convencionales, como amenazas, ataques psicológicos o sobornos (entrevista).
Mantenimiento	Acceso Físico no Autorizado: Manipulación física del UAV durante el mantenimiento para instalar dispositivos de espionaje o sabotaje(entrevistas).	Controles de acceso y seguridad en áreas de mantenimiento, e Inspecciones antes y después del mantenimiento(de Vergara & Trama, 2016).

Cabe destacar que algunos de estos pueden darse en más de una etapa.

5.2 Ataques cibernéticos a UAVs -Contramedidas

Dada la naturaleza de la maestría en ciberdefensa y ciberseguridad, a continuación se describen algunos tipos de ciberataques a los que están expuestos los UAV militares y que afectan las diferentes etapas del ciclo de vida, y sus contramedidas. Es fundamental implementar medidas de seguridad cibernética sólidas y actualizadas para proteger los sistemas críticos y reducir la probabilidad de que sufran interferencias o compromisos durante sus operaciones, para lo cual se proponen contramedidas a las mismas.

Las mismas tendrán en cuenta las vulnerabilidades a las que es propenso un UAV durante su ciclo de vida, las cuales se relacionan directamente con las amenazas:

1. **Diseño y Construcción:** Backdoors en el firmware, errores en el diseño de comunicación segura (según entrevista a Comodoro de la FAA y a ex Jefe del Comando Conjunto de la Ciberdefensa)
2. **Logística:** Compromiso en la cadena de suministro (Entrevista a ex Jefe del Comando Conjunto de la Ciberdefensa);
3. **Operación:** Interferencia en comunicaciones, acceso no autorizado a la estación de control y al propio UAV (Entrevista al capitán de la FAA y a ex Jefe del Comando Conjunto de la Ciberdefensa); y
4. **Mantenimiento:** Actualizaciones de software no verificadas.(Entrevista a ex Jefe del Comando Conjunto de la Ciberdefensa).

En ciberdefensa, se menciona el término superficie de ataque, que es el vector de ataque que puede ocurrir sobre un UAV, entre los cuales se consideran principalmente: El enlace y actualización de software (Mayor jefe del Centro de Investigaciones Aplicadas (CIA)

de la de la FAA).

Las mención a los ciberataques y contramedidas que se mencionan a continuación, están basadas en la revisión bibliográfica y las entrevistas realizadas a personal especializado de las FFAA. Las entrevistas se encuentran en el ANEXO 2.

Se describen en la tabla 5.2-1 los ciberataques más comunes que pueden afectar los UAVs durante las etapas de diseño, construcción, operación y mantenimiento y sus contramedidas correspondientes.

Tabla 5.2-1: Ciberataques y contramedidas Ciclo de Vida VANTs

ETAPA	CIBERATAQUE	CONTRAMEDIDAS
Diseño	Robo de Propiedad Intelectual: Ataques dirigidos a extraer información sobre el diseño del UAV (Ciberseguridad En El Sector Aeroespacial: Escenario, Riesgos Y Retos De Futuro, n.d.).	1. Encriptar toda la información sensible y los datos de diseño (¿Qué es el Cifrado De Datos?, n.d.). 2. Implementar controles de acceso estrictos, incluyendo autenticación multifactor (MFA) para acceder a información crítica. (¿Qué es la Autenticación Multifactor? - Explicación De La Autenticación Multifactor, n.d.) 3. Registrar y monitorear todas las actividades en los sistemas de desarrollo para detectar accesos no autorizados (Borges & Carvalho, 2024). 4. Patentar las Tecnologías Estratégicas (Plataformas Abiertas Para Tecnologías Estratégicas, 2017)
	Inserción de Backdoors: Colocar puertas traseras en el software de control del UAV durante la etapa de desarrollo (de Vergara & Trama, 2016).	1. Implementar revisiones de seguridad profundas y forenses del código fuente (Revisión De Código Fuente, n.d.). 2. Utilizar firmas digitales y comprobaciones de integridad para verificar la autenticidad del software desarrollado (Utilización De Firmas Digitales Para Proteger La Integridad Del Software, 2024).
	Malware en Herramientas de Desarrollo: Infectar herramientas de diseño y desarrollo con malware para comprometer el software del UAV (de Vergara & Trama, 2016).	1. Usar herramientas de seguridad y antivirus actualizados en todas las estaciones de desarrollo (de Vergara & Trama, 2016). 2. Revisar y validar regularmente la integridad y seguridad de las herramientas de desarrollo utilizadas (Garzón, 2024).
Construcción	Compromiso de Cadena de Suministro: Introducción de malware en componentes electrónicos durante la fabricación (Huichalaf, 2024).	Evaluar a los proveedores en términos de seguridad y fiabilidad antes de trabajar con ellos (Huichalaf, 2024).
	Modificación de Firmware: Alterar el firmware de los componentes críticos para incluir código malicioso (Puodzius, 2017).	1. Implementar sistemas de actualización de firmware con cifrado y firma digital (Puodzius, 2017). 2. Escaneo de Firmware: Realizar escaneos de vulnerabilidades y pruebas de integridad en el firmware recibido (Puodzius, 2017).

OPERACIONES CIBERNÉTICAS EN EL CICLO DE VIDA DE VANTs DE USO MILITAR, SUS VULNERABILIDADES, AMENAZAS, CIBERATAQUES, CONTRAMEDIDAS Y PROPUESTA DE HERRAMIENTAS PREVENTIVAS

Maestría en Ciberdefensa y Ciberseguridad UBA-FCE Posgrado

ETAPA	CIBERATAQUE	CONTRAMEDIDAS
Operación	Secuestro de UAV: Tomar el control del UAV mediante la interceptación y manipulación de sus señales de comunicación (Zapata Madrigal & García Sierra, 2021).	1. Asegurar que todas las comunicaciones entre el UAV y la base de control estén cifradas (entrevistas a personal de FAA). 2.Monitoreo de Tráfico: Implementar monitoreo continuo del tráfico de red para detectar actividades sospechosas(de Vergara & Trama, 2016).
	Ataques de Denegación de Servicio (DoS): Interrumpir las operaciones del UAV sobrecargando sus sistemas de control (de Vergara & Trama, 2016).	Utilizar firewalls y sistemas IDS/IPS para filtrar y bloquear ataques DoS (Pathak, 2024).
	Intercepción y Manipulación de Datos: Provocan la pérdida de enlace UAV-Estación de control, capturar y alterar los datos transmitidos entre el UAV y la estación de control, y realizar cambios en la misión, plan de vuelo, utilización de sus sensores, pérdida de datos de comando y control, entre otras (entrevistas).	1.Utilizar cifrado de extremo a extremo para proteger los datos que son transmitidos(entrevistas). 2.Implementar mecanismos de validación de integridad de datos para detectar y corregir manipulaciones (Zapata Madrigal & García Sierra, 2021).
	Ataques de red: Comprometer las redes de comunicación utilizadas por el UAV para insertar código malicioso o robar datos (de Vergara & Trama, 2016).	Mantener los sistemas y componentes de red actualizados con los últimos parches de seguridad(de Vergara & Trama, 2016).
	Señales Falsas (Spoofing): Enviar señales falsas al UAV para alterar su trayectoria y control (de Vergara & Trama, 2016). Interferir la señal del GPS (ó GNSS) con ataques de Interferencia Electrónica (Jamming) para confundir al UAV en su posicionamiento, y así bloquear la señales GPS o las comunicaciones del UAV(entrevistas).	1.Utilizar autenticación criptográfica en las señales de control y navegación (de Vergara & Trama, 2016). 2.Implementar sistemas de detección de spoofing para identificar y mitigar señales falsas de GPS (entrevistas). 1. Contar con un motor alternativo, turbo hélice o un reactor. Teniendo en cuenta la autonomía y la necesidad de operar a grandes alturas (entrevistas). 2. Utilizar frecuencias alternas y tecnología anti-jamming e Integración de navegación inercial (entrevistas) En Anexo 3 se amplía este concepto.
Mantenimiento	Inserción de Malware en Actualizaciones: Comprometer el proceso de actualización del software o firmware para introducir malware(entrevistas).	1.Utilizar métodos seguros y cifrados para la distribución de actualizaciones de firmware y software(de Vergara & Trama, 2016). 2. Verificación de Actualizaciones: Implementar sistemas automatizados para verificar la integridad y autenticidad de las actualizaciones antes de la instalación(de Vergara & Trama, 2016). 3. Preparar el software para atacar específicamente las vulnerabilidades y explotarlas después, ello fue estandarizado por Lockheed Martin como cybersecurity kill chain (entrevista).

Ing.Pamela Ivana Strusiat.

ETAPA	CIBERATAQUE	CONTRAMEDIDAS
	Ataques Internos: Empleados maliciosos que insertan código malicioso durante el mantenimiento (entrevista).	1.Mantener registros detallados y monitorear las actividades de mantenimiento realizadas por los empleados (entrevista).

En resumen, se puede atacar un VANT tanto en operación, como cuando no está en operación. También se puede afectar la estación de control en tierra, y/o al operador/piloto. Esto permite observar que existen vulnerabilidades tanto en la fase de diseño del VANT como producto terminado, en su fase de desarrollo, producción y/o logística y mantenimiento.

Por lo tanto, es crucial abordar y mitigar estas vulnerabilidades para proteger la integridad y seguridad de los UAV militares y las misiones en las que se utilizan contra ataques y ciberataques.

7. CONTROL DE FRONTERAS

7.1. UAV para control de fronteras - Casos internacionales

Se mencionan a continuación algunos ejemplos generales de países que planean utilizar o se encuentran utilizando UAV en sus operaciones de control de fronteras:

1. **Israel:** Israel ha sido pionero en el uso de UAV para seguridad fronteriza. El país ha implementado drones para la vigilancia de sus fronteras con Cisjordania, Gaza y otros territorios (Knipp, 2019), lo que ha demostrado ser una herramienta efectiva en la detección de amenazas y actividades sospechosas. Junto a la Policía de Fronteras de Israel, los drones son una herramienta diaria de gestión militar de las fronteras (*Israel, Una Superpotencia De Drones*, 2019).
2. **Estados Unidos:** La Patrulla Fronteriza de Estados Unidos ha implementado con éxito UAV para la vigilancia de sus fronteras con México y Canadá. A mediados de 2012 EE UU invirtió 250M de USD en el programa de vigilancia con UAV en la frontera y contaba con 9 aparatos (*Casi La Mitad De La Frontera Entre Estados Unidos Y México Vigilada Por UAV Predator*, 2014). Los UAV les permiten extender su alcance y monitorear áreas remotas de manera más eficiente, y detectar actividades ilegales. Para ello cuentan con la Oficina de Aduanas y Protección Fronteriza de los Estados Unidos (CBP). y la Patrulla Fronteriza de los Estados Unidos (USBP).
3. **Australia:** La Real Fuerza Aérea Australiana anunció en junio de 2024 que recibirá su primer drone MQ-4C Triton, provenientes de Estados Unidos, como parte del objetivo del país para reforzar las capacidades de vigilancia marítima. Previo a ello, se habían instalado los sistemas de apoyo en tierra para mejorar las operaciones de inteligencia, vigilancia y reconocimiento (ISR) (*La Real Fuerza Aérea Australiana Recibe Su Primer Drone MQ-4C Triton Proveniente De EE. UU.*, 2024). Los UAV serán utilizados para patrullar y proteger las fronteras marítimas del país, detectar embarcaciones sospechosas y en la lucha contra la pesca ilegal. El proyecto había sido anunciado en el año 2014. (*Australia Reforzará Su Seguridad Marítima Con El UAV MQ-4C "Triton"*, 2014)
4. **Corea del Sur:** En enero de 2024 Corea del Sur anunció que comenzará la producción de su más moderno drone de vigilancia y reconocimiento MUAV. Cabe recordar que en agosto del año 2023, el Ministerio de Defensa surcoreano anunció sus planes para impulsar la producción masiva de los nuevos MUAVs. Posteriormente la Administración de Programas de Adquisición de Defensa (DAPA) de Corea del Sur firmó un acuerdo de

producción por aproximadamente 352,8M de USD con Korean Air, la aerolínea surcoreana de mayor tamaño, y con dos empresas especializadas en defensa: LIG Nex1 y Hanwha Systems, para la confección del mismo (Cepeda, 2024). Los mismos podrían ser respuesta a las actividades de inteligencia realizadas por parte de Corea del Norte, en la frontera con Corea del Sur, los cuales fueron registrados en los años 2014 (*Cayó En Corea Del Sur Un Drone Espía*, 2014) y 2022 (*Drones De Corea Del Norte Llegan Al Territorio De Corea Del Sur En Pleno Aumento De La Tensión Entre Ambos Países*, 2022).

5. **Chile:** en mayo de 2024 el gobierno de Chile presentó el Proyecto Muralla digital, que planea resguardar la fronteras norte del país, por medio de puestos de observación fronteriza, y vehículos de respuesta táctica, entre los que se incluyen vehículos aéreos no tripulados. La adquisición de equipamiento y medios planean ser desplegados en la frontera en las regiones de Arica y Parinacota, Tarapacá y Antofagasta, al norte del país. Por otra parte, está en implementación el proyecto de Sistema Integrado de Frontera (SIFRON) que considera la compra de vehículos (33 camionetas, cuatrimotos, furgones), para el despliegue de las fuerzas. Los primeros vehículos llegarán entre agosto y septiembre de este año y antes de fin de año se dispondrá de apoyo de nuevas cámaras de televigilancia (Eberlein, 2024). Asimismo, en el marco del proyecto Muralla Digital, se aumentará la capacidad de vigilancia aérea, incluyendo la adquisición de drones y una nueva cámara para el avión vigía que Carabineros dispone en la zona norte del país. Los recursos están disponibles y se ha dado urgencia a las compras para disponer de este equipamiento (*Colchane: Subsecretario Del Interior Anunció Medidas De Reforzamiento Del Control Fronterizo*, 2024).

Estos ejemplos ilustran cómo varios países han incorporado con éxito o planean incorporar UAV en sus operaciones de control de fronteras para mejorar la vigilancia, la detección de amenazas y la seguridad fronteriza. Estos casos podrían servir de referencia para explorar posibles estrategias en el contexto del control de fronteras argentinas, adaptándolas a las necesidades y desafíos específicos del país.

7.2. Aplicación al control de fronteras en Argentina

Una amenaza factible al territorio nacional se da por pérdida del control de las fronteras. Particularmente la frontera Norte involucra un problema de alta complejidad, por su extensión, por su geografía y por los diferentes tipos de tráfico ilegal.

Con respecto a la geografía lo más relevante que podemos encontrar para la dificultad del control son las zonas selváticas y sus ríos, con climas extremos de día y de noche.

Con respecto a la extensión, de Este a Oeste, mide aproximadamente 3.500 km, siendo las fronteras con:

- Brasil: 1.132 km

- Bolivia: 742 km
- Paraguay: 1.699 km

Con respecto a la actividad, existe circulación de productos legales e ilegales.

De acuerdo a las entrevistas realizadas a personal de Gendarmería Nacional de Frontera Norte, las actividades de ingreso de mercancías ilegales al territorio nacional desde la frontera norte, son efectuados por vía aérea en su mayoría, y presentan la problemática de que no pueden ser derribados ya que no existe una Ley de Derribos nacional. Por otro lado se llevan a cabo en operaciones clandestinas nocturnas, donde la coordinación entre las fuerzas de seguridad y las fuerzas militares no es óptima o no existe. Finalmente, a pesar de los proyectos y capacidades de que dispone gendarmería, no cuenta con radares, aviones interceptores, drones de gran envergadura, ni los recursos necesarios para hacer el seguimiento y llegar a la zona de entrega para actuar rápidamente.

