ESCUELA MILITAR DE CHORRILLOS

"CORONEL FRANCISCO BOLOGNESI"

Trabajo de Suficiencia Profesional para optar el Título Profesional de Licenciado en Ciencias Militares con Mención en Ingeniería

Titulo

"PROPUESTA PARA EL DESARROLLO DE CAPACIDADES BÁSICAS DE GUERRA ELECTRÓNICA EN OPERACIONES FRONTERIZAS DEL SERVICIO NACIONAL DE FRONTERAS"

Autor

Martin Morales Vásquez

0009-0007-4790-927X

Ciudad de Panamá – República de Panamá

2026

3% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Texto mencionado
- Coincidencias menores (menos de 10 palabras)

Fuentes principales

2%	Fuentes de Internet
0%	Publicaciones
2%	Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

DEDICATORIA

Hijo, lógicamente en estos momentos no comprenderás mis palabras, pero para cuando seas consciente de ello, quiero que sepas lo importante que eres para mí. Yerelys, gracias por tu amor puro y sincero.

AGRADECIMIENTO

A Jehová porque por tu misericordia todo es posible, madre, padre y hermana por ser mi eje principal para la consolidación de mis objetivos.

ÍNDICE

Contenido

RESUMEN

La investigación actual se centra en el desarrollo de habilidades fundamentales en guerra electrónica que son aplicables a las operaciones del Servicio Nacional de Fronteras, teniendo en cuenta la evolución de las amenazas transnacionales y el aumento del uso de tecnologías de comunicación y vigilancia por parte de organizaciones criminales en áreas fronterizas.

El estudio adoptó un enfoque exploratorio, doctrinal y basado en proposiciones, que incluyó un análisis conceptual y bibliográfico de aspectos relacionados con la Guerra Electrónica, el Espectro Electromagnético, la Inteligencia Electrónica (ELINT), las Comunicaciones Tácticas, la Seguridad de las Comunicaciones y las Amenazas Híbridas. Asimismo, las vulnerabilidades identificadas para las operaciones fronterizas se analizaron en términos de usos ilícitos de radios de comunicaciones, drones comerciales y otras tecnologías explotadas por organizaciones criminales en áreas de difícil acceso. Todos estos escenarios ponen en evidencia la seguridad de las comunicaciones tácticas, lo que puede afectar la coordinación entre las unidades desplegadas en el terreno.

Además, se estudiaron muchas situaciones provenientes de operaciones fronterizas en las que se identificaron posibles vulnerabilidades que afectan a las unidades en operación. De entre ellas, destaca el uso ilícito de radios de comunicación, de manera similar a la presencia cada vez más frecuente de drones comerciales y otros recursos tecnológicos en zonas con un mayor grado de infiltración por parte de organizaciones criminales que operan en áreas de difícil acceso. De hecho, estos escenarios ponen de manifiesto un dilema creciente para las fuerzas de seguridad, al evidenciar el alcance en que la tecnología puede explotarse para crear ventajas operativas, retrasar el reconocimiento de la ilegitimidad y eludir las fuerzas de seguridad.

Estas situaciones representan riesgos para la seguridad de las comunicaciones tácticas y pueden afectar la coordinación de las unidades desplegadas en el terreno. A partir del análisis realizado, se evidenció la necesidad de fortalecer capacidades relacionadas con el monitoreo de radiofrecuencias, la protección de las comunicaciones tácticas y la vigilancia del espectro electromagnético.

Estas capacidades contribuirían a mejorar la seguridad operacional de las unidades desplegadas en áreas fronterizas y a incrementar la capacidad institucional para detectar y responder oportunamente al uso de tecnologías por parte de organizaciones criminales.

Estas situaciones generan riesgos para la seguridad de las comunicaciones tácticas y pueden dificultar la coordinación de las unidades en el terreno. El análisis mostró que es necesario fortalecer el monitoreo de radiofrecuencias, la protección de las comunicaciones tácticas y la vigilancia del espectro electromagnético. Mejorar estas capacidades ayudaría a aumentar la seguridad operacional de las unidades en zonas fronterizas y a reforzar la capacidad institucional para detectar y responder a tiempo al uso de tecnologías por organizaciones criminales.

Con base en las necesidades identificadas durante el trabajo, se planteó una propuesta orientada al fortalecimiento escalonada de capacidades básicas de guerra electrónica dentro del Servicio Nacional de Fronteras. Esta iniciativa busca mejorar la protección de las comunicaciones tácticas, fortalecer las actividades de vigilancia tecnológica, así como optimizar el control del espectro electromagnético en las operaciones fronterizas. Para ello, se consideran aspectos operativos, tecnológicos y doctrinales acordes con la realidad institucional y las exigencias del entorno de seguridad actual.

En función de los resultados obtenidos, se considera que el fortalecimiento escalonado o gradual de capacidades básicas de guerra electrónica debe aportar beneficios significativos a las operaciones fronterizas desarrolladas por el Servicio Nacional de Fronteras. La implementación de estas capacidades permitiría mejorar la protección de las comunicaciones tácticas, fortalecer los procesos de mando y control y aumentar la capacidad institucional para enfrentar amenazas tecnológicas que actualmente inciden en el entorno operativo fronterizo.