Entonces, podemos resumir los desafíos del control de la frontera norte argentina en:

1. La extensa línea fronteriza, que dificulta la vigilancia y control efectivo de todas las áreas;
2. El terreno variado y difícil de acceder en algunas zonas fronterizas, que puede dificultar la instalación de sistemas de vigilancia y patrullaje;
3. El flujo constante de migrantes, solicitantes de asilo y refugiados, que puede sobrecargar los recursos de control fronterizo y dificultar la detección de otras actividades delictivas;
4. La forma clandestina en que la mercancía ilegal ingresa por vía aérea;
5. La corrupción en algunas agencias de seguridad y aduanas puede comprometer los esfuerzos de control fronterizo y facilitar actividades ilícitas.
6. Finalmente, el aumento de ciberamenazas, a nivel mundial, puede representar un desafío adicional en la protección de infraestructuras críticas de control fronterizo.

Se observa entonces que, en el contexto del control de la frontera norte argentina, surge la necesidad de identificar y abordar eficazmente posibles amenazas como el contrabando, el tráfico de drogas, y otras actividades ilícitas, para lo cual se debe garantizar una vigilancia adecuada de las fronteras y así prevenir la entrada ilegal de personas y mercancías.

Para ello, implementar tecnologías avanzadas, como el uso de UAV, y la colaboración y coordinación entre agencias gubernamentales, fuerzas de seguridad y fuerzas armadas, contribuye a detectar actividades sospechosas en las fronteras.

Abordar estas necesidades y desafíos en el control de fronteras argentinas requiere de una combinación de estrategias integrales que incluyan tecnologías avanzadas, capacitación del personal, coordinación interinstitucional y enfoques innovadores para garantizar la seguridad y protección de las fronteras del país.

Ing.Pamela Ivana Strusiat.

7.3. Ventajas de utilizar UAV en el control de fronteras argentinas

La utilización de Vehículos Aéreos No Tripulados en el control de fronteras argentinas ofrece ventajas como:

1. Proporcionar vigilancia aérea continua y en tiempo real de áreas remotas y de difícil acceso a lo largo de las fronteras, lo que ayudaría a detectar actividades sospechosas con mayor eficacia;
2. Cubrir grandes extensiones de terreno de manera rápida y eficiente, ampliando la cobertura de vigilancia más allá de lo factible con patrullas terrestres tradicionales;
3. Detectar amenazas de forma temprana, como el contrabando, la migración ilegal, el tráfico de drogas y otras actividades delictivas en las fronteras, por medio de la combinación de UAV con tecnología cibernética avanzada;
4. Reducir riesgos para el personal militar y de seguridad, al utilizar UAV en lugar de desplegar personal en zonas peligrosas;
5. Recopilar información útil sobre movimientos de contrabando, rutas de tráfico ilícito y otras actividades delictivas;
6. Implementar contramedidas rápidas y efectivas en caso de detección de amenazas.
7. Reducir costos, en comparación con métodos tradicionales de vigilancia fronteriza, dado que puede resultar más rentable a largo plazo, al reducir la necesidad de recursos humanos y operativos.

7.4. Empleo de UAVs en ARGENTINA - Antecedentes

En 2017, se inauguró en La Quiaca, Jujuy, el primer centro integrado de control de fronteras. Además de cámaras y radares, se incorporó un conjunto de sensores móviles, que incluyen drones, drones cautivos [colgados de camionetas que cuentan con un sistema de elevación] y un camión con un centro de comando móvil (*Cámaras, Radares Y Drones: Así Funciona La Tecnología Traída De Israel Para Controlar Las Fronteras*, 2014).

En abril de 2018, se puso en marcha el Plan de Fronteras Seguras, donde participan diferentes provincias del norte del país. Este plan de protección de las fronteras dio lugar al Operativo Integración Norte que permite combinar esfuerzos y mejorar el desempeño de las fuerzas de seguridad y militar en los kilómetros de frontera a lo largo de Jujuy, Salta, Formosa, Corrientes y Misiones, en el contexto de los problemas de inseguridad que se originan en zonas poco pobladas (*El Presidente Mauricio Macri Puso En Marcha El Primer Operativo Del Programa Fronteras Protegidas*, 2018).

En octubre de 2019, el Ministerio de Seguridad de la Nación y el jefe de Prefectura Naval presentaron el primer sistema integrado inteligente de América Latina denominado Sistema de Vigilancia Integrada de Fronteras (SITEVIF). El sistema plantea como objetivo fortalecer el control de la frontera norte a través de tecnología de punta en materia de vigilancia y procesamiento de información, y así combatir el delito complejo. En el acto se anunció la incorporación de sensores móviles, vehículos, drones y equipamiento para combatir el delito complejo en la frontera norte (*Bullrich Presentó La Entrega De Sensores Móviles Del Sistema De Vigilancia Integrada De Fronteras*, 2019).

En mayo de 2024, en el marco del Plan Operativo de Fronteras Seguras, el Ministerio de Seguridad de la Provincia de Jujuy, anunció la creación de un Grupo de Operaciones de Frontera (GOF), con personal del Cuerpo Especial de Operaciones Policiales (CEOP) y con los elementos instruidos para actuar en zonas de campaña, con equipo pesado, y armamento acorde a los riesgos derivados de paso de frontera (*Grupo De Operaciones De Frontera Trabaja Para Evitar El Ingreso Ilegal Al País*, 2017).

Según entrevista a cuerpo de gendarmería en la zona norte del país, particularmente de la frontera norte de Jujuy, los UAV de que dispone la fuerza son operados por personal certificado que se encuentra en estaciones dispuestas para comando y control, carga de combustible y baterías y bajada de datos en tiempo real.

Los programas de Vigilancia por medio de UAV, radican en la combinación de recursos, y actividades compartidas por medio del sistemas de seguridad argentino y de las fuerzas militares.

Según entrevista a personal de la FAA, se debe tener en cuenta que cuando se realiza la programación en un sistema de planeamiento de misión se deben tener en cuenta variables como: Amenazas, y orden de batalla propio y del enemigo, sistemas antiaéreos; Zonas de vuelo restringidas; Información de inteligencia previa; Tipos de sensores a emplear ; Información de los blancos atacados y aspectos centrales a relevar; Coordinaciones con el control de tránsito y Alternativas y punto de espera.

Por otra parte, debido al desafío de la extensa frontera norte, realizar las operaciones en la forma que las realiza Gendarmería Nacional, y en la forma que planifica realizar Chile por medio de su muralla digital, es decir, considerando una correcta distribución de puestos de control y estaciones terrenas para carga y descarga de datos, y para carga de combustible y baterías del UAV, es un factor que contribuye al éxito de las misiones.

En resumen, extender el uso de UAVs y ampliar la superficie de control de fronteras argentinas, con un correcto análisis de las necesidades de cada región, ya sea por sus características geográficas, climatológicas, o de flujo de actividades, y una correcta

planificación de las misiones, proporciona una solución eficaz y avanzada para abordar los desafíos de seguridad y proteger las fronteras de manera eficiente y efectiva.

8. PROPUESTA DE HERRAMIENTAS PREVENTIVAS ANTE AMENAZAS EN CIBERSEGURIDAD DE UAVs

La defensa cibernética de los UAV militares es crucial para proteger estos sistemas de posibles ciberataques y garantizar su funcionamiento seguro y efectivo.

Dadas las necesidades específicas del control de la frontera norte argentina se propone una serie de herramientas preventivas que permita mejorar la seguridad cibernética en UAV y posibles colaboraciones o alianzas estratégicas, para así fortalecer la capacidad de seguridad del país y mejorar la eficacia en la protección de sus fronteras contra amenazas transfronterizas.

Si bien no existe una solución única que proteja al UAV de una variedad de amenazas, se puede decir que son necesarios varios niveles de seguridad¹⁶. Si un nivel falla, los demás siguen en pie. La estrategia de los sistemas de seguridad radica en su resiliencia, y en que no esté toda la seguridad enfocada en un único punto de defensa.

Entre las propuestas de herramientas preventivas para UAVs, que surgen el análisis de ciberataques y contramedidas, se tiene:

- Implementar firewalls y sistemas de detección de intrusiones para monitorear y proteger las redes de comunicación del UAV contra intentos de acceso no autorizado.
- Utilizar canales de comunicación seguros y encriptados para evitar la interceptación y manipulación de datos que puedan comprometer el control del UAV.
- Mantener actualizados los sistemas operativos, software y firmware de los UAV con los últimos parches de seguridad para protegerlos contra vulnerabilidades conocidas.
- Aplicar encriptación de extremo a extremo para proteger la confidencialidad e integridad de los datos transmitidos entre el UAV y la estación terrestre.
- Implementar medidas robustas de control de acceso y autenticación, como la autenticación de dos factores, para garantizar que solo usuarios autorizados puedan acceder al sistema de control del UAV.
- Implementar sistemas de detección de intrusiones para monitorear y detectar actividades sospechosas en tiempo real, lo que permite una respuesta rápida a posibles ciberataques.
- Realizar evaluaciones de seguridad periódicas para identificar posibles vulnerabilidades en los sistemas de UAV y tomar medidas correctivas.

¹⁶ Modelo OSI y Seguridad en las diferentes capas. Al verificar las 7 capas de seguridad, para que la empresa esté protegida al mínimo se hace necesario más que algunos protocolos de seguridad. Por lo que es preciso considerar todos los puntos de acceso potenciales, además de las áreas donde los cibercriminales pueden acceder a la red. Lo que sería lidiar con la capa más importante de las siete: la capa humana. (OSTEC, 2021)

- Brindar formación en ciberseguridad al personal encargado de operar y mantener los UAV, para concienciar sobre las amenazas cibernéticas y las mejores prácticas de seguridad.
- Establecer planes de respuesta a incidentes cibernéticos para actuar de manera rápida y eficaz en caso de un ciberataque exitoso contra los UAV. Entre otras.

Al implementar estas herramientas y medidas de defensa cibernética de manera integral, se puede fortalecer la seguridad de los UAV militares y reducir la probabilidad de ciberataques que puedan comprometer sus operaciones y misiones.

Es de importancia establecer una cultura de ciberseguridad sólida que involucre a todo el personal relacionado con los UAV, desde los operadores hasta los desarrolladores de software, proporcionando formación continua en materia de ciberseguridad para concientizar sobre las amenazas y mejores prácticas de seguridad, a la vez se recomienda implementar políticas de seguridad cibernética claras y detalladas que aborden aspectos como el control de accesos, gestión de contraseñas y respuesta a incidentes.

Por otra parte, contar con la colaboración de empresas de ciberseguridad especializadas, instituciones académicas y centros de investigación, podrían permitir desarrollar soluciones a medida para proteger la integridad de los sistemas de UAV, así como estar al tanto de las últimas tendencias y tecnologías en ciberseguridad aplicada a sistemas de UAV, o contar con alianzas estratégicas con agencias gubernamentales de ciberseguridad para compartir información sobre amenazas y colaborar en la protección de los sistemas de UAV contra posibles ataques.

Al implementar estas herramientas preventivas, recomendaciones y buscar colaboraciones estratégicas, se podría lograr reforzar la seguridad cibernética de los UAV y protegerlos de amenazas potenciales en entornos operativos críticos.

Se puede concluir, parcialmente, que proponer herramientas preventivas tendientes a fortalecer el ciclo de vida de vehículos aéreos no tripulados militares ante ataques cibernéticos permitiría optimizar su operación a lo largo de extensas y diferentes fronteras, dando apoyo al control de los UAVs, para así concluir las tareas de modo satisfactorio, sin ser vulnerado en ninguna fase, lo que pueda, posteriormente, comprometer las misiones.

9. CONCLUSIONES Y PROPUESTAS PARA FUTURAS INVESTIGACIONES

9.1. Conclusiones

Luego de realizar una investigación de la bibliografía y entrevistas sobre las etapas del ciclo de vida de los UAV militares, se observa que las operaciones cibernéticas desempeñan un papel crucial en el ciclo de vida de los UAV militares, pero también introducen vulnerabilidades que pueden ser explotadas por ciberatacantes.

Las operaciones cibernéticas perjudiciales, como ser los ciberataques, pueden entorpecer o suspender una misión.

Por contrapartida, una operación cibernética beneficiosa, como ser las contramedidas, o el aplicar la normativa internacional correspondiente durante el desarrollo, producción, operación y mantenimiento del UAV, puede contribuir a alcanzar los objetivos de la misión fijada.

Las amenazas cibernéticas representan riesgos significativos para la seguridad de los UAV en operaciones fronterizas. La implementación de contramedidas efectivas, es fundamental para proteger los sistemas de UAV contra ataques cibernéticos, así como establecer herramientas preventivas, pueden contribuir a mitigarlas o evitarlas.

El aumento de las operaciones militares multinacionales transfronterizas exige coordinación y planificación complejas para así obtener el nivel requerido de seguridad operacional. (Cir 330 AN/189 Cooperación Cívico-Militar Para La Gestión Del Tránsito aéreo, 2011, p. 2)

Para garantizar una vigilancia adecuada de las fronteras y prevenir la entrada ilegal de personas y mercancías, surge la necesidad de identificar y abordar eficazmente posibles actividades ilícitas.

Los ciberataques a los que están expuestos los UAV militares, requieren de una serie de estrategias de mitigación o contramedidas, entre las que se destacan realizar: encriptación de comunicaciones; análisis de vulnerabilidades; controles de integridad, y actualizaciones periódicas de software y firmware, las cuales pueden ser implementadas en cada fase del ciclo de vida.

Dadas las vulnerabilidades que presentan los UAVs, y los ciberataques a los que pueden estar expuestos, implementar medidas preventivas sólidas en la protección de los UAV militares en operaciones de control fronterizo en Argentina podría mejorar la integridad y seguridad de las mismas, reducir los riesgos de ciberataques y protección de la información

sensible, y aumentar la eficacia y eficiencia en la detección y prevención de amenazas en las fronteras.

Las herramientas preventivas que puedan ser implementadas para mitigar los riesgos de ciberataques en los UAV militares utilizados en el control de la frontera norte Argentina, con el objetivo de fortalecer la seguridad cibernética en esa área, incluyen: implementar firewalls y sistemas de detección de intrusiones; utilizar canales de comunicación seguros y encriptados; mantener actualizados los sistemas operativos, software y firmware de los uav; implementar sistemas de detección de intrusiones; realizar evaluaciones de seguridad periódicas para identificar vulnerabilidades; y establecer planes de respuesta a incidentes cibernéticos.

El impacto potencial de los ciberataques en los UAV militares, como interferir las señales o insertar malware, es significativo dado que pueden incluir: pérdida de control de la aeronave, sabotaje de misiones, y recolección de información sensible que comprometa la seguridad nacional y la integridad de las operaciones militares, entre otras.

Países como Israel y Estados Unidos han implementado exitosamente el uso de UAV para el control de sus fronteras, mientras que en los últimos años, países como Australia, Chile y Corea del Sur, han avanzado en inversiones y proyectos para la adquisición de estos vehículos destinados a mejorar la vigilancia, la detección de amenazas y la seguridad fronteriza de sus países.

El norte de Argentina presenta una geografía que, dada su gran extensión y características, posibilita el tráfico ilegal de productos y personas, en la frontera con Bolivia, Paraguay y Brasil, mayormente por vía aérea y fluvial.

La falta de una ley de derribos, que no permite interceptar aeronaves ilegales, sumado a la falta de coordinación entre las fuerzas militares y las de seguridad, dan lugar a un delay en la comunicación, desde que los radares detectan el ingreso ilegal de aeronaves, hasta que se efectúa la orden para seguimiento y actúa el comando Frontera Norte. Por otra parte, Frontera Norte, perteneciente a Gendarmería Nacional, no cuenta con los recursos necesarios para llevar a cabo el control fronterizo, recursos respecto a: radares, aviones interceptores, drones de gran envergadura, y andamiaje necesarios para llegar y actuar en contra de la operación ilegal.

Se concluye entonces que:

1. Implementar tecnologías avanzadas, como el uso de UAV, contribuiría en la detección de actividades sospechosas en la frontera norte argentina.
2. La ciberseguridad ayuda a fortalecer la resiliencia de los UAV militares ante posibles amenazas cibernéticas. La capacidad de detectar, responder y

Ing.Pamela Ivana Strusiat.

recuperarse de ciberataques de manera efectiva mejora la capacidad de defensa de los sistemas de UAV.

3. La correcta implementación de la normativa internacional, durante todas las etapas del ciclo de vida de estos vehículos, como ser la STANAG o la STD-MIL, podrían asegurar, en mayor medida que los mismos no serán víctimas de sabotaje cibernético, antes y durante la misión.
4. Valerse de la experiencia de países pioneros en la tecnología, en los cuales ha tenido éxito la aplicación de los UAV para control de la frontera, podría ser una solución, en el mediano plazo, para aumentar la seguridad en la frontera norte argentina.
5. Establecer estrategias de colaboración entre las fuerzas de seguridad y las fuerzas militares en la región norte, por medio de una actuación sincronizada que se efectúe de modo ágil, podría llevar a que se interrumpan las operaciones ilegales en la zona.
6. Evaluar la posibilidad de que se acceda a financiamiento para proceder a la compra de UAV nacionales o extranjeros, para dotar a Frontera Norte de los recursos necesarios para llevar a cabo su tarea.
7. Contar, en el corto plazo, con una ley de derribos, contribuiría a que las actividades ilícitas se suspendan antes de llegar a su destino, lo que, consecuentemente, llevaría a una disminución de las operaciones ilegales.
8. El establecimiento de herramientas preventivas, y su implementación de manera exhaustiva y continua, podría proporcionar un nivel significativo de seguridad y resiliencia a los UAVs contra una amplia gama de amenazas y ataques a lo largo de su ciclo de vida. Anticipar incidentes cibernéticos, contribuye a garantizar la culminación correcta de las misiones de seguridad.

En conjunto, estos hallazgos y recomendaciones pueden respaldar el fortalecimiento de la seguridad cibernética en las operaciones de UAV militares utilizadas en el control de fronteras en Argentina, garantizando su eficacia y protección en entornos operativos críticos.

Finalmente, se debe recordar que los UAV desempeñan un papel crítico en la Seguridad Nacional al proporcionar capacidades de vigilancia, reconocimiento y ataque. La protección de estos activos contra ciberataques es esencial para preservar la soberanía y la integridad territorial del país.

9.2. Propuestas para futuras investigaciones

Dado que algunas temáticas abordadas durante el transcurso de esta tesis son de gran interés, y que exceden los objetivos y alcances de la misma, se propone que sean disparadores de temas a desarrollar en futuras investigaciones.

Temáticas para futuras investigaciones:

1. Realizar estudios más detallados sobre las vulnerabilidades específicas de los UAV militares en operaciones de control fronterizo en Argentina y explorar nuevas técnicas de protección contra ciberataques.
2. Investigar la efectividad de la colaboración interinstitucional y la aplicación de estándares de ciberseguridad en el contexto de operaciones de UAV para el control de fronteras.
3. Analizar cómo se puede contribuir a la seguridad cibernética, y evitar puertas trasera, el que la tecnología asociada a los VANTs sea desarrollada en el país y que se confeccionen con compuestos nacionales. Teniendo en cuenta los costos y tiempos asociados al crecimiento de estos sectores a nivel nacional.
4. Realizar un análisis más profundo respecto de las etapas del Ciclo de Vida de los UAVs, dado que en la presente no se profundizaron temas como la forma en que afecta cada sistema y a su conjunto el que los mismos sean sometidos a ataques cibernéticos y no cibernéticos, en su conjunto.¹⁷

¹⁷ Por otra parte, y no teniendo relación con la temática de la maestría, se podrían analizar cuestiones respecto al nivel táctico de las operaciones, así como analizar los efectos de ataques no cibernéticos.

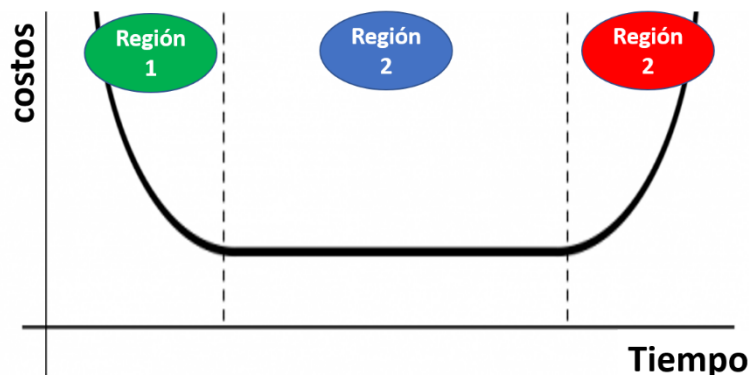
ANEXO 1

CURVA DE DAVIES EN EL CICLO DE VIDA DE VANTs

La curva de Davies refleja el comportamiento de la Tasa de fallas λ de los elementos en funcionamiento, también recibe el nombre de curva de la bañera. Dicha curva es un referente para analizar el comportamiento de la vida útil de los diferentes sistemas, máquinas o equipos existentes dentro de un sistema. La forma que describe la gráfica forma una curva que se asemeja a una bañera, de allí su nombre, en la cual se enmarcan tres regiones, etapa inicial, madurez y envejecimiento. La ubicación de una fase en la curva de Davies, proporciona información sobre la etapa de vida útil en la que se encuentra dicha fase; con esto se definen el tipo de actividades y planes de mantenimiento, pertinentes que se deben realizar. (Amaya Cataño, 2014, p. 10).

En la **Figura ANEXO 1-1**, la región 1 (izquierda) es la que implica mayores costos, y es donde existe mayor cantidad de fallas por tiempo. Por su parte, la región 2 (centro) es donde las fallas se minimizan, por lo tanto los costos se minimizan y el sistema se estabiliza. En dicha zona las fallas son estadísticas. Finalmente, la región 3 (derecha) es la de obsolescencia o final de vida.

Figura ANEXO 1-1: Curva de Davies del Ciclo de Vida y Operación de los VANTs



A medida que se avanza en el tiempo, se observa, para las cuatro fases, que los costos pasan de ser altos a estar en una zona de costo constante, para finalmente volver a aumentar. Este efecto será explicado en la **Tabla ANEXO 1-1**. Por otra parte, en las tres regiones aparecen inconvenientes de ciberseguridad a tener en cuenta.

Las regiones I, II y III, se describen para las fases de su ciclo de vida: Diseño; Construcción y Logística; Mantenimiento; y Operación.

Tabla ANEXO 1-1: Curva de Davies del Ciclo de Vida de un VANTs

Fases	Región I	Región II	Región III
Diseño	Aprendizaje y desarrollo de conocimientos	Diseño óptimo de conocimientos tecnológicos desarrollados. Máxima expertise de los diseñadores alcanzada.	Insuficiente inversión en I+D. No hay traspaso de conocimiento de viejas a nuevas generaciones. Mala selección de los nuevos mandos altos (la política termina teniendo más peso en la selección que la calidad y trayectoria profesional). Lo anterior impacta como disminución de la calidad de los VANTs (cada vez más vulnerables ante enemigos).
Construcción y Logística	Desarrollo de habilidades. Desarrollo de proveedores. Obtención de materias primas deseables. Desarrollo de calidad óptima.	Nivel óptimo de todas las anteriores.	Pérdida de: • Presupuesto • Desarrollo de trabajadores calificados por falta de motivación laboral • Proveedores externos Dificultad para: • Conseguir materias primas • Realizar ensayos adecuados
Mantenimiento	Compra de tecnología nueva no conocida en el país o desarrollo de un prototipo nuevo. Implicará entrenar al personal técnico que realizará el mantenimiento de dichos equipos. Costos de capacitación. Al inicio el	Conocimiento óptimo del mantenimiento, se poseen estadísticas, se establece el momento y a que pieza o equipo realizarle mantenimiento. Se cuenta con una lista de proveedores que aseguran cumplir con los criterios de calidad.	Equipo obsoleto. Requiere de mantenimiento casi continuo, superando a las prestaciones que genera. El equipo permanece más inoperativo que el que permanece operativo, afectando al costo de oportunidad. Aumento en la tasa de fallas y costo de mantenimiento.

Fases	Región I	Región II	Región III
	mantenimiento no será eficiente por el desconocimiento que llevará a errores (se tendrá la teoría pero no la práctica).		
Operación	Familiarización en el manejo de VANTs, donde mejora la confianza y experticia de los pilotos.	Máximo beneficio de uso por experiencia adquirida con las horas de pilotaje remoto. Mejora en los objetivos por mayor entendimiento entre los tomadores de decisiones con respecto a las habilidades de los recursos humanos y de la tecnología adquirida.	Tecnología conocida por el enemigo, entonces los VANTs comienzan a ser vulnerables.

A partir del análisis de los gráficos, se debe tener en cuenta que uno de los factores de éxito en el desarrollo de sistemas , particularmente cuando estos son muy onerosos, consiste en prolongar la Región II y no llegar a la zona 3 para ello se recomienda una serie de medidas que se observan en la Tabla **ANEXO 1-2**.

Tabla ANEXO 1-2: Recomendaciones para extender la región II

Fase	Recomendaciones	Observaciones
Diseño	Mantener un flujo de dinero creciente al área de I+D	Solo es factible en países de economía pujante y creciente.
	Tener equipos de trabajo “observando” que hace el mundo para adelantarse tecnológicamente	Realmente la única forma de “adelantarse” es realizando tareas de espionaje. Lo que se haría es ir a la par de otras tecnologías.
	Tener un modelo de desarrollo tecnológico que	Los capitales de inversión pueden ser públicos y/o

Fase	Recomendaciones	Observaciones
	compita en el mercado	privados. Las empresas de desarrollo, construcción y mantenimiento pueden ser públicas, privadas o mixtas.
Construcción y Logística	Tener un modelo de desarrollo tecnológico que compita en el mercado	Idem Diseño
Mantenimiento	Tener un modelo de desarrollo tecnológico que compita en el mercado	Idem Diseño
	Conviene reemplazar el equipo por equipo nuevo	El momento exacto del reemplazo lo debe recomendar un experto a partir de un análisis de costo-beneficio.
Operación	Conviene reemplazar el equipo por mejores tecnologías.	Mejor tecnología disponible.

ANEXO 2

1. Entrevista con el Capitán Salinas, personal militar de la Fuerza Aérea Argentina

El siguiente ítem corresponde a la recopilación de la entrevista con el Capitán Salinas, personal militar de la Fuerza Aérea Argentina.

1.1. Etapa de diseño

Sistema operativo

El diseño de Aeronaves Remotas en el ámbito de las Fuerza Aérea se realiza en el Centro de Investigaciones Aplicadas en la Ciudad de Córdoba. La mayoría de las PCs utilizadas, utilizan Windows pero algunos ingenieros usan Linux.

El sistema operativo depende, en mayor medida, de la compatibilidad de los programas.

Ejemplos de Programas

Para diseño aerodinámico y estructural se utiliza el programa CATIA.

Acceso al Servidor

No hay acceso por VPN. Todas las PCs están conectadas a la red interna de la Fuerza Aérea que posee seguridad propia.
Los trabajadores que pertenecen a las áreas de diseño deberían solo trabajar desde la oficina.

Lenguajes de programación

Existe en la FAA la dirección CES (Centro de Entrenadores y Simuladores de Vuelo) que se dedican a la programación ya que trabajan con simuladores.

software de diseño

Para software de diseño se utiliza AutoCAD y CATIA.

CATIA te permite simular el comportamiento aerodinámico del diseño.

Para la simulación de la operación de la Aeronave Remota, se utiliza el mismo software que se sirve para controlar la aeronave.

Cuenta con una herramienta que se denomina HIL (hardware in the loop) que permite conectar el software de control con un programa de simulación (puede ser Xplane o Flight Simulator) para corroborar el comportamiento de la Aeronave Remota.

Para que el HIL funcione correctamente es necesario contar con un modelo digital de la Aeronave Remota, lo más realista posible. Además las condiciones ambientales son dados por los programas de simulación. A partir de ahí se puede lograr un acercamiento muy bueno a la configuración ideal del sistema. Pero la configuración final de una aeronave es necesaria realizarla durante un vuelo real.

Es importante destacar que una vez que se logra construir una aeronave funcional es necesario sintonizar o calibrar los PID (proporcional, Integral y derivativa o comúnmente conocida las como ganancias de control) del autopiloto en esa aeronave. Se podría decir que es como una programación y es independiente para cada aeronave a pesar que sean del mismo modelo. Este proceso suele ser uno de los más complicados de realizar y requiere de tiempo y experiencia.

Algunos autopilotos cuentan con la función de “Autotune o Autocalibración” pero en general, al día de fecha, no tienen buenos resultados. La calibración final termina siendo manual por un experto.

Simulador Hardware in the Loop (HIL) para una calibración de PID. Hay que tener en cuenta que muy pocas personas hacen en la

El simulador (HIL) es una muy buena herramienta para reducir las horas de vuelo necesarias actualidad esa tarea.

El simulador (HIL) es una herramienta muy buena pero hay que dedicarle bastante tiempo para lograr resultados aceptables.

Automatización de vuelo

Es necesario confiar plenamente en los controles automáticos de la aeronave, ya que, en el supuesto de perder el control manual de la misma el control automático es quien debe controlarla y evitar un problema mayor.

Una de las funciones fundamentales con las que debe contar cualquier sistema de este tipo es el de RTL (Return to Land) o RTH (Return to Home), que ante una pérdida de enlace entre la Estación de Control (ECT) y la Aeronave Remota debe poder regresar a un punto preestablecido.

En general el punto preestablecido es una zona en donde ante una eventual caída no dañe a ninguna persona o se minimice el daño material.

Automatización de vuelo

La automatización de vuelo es la parte fundamental del sistema.

Las aeronaves remotas o RPAs son sistemas que cuentan con la capacidad de operar de manera autónoma pero que en cualquier momento de sus operación el piloto remoto puede tomar el control manual de la misma.

Las operaciones totalmente autónomas deben ser restringidas por seguridad.

Ing.Pamela Ivana Strusiat.

Pensando en un futuro, no se le debe dejar a una máquina tomar decisiones que puedan afectar a un tercero. Por eso siempre se cuenta con un piloto que es el responsable del accionar de la Aeronave. Este tema se desarrolla en el documento 10.019 de OACI.