Palabras clave: guerra electrónica, espectro electromagnético, comunicaciones tácticas, seguridad fronteriza, vigilancia electromagnética, COMSEC, amenazas híbridas, operaciones fronterizas.

ABSTRACT

This study examines the need to strengthen basic electronic warfare capabilities within the National Border Service (SENAFRONT), based on the operational challenges observed in border areas. Particular attention is given to the growing use of communication systems, drones, and surveillance technologies by criminal organizations, which have increased the complexity of border security operations and highlighted the importance of protecting tactical communications and the electromagnetic spectrum.

This study begins with an analysis of operational limitations related to tactical communications, radio frequency (RF) coverage, electromagnetic surveillance, and electromagnetic spectrum protection in jungle environments and difficult-access areas. In these contexts, both geographical and technological conditions represent continuous challenges for border security operations.

A descriptive and propositional research approach was adopted, including a doctrinal and technical analysis of concepts associated with electronic warfare, the electromagnetic spectrum, electronic intelligence, tactical communications, communications security, and hybrid threats. Furthermore, the study evaluated operational vulnerabilities derived from the illicit use of radios, drones, and communication systems by irregular actors in contemporary border scenarios.

The findings revealed the need to progressively strengthen capabilities related to electromagnetic surveillance, RF monitoring, communications security (COMSEC), and the detection of emerging technological threats, with the purpose of increasing operational security and enhancing institutional response capacity within the electromagnetic environment.

Based on the analysis conducted, the study proposes the gradual development of basic electronic warfare capabilities aimed at reinforcing tactical communications, improving technological surveillance, and protecting the electromagnetic spectrum during border operations. This proposal incorporates operational, technological, and doctrinal approaches adapted to the institutional needs of SENAFRONT.

In conclusion, the gradual incorporation of basic electronic warfare capabilities constitutes a viable option for strengthening modern border security operations, optimizing command and control processes, ensuring continuity of tactical communications, and maintaining adequate operational security against emerging technological threats.

Keywords: electronic warfare, electromagnetic spectrum, tactical communications, border security, electromagnetic surveillance, COMSEC, hybrid threats, border operations.

INTRODUCCIÓN

Las amenazas transnacionales están creciendo hoy en día con la innovación tecnológica y el aumento de oportunidades para los sistemas de comunicación, drones y medios electrónicos, y su uso por parte de organizaciones criminales y actores irregulares, y el entorno actual de seguridad y defensa ha experimentado un cambio significativo.

Este es un desafío para las organizaciones responsables de la aplicación y protección de fronteras, ya que las organizaciones que se centran únicamente en la vigilancia fronteriza deben adaptarse y mejorar sus enfoques operativos y tecnológicos para hacer frente.

En términos de operaciones de seguridad, la guerra electrónica, que implica el control, explotación y protección del espectro electromagnético como un elemento crucial para el desarrollo operativo, se ha vuelto fundamental. Desde esta perspectiva, las capacidades de guerra electrónica son una piedra angular para la detección, monitoreo, interferencia y protección de los sistemas de comunicación, contribuyendo directamente al fortalecimiento del mando y control, vigilancia y seguridad operativa.

Para la república de Panamá, la institución que asegura las fronteras es el Servicio Nacional de Fronteras, operando en áreas de difícil accesibilidad y complejidad, donde las comunicaciones tácticas son una parte vital de la coordinación y ejecución de misiones. No obstante, las aplicaciones ilegales del espectro electromagnético, interferencias, comunicaciones encubiertas y el uso de drones comerciales por parte de organizaciones criminales implican la necesidad de desarrollar capacidades tecnológicas y operativas institucionales.

La intención de esta experiencia profesional es sugerir el desarrollo de habilidades rudimentarias de guerra electrónica para la operación fronteriza de SENAFRONT, a la luz de una serie de amenazas recientes, barreras operativas y la urgencia estratégica del control del dominio electromagnético en las situaciones de seguridad actuales.

La investigación se basa en métodos descriptivos y propositivos, con un enfoque en el examen de capacidades, debilidades operativas y soluciones a la situación en la práctica. Trata sobre la base doctrinal en cuanto a guerra electrónica, comunicaciones tácticas y seguridad electromagnética, abordando también la teoría frente a la realidad operativa de las unidades fronterizas.

El trabajo está organizado en tres capítulos. El primero proporciona información general sobre la dependencia y funciones desarrolladas en el área de comunicaciones. El segundo revela los fundamentos y principios de la guerra electrónica, el espectro electromagnético y las operaciones tácticas.

Por último, el capítulo tres desarrolla el diagnóstico institucional y la Propuesta de Innovación, que busca enriquecer las capacidades de guerra electrónica elemental como parte de las operaciones fronterizas.