Sensores de un VANT moderno

Podemos dividir los sensores en dos partes para su análisis:

- Sensores de control
- Sensores de carga útil

Los sensores de control son los que le proporcionan información al autopiloto para que pueda mantenerse en vuelo: Acelerómetros (similares al de un smartphone moderno), giróscopos (para obtener la actitud y rumbo de la aeronave), sensores Barométricos(para obtener altura y velocidad indicada), Láser altímetro, y sistema de posicionamiento global (el más utilizado es el GPS para la posición), sensores de motor (temperatura, medición de baterías, rpm, presión de aceite y combustible, etc), medición de combustible entre otros.

En algunos casos estos sensores son redundantes.

Los sensores de control son los necesarios para el vuelo.

Los sensores de carga útil son aquellos que transporta la aeronave para cumplir con la misión o el objetivo del vuelo.

Los más conocidos son sensores electroópticos con cámaras diurnas y térmicas giro estabilizadas y con trackeo de objetivos, SAR (radar de apertura sintética, telémetro láser, sistemas de guerra electrónica como SIGINT, o COMINT, etc.

En el caso particular de FAA solo se cuenta con un sensor electro óptico diurno giroestabilizado.

Ejemplos de carga útil que debe cargar un VANT militar

Debería tener la capacidad de poder montar diferentes tipos de sensores de acuerdo a la misión asignada. Pero la principal es un sensor electro óptico con capacidad diurna y nocturna.

Encriptado y comunicaciones entre aeronave y control

Los sistemas de comunicaciones que se utilizan en este tipo de sistemas debieran contar con encriptación para evitar interferencias, ya sean, de manera accidental o de terceros. Los sistemas con los que se cuentan, tienen un grado de encriptación, pero muy bajo.

Existen muchas combinaciones de comunicación entre la aeronave y la sala de control. Por ejemplo para el aterrizaje se utiliza un enlace LOS (Line of Sight o de Línea de Vista) ya que no tiene ningún delay a la hora de transmitir órdenes a la aeronave. En el caso de un enlace satelital sería peligroso debido a que si hay un delay.

Tiempo sin contacto entre el VANT y sala de control

Depende la situación, pero la aeronave puede volar sin comunicación con sala de control hasta que se le acabe el combustible.

Ing.Pamela Ivana Strusiat.

Si la aeronave perdió contacto con la aeronave más de un par de segundos ingresa a modo automático, sino se recupera ingresara a RTH o RTL.

Auto-ataque

Si se le dio una orden al VANT de atacar un blanco y el VANT pierde el enlace, la aeronave debería abortar hasta tener enlace con la sala de control. Ninguna aeronave debería poder atacar de manera autónoma.

Sugerencias de Diseño

Si se podría sugerir características que debe incluir un VANT para uso militar y de seguridad en la Argentina y otros países de Latinoamérica, debería tenerse en cuenta las siguientes variables:

- Autonomía: más de 15 hs
- Techo de servicio: +20.000 ft
- Sensores Electro Ópticos diurnos y nocturnos. (Posibilidad de intercambiar sensores)
- Posibilidad de contar enlace Blos y Los (Satelital y de VHF o UHF) según el tipo de operación.
- Una red propia y segura de traspaso de información en tiempo real.
- Paracaídas de emergencia.
- Redundancia en los distintos tipos de sistemas, control, energía, etc.
- Transponder ADS-B
- Pitot calefaccionado.

Propulsión VANTs militares modernos

Los VANTs deberían contar con un motor alternativo, turbo hélice o un reactor. Teniendo en cuenta la autonomía y la necesidad de operar a grandes alturas.

1. 2. Etapa de Construcción y Logística

1.2.1. Construcción de un VANT

Autopilotos utilizados

Los autopilotos comerciales que se utilizan en el país son:

- Micro Pilots
- Piccolo (Cloud Cap)
- Veronte (Embention)
- Uav Navigation
- PixHawk (en varias versiones V4, Cube, 6x, etc)

Fallas en memoria por radiación

Ing.Pamela Ivana Strusiat.

Con respecto a las fallas en las memorias por radiación, en general, la mayoría de ellos vienen blindados para evitar las radiaciones electromagnéticas, interferencias más que nada.

Respecto a radioactividad no hay registro de que se esté trabajando con seguridad para radiactividad.

Controles de calidad que se le realizan al firmware

Con respecto a la certificación se utiliza el protocolo DO-178B, Software Considerations in Airborne Systems and Equipment Certification (en español: Reglas para la certificación de software aeronáutico) es un estándar para el desarrollo de software en el sector de seguridad crítica de la aviación.

El estándar fue desarrollado por la RTCA.

La EUROCAE ha adoptado este estándar de forma íntegra, de forma que en Europa se denomina de forma oficial ED-12B.

Las autoridades de aviación FAA y EASA exigen la conformidad con el estándar para el proceso para el desarrollo de software.

La prueba se realiza por medio de la documentación y es requisito para la cualificación del software para su uso en el sector aeronáutico. A menudo se habla también de una certificación del software. Sin embargo, la EASA, así como la mayoría de autoridades militares europeas, sólo utilizan el término de la certificación para un avión completo. Por ello no es posible adoptar el software de un modelo a otro de forma automática.

Según las funciones que tiene que cumplir el software, puede poner en peligro la seguridad del avión en mayor o menor medida. La DO-178B establece 5 niveles de seguridad (Design Assurance Level, DAL) de A a E según el daño que puede conllevar un mal funcionamiento del software, desde «catastrófico» hasta «sin consecuencias». Según el nivel que reciba el software, se establecen los métodos permitidos para el desarrollo del software dando lugar a diferentes obligaciones de documentación y revisión. Los cinco niveles de DAL: A hasta E se corresponden de forma aproximada con el Safety Integrity Level SIL 4 hasta SIL 0.

Controles de calidad a la aeronave terminada

Todas las aeronaves deben realizar ensayos en tierra y vuelo para asegurar la seguridad en la operación.

Los ensayos los determinan los ingenieros de ensayos de la Dirección Gral de Investigación y Desarrollo. Todo informe se eleva a la Dirección de Aeronavegabilidad Conjunta.

A la fecha no se han desarrollado autopilotos en las FAA.

En general, se busca cumplir con la mayor cantidad de normas STANAG. Entre ellas podemos encontrar:

Ing.Pamela Ivana Strusiat.

- STANAG 4671, aplicable a los Sistemas con Aeronave de ala fija y con un MTOW (Peso máximo de despegue) entre los 150 y 20.000 kg
- STANAG 4703, Aplicable a los sistemas con Aeronaves de ala fija con un MTOW igual o inferior a los 150 kg
- STANAG 4702, Aplicable a Sistemas con aeronaves de ala rotatoria y MTOW entre 150 y 3.175 kg
- STANAG 4746, aplicable a sistemas con aeronaves de ala rotatoria y con MTOW igual o inferior a los 150 kg.

Pruebas que debe pasar un VANT terminado para ser apto para su uso

En el caso de la FAA se realizan pruebas de vuelo, teniendo en cuenta alcance, autonomía, interferencia con todos los equipos.

Una vez superado se solicita un certificado de matrícula elevando la documentación pertinente.

1.3. Etapa de operación

1.3.1. Ejemplo de etapa de operación de un VANT

Orden de Misión

En la actualidad la doctrina utilizada por parte de la FAA se encuentra adaptada o derivada de la doctrina OTAN.

Antiguamente las órdenes se denominaban “Órdenes Fragmentarias”, donde se determinaba la misión a cumplir.

Actualmente, el documento que se recibe durante una operación se denomina ATO (Air Task Order) por parte del organismo que se encuentre a cargo de las operaciones, siendo este el CAOC (Centro de Operaciones Aéreas).

En la actualidad, quien pudiese cumplir el rol de Operaciones de VANTs militares es el Comando Aeroespacial con asiento en la Base Aérea Militar Merlo.

Las distintas tareas a cumplir tienen diferentes designaciones. Por ejemplo, la tarea “control de daños en batalla” es conocida como BDA (Battle Damage Assessment) y en el mundo es una de las tareas que más se cumplen con sistemas aéreos remotamente tripulados.

Hasta el día de la fecha no se ha cumplido tareas de este tipo con los medios con los que cuenta la FAA, por este motivo, la descripción que a posterior se describe es “deber ser” en el supuesto de realizar una operación de este tipo.

Las tareas que nos encontramos realizando en la actualidad son la de Instrucción, Adiestramiento y Ensayos. Además de cumplir misiones de colaboración con la comunidad como por ejemplo el apoyo del sistema de lucha contra el fuego durante incendios forestales.

Siguiendo con el ejemplo de la instrucción BDA, bajo el modelo “debe ser”, se ejemplifica utilizando un sistema ficticio Clase 3 MALE, como podría ser un Hermes 900, un Heron TP, MQ-Reaper o un TAI Anka.

Posterior a recibir una ATO se realiza lo que denominamos un briefing previo. Allí se repasa la misión y se asignan tareas dentro de la tripulación: Piloto, Operador de carga Paga, personal de mantenimiento, y todos los actores intervinientes.

Programación de un Sistema

Cuando se realiza la programación en un sistema de planeamiento de misión se tienen en cuenta las siguientes variables:

- Amenazas, y orden de batalla propio y del enemigo, sistemas antiaéreos
- Zonas de vuelo restringidas
- Información de inteligencia previa
- Tipos de sensores a emplear
- Información de los blancos atacados y aspectos centrales a relevar
- Coordinaciones con el control de tránsito
- Alternativas y punto de espera

Estas variables vienen en la ATO o en documentos adjuntos a la ATO como enmiendas o aclaraciones de la operación.

Preparación del UAS

Con respecto al combustible, comúnmente, las aeronaves de este tipo despegan siempre full de combustible para aprovechar su máxima autonomía en vuelo.

La planificación de la misión y su posterior carga en el sistema es responsabilidad del piloto, siempre con colaboración del operador de Carga Paga, para lograr que la misión se cumpla. En este punto se considera que el sistema se encuentra en condiciones de operar.

Preparación previa al vuelo

La previa al vuelo es realizada por los mecánicos y posterior por el piloto. Esta secuencia es

igual que una aeronave tripulada. En este caso se realiza una última recorrida por la aeronave y estación de control para inspeccionar que todo funcione correctamente.

Durante la puesta en marcha del sistema, se prueban todos los sensores nuevamente y posterior a eso se realiza un nuevo briefing (instrucciones) con la tripulación de vuelo, teniendo en cuenta la misión, alternativas y posibles emergencias.

Ejecución de la Misión

El vuelo de la aeronave se lleva a cabo respetando estrictamente el manual de la aeronave y su respectiva LCP. En este punto se debe tener la posibilidad de transmitir la imagen obtenida en tiempo real al centro de comando y control, es decir el lugar donde se encuentra una autoridad con poder de decisión en lo que respecta al campo de batalla y desde allí se puede solicitar alguna modificación al objetivo o darla por finalizada.

En el supuesto que la misión se extienda por mucho tiempo, algunos sistemas contemplan la posibilidad de relevar a la tripulación de vuelo cada 4 horas máximo.

Informe Post-Misión

Una vez finalizada la misión, se debe elaborar un uniforme de inteligencia y hacer un Debriefing (responder preguntas) con todo lo sucedido y si fuese necesario. De estos informes pueden salir correcciones para próximas misiones.

2. Entrevista con el Comodoro Ingeniero y Jefe de proyectos de la DGID (Dirección General de Investigación y Desarrollo) de la FAA

El siguiente ítem corresponde a la recopilación de la entrevista con el Comodoro Ingeniero y Jefe de proyectos de la DGID (Dirección General de Investigación y Desarrollo) de la FAA y personal militar de la Fuerza Aérea Argentina. El comodoro destacó que cierta información no iba a poder ser brindada, por ser confidencial.

Controles de Calidad

En respuesta a las preguntas: ¿Que controles de calidad realizan a la aeronave terminada?, y ¿Qué pruebas debe pasar un VANT terminado para ser apto?

Hay múltiples ensayos para esto, de acuerdo con el tamaño del UAV, y la exigencia de sus misiones. Si el UAV debe recibir su certificación para su fabricación en serie y/o su venta a otros países, en general se utiliza como normativa de referencia a las normas de NATO (las STANAG).

Las normas de certificación que una "occidente", incluidos nosotros (Argentina) son las

Ing. Pamela Ivana Strusiat.

STANAG (de la NATO): 4703 hasta 150 kg y la 4671 de 150 kg hasta infinito.

Existen también normas para ensayos ambientales de carácter militar (MIL STD), aplicable también a UAV y sus equipos. Como la MIL STD 810F.

Operación de UAV

¿Qué propulsión usan los VANTs militares modernos?

Lo que se te ocurra: motores alternativos para los medianos, motores eléctricos con baterías de buen rendimiento los más chicos, turbohélices y turbinas para los mayores.

Normativa UAV: Del ámbito militar argentino, la CAM 4-1 "SISTEMAS DE AERONAVES NO TRIPULADAS MILITARES", habla algo de la operación. Para ampliar los Conceptos, ver más en la Dirección General de Aeronavegabilidad Militar Conjunta del Estado Mayor Conjunto de las Fuerzas Armadas¹⁸: Directivas del Reglamento de Aeronavegabilidad, Quizás te pueda servir alguna que tenga nomenclatura: DIRAM 2 Rev. 8 - Definiciones y abreviaturas

Mantenimiento de UAV

No he visto normativa de mantenimiento. El mantenimiento se hace de acuerdo con lo indicado en el Manual de Mantenimiento que confecciona cada fabricante. Y lo mismo sucede con el Manual de Vuelo para la operación. Cada fuerza armada puede tener una Doctrina de Empleo, en la cual se desarrolla la estrategia para la utilización de cualquier medio militar (avión, UAV, buque, tanque, etc.); estos documentos son en general de carácter reservado.

Vulnerabilidades/amenazas/ataques a UAV

Las amenazas principales están en general basadas en el ataque y la vulnerabilidad del enlace del UAV con la estación de control terrestre, desde donde recibe sus órdenes, cambios en la misión, plan de vuelo, utilización de sus sensores, etc.

Si bien se encripta la comunicación, la misma puede ser interferida si se conoce su frecuencia o por una señal de gran potencia, como por ejemplo, pasar en cercanías de un RADAR activo. No hay muchas contramedidas, un buen blindaje de la electrónica puede contribuir un poco. Además del enlace puede también interferirse la señal del GPS (ó GNSS), para confundir al UAV en su posicionamiento, Generalmente, si la interferencia es larga, el UAV por programación, vuelve a su base o algún punto pre-cargado, y su misión se invalida. En general, las frecuencias de control, sensores y GPS son diferentes y son un secreto bien reservado.

Fabricación.

¿Qué microcontroladores usan? No lo sé, pero se busca electrónica robusta.

¿Tienen en cuenta fallas en memoria por radiación? No.

¿Qué controles de calidad realizan en el firmware? En general, se aplica la normativa de testeo para software, no creo que haya algo específico. De ISO, las más relevantes son: 25000, 9126 y 15504.

¹⁸ <https://www.fuerzas-armadas.mil.ar/Dependencias-DIGAMC-Normas-Vigentes.aspx>

3. Entrevista al Mayor y Jefe del Centro de Investigaciones Aplicadas (CIA) de la Fuerza Aérea Argentina.

Resumen de la encuesta realizada al Mayor y Jefe del Centro de Investigaciones Aplicadas (CIA) de la Fuerza Aérea Argentina.