Este trabajo tiene como objetivo proporcionar una visión técnica y estratégica sobre la importancia de introducir capacidades de guerra electrónica en el dominio de la seguridad fronteriza, fortaleciendo así las capacidades operativas y tecnológicas de SENAFRONT además de su capacidad existente contra las nuevas amenazas presentadas en el escenario actual.

CAPITULO I. INFORMACIÓN GENERAL

1.1 Descripción de la dependencia o Unidad

La Dirección de Telemática y Ciberseguridad es una parte del nivel auxiliar en el organigrama del Servicio Nacional de Fronteras. Su objetivo principal es gestionar los sistemas de telecomunicaciones e informáticos, desarrollando proyectos a corto, mediano y largo plazo en estas áreas, con el fin de extender la red de comunicaciones a todo el territorio de la República de Panamá, especialmente en las zonas bajo su responsabilidad.

1.2. Tipo de actividad que desarrollo

Esta Dirección se encarga de planificar, gestionar y supervisar los sistemas tecnológicos y de telecomunicaciones dentro de la organización, asegurando su funcionamiento tanto en condiciones normales como excepcionales. Esto incluye redes de comunicación y equipos tecnológicos, ya sea para operaciones regulares o para situaciones emergentes.

Además, proporciona asesoría a la Dirección General sobre decisiones relacionadas con la creación, modernización y fortalecimiento de sistemas estratégicos para la información y comunicación, así como otras infraestructuras relevantes. Las funciones técnicas y operativas se centran en el manejo de equipos tecnológicos y sistemas comunicativos que abarcan telefonía, radiocomunicación y tecnología satelital, conforme a los requerimientos operativos del Servicio Nacional de Fronteras.

Para gestionar situaciones de emergencia, accidentes o desastres naturales a nivel nacional, esta Dirección colabora estrechamente con entidades gubernamentales y empresas privadas en temas relacionados con telemática y comunicaciones.

También se encarga del manejo seguro de información sensible para salvaguardar la seguridad nacional, garantizando una comunicación eficiente hacia los niveles superiores del mando e impulsando el fortalecimiento tecnológico y operativo dentro de la institución.

1.3. Lugar y fecha

Las actividades se llevaron a cabo durante mi trayectoria profesional.
Periodo: Panamá 2019 – 2026.

1.4 Misión

La misión principal del Servicio Nacional de Fronteras es:

> "Proteger la vida, honra, bienes y demás derechos y libertades de quienes se encuentren bajo jurisdicción estatal; mantener el orden público; prevenir, reprimir e investigar delitos; así como resguardar las fronteras terrestres y fluviales de la República de Panamá."

En este contexto, la misión específica de la Dirección de Telemática y Ciberseguridad es:

> Planificar, organizar, dirigir, asesorar, supervisar y controlar los sistemas informáticos y telecomunicaciones que operan dentro del Servicio Nacional de Fronteras mediante el desarrollo estratégico a corto, mediano y largo plazo.

1.5 Visión

La visión institucional del Servicio Nacional de Fronteras establece que:

> "Seremos reconocidos como la entidad líder dentro Fuerza Pública capacitada para planificar organizar dirigir todas las acciones necesarias para garantizar tanto la seguridad territorial como poblacional dentro nuestra jurisdicción soberana respetando siempre el orden constitucional vigente".

La visión particular para la Dirección es:

> "Asegurar que los sistemas informáticos y comunicacionales satisfagan las demandas inmediatas necesarias para llevar a cabo efectivamente tanto actividades rutinarias como emergencias que enfrenta el Servicio Nacional de Fronteras en todo el país."

1.6 Funciones del puesto que ocupo

En mi rol dentro de la Dirección de Telematica y Ciberseguridad, específicamente en el Departamento Comunicaciones es proporcionar servicios comunicacionales esenciales que faciliten adecuadamente las funciones en todas las áreas bajo responsabilidad institucional minimizando interrupciones entre unidades operativas administrativas.

Tareas principales:

a. Controlar distribución equipos comunicacionales tales como radios portátiles tarjetas satelitales entre otros.

b. Diagnosticar reparar fallos presentados por equipos radioeléctricos.
c. Mantener un ambiente laboral adecuado equipado con herramientas analíticas esenciales para realizar mantenimiento reparaciones diversas telecomunicaciones Servicios Nacionales Fronteras.
d. Establecer conexiones eléctricas seguras a tierra garantizando conservación equipo seguridad unidades.
e. Operar equipos comunicación tácticos HF/VHF/UHF cifrados instalados Batallones correspondientes.

Otras funciones propias del puesto
a. Capacitar al personal del Servicio Nacional Fronteras sobre uso adecuado equipos comunicacionales: radios base móviles vehiculares repetidoras rastreadores frecuencias satelitales torres estructuradas antenas.
b. Gestionar proyectos enfocados innovación modernización sistemas comunicación institucional.
c. Llevar a cabo estudios frecuencia diseñar tecnologías orientadas optimización expansión redes transmisión VHF UHF Servicio Nacional Fronteras."