Ciberdefensa y contramedidas: En base a esto y recurriendo a la tecnología que actualmente se posee en nuestro país, se utilizan inhibidores de señal que apuntan a hacer un anulamiento por completo de señal y cualidades propias del vehículos, casi matando de forma automática el cerebro del avion/ dron.

Actualmente es utilizado por lo que es la Artillería de la FAA, dicho sistema es Elta ELI-4030, de IAI.

La base de certificación de nuestro vehículo es la STANAG 4703, y recurrimos a la FAR23 para sustanciar algunos puntos endebles que la STANAG no logra completar.

En cuanto a los estándares STD MIL, se esta aplicando STD MIL-810g para cuestiones de avionica y comunicacion, aunque es un paso de revision actualmente.

Actualmente el vector desarrollado esta siendo aplicado para la instruccion de operadores militares, y como mision subsidiaria la observacion estrategica y operativa siempre y cuando este dentro del espectro de uso de la Aeronave AR-1F

El “vector”de ataque (o “superficie de ataque” en ciberdefensa se usan los dos términos, principalmente el segundo) sobre un uav serían principalmente dos:

1) El enlace:

* efectivamente se podría producir interferencia electromagnética destructiva al principio, anulando el control desde tierra, lo que según la programación del control de misión (el software que controla el uav) podría hacer que no solo la aeronave sea ingobernable, que por lo tanto no pueda cumplir su misión, sino que en muchos casos al producirse una pérdida de enlace el uav regresa automáticamente a su base, lo que le permite al enemigo saber desde donde despegó y consecuentemente se revela la posición de los operadores y esta puede ser bombardeada. Es lo que pasa en Ucrania por ejemplo.

* Por otro lado también tendríamos en algunos casos la toma de control del uav por parte del enemigo, esto sería posible si se conociese en qué frecuencia y bandas esta operando el uav. Si la programación del autopiloto lo permite, al tener una fuente de señal (radio) más potente, podría conectarse a esa y el control del uav pasaría a estar en manos del enemigo.

* Otra alternativa relacionada al uso del espectro es que simplemente el uav sea inoperable y se vea forzado a aterrizar

Eso respecto del enlace, además Hay que agregar los peligros de actualización de software. Esto es fundamental en casos como el nuestro que confiamos en software que no desarrollamos nosotros. En ciberseguridad, todas las vulnerabilidades de cualquier tipo de software se publican en bases de datos CVE, en distintas páginas. Lo que uno hace normalmente, como atacante y también como defensor, es escanear el software que está corriendo en una red o en otros dispositivos, para saber qué versión tiene y en base a eso buscar las vulnerabilidades que puedan estar publicadas.

En base a eso, uno conoce la superficie de ataque y las vulnerabilidades que pueden ser explotadas. Entonces prepara el software para atacar específicamente esas vulnerabilidades y explotarlas después.

<https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

El procedimiento lo estandarizó la Lockheed Martin como cybersecurity kill chain. Básicamente es el reconocimiento del objetivo, detección de vulnerabilidades, preparación de software para atacar, envío y explotación de vulnerabilidades hasta la toma de control del sistema por parte del atacante.

Si no tenemos control sobre el software que usamos, es muy probable que tengamos una puerta abierta ahí.

Por otro lado, durante el mantenimiento, puede haber un acceso Físico no Autorizado por manipulación física del UAV, por ejemplo para instalar dispositivos de espionaje..

4. Entrevista al Jefe del Proyecto RUAS (Rotary-Wing Unmanned Aerial System) , INVAP- Division of Aerospace and Government.

Normativa que cumple el RUAS o se utiliza como guía para Diseño, Fabricación, Mantenimiento y/o Operación

- Requisitos de aeronavegabilidad (para diseño, construcción y pruebas)

Requerimiento de DIGAMC militar CAM 4-1

Lista de verificación de cumplimiento basada en los requisitos de NATO STANAG 4738

- Guías de:

- FAA Order 8230.34D

- ASTM F38.01

- ASTM F38.02

- MIL-HDBK-516C

- RTCA DO-160

- MIL-STD-461 EMI/EMC

- Registro de Matrícula

- conformidad Militar con DIGAMC CAM 4-1

- Conformidad civil con: ANAC RS885

- Certificado de Aeronavegabilidad (Experimental para I+D)

Ing.Pamela Ivana Strusiat.

- conformidad militar con DIGAMC CAM 4-1
- Conformidad civil con: ANAC RS885
- Calidad
 - SAE AS-9100
- Producción
 - Guías de ASTM F2911, F3003-14
- Mantenimiento (guías)
 - ASTM F2909-19
- ASTM F3366-19
- Manual de Operaciones
 - Guía para la elaboración de un Manual de Operación de UAV ~"Guía para la confección de un MOE VANT", ANAC, 2018
- Seguridad Operacional
 - Evaluación de riesgos de operación específica SORA, de JARUS, con directrices de la autoridad suiza Oficina Federal de Aviación Civil (FOCA)
- Evaluación de seguridad del sistema conforme a SAE ARP 4761 y MIL-STD-882E
 - Análisis de riesgos funcionales (FHA)
 - Análisis modal de fallas, efectos y criticidad (FMECA)
 - Análisis de árbol de fallas (FTA)
- Licencias de personal: Tripulación remota
 - Roles y responsabilidades durante el desarrollo y las pruebas de vuelo de operaciones con el cliente.
 - Circular 381 de la OACI
 - ANAC RS885
- Entrenamiento de la tripulación
 - Militar EMCO DHAM PC 13-04 (militar)
 - Simulador y entrenador de la Crew: Piloto remoto y operador de carga útil.
- Licencias
 - Militar EMCO DHAM PC 13-04
 - Civil: ANAC RS885

5. Entrevista al ex Jefe Del Comando Conjunto de la Ciberdefensa General de Brigada (R) Mg. Ing. I

1. Las Normas, (números, etc.) utilizadas en el diseño, construcción y logística, mantenimiento y operación de VANTs,

No hay normas concretas en la Argentina aplicables a "Vehículos Aéreos No Tripulados" o UAVs (Unmanned Aerial Vehicles). Existen normas en otros países que se siguen en estos casos como ser:

- DO-178C: Software Considerations in Airborne Systems and Equipment Certification.

- DO-254: Design Assurance Guidance for Airborne Electronic Hardware.

En forma genérica también están normas serían aplicables

- STANAG 4586: interoperabilidad de sistemas VANT para la NATO.
- ISO 27001: Gestión de seguridad de la información, aplicable para la protección de datos de VANTs.
- DO-160G: Environmental Conditions and Test Procedures for Airborne Equipment.
- STANAG 4671: UAV system airworthiness requirements.

Seguramente, hay otras normas que deben seguirse en el desarrollo de los subsistemas y partes del conjunto.

2. Vulnerabilidades, amenazas, ataques y contramedidas:

Diseño y Construcción:

- Amenazas: Backdoors en el firmware, errores en el diseño de comunicación segura.
- Ataques: Compromiso de software, spoofing de señales de GPS.
- Contramedidas: Implementación de cifrado robusto, verificación de integridad del software mediante técnicas de hash, pruebas de penetración exhaustivas, etc.

Logística:

- Amenazas: Compromiso en la cadena de suministro.
- Ataques: Introducción de hardware malicioso durante el transporte.
- Contramedidas: Auditorías de seguridad a proveedores, uso de Blockchain para trazabilidad, control riguroso de acceso durante el transporte.

Mantenimiento:

- Amenazas: Actualizaciones de software no verificadas.
- Ataques: Inyección de malware durante la actualización.
- Contramedidas: Firmado digital de actualizaciones, uso de entornos seguros para mantenimiento.

Operación:

- Amenazas: Interferencia en comunicaciones, acceso no autorizado a la estación de control y al propio UAV.
- Ataques: Interceptación de señales, hacking de la estación de control.
- Contramedidas: Cifrado de extremo a extremo en comunicaciones, autenticación multifactor en estaciones de control, detección de intrusiones en tiempo real.

Estas son ideas generales que aplican a los UAV.

6. Entrevista a Jorge perteneciente al Ministerio de Seguridad de la Provincia de Buenos Aires, responsable del sector táctico de UAV, puestos a disposición de la Policía Bonaerense

En el ministerio de seguridad, los UAVs son utilizados para llevar a cabo tareas de seguridad,

Ing.Pamela Ivana Strusiat.

investigaciones y de ser requerido, contribuir en oficios judiciales. Estos UAVs están a disposición de la Provincia de Buenos Aires.

En referencia a los drones utilizados por la policía de la provincia, los mismos fueron adquiridos en 2023 a la empresa china JOUAV. Su característica principal es que son los únicos en Sudamérica de tipo VITOL, es decir, despegan en vertical, pero al adquirir altura, vuelan como un avión. No realizan un vuelo estacionario, sino que transitan realizando el vuelo como un avión.

Poseen motor de 4 tiempos, con combustible aeronáutico o combustible super. Su alcance es de 100 km cuadrados, con una autonomía de 10 horas, consumiendo 30 litros, la capacidad de almacenamiento máxima que posee. Alcanza una altura de 4 mil a 5 mil metros de altura. De payload posee una cámara de 30 megapíxeles, un láser que apunta al objetivo, y una cámara térmica para operaciones con poca o sin luz. Mide 5,5 m de ala a ala, y 3,5 de envergadura.

Al poseer un tanque de 30 litros de combustible, entonces gasta 3 litros/hora, a un costo de 4mil\$/hora, para brindar el mismo servicio, de control desde el cielo, lo hace a un costo menor al que requiere utilizando un helicóptero, el cual posee un costo de 3milUSD/hs, y con el riesgo de llevar un piloto a bordo.

Al día de la fecha, hay 15 operadores entrenados, todos pertenecen a la policía bonaerense. Durante la operación se requiere de 5 pilotos de la policía bonaerense capacitados y ANAC es quien le otorga la licencia habilitante, por otro lado, deben contar con sus certificados médicos al día. 2 operadores realizarán las tareas de armado, despliegue, y desarmado al final de los UAV; 2 operadores realizarán las tareas de manejo de consolas de operación, y de control de las cámaras del UAV y de efectuar el plan de vuelo. El último operador se encarga de supervisar que los otros realicen las actividades de modo correcto.

Su uso principal es para seguridad rural brindando apoyo a la policía rural. Brindan seguridad operacional, mediante el patrullaje, analizando los datos en tiempo real. Al efectuar control rural, vuela sobre sectores donde no hay mucha población. Es versátil, dado que la estación de comando se puede desplegar casi en cualquier tipo de terreno (por ejemplo se puede utilizar en planos de seguridad de fronteras; y para control del escudo norte o la mesopotamia, por medio de personal militar del estado).

Los datos recolectados, además de ser analizados en tiempo real, se bajan a un puesto comando, y pueden ser retransmitidos a un puesto comando mayor, allí se graban en los equipos, y también queda almacenado en la memoria del UAV. La información puede ser otorgada a quien lo requiera, si existe un pedido judicial.

Entre sus principales características respecto a ciber operaciones, es que realiza un barrido de frecuencia, lo que lo hace seguro para evitar ciberataques, pero sin contar con un inhibidor de

frecuencia. Como contrapartida se puede tener que mientras más distancia realiza y a mayor altura de vuelo, se requiere tener una línea directa para comunicación. También requiere de un lugar de despegue que permita despegue vertical. Debe contar con apoyo logístico, dado que los UAV son transportados en trailers, y son dispuestos en el terreno que, además de permitir el despegue vertical, se encuentre entre 50 y 200 metros del puesto de comando. El puesto comando puede instalarse en casi cualquier tipo de terreno. Por otra parte, al igual que los aviones, se debe tener en cuenta que son susceptibles a las condiciones climatológicas, es decir al clima, las cuales deben ser analizadas antes de su uso.

EANA es quien otorga el permiso y los cajones de vuelo, por ejemplo para defensa nacional con tecnología de UAV.

Inicialmente, en el cajón de vuelo indica que se tendrá un espacio restringido, por un fecha determinada, por ejemplo un mes, en donde se indican las 4 coordenadas, y altura en la que operará, sin indicar fecha específica, horarios ni la actividad de seguridad a desarrollar. Esa información es retransmitida a los aeródromos locales, y en principio a los aeródromos por los que pasará, para que estén informados y, en caso de corresponder, den aviso a los aviones, según el tránsito aéreo, si debe ir de una provincia a otra pasando por otras provincias. El informe que detalla esta información se denomina NOTAM. De este modo los pilotos están en conocimiento de la zona de vuelo que llevarán. El UAV posee un transponder (valizas), dado que el piloto del avión es quien ve el UAV, el UAV no es quien ve si se acercarse al avión. Con todo ello, se tiene cobertura legal.

Se debe tener en cuenta que el UAV es un medio para control, para prevención, para dar seguridad, para búsqueda, para detectar incendios, entre otros.

Cabe aclarar que la jurisdicción de este Ministerio de Seguridad es en la provincia de Buenos Aires, aunque puede brindar ayuda a otras provincias del ministerio de seguridad nacional, si así lo solicitan.

Por otro lado, se debe tener en cuenta, que el UAV seleccionado debe cumplir con las actividades específicas a las que será destinado, y según sus características, dimensiones, alcance y autonomía. En este caso, la selección se debió a los requerimientos, pero existen otros modelos de UAV con otras capacidades.

Para finalizar recordar que el UAV es una herramienta que actúa como complemento de la actividad humana en sus distintas actividades.

7. Entrevista a J., operador personal de Gendarmería Nacional, designado en una base de control de frontera norte en la provincia de Jujuy. Por sus actividades debe permanecer en anonimato.

Para el control de fronteras mediante drones o vehículos aéreos no tripulados, es común que se utilicen estaciones de control terrestres que permiten realizar varias tareas esenciales, como:

1. Carga de baterías o combustible: Estas estaciones pueden estar equipadas con sistemas de recarga de baterías o suministro de combustible, lo que permite a los drones prolongar su tiempo de vuelo y realizar misiones más largas sin necesidad de regresar a una base principal para recargar.
2. Bajada de datos: Las estaciones de control terrestre suelen contar con sistemas para la transferencia de datos desde el drone, lo que permite a los operadores descargar información recopilada durante el vuelo, como imágenes, videos o datos de sensores. Esto es crucial para el análisis y la toma de decisiones en operaciones de vigilancia fronteriza.

Además, estas estaciones pueden ofrecer otras funcionalidades, como:

- Mantenimiento y reparación de drones
- Actualización de software y firmware
- Integración con sistemas de comando y control
- Soporte para operaciones de vuelo autónomo o teleoperado

El uso de drones para el control de fronteras ofrece ventajas significativas, incluyendo una mayor cobertura, flexibilidad y capacidad de respuesta rápida, además de reducir los riesgos para el personal y los costos operativos asociados con la vigilancia tradicional.

8. Entrevista presencial con el Comandante (R), M., de Gendarmería Nacional.

Respecto al funcionamiento y estado de situación del sistema de vigilancia integrada de fronteras (SITEVIF)

El programa, a la fecha, funciona sólo en aproximadamente un 10%, se cuenta con 1, 2 o ningún drone en los escuadrones de gendarmería situados en la frontera norte, por ejemplo en Las Lomitas, Formosa. Algunos son utilizados para ceremonias, y no para actividades tácticas. Otros son utilizados para operaciones de lucha contra el narcotráfico, para realizar un estudio del terreno previo a tomar alguna acción. No se realiza vigilancia de fronteras con drones. Los drones utilizados por la Gendarmería Nacional se asemejan más a los de uso civil que a los de uso militar.