CAPITULO II. MARCO TEORICO

2.1 Antecedentes

Los cambios provocados por los conflictos actuales y las amenazas extranjeras también han llevado a la necesidad de fortalecer las capacidades tecnológicas y operativas de las organizaciones militares y de seguridad.

En este contexto, la guerra electrónica es un aspecto esencial de las operaciones contemporáneas que permite el control, la explotación y la protección del espectro electromagnético y es una parte muy importante del entorno operativo.

En los últimos años, numerosos países han desarrollado capacidades de guerra electrónica basadas en tecnología con el objetivo de mejorar la vigilancia, la protección y el dominio electromagnético en el combate militar y en las operaciones de seguridad.

Estas habilidades incluyen sistemas de interceptación de señales, sistemas de interferencia, sistemas de inteligencia electrónica para la recopilación de inteligencia y la neutralización de amenazas tecnológicas, particularmente la amenaza de drones y comunicaciones clandestinas. (ver anexo E)

La creciente incidencia de peligros híbridos, el crimen organizado transnacional y el abuso de los medios de comunicación también impulsan la actualización de las doctrinas militares y de seguridad en varios países, adoptando instalaciones de guerra electrónica como piedra angular en las operaciones terrestres, aéreas y fronterizas.

Por lo tanto, la comprensión de los antecedentes internacionales y nacionales sobre la guerra electrónica forma la base central de la importancia estratégica de controlar el espectro electromagnético y la implementación del concepto en el escenario operativo actual, particularmente en las empresas responsables de la seguridad fronteriza y las amenazas transnacionales.

2.1.1 Antecedentes internacionales

Las capacidades de guerra electrónica han experimentado una evolución global drástica debido a la evolución de la tecnología y la transformación de las amenazas contemporáneas. Sistemas especializados que incluyen vigilancia, protección y explotación del espectro electromagnético se han integrado en el arsenal de diversas fuerzas armadas y agencias de seguridad porque se considera un componente crítico para el éxito operativo.

Un recurso importante para la guerra electrónica se encuentra en las Fuerzas Armadas de los Estados Unidos, que desarrollan doctrinas para el uso integrado de inteligencia electrónica, protección de comunicaciones e interferencia de señales en operaciones militares y de seguridad.

El dominio del espectro electromagnético es el parámetro crucial para garantizar el mando y control de las fuerzas desplegadas en entornos operativos complejos. La Organización del Tratado del Atlántico Norte (OTAN) también ha

implementado mejoras continuas y desarrollo de sus capacidades de guerra electrónica debido a las amenazas híbridas y los conflictos modernos.

La OTAN también acepta que el espectro electromagnético es un entorno operativo vital donde las interferencias, los ataques electrónicos, las debilidades en las comunicaciones y otras formas de interferencia pueden causar daños extensos al mando y control militar como sus capacidades clave en el campo de batalla.

Por otro lado, conflictos recientes como el conflicto de Rusia con Ucrania han mostrado la importancia de la guerra electrónica en el campo de batalla moderno. El uso de sistemas de interferencia, detección de señales, neutralización de drones y vigilancia electromagnética durante este tiempo ha demostrado muy claramente la importancia estratégica que estas capacidades tienen ahora en el terreno y para la comunicación.

Asimismo, Israel ha desarrollado capacidades avanzadas de guerra electrónica para promover la protección fronteriza, neutralizar riesgos provenientes de drones y vigilancia tecnológica. Estas tecnologías han reforzado los sistemas de seguridad y enfrentado amenazas asimétricas y organizaciones irregulares a medida que utilizan cada vez más tecnologías para llevar a cabo actividades ilícitas.

En América Latina, varios países han iniciado procesos de modernización tecnológica en torno a la inteligencia electrónica y la vigilancia del espectro electromagnético principalmente para operaciones de seguridad fronteriza y contraataques a organizaciones criminales transnacionales. Sin embargo, muchas instituciones de seguridad en la región todavía enfrentan desafíos relacionados con la creación de capacidades especializadas de guerra electrónica.

El contexto internacional mencionado describe la creciente importancia de la guerra electrónica como un arma estratégica para varios sectores, incluidas las operaciones militares y de seguridad, y la necesidad de mejorar la capacidad

en cuanto a vigilancia electromagnética, protección de comunicaciones y neutralización de amenazas tecnológicas en contextos operativos modernos.

2.1.2 Antecedentes Nacionales

En la República de Panamá, las operaciones de seguridad fronteriza han evolucionado progresivamente como respuesta al incremento de amenazas transnacionales vinculadas al narcotráfico, tráfico ilícito de migrantes, crimen organizado y otras actividades desarrolladas por grupos irregulares en áreas de difícil acceso.

Estas amenazas han obligado a las instituciones de seguridad a fortalecer sus capacidades operacionales, tecnológicas y de comunicaciones para garantizar una respuesta efectiva en entornos complejos.

El Servicio Nacional de Fronteras, como institución de seguridad bajo el liderazgo del Ministerio de Seguridad Pública, es la encargada de la vigilancia y protección de las zonas fronterizas del país; para esto, desarrolla operaciones en áreas selváticas, montañosas y de condicionada cobertura tecnológica, donde las comunicaciones tácticas son un elemento fundamental para el mando y control de las tropas apostadas.

En las operaciones realizadas en zonas fronterizas, las comunicaciones son una parte indispensable de las unidades de coordinación operativa en tierra. La interconexión permanente de los puestos de mando, las patrullas terrestres, las unidades fluviales y los medios aéreos permite una mejor ejecución de diversas misiones y la transmisión oportuna de información mientras se realizan las tareas asignadas.

No obstante, durante las operaciones desarrolladas en áreas de difícil acceso se ha observado que factores como la geografía del terreno, la vegetación densa y las limitaciones propias de la cobertura radioeléctrica pueden afectar el alcance de las comunicaciones y la estabilidad de los enlaces entre las unidades desplegadas. Esto representa un desafío permanente para dar continuidad y resguardar las comunicaciones tácticas.

En este sentido, hay que destacar que grupos delictivos utilizan aparatos de radio, dispositivos de satélite y drones para coordinar sus acciones, vigilar lugares importantes y llevar a cabo actividades ilegales en zonas cercanas a las fronteras. Esto supone un reto para los organismos que se encargan de la seguridad en estas zonas, ya que necesitan mejorar su capacidad para vigilar y proteger las comunicaciones que utilizan.

Estas tecnologías se usan para realizar vigilancia no autorizada y monitorear los movimientos de unidades operativas. Esto facilita la coordinación de actividades ilícitas y representa un reto importante para las instituciones responsables de la seguridad nacional. Aunque en Panamá no hay una estructura formal de guerra electrónica enfocada en la seguridad fronteriza, en los últimos años se han promovido iniciativas para mejorar las capacidades tecnológicas y de comunicación mediante la modernización de radios, sistemas de retransmisión y plataformas de coordinación operativa.

La experiencia en operaciones fronterizas ha mostrado que es necesario reforzar la vigilancia del espectro electromagnético, proteger las comunicaciones tácticas y detectar amenazas tecnológicas causadas por el uso indebido de medios electrónicos por actores irregulares. Por eso, desarrollar capacidades básicas de guerra electrónica podría fortalecer las operaciones del Servicio Nacional de Fronteras, mejorando la seguridad de las comunicaciones, la vigilancia tecnológica y la capacidad de respuesta en zonas fronterizas de difícil acceso.

Los antecedentes analizados también indican que existen desafíos operativos y tecnológicos relacionados con el control del espectro electromagnético, lo que justifica implementar iniciativas para fortalecer las capacidades institucionales en guerra electrónica en el ámbito fronterizo.

2.2 Bases Teóricas

2.2.1 Guerra electrónica

La guerra electrónica es una capacidad militar especializada para la utilización inteligente del espectro electromagnético con el fin de

detectar, interceptar, degradar, neutralizar o proteger los sistemas electrónicos y de comunicación utilizados durante operaciones militares y de seguridad. Como función de la creciente dependencia de los sistemas de mando, control, comunicaciones e inteligencia, hoy en día, esta capacidad constituye un aspecto crucial de muchas situaciones operativas (Jefes del Estado Mayor Conjunto, 2020).

Esto se observa particularmente en el combate de defensa, donde la guerra electrónica ha evolucionado hacia un nuevo estándar que se entiende como acciones diseñadas para dominar el espectro electromagnético, permitiendo que las capacidades del adversario se vean afectadas mientras se protegen simultáneamente los sistemas electrónicos y de comunicación propios. En este sentido, el espectro electromagnético es un entorno operativo estratégico similar a los dominios terrestre, marítimo, aéreo y cibernético (OTAN, 2022).

La guerra electrónica se desarrolló por primera vez en la Segunda Guerra Mundial, donde se basaba principalmente en radares, interceptación de señales y sistemas de interferencia para degradar las capacidades de detección del enemigo. Durante la Guerra Fría, las tecnologías de comunicaciones y los sistemas electrónicos militares se desarrollaron mucho más rápido, y estas capacidades evolucionaron drásticamente (Schwartau, 2018).

Debido al uso extensivo de sistemas digitales, incluido el aumento de drones, comunicaciones satelitales, vigilancia digital y redes inalámbricas, la guerra electrónica ha cobrado aún más importancia hoy en día.

Como destaca Boyd (2019), esa creciente dependencia de la tecnología ha hecho del espectro electromagnético una 'prioridad' para el uso de sistemas militares en la guerra actual. Las teorías de la doctrina militar moderna actualmente categorizan la guerra electrónica en tres categorías principales: apoyo electrónico, protección electrónica y

ataque electrónico. Todos estos elementos desempeñan funciones dedicadas al control y explotación del entorno electromagnético. (ver anexo A)

El apoyo electrónico incluye la búsqueda, detección, identificación y localización de emisiones electromagnéticas para obtener datos del mundo real. Está estrechamente integrado con la inteligencia electrónica y proporciona la capacidad de detectar amenazas, movimientos y sistemas de comunicación de actores adversarios (Jefes del Estado Mayor Conjunto, 2020).