Ing.Pamela Ivana Strusiat.

En los papeles, se podría decir, existe una coordinación entre radares y gendarmería, pero solo funciona un porcentaje bajo. Existe la intención, pero considero que no existe dinero suficiente para lograrlo.

Cuando viajé a Israel, hace varios años, presencie prácticas tácticas nocturnas, donde nos acercábamos en jeep hasta la frontera. Allí se utilizaban estas tecnologías, y por medio de visión nocturna se localizaba al supuesto enemigo, y por medio de láseres se derribaba el intruso. Acá no ocurre eso.

Pero se debe tener en cuenta que existen expertos con capacidad de hacer esto, y de proveer esta tecnología.

Argentina posee fronteras muy grandes, y cada vez son más los requerimientos, haciendo casi imposible controlar la totalidad.

Se debe tener en cuenta que lo que pasa por tierra es casi nada, el mayor tráfico ocurre por la hidrovía (el Río Paraguay en un colador), y por vía aérea. Algo pasa por la ruta nacional 11, pasando por Asunción, el puerto de Rosario hasta llegar a Buenos Aires.

Anteriormente la masa de la droga que ingresaba iba a Europa, pero ahora solo es un porcentaje pequeño, la mayoría llega a Rosario, donde cada vez aumenta más el consumo.

Podemos decir que existen tres grandes problemáticas en el control de la frontera norte:

1) No existe una ley de derribos de aeronaves, lo que hace imposible interceptar aviones ilegales que cruzan la frontera norte. Por ejemplo, Brasil sí posee Ley de Derribo.

2) No existe trabajo conjunto de protección de fronteras entre EA, FAA y gendarmería.

3) Una cosa es en tiempos de paz, donde, por la Ley de Seguridad Interior, se impide trabajar hacia adentro del país, sino que todo es hacia el exterior. Ello es una traba muy grande, dado que únicamente pueden apoyar logísticamente. Es un grave problema porque las fuerzas de seguridad no tienen la capacidad que poseen las fuerzas militares (radares, aviones interceptores, ni drones de gran envergadura, ni andamiaje para llegar y poder actuar)

Otra cosa es en tiempos de guerra, dado que allí los temas abarcan a las fuerzas armadas, que trabajan de forma conjunta, aunque aparentemente no exista una doctrina de actuación conjunta.

Por ello digo que no existe un comando integral ni una doctrina unificada para poder actuar.

Gendarmería tiene la orden de mirar hacia arriba todo el día, pero existen momentos, por ejemplo durante la noche, que pasan aviones y tiran la mercancía ilegal en lugares específicos

donde los están esperando camionetas. Si bien se da el aviso, para cuando llega la orden ya no hay nadie en el lugar.

La zona norte está colmado de Unidades de Gendarmería, y a la vez hay Unidades especiales que dependen de Frontera Norte. El Programa Integral de Frontera Norte posee sus propios gendarmes y sus propias escuelas de formación de gendarmería.

Algunos datos específicos se suprimieron dada la sensibilidad del tema, y por la confidencialidad de la entrevista.

9. Entrevista presencial a J., personal retirado de Gendarmería Nacional, zona norte.

Respecto del plan Escudo del Norte.

Existen tropas de Gendarmería Frontera Norte. Esto es, Gendarmería Nacional en la zona norte no es lo mismo que el cuerpo Frontera Norte. Allí, Gendarmería Nacional está a disposición del equipo Frontera Norte. Por ejemplo, Frontera Norte posee dependencias en Las Lomitas, Formosa, y en Salta Capital, mientras que su escuelita se encuentra en Mosconi, Salta.

Cabe destacar que Frontera Norte abarca desde Formosa a Jujuy, e incluye las provincias: Formosa, Salta, Jujuy y Tucumán.

Gendarmería posee Agrupaciones por provincia, con asientos, generalmente en cada capital. Por debajo de estas se encuentran los Escuadrones, que son los que salen al terreno y que están más distribuidos en las provincias. Por debajo de estas están las Secciones, y se ubican prácticamente, una al lado de otra, sobre la frontera norte del país. Pero no existe despliegue de frontera norte que se apoye sobre los escuadrones.

Lo que es el sistema de vigilancia integrada de fronteras comenzó con la gestión de Macri, allí, por ejemplo en Mosconi y Comandante Fontana, se iban a instalar radares que iban a ser operados por la FAA y gendarmería le iba a dar la seguridad perimetral. Teóricamente los radares de FAA detectan la aeronave furtiva, dan aviso a los aviones interceptores, que serán los Pampa, pero no pueden salir porque no existe una Ley de Derribo, y tampoco un sistema integrado de actuación, ya que lo que sigue sería perseguirlo, dar aviso a gendarmería para que donde paren los intercepten; pero los datos de los radares son triangulados, enviados a San Fernando, Bs. As., que centraliza la información, y para cuando llega la información, no hay nadie en el lugar.

Ing.Pamela Ivana Strusiat.

El operativo en general es, los aviones pasan por un lugar designado, y tiran la mercancía ilegal, es proceso de tirar no recuerdo si se denomina, bombardeo o algo así. Pero como no hay Ley de Derribo, no se puede interceptar. Luego de lanzar la carga, camionetas esperando en el lugar las recogen rápido. En Argentina, además, se tiene la particularidad de que se puede aterrizar en cualquier lado, dado su terreno. Por ejemplo, los casos más comunes de entregas se dan por la noche, en las provincias de Entre Ríos (la mayoría en Gualeguaychú), Santiago del Estero y Bs. As.

Se sabe que la mayoría de los aviones con mercancía ilegal sale de Bolivia, dado que se dice que con estas actividades se financia el gobierno. Es decir, viajan varios kilómetros.

Por ejemplo los que viajan por la Hidrovía, incumbencia Paraguay-Brasil, no salen con toda la carga, se van acopiando en el camino, por medio de canoas que salen desde la frontera argentina, en navegación clandestina, De ahí embarcan y traen, cargas mayores a 100 kilos de marihuana. Allí existe una primera línea que es Prefectura, y atrás está Gendarmería. Pero allí no hay incumbencia del grupo Frontera Norte.

Aun, para el norte, falta ser expeditivo, falta coordinación, y la Ley de derribo.

Recuerdo una vez, hace un tiempo, que personal de gendarmería, quiso entorpecer el recorrido de una avioneta que pasaba de modo ilegal por el territorio, por medio de un helicóptero y eso casi le costó la vida institucional.

10. Entrevista con el Brigadier Mayor (R) de la FAA

¿Cómo es una misión de tipo control de daños de batalla?

Muchas de las preguntas que están en este cuestionario son relativamente reservadas, pero se podría decir que los pasos siguientes son bastante acordes a la realidad:

1. SE RECIBE UNA ORDEN DE MISIÓN ;
2. SE REALIZA UNA PROGRAMACIÓN EN UN SISTEMA DE PLANEAMIENTO DE MISIÓN QUE TIENE EN CUENTA ASPECTOS COMO.

Posibles amenazas, y orden de batalla propio y del enemigo, sistemas antiaéreos

Zonas de vuelo restringidas

Información de inteligencia previa

Tipos de sensores a emplear

Información de los blancos atacados y aspectos centrales a relevar

Coordinaciones con el control de tránsito

Alternativas y punto de espera

Niveles de vuelo y horarios específicos

otras

3. CARGA DE LA MISIÓN Y PREPARACIÓN DEL UAS

Carga de combustible, prueba de equipos, pruebas de sensores

Ing.Pamela Ivana Strusiat.

Carga de la misión de manera remota o por dispositivos físicos

Otras

4. PREPARACIÓN PREVIA AL VUELO

Briefing prevuelo

Prueba de sensores

Prueba de enlaces y datalink

Otras

5. EJECUCIÓN DE LA MISIÓN

Blancos y efectos a relevar

Empleo de sensores múltiples visuales , IR, etc.

Tareas de relevamiento automático, semiautomático o manual

Necesidad de sobrevuelos

Otras

6. INFORME POST MISIÓN:

Análisis de información

Elevación de resultados de la observación

a. otras

Durante la operación de una VANT en una misión, la misma se puede ver entorpecida porque el operador se encuentra distraído o persuadido en alguna forma, por ejemplo por un soborno, o un operador retirado puede ser extorsionado en alguna forma para entregar información relevante. Por ello, en operaciones con VANTs, el anonimato de los operadores resulta de vital importancia, dado que pueden ser víctimas de persuasión por métodos no convencionales, como amenazas o ataques psicológicos.

ANEXO 3

En general los inhibidores de señal son desde pequeños equipos electrónicos que pueden ser transportados en la mano hasta equipos más grande que una valija (Cid, 2016) pero estos equipos se usan para inhibir la señal de comunicación de edificios como comisarías, cárceles, casas de gobierno, universidades, etc. Como se observa en estos ejemplos la esfera volumétrica de contención donde se desea suprimir la señal es pequeña en comparación con el objetivo de sabotear las comunicaciones de un VANT militar que vuela a kilómetros de la superficie terrestre a gran velocidad. Por eso, conociendo el tamaños de radares que se utilizan para controlar el espacio aéreo (Figura ANEXO 3-1) (*Fundamentos De Radar - Alcance Instrumentado*, n.d.), podemos extrapolar la información y decir que los inhibidores de VANT militar serán también de gran tamaño. Sumado a lo anterior, hay que pensar la fuente de energía que utilice los inhibidores, donde ya sean baterías, generadores eléctricos, almacenamiento de combustible para los generadores, ocupan gran volumen y además del peso de carga si se desea que el sistema pueda ser transportado en camión.

Por lo anterior, podemos decir, que la intensidad en el ataque con señales electromagnéticas por efecto de jammig requiere altos niveles de potencia, ya que para atacar a VANTs militares que operan a gran altitud. Pero físicamente, con antenas adecuadas y generadores de gran potencia, es posible el ataque.

Los misiles anti VANTs pueden ser de impacto directo con carga explosiva pero existe un método de ataque mucho más eficiente para atacar un VANTs con menor impacto en la población civil si el desenlace de la contienda se lleva a cabo sobre la población.¹⁹

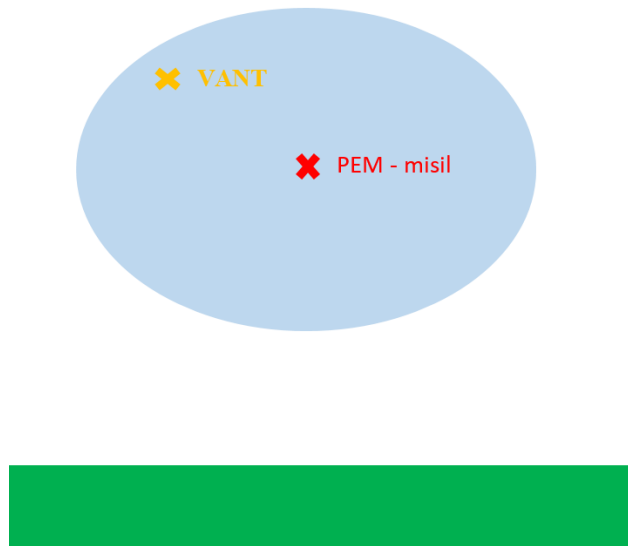
El objetivo es utilizar un misil que emita un pulso electromagnético a gran altura, que tenga el potencial de destruir la electrónica del VANT, haciendo que el mismo pueda terminar destruyéndose al caer en tierra. El misil se autodestruirá al emitir el pulso, disminuyendo el impacto sobre la población civil. (Kindelán, 2022)

La ventaja de un misil de pulso electromagnético está dada en que el misil solo debe llegar a una esfera de acción²⁰ en la que se encuentre el VANTs con ayuda de los sistemas de tierra y no tener que dar con precisión en el objetivo (VANT). Esto aumentaría la probabilidad de éxito.

¹⁹ Esta idea nace de analizar potenciales escenarios de un enfrentamiento sobre el espacio aéreo civil.

²⁰ El radio de alcance de acción de un arma de pulso electromagnético debería ser calculado por los especialistas en armas de pulsos electromagnéticos.

Figura ANEXO 3-1: Esfera de acción de un PEM



Fuente: producción propia

Por otro lado, es importante un sistema en tierra de detección temprana y respuesta ágil. Esto disminuiría la probabilidad de que restos del misil y del VANT impacten sobre la población civil.

ANEXO 4

A continuación, se propone una serie de normas STANAG que podrían ser utilizadas para certificar los VANTs de uso militar. Se distinguen entre las de diseño (Tabla **ANEXO 4-1**), construcción y logística (Tabla **ANEXO 4-2**), mantenimiento (Tabla **ANEXO 4-3**) y operación (Tabla **ANEXO 4-4**). Cabe destacar que algunas de estas normas son propias de los VANTs, pero otras, aunque no sean Normativas específicas para VANTs, se recomienda tenerlas en cuenta. Fuente: Producción propia, a partir de análisis de normas STANAG.

Tabla ANEXO 4-1: Normas de Diseño

STANAG para Diseño	REFERENCIA	DESCRIPCIÓN
4703	REQUISITOS DE AERONAVEGABILIDAD DE LOS SISTEMAS DE AERONAVE LIGERA NO TRIPULADA	contiene requisitos técnicos mínimos de aeronavegabilidad destinados a la certificación de aeronavegabilidad de aeronaves ligeras no tripuladas de ala fija con un peso máximo de despegue de no más de 150 kg y una energía de impacto de más de 66 J, y que están destinadas a la certificación de aeronavegabilidad en forma regular. espacio aéreo no asignado.
4586	Interfaces estándar del sistema de control de UAV para Interoperabilidad de UAV de la OTAN	Define arquitecturas, interfaces, protocolos de comunicación, elementos de datos y formatos de mensajes.
4606	FORMA DE ONDA EPM DE COMUNICACIONES MILITARES POR SATÉLITE (MILSATCOM-Military Satellite Communications) DE SUPER ALTA FRECUENCIA (SHF) PARA SERVICIOS DE CLASE B - CLASIFICADOS	Equipo de capacidad de comunicación por satélite. Para saber la frecuencia a utilizar y la forma de encriptación.
4609	Imágenes de movimiento digital OTAN	El propósito es promover la interoperabilidad de los sistemas cinematográficos actuales y futuros en un entorno de servicio conjunto o convergente de la OTAN.
4660	ENLACE DE DATOS DE MANDO Y CONTROL	Enlace de datos de comando y control interoperable para sistemas no tripulados (IC2DL)

STANAG para Diseño	REFERENCIA	DESCRIPCIÓN
	INTEROPERABLE	
7023	Estándar de datos de imágenes primarias de reconocimiento aéreo	El objetivo de este acuerdo es establecer los datos auxiliares que se requieren para las imágenes de reconocimiento aéreo y el formato para la transmisión de estos datos con imágenes de reconocimiento aéreo.
7085	Enlaces de datos interoperables para sistemas de imágenes	Los sistemas de transmisión de datos conformes con el estándar STANAG 7085 permiten reducir el tiempo necesario para el proceso de toma de decisiones en sus cuatro etapas: observar, orientar, decidir y actuar (OODA). Aprovechando la información disponible, las fuerzas armadas analizan las distintas opciones y toman rápidamente la mejor decisión posible para sacar ventaja frente al adversario.
4607	FORMATO DE INDICADOR DE OBJETIVOS EN MOVIMIENTO TERRESTRE (GMTI) DE LA OTAN	El objetivo de este acuerdo es promover la interoperabilidad para el intercambio de datos de radar indicador de blanco en movimiento terrestre entre los sistemas de inteligencia, vigilancia y reconocimiento (ISR) de la Organización del Tratado del Atlántico Norte (OTAN).
4671	REQUISITOS DE AERONAVEGABILIDAD DE LOS SISTEMAS DE AERONAVES NO TRIPULADAS (USAR)	El propósito de este acuerdo es utilizar estándares comunes para la producción de requisitos de aeronavegabilidad para sistemas de aeronaves no tripuladas. Está destinado a permitir que los vehículos aéreos no tripulados militares operen en el espacio aéreo de otros miembros de la OTAN.
3784	INSTRUCCIONES TÉCNICAS PARA EL DISEÑO Y CONSTRUCCIÓN DE LAS INSTALACIONES DE COMBUSTIBLE DE AVIACIÓN Y AUTOMOCIÓN EN LOS CAMPOS DE AVIACIÓN OTAN	Brinda orientación técnica para el diseño y la construcción de instalaciones de combustible terrestre y de aviación en los aeródromos de la OTAN.
3441	DISEÑO DE CARGA Y TIENDAS PARA AERONAVES	Especifica el diseño estructural y mecánico de los almacenes de aeronaves y sus interfaces de equipos de suspensión asociados para facilitar la intercambiabilidad y el servicio cruzado de aeronaves.
3967	REQUISITOS DE	El propósito de este acuerdo es establecer estándares

STANAG para Diseño	REFERENCIA	DESCRIPCIÓN
	DISEÑO Y DE PRESTACIONES PARA CARCASAS Y ELEMENTOS FILTRANTES DE COMBUSTIBLE UTILIZADOS EN TURBOMOTORES DE AVIACIÓN	mínimos de diseño y desempeño para recipientes separadores de filtro de sistema fijo y elementos coalescentes y separadores para la filtración de combustibles de aviación.
4452	GUIA PARA EL DISEÑO SEGURO Y EVALUACIÓN DE SOFTWARE DE APLICACIÓN EN SISTEMAS DE ARMAS	El propósito de este acuerdo es lograr un nivel razonable de garantía de que el software relacionado con las municiones y los dispositivos similares al software se comportarán dentro del contexto del sistema y el entorno operativo con un nivel de riesgo aceptable.
4608	SEGURIDAD EN EL DISEÑO Y EVALUACIÓN DE SEGURIDAD Y APTITUD PARA EL SERVICIO	Proporciona un método uniforme para establecer los requisitos de seguridad de diseño y para la evaluación y prueba de la seguridad e idoneidad para el servicio (S[3]) de municiones de calibre inferior a 12,7 mm dentro de la OTAN.
7071	REQUISITOS DE DISEÑO Y FUNCIONAMIENTO DE LOS EQUIPOS DE INYECCIÓN DE ADITIVOS UTILIZADOS EN COMBUSTIBLES DE AVIACIÓN	Normativa no específica para VANTs, pero se debería tener en cuenta en el diseño.
7140	INSTRUMENTOS DE VUELO DE AERONAVES - DISEÑO Y PRESENTACIÓN	El objetivo de este acuerdo es estandarizar el diseño de los datos de vuelo en las pantallas de los pilotos y las características de los altímetros, tacómetros e indicadores de las aeronaves.
3098	PUNTOS DE APOYO DE LAS AERONAVES	Especifica que las aeronaves estén provistas, en todos los puntos de apoyo, con: a. Almohadillas para tomas, que tienen una forma común de asiento; b. Espacio libre suficiente para acomodar tomas, asegurando espacios libres adecuados entre tomas y las partes adyacentes de la aeronave.
3455	SÍMBOLOS BÁSICOS PARA CIRCUITOS ELÉCTRICOS DE	El objeto de este acuerdo es establecer los símbolos básicos para los circuitos eléctricos de las aeronaves.

STANAG para Diseño	REFERENCIA	DESCRIPCIÓN
	AERONAVES	
3456	CARACTERÍSTICAS DEL SISTEMA DE ENERGÍA ELÉCTRICO EN AERONAVES	Propiedades para la alimentación eléctrica de la aeronave.
3457	EQUIPOS DE APOYO EN TIERRA PARA SUMINISTROS DE ENERGÍA ELÉCTRICA A AERONAVES	Acuerdo para estandarizar las características esenciales de la energía eléctrica suministrada desde fuentes terrestres a las aeronaves. Los detalles se dan en el texto.
3531	INFORME E INVESTIGACIÓN DE SEGURIDAD DE VUELO ACCIDENTES/INCIDENTES AERONAVES Y/O MISILES MILITARES	El presente acuerdo de estandarización de la OTAN (STANAG) tiene como objetivo dar respuesta a los siguientes requisitos de interoperabilidad: - Estandarizar procedimientos para la investigación y notificación de seguridad de accidentes/incidentes de aeronaves militares, misiles y/o UAS que involucren equipos, propiedades, instalaciones y /o personal de dos o más naciones.
3556	CARTUCHOS EYECTORES DE CARGAS DE AERONAVES	Acuerdo para establecer los criterios de diseño de cartuchos eyectores de almacén para aeronaves. Los detalles se dan en el texto y la configuración externa en un anexo.
3632	CONTROL Y SEGURIDAD EN LAS CONEXIONES ELÉCTRICAS ENTRE AERONAVES Y EQUIPO DE APOYO EN TIERRA	Acuerdo para estandarizar las conexiones eléctricas de seguridad a utilizar en aeronaves y equipos de apoyo en tierra. Los detalles se dan en el texto y los anexos.
3659	PROTECCIÓN CONTRA DESCARGAS ELÉCTRICAS EN VUELO Y CONEXIONADO A MASA PARA AERONAVES	Acuerdo para establecer requisitos de rendimiento de unión y disposiciones de verificación para sistemas metálicos de aeronaves y equipos de apoyo asociados.
3660	CLAVIJA DE CONEXION ELECTRICA DE LA BATERIA PRINCIPAL DE LAS AERONAVE	Acuerdo para estandarizar las características y las dimensiones de la envolvente de los enchufes para baterías de almacenamiento de aeronaves para permitir un servicio cruzado eficiente. Los detalles se dan en los

STANAG para Diseño	REFERENCIA	DESCRIPCIÓN
		anexos.
3726	ANILLAS DE SUSPENSIÓN PARA CARGAS DE AERONAVES	Agreement to standardize aircraft lugs to be compatible with stores and suspension equipment. Details are given in text and annexes.
3765	RELLENO A PRESIÓN DE ACEITE EN MOTORES DE AERONAVES	Acuerdo para estandarizar requisitos mínimos para el reabastecimiento a presión de aceite de motor de aeronaves. Los detalles se dan en el texto.
3817	FRASEOLOGÍA ESTÁNDAR R/T(radiotelefónicos) PARA USO DE AERONAVES	El propósito de este acuerdo es registrar la aceptación nacional de AATCP-2(A).
7013	ZONAS DE RIESGO DURANTE EL SUMINISTRO DE COMBUSTIBLE A AERONAVES	El acuerdo establece una definición mínima de las zonas peligrosas alrededor de las aeronaves y el equipo de abastecimiento de combustible cuando las operaciones de abastecimiento de combustible están en curso.
7042	INTENSIFICADORES DE VISIÓN NOCTURNA PARA AERONAVES.	El objetivo es establecer estándares para los sistemas de dispositivos de visión nocturna intensificadores de imagen (IINVD) que son para aeronaves de ala fija y giratoria.
7073	CONECTORES PARA SUMINISTRO DE ENERGÍA ELÉCTRICA A AERONAVES	El propósito de este acuerdo es estandarizar las conexiones externas de energía de servicio de corriente continua (CC) y corriente alterna (CA) a las aeronaves, para facilitar el intercambio de información comparable entre naciones y mejorar la interoperabilidad.
7140	INSTRUMENTOS DE VUELO DE AERONAVES - DISEÑO Y PRESENTACIÓN	El objetivo de este acuerdo es estandarizar el diseño de los datos de vuelo en las pantallas de los pilotos y las características de los altímetros, tacómetros e indicadores de las aeronaves.

Fuente: Producción propia a partir de entrevistas y consultas en standards.globalspec.com. y infostore.saiglobal.com

Tabla ANEXO 4-2: Normas de Construcción y Logística

STANAG para Construcción y Logística	REFERENCIA	DESCRIPCIÓN
4280	EMBALAJE Y CONSERVACIÓN NATO	El propósito de este acuerdo es establecer niveles de empaque y métodos estándar de conservación, que protegerán los bienes del deterioro, daño físico y mecánico, y garantizar que los bienes permanezcan en buenas condiciones desde el momento de la compra hasta su uso, a pesar de los períodos prolongados. de almacenamiento y/o envíos múltiples.
7017	ANÁLISIS ESPECTROMÉTRICO DE LUBRICANTES PARA MOTORES DE AERONAVES	El propósito de este acuerdo es definir procedimientos y responsabilidades para el análisis de lubricantes transitorios de motores de aeronaves en la nación anfitriona.
7039	PROCEDIMIENTOS DE PRUEBA PARA ASEGURAR LA COMPATIBILIDAD DEL EQUIPO CON LOS SISTEMAS DE ENERGÍA ELÉCTRICOS DE LAS AERONAVES	El propósito de este acuerdo es responder a los siguientes requisitos de interoperabilidad: a) Asegurar que se logre el nivel apropiado de estandarización de equipos, repuestos, herramientas y equipos de prueba, documentación técnica, procedimientos y capacitación antes de la misión, y b) identificar requisitos de potencia de equipos de utilización de energía eléctrica que cumplan con el requisito de interoperabilidad detallado en CM(2006)0013 - MC 533 Principios y políticas de la OTAN para el mantenimiento de equipos.

Tabla ANEXO 4-3: Normas de Mantenimiento

STANAG para Mantenimiento	REFERENCIA	DESCRIPCIÓN
3609	NORMAS PARA EL MANTENIMIENTO DE SISTEMAS FIJOS DE RECEPCIÓN, ALMACENAMIENTO Y SUMINISTROS DE COMBUSTIBLE DE AVIACIÓN	El propósito de este acuerdo es establecer estándares mínimos de mantenimiento para las instalaciones fijas de almacenamiento de combustible para aviones (JFSI) utilizadas por las naciones de la OTAN.
4712	NORMAS PARA MANTENIMIENTO DE SISTEMAS DESPLEGABLES	

	DE RECEPCIÓN, ALMACENAMIENTO Y DISPENSACIÓN DE COMBUSTIBLE	
7105	ACUERDOS DE MANTENIMIENTO PARA AERONAVES SIMILARES	

Tabla ANEXO 4-4: Normas de Operación

STANAG para Operación	REFERENCIA	DESCRIPCIÓN
4670	REQUISITOS MÍNIMOS DE ENTRENAMIENTO PARA OPERADORES Y PILOTOS DE SISTEMAS DE AERONAVES NO TRIPULADOS (AAS) - ATP-3.3.8.1 EDICIÓN B	El presente acuerdo de estandarización de la OTAN (STANAG) tiene por objeto dar respuesta a los siguientes requisitos de interoperabilidad: - El campo de estandarización de este STANAG es Formación. ATP-3.3.8.1 afectará principalmente a los dominios Conjunto y Aéreo, y en segundo lugar a los dominios Terrestre y Marítimo.
7025	GESTIÓN DE TRÁNSITO AÉREO Y CONTROL DE OPERACIONES DESDE PISTAS DE OPERACIÓN MÍNIMAS (MOS)	El objetivo de este acuerdo es estandarizar los procedimientos para garantizar la gestión y el control seguros y eficientes de las aeronaves y los vehículos terrestres que operan en un MOS y áreas de maniobra asociadas, en tiempos de crisis y ejercicios de guerra y tiempos de paz.
1183	CUALIFICACIONES DE LA OTAN PARA ALA FIJA SOBRE EL AGUA CONTROLADORES DE AERONAVES DE GUERRA (AWW)/DEFENSA AÉREA (AD)	Proporciona calificaciones estándar para controladores de aeronaves de ala fija sobre el agua (AWW)/defensa aérea (AD) en unidades del Sistema de control y vigilancia aeroespacial (AASACS) de ACE y embarcadas en barcos o aeronaves de la OTAN.
2970	TÉCNICAS Y EQUIPOS PARA LA RECUPERACIÓN DE AERONAVES UTILIZANDO HELICÓPTEROS	Proporciona requisitos de rendimiento de equipos estandarizados y técnicas de recuperación para permitir que los países miembros levanten por aire helicópteros derribados y aviones ligeros de ala fija desde sitios remotos o inaccesibles.
3101	DIFUSIÓN DE LA INFORMACIÓN SOBRE ACCIDENTES DE AERONAVES Y MISILES	El propósito de este acuerdo es establecer procedimientos para el intercambio de información de seguridad peculiar a los contactos de seguridad de vuelos nacionales,

		tipos de aeronaves, sistemas de aeronaves no tripuladas y misiles en uso por las naciones de la OTAN.
3650	EQUIPO DE LOCALIZACIÓN SAR (Radar de Apertura Sintética) ESENCIAL Y CARACTERÍSTICAS ASOCIADAS(AERONAVES)	Acuerdo para estandarizar el equipo esencial de búsqueda y salvamento (SAR) que se lleva en las aeronaves para mejorar las operaciones.
3712	CATEGORÍAS DE IDENTIFICACIÓN DE SERVICIOS CONTRA INCENDIOS Y DE RESCATE DE AERONAVES	Especifica un método común para identificar el nivel de los servicios de salvamento y extinción de incendios de aeronaves (ARFF) proporcionados en aeródromos y helipuertos de ala fija; y hacer que esta información esté disponible para su inclusión en las publicaciones ARFF.
3812	RESPONSABILIDADES EN EL ENTRENAMIENTO DEL PERSONAL DE TIERRA PARA EL APOYO DE AERONAVES	Describe las responsabilidades de los comandantes de la OTAN y las naciones para el entrenamiento del personal de tierra de servicio cruzado (ACS) de aeronaves.