La protección electrónica significa los medios para proteger la seguridad y funcionalidad de los propios sistemas contra interferencias, ataques electrónicos o vulnerabilidades electromagnéticas. Estas tareas comprenden protocolos de seguridad de comunicaciones, protección de frecuencias, encriptación y esfuerzos de defensa técnica (OTAN, 2022).

El ataque electrónico: degradar, interrumpir o neutralizar las capacidades electrónicas del adversario en forma de técnicas de interferencia, bloqueo o engaño electrónico. Según Boyd (2019), estas capacidades pueden aplicarse contra sistemas de comunicación, radares, drones y otros equipos que dependen del espectro electromagnético.

La guerra electrónica opera como un complejo de operaciones C2, y las comunicaciones son críticas para asegurar la coordinación de todas las tácticas, la transmisión de órdenes y las operaciones tácticas operativas. Como resultado, la pérdida o deterioro de las comunicaciones tiene el potencial de obstaculizar gravemente la capacidad operativa de una unidad desplegada (Departamento del Ejército, 2021).

De manera similar, el desarrollo de amenazas híbridas y transnacionales ha amplificado la importancia de las capacidades de guerra electrónica

en las actividades de seguridad fronteriza. Los delincuentes utilizan radios, dispositivos satelitales, drones comerciales y tecnologías de vigilancia de manera ilícita, subrayando que es hora de reforzar las capacidades para proteger y monitorear el espectro electromagnético.

Las capacidades básicas de guerra electrónica en el contexto de las operaciones fronterizas por parte del Servicio Nacional de Fronteras podrían mejorar en gran medida la seguridad operativa, lo que puede facilitar una mejor vigilancia tecnológica y protección para las comunicaciones tácticas junto con la detección de amenazas del uso delictivo de sistemas electrónicos.

Asimismo, las capacidades de guerra electrónica cada vez más sofisticadas mejorarían las operaciones en regiones de difícil acceso donde las limitaciones de cobertura y las limitaciones geográficas se han convertido en barreras perennes para las comunicaciones tácticas y el mando operativo. (ver anexo D)

Por esta razón, la guerra electrónica no solo debe ser una capacidad militar ofensiva por sí sola, sino también un arma estratégica que avance la seguridad, la protección de las comunicaciones y la superioridad operativa en las aplicaciones modernas de seguridad fronteriza.

2.2.2 Espectro electromagnético

El espectro electromagnético se refiere a las frecuencias que permiten la transmisión de energía, datos y comunicaciones de una fuente de comunicación a otra. Este recurso se considera un componente estratégicamente significativo de las operaciones militares y de seguridad con respecto a los sistemas de comunicación táctica, radares, navegación, vigilancia, enlaces satelitales y plataformas electrónicas utilizadas en contextos operativos (Departamento de Defensa, 2020).

El espectro electromagnético está técnicamente compuesto por bandas de frecuencia distintas basadas en sus propiedades físicas y

capacidades de propagación. Estas incluyen alta frecuencia (HF), muy alta frecuencia (VHF), ultra alta frecuencia (UHF) y súper alta frecuencia (SHF) y se utilizan para diferentes sistemas de comunicación en tiempo real. (ver anexo B)

Las bandas de frecuencia HF van de 3 a 30 MHz y abarcan largas distancias mediante reflexión ionosférica para que las comunicaciones pasen más allá de la línea de visión. Debido a estas características, son un instrumento común de comunicación para uso estratégico, comunicación rural y escenarios donde no hay infraestructura de retransmisión (FAS, 2021).

Por otro lado, las radios VHF y UHF han encontrado popularidad en las comunicaciones tácticas terrestres debido a su operación estable, buena calidad de sonido, alta compatibilidad con plataformas móviles y portátiles, y portabilidad. Se recomiendan tales frecuencias para habilitar conexiones operativas eficientes entre puestos de mando, patrullas y unidades basadas en el campo y el mantenimiento de los enlaces operativos de esas formaciones, según el mando de seguridad y operativo contemporáneo, el militar (OTAN, 2022).

El espectro electromagnético es de preocupación central en el dominio militar y de seguridad debido a la necesidad de infraestructura tecnológica para la operación. Según el Departamento de Defensa (2020), las capacidades de mando y control, inteligencia, vigilancia y reconocimiento están directamente influenciadas por la superioridad en el espectro electromagnético.

Las amenazas al uso ilegal del espectro electromagnético han crecido dramáticamente en este momento. Las radios comerciales, dispositivos satelitales, sistemas GPS y drones también son utilizados por organizaciones criminales y actores irregulares para coordinar actividades ilegales, monitorear movimientos operativos e impedir las actividades de las fuerzas de seguridad.

El control y monitoreo del espectro electromagnético en este sentido han demostrado ser un requisito estratégico para las instituciones que operan en la seguridad fronteriza. La capacidad de detectar emisiones, identificar interferencias y monitorear el uso del espectro electromagnético contribuye al fortalecimiento de las operaciones de seguridad nacional, ya que permite conocer posibles riesgos que pueden afectar las comunicaciones tácticas. Del mismo modo, las interferencias electromagnéticas pueden provocar interrupciones en los enlaces de comunicación, afectar la calidad de las señales y dificultar la transmisión oportuna de información entre las unidades desplegadas. Estas situaciones pueden originarse tanto por factores ambientales como por acciones deliberadas orientadas a afectar sistemas de comunicación electrónicos.

En las operaciones desarrolladas en áreas selváticas y de difícil acceso, como las que ejecuta el Servicio Nacional de Fronteras, las condiciones geográficas y ambientales influyen directamente en la propagación de las señales de radio.

La vegetación densa, la topografía del terreno y las condiciones atmosféricas pueden limitar el alcance de las comunicaciones y generar dificultades para mantener enlaces estables entre las unidades operativas, razón por la cual el conocimiento del comportamiento del espectro electromagnético resulta fundamental para la planificación y ejecución de las operaciones. Factores como la densidad de la vegetación, la humedad, las elevaciones del terreno y las condiciones atmosféricas pueden influir directamente sobre el alcance y calidad de las comunicaciones tácticas.

Por esta razón, el conocimiento relacionado con el espectro electromagnético es crucial tanto en la planificación como en la ejecución de todas las operaciones fronterizas; dicha información es útil para seleccionar qué frecuencias se pueden utilizar y así optimizar la

cobertura, así como para fortalecer la seguridad de las comunicaciones operativas.

Lo mismo se aplica a la construcción de capacidades de monitoreo y vigilancia del espectro electromagnético para identificar actividades ilegales asociadas con el uso de tecnologías de comunicación por parte de organizaciones criminales para reforzar aún más las fronteras y operar a costa de la superioridad operativa. Así, el espectro electromagnético es un recurso estratégico en las operaciones contemporáneas que debe ser protegido, controlado y explotado, como elementos clave tanto de la efectividad de las comunicaciones tácticas como de una operación efectiva de seguridad fronteriza.

2.2.3 Inteligencia electrónica (ELINT/COMINT)

La inteligencia electrónica es una capacidad destinada a recibir, analizar e interpretar información derivada de emisiones electromagnéticas provenientes de sistemas electrónicos y de comunicación. En operaciones militares y de seguridad nacional, también es una capacidad destinada a rastrear acciones delictivas y mejorar el proceso de toma de decisiones utilizando medios tecnológicos avanzados (Estado Mayor Conjunto, 2020).

Dentro del contexto doctrinal, la inteligencia electrónica forma parte de la guerra electrónica y la inteligencia de señales, y es un elemento clave para garantizar la conciencia situacional y el dominio del espectro electromagnético. Tales capacidades permiten la detección de emisiones, localizar transmisores y comprender los modos de comunicación de las partes adversarias.

SIGINT, inteligencia de señales, es la recopilación y uso de información proporcionada por señales electromagnéticas. Según el Departamento de Defensa (2021), esta área se categoriza principalmente en inteligencia de comunicaciones (COMINT) e inteligencia electrónica (ELINT), ambas de las cuales tratan solo con tipos específicos de emisiones

y sistemas tecnológicos.

La inteligencia de comunicaciones, o COMINT, se centra en la interceptación, monitoreo y análisis de comunicaciones que pasan a través de redes de radio, satélite e inalámbricas. Este tipo de inteligencia puede ayudar a identificar frecuencias utilizadas, patrones de comunicación, dónde se realizan las actividades y el potencial de actividad ilegal de actores criminales y/o irregulares.

Por el contrario, la inteligencia electrónica, o ELINT, también se ocupa de la interceptación y análisis de emisiones no asociadas con la comunicación de voz, incluyendo radares, sistemas de navegación, sensores electrónicos y otros medios electromagnéticos. Su capacidad de adquisición de información proporciona información técnica sobre los sistemas electrónicos utilizados en un entorno operativo (OTAN, 2022).

La importancia estratégica de las capacidades ELINT y COMINT es fundamental en las operaciones militares contemporáneas, ya que permiten la detección de amenazas antes de que sean evidentes. Según Lowenthal (2022), la inteligencia de señales permite la organización de operaciones preventivas, observación táctica y defensa de las fuerzas desplegadas.

De manera similar, los avances en tecnología han aumentado sustancialmente la importancia de estas capacidades en entornos de seguridad fronteriza. Con la adopción de radios comerciales, dispositivos satelitales y drones por parte de organizaciones criminales, surgen nuevas necesidades de vigilancia electromagnética y monitoreo de señales ilícitas.

En áreas fronterizas y zonas de difícil acceso, las capacidades de inteligencia electrónica permiten fortalecer el conocimiento del entorno operacional mediante la detección de emisiones asociadas a actividades sospechosas. Esto contribuye a mejorar la capacidad de

respuesta de las unidades desplegadas y facilita el desarrollo de operaciones de interdicción y vigilancia.