10. REFERENCIAS

- Aleo, J. D. (2021). La integración de tecnologías en vehículos aéreos no tripulados y su impacto en el ejercicio del Comando y Control del Atlántico Sur. cefadigital.
<https://cefadigital.edu.ar/bitstream/1847939/2206/1/TIF%20ECTON%202021%20-%20CC%20ALEO%2C%20Jes%C3%BAs%20David.pdf>
- Amaya Cataño, J. A. (2014). ESTUDIO DEL COMPORTAMIENTO REAL DE LA FASE III DE LA CURVA DE LA BAÑERA A TRAVÉS DE LA APROXIMACIÓN DE UNA DISTRIBUCIÓN A LA VIDA ÚTIL DE BOMBILLOS DE FRENADO AUTOMOTRIZ. <https://core.ac.uk/download/pdf/47246325.pdf>
- Anexo 11 al Convenio sobre Aviación Civil Internacional. (2016, julio). OACI. Administración Nacional de Aviación Civil. Retrieved January 16, 2023, from
<https://www.anac.gov.ar/anac/web/uploads/normativa/anexos-oaci/anexo-11.pdf>
- Borches, M. (2011, July 29). La Armada Argentina apuesta al desarrollo técnico del UAV Guardián. Infodefensa. Retrieved September 16, 2023, from
<https://www.infodefensa.com/texto-diario/mostrar/3145002/armada-argentina-apuesta-desarrollo-tecnico-ua-v-guardian>
- Borges, V., & Carvalho, M. (2024, May 15). Monitoreo de logging de aplicaciones: Cómo identificar y resolver problemas. Listopro Community. Retrieved August 22, 2024, from
<https://community.listopro.com/monitoreo-de-logging-de-aplicaciones-como-identificar-y-resolver-problemas/>
- Bressano, V. E., Klecha, V. D., & Gieres, V. O. (2014). UAS - EL FUTURO, HOY. Escuela Superior de Guerra Aérea. Retrieved September 16, 2023, from https://www.esga.mil.ar/resga/RESGA_233.pdf
- CAM 4-1 Sistemas de Aeronaves no Tripuladas (SANT). (2016). Estado Mayor Conjunto de las Fuerzas Armadas Normas Vigentes. <https://docplayer.es/39174923-Cam-4-1-sistemas-de-aeronaves-no-tripuladas-sant.html>
- Centro Argentino de Ingenieros. (n.d.). Alcances de Ingeniería. Centro Argentino de Ingenieros. Retrieved July 24, 2024, from https://www.cai.org.ar/wp-content/uploads/CEPSI/SC01-01-0-Alcances_de_Ingenieria.pdf
- Ciberseguridad en el sector Aeroespacial: escenario, riesgos y retos de futuro. (n.d.). Safecore.
<https://safecore.io/es/industries/la-cyber-security-nel-settore-aerospaziale-lo-scenario-i-rischi-e-le-sfide-futur e/>
- Cid, M. (2016, May 6). Cómo funcionan los inhibidores de frecuencia y por qué está prohibido su uso. Xataka. Retrieved September 3, 2023, from

OPERACIONES CIBERNÉTICAS EN EL CICLO DE VIDA DE VANTs DE USO MILITAR, SUS VULNERABILIDADES, AMENAZAS, CIBERATAQUES, CONTRAMEDIDAS Y PROPUESTA DE HERRAMIENTAS PREVENTIVAS

Maestría en Ciberdefensa y Ciberseguridad UBA-FCE Posgrado

<https://www.xataka.com/otros-dispositivos/como-funcionan-los-inhibidores-de-frecuencia-y-por-que-esta-prohibido-su-uso>

Cir 330 AN/189 Cooperación cívico-militar para la gestión del tránsito aéreo. (2011). OACI.

https://www.icao.int/sam/documents/2011/civmilc.11/330_es.pdf

de Vergara, E., & Trama, G. A. (2016, November 4). OPERACIONES MILITARES CIBERNÉTICAS. Escuela Superior de Guerra Conjunta. https://www.esgcffaa.edu.ar/pdf/ESGCFFAA-2016_pdf-49.pdf

Delgado, V. (2016). Historia de los drones. El Drone. Retrieved August 21, 2023, from

<http://eldrone.es/historia-de-los-drones/>

Drones y Seguridad Nacional. (2023, January 26). DSN.

<https://www.dsn.gob.es/sites/dsn/files/Drones%20y%20Seguridad%20Nacional%20ACCESIBLE.pdf>

Duarte, M. R. (2019, December 16). Drones, desafíos estratégicas en tiempos 4.0 – Dossier Geopolítico. Dossier Geopolítico. Retrieved August 19, 2024, from

<https://dossiergeopolitico.com/2019/12/16/drones-desafios-estrategicas-en-tiempos-4-0/>

Elaskar, O., Calcagni, E., & Vitulich, A. (2019). Análisis de la actual normativa regulatoria para el diseño de Aeronaves No Tripuladas militares. <file:///home/u60733/Descargas/revistas,+analisis.pdf>

Frederic, S. (2020). Crisis de soberanía y militarización de la frontera norte. La fragilidad estatal ante la amenaza de los crímenes organizados en Argentina*. Redalyc. <https://www.redalyc.org/journal/4763/476368270002/html/>

Fundamentos de radar - Alcance instrumentado. (n.d.). radartutorial.eu. Retrieved May 1, 2023, from

<https://www.radartutorial.eu/01.basics/rb69.es.html>

General de División de Vergara, E., & Contraalmirante Trama, G. A. (2016). Operaciones Militares Cibernéticas. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

https://www.esgcffaa.edu.ar/pdf/ESGCFFAA-2016_pdf-49.pdf

Hidalgo, Á. (n.d.). Patentes en el sector tecnológico. Iglobax. Retrieved August 22, 2024, from

<https://www.iglobax.es/patentes-en-sector-tecnologico/>

Hochauer, D. (2023, July 6). Mejora de la seguridad fronteriza: El papel de los drones en la protección de las fronteras de Estados Unidos y Canadá. Sentrycs.

<https://sentrycs.com/es/the-counter-drone-blog/border-security-drones-at-americas-canadas-front-line/>

Informe 133. Jefatura de Gabinete de Ministros. (2022, septiembre). Senado Argentina.

<https://www.senado.gob.ar/parlamentario/InformesJgm/>

Integración Territorial Internacional. (2011). https://www.argentina.gob.ar/sites/default/files/as_13663122172.pdf

Ing.Pamela Ivana Strusiat.

- Jacob, J. P., Noura, H., & Salman, H. (2020, septiembre). Security analysis of drones systems: Attacks, limitations, and recommendations. ScienceDirect.com. Retrieved July 23, 2024, from <https://www.sciencedirect.com/science/article/pii/S2542660519302112#sec0034%208/106%2023/7/24,%2023:24%20An%C3%A1lisis%20de%20seguridad%20de%20sistemas%20de%20drones:%20ataques,%20limitaciones%20y%20recomendaciones%20-%20ScienceDirect>
- Jeler, G. E., & Alexandrescu, G. (2020). ANALYSIS OF THE VULNERABILITIES OF UNMANNED AERIAL VEHICLES TO CYBER ATTACKS. Review of the Air Force Academy; Brasov N.º 2.
- Jordán, J. (2012, June 9). Drones Valle Bekaa. Global Strategy. Retrieved July 2, 2024, from <https://global-strategy.org/drones-israelies-batalla-valle-bekaa/>
- Jorquera, R. (2023, October 17). Drones suicidas de bajo costo, una amenaza emergente. Pucará Defensa. Retrieved August 20, 2024, from <https://www.pucara.org/post/drones-suicidas-de-bajo-costos-una-amenaza-emergente>
- Julio Herrero Isla. (2003). Vigilancia y reconocimiento el papel de los UAV. <https://dialnet.unirioja.es/servlet/articulo?codigo=5472108>
- Kindelán, C. G. (2022, October 1). Y si Putin usa armas nucleares... cómo es un ataque con pulso electromagnético de gran altitud. 20Minutos. Retrieved September 3, 2023, from <https://www.20minutos.es/noticia/5064423/0/y-si-putin-usa-armas-nucleares-como-es-un-ataque-con-pulso-electromagnetico-de-gran-altitud/>
- Libro blanco de la Defensa. (2023). https://www.argentina.gob.ar/sites/default/files/2021/11/libroblancodeladefensa2023_.pdf
- Límites Territorio Argentino. (n.d.). Argentina.gob. <https://www.argentina.gob.ar/pais/territorio/limites>
- Los Sistemas no Tripulados. (2012). Publicaciones Defensa. <https://publicaciones.defensa.gob.es/media/downloadable/files/links/P/D/PDF223.pdf>
- Marquez, J. (2024, May 29). La autonomía es una de las grandes limitaciones de los drones. Estos investigadores proponen cargarlos en pleno vuelo. Xataka. <https://www.xataka.com/drones/autonomia-grandes-limitaciones-drones-estos-investigadores-proponen-cargarlos-pleno-vuelo>
- Martí Sampere, C. (2018, mayo 31). Tecnología de la Defensa. Análisis de la situación española. Retrieved mayo 16, 2021, from <https://iugm.es/publicacion/tecnologia-de-la-defensa-2/>

- Martinez, A. (2023). "Ciberdefensa y ciberseguridad en las operaciones militares en el Comando de Operaciones de. El Repositorio Digital del Centro Educativo de las Fuerzas Armadas.
<https://cefadigital.edu.ar/bitstream/1847939/2598/1/TFI%20-%20My%20Ariel%20Martinez%20-%204%20de%20julio%20docx.pdf>
- Mary, I. (2024, April 22). El Impacto de los drones en la guerra moderna. Pucará Defensa. Retrieved August 16, 2024, from <https://www.pucara.org/post/el-impacto-de-los-drones-en-la-guerra-moderna>
- Mazza, M. (2023). DETERMINACIÓN Y CONOCIMIENTO DE LA CAPACIDAD DE LOS VEHÍCULOS AÉREOS NO TRIPULADOS PARA SU EMPLEO EN LA VIGILANCIA Y CONTROL DE LOS ESPACIOS MARÍTIMOS. INSTITUTO UNIVERSITARIO NAVAL.
https://cefadigital.edu.ar/bitstream/1847939/2693/1/TESIS%20MAESES%202023_MAZZA.pdf
- Ministerio de Gobierno – Policía de Misiones. (2024). SEGURIDAD Y PREVENCIÓN EN LA FRONTERA A TRAVÉS DE MAPEO CON DRONES.
<https://comunicacion.misiones.gob.ar/seguridad-y-prevencion-en-la-frontera-a-traves-de-mapeo-con-drones/>
- Moresi, A. (2009). AERONAVES NO TRIPULADAS. Fuerza Aerea Argentina.1
- Noción de Sistemas: Cibernética y Dinámica. (2016). INFORMACIÓN DIGITAL.
<https://infodgl.wordpress.com/2016/11/12/nocion-de-sistemas-cibernetica-dinamica-de-sistemas-y-analisis-y-sintesis/>
- Normativa Disposición 1/2015. (2015, February 25). ANEXO I Política Modelo de Seguridad de la Información. Retrieved April 30, 2023, from <https://www.argentina.gob.ar/normativa/nacional/242859/text>
- Nuevas Tecnologías en la Seguridad Transfronteriza. (2010). CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL. <https://publicaciones.defensa.gob.es/media/downloadable/files/links/P/D/PDF26.pdf>
- Observatorio Aeroespacial. (2020, July 17). LA Evolución DE LOS DRONES. INFORME # 3.
<https://www.esga.mil.ar/Observatorio/Informes/Informe%203-EVOLUCION-DE-LOS-DRONES%20COVID-19.pdf>
- Paaukas. (2021). Origen del drone timeline. Timetoast timelines. Retrieved August 21, 2023, from <https://www.timetoast.com/timelines/origen-del-drone>
- Plataformas Abiertas para Tecnologías Estratégicas. (2017). MINCyT.
https://www.argentina.gob.ar/sites/default/files/plataformas-abiertas-para-tecnologias-estrategicas_-_informe_final.pdf
- ¿Qué es el cifrado de datos? (n.d.). Kaspersky.

<https://latam.kaspersky.com/resource-center/definitions/encryption?srsId=AfmBOoqKEPBi8tVeCgSxHQYNtHXvmNSjirGIGNnb4cneWQ-8b-SIXBSX>

¿Qué es la autenticación multifactor? - Explicación de la autenticación multifactor. (n.d.). AWS. Retrieved August 22, 2024, from <https://aws.amazon.com/es/what-is/mfa/>

Reglas de Vuelo y Operación General. (2022, August 9). ANAC.

https://www.argentina.gob.ar/sites/default/files/raac_parte_91_2.pdf

Revista de la Escuela Superior de Guerra Aérea. (n.d.). “(UAS) Análisis y comparación de la evolución y desarrollo en el marco mundial y regional”. UAS - EL FUTURO, HOY Su integración a la Fuerza Aérea.

Rhi Sausi, J. L., & Oddone, N. (2013). BREVES APROXIMACIONES A LAS POLÍTICAS FRONTERIZAS DE ARGENTINA, BRASIL Y PARAGUAY. In Gobernanza y Prevención Transversal en la Frontera Norte de México (p. 211).

https://www.casade.org/BibliotecaCasade/GOBERNANZA_PREVENCION_TRANSVERSAL FronTERANORTE_MEXICO.pdf#page=158

Rodríguez, D. M. (n.d.). La construcción de una frontera “caliente” | Fronteras en construcción. TeseoPress.

<https://www.teseopress.com/fronterasenconstruccion/chapter/la-construccion-de-una-frontera-caliente/>

Rojo, A. (2022, August 5). Drones de combate chinos. Zona Militar. Retrieved September 2, 2023, from <https://www.zona-militar.com/2022/08/05/drones-de-combate-chinos/>

Santa, A. (2022, diciembre). Vehículos Aéreos No Tripulados y Sistemas de Vehículos Aéreos No Tripulados.

Biblioteca del Congreso de la Nación, X(240), 21.

<https://bcn.gob.ar/uploads/adjuntos/Dossier-240-legis-nacional-vehiculos-aereos-no-tripulados-drones-dic-2022.pdf>

Silva, E. (n.d.). Los espacios de fronteras entre Argentina, Brasil y Uruguay. TeseoPress. Retrieved August 19, 2024, from

<https://www.teseopress.com/fronteras/chapter/los-espacios-de-fronteras-entre-argentina-brasil-y-uruguay-relaciones-de-cooperacion-entre-los-anos-2002-2016/>

Sistemas de Aeronaves no Tripuladas (UAS) Cir 328 AN/190. (2011). Sistemas de aeronaves no tripuladas (UAS).

OACI. https://www.icao.int/Meetings/UAS/Documents/Circular%20328_es.pdf

Sistemas de aeronaves no tripuladas Cir 328 AN/190 (UAS). (2011). ICAO. Retrieved July 20, 2024, from

https://www.icao.int/Meetings/UAS/Documents/Circular%20328_es.pdf

Soluciones C4ISR para sistemas de aeronaves no tripuladas (UAS). (2021). CarteNav. Retrieved septiembre 26,

2021, from

https://cartenav.com/unmanned-aircraft-systems-uas/?utm_term=uav%20system&utm_campaign=Search+-%3E+New+Lead+Generated&utm_source=adwords&utm_medium=ppc&hsa_acc=2440764650&hsa_cam=11313774675&hsa_grp=110981919756&hsa_ad=501783057529&hsa_src=g&hsa_tgt=kwd-29

Tecnologías asociadas a sistemas de Enjambres de UAVs-La Carga Útil. (2010). XIV Jornadas UPM-FAS.

<https://www.upm.es/sfs/Rectorado/Gabinete%20del%20Rector/Agenda/2010/2010-11/3CargaUtil.pdf>

Varela Sabando, P. (2014). Desarrollo e Integración del Concepto ISTAR (Inteligencia, Vigilancia, Adquisición de Objetivos y Reconocimientos) en el Campo. El Repositorio Digital del Centro Educativo de las Fuerzas Armadas. https://cefadigital.edu.ar/bitstream/1847939/622/1/TFI%20ECS%202014%20V1S1D2_47.pdf

Vicejefatura de Gabinete del Interior. (2021). Con más de 630 millones de pesos, el Gobierno nacional realiza la mayor inversión de la historia en los Centros de Frontera.

<https://www.argentina.gob.ar/noticias/con-mas-de-630-millones-de-pesos-el-gobierno-nacional-realiza-la-mayor-inversion-de-la>