La misma lógica se aplica también a COMINT, que permite detectar las redes de comunicación de actores criminales, determinar patrones operativos y la forma en que se mueven colectivamente dentro de áreas de interés estratégico. Por ejemplo, para el Servicio Nacional de Fronteras, la integración avanzada de un conjunto mínimo de funciones de inteligencia electrónica mejoraría en gran medida las operaciones fronterizas, especialmente cuando la vigilancia convencional no puede debido a la geografía y las tecnologías.

Significaría que la integración de capacidades de inteligencia electrónica con sistemas de comunicación táctica y operaciones de mando y control para una mejor conciencia situacional, así como la coordinación operativa de las unidades enviadas al terreno.

Por otro lado, el establecimiento de capacidades ELINT y COMINT requiere personal especializado, hardware especial y procedimientos para garantizar que el uso del espectro electromagnético se lleve a cabo correctamente en un contexto legal y operativo.

Por lo tanto, la inteligencia electrónica juega un papel clave en la mejora de las operaciones modernas de seguridad fronteriza y sirve como una capacidad estratégica para mejorar la vigilancia tecnológica, detectar amenazas emergentes a la seguridad fronteriza y, por lo tanto, fortalecer la seguridad operativa a través del dominio del entorno electromagnético.

2.2.4 Comunicaciones tácticas militares

Las comunicaciones tácticas militares son los sistemas, procesos y métodos para garantizar la seguridad de la transferencia de información crítica en tiempo para desarrollar operaciones de seguridad y militares de manera oportuna. Tales comunicaciones son clave para el C2 porque

aseguran la coordinación de unidades, la comunicación de órdenes, el reporte de situaciones operativas y los enlaces entre fuerzas desplegadas en el terreno (Departamento del Ejército, 2021).

Hoy en día, los comandos tácticos apoyan la continuidad de las operaciones en situaciones con entornos dinámicos y complejos, significativos y de rápido cambio. Como lo define la doctrina militar moderna, la efectividad de una operación depende predominantemente de la presencia de enlaces de comunicación continuos, seguros y permanentes entre las unidades dentro de una operación (OTAN, 2022).

Los sistemas de comunicación táctica militar utilizan una variedad de bandas de frecuencia, HF, VHF y UHF, que se eligen en función del área de operación, el alcance requerido y las características geográficas del entorno operativo. Cada una de estas bandas proporciona un conjunto diferente de propiedades que impactan la transmisión, cobertura y capacidades de propagación.

Las comunicaciones de alta frecuencia (HF) se utilizan comúnmente para enlazar datos a largas distancias, porque pueden propagarse a través de la reflexión ionosférica. Por lo tanto, son importantes porque estas comunicaciones crean enlaces más allá de la línea de visión, lo cual es extremadamente útil con respecto a misiones realizadas en sitios remotos, o donde una infraestructura de retransmisión está ausente (Federación de Científicos Americanos [FAS], 2021).

En contraste, las comunicaciones VHF y UHF se utilizan extensamente en operaciones tácticas terrestres debido a su estabilidad, calidad de audio, simplicidad de integración con radios portátiles, unidades móviles y estaciones base. Estas permiten conexiones efectivas entre puestos de mando, equipos de patrulla y unidades terrestres (Departamento de Defensa, 2020).

Las comunicaciones tácticas en áreas de jungla y de difícil acceso están asociadas con numerosos desafíos relacionados con la geografía, la vegetación y las condiciones atmosféricas en escenarios operativos. Factores como la elevación del terreno, la densidad forestal y las condiciones climáticas pueden afectar seriamente la propagación de señales de radio y reducir el rango abierto para el intercambio de información. Por lo tanto, las operaciones tácticas requieren el uso de sistemas de retransmisión y repetidores para mejorar el alcance de las operaciones y mantener una comunicación continua.

Estos sistemas facilitan la conexión entre unidades en ubicaciones remotas o fuera de la línea de visión directa. Es lo mismo en las comunicaciones tácticas militares, ya que se requiere interoperabilidad para permitir la integración entre diferentes tipos de unidades, plataformas y agencias de seguridad. La interoperabilidad permite el intercambio de información y facilita la coordinación operativa durante la planificación de misiones conjuntas y operaciones combinadas.

La seguridad operativa y las comunicaciones tácticas tienen una relación estrecha. La protección de frecuencias y seguridad, el uso adecuado de procedimientos de comunicación y la seguridad de la información transmitida son componentes clave para evitar vulnerabilidades en el entorno operativo (Jefes de Estado Mayor Conjunto, 2020).

En la actualidad, las amenazas relacionadas con la interferencia, la interceptación de señales y la explotación ilegal del espectro electromagnético están aumentando la necesidad de reforzar la seguridad de las comunicaciones tácticas.

Una amplia gama de organizaciones criminales y actores ilícitos han aprovechado las plataformas de comunicaciones comerciales para facilitar la coordinación y vigilancia de conductas no autorizadas y actividades operativas para generar nuevos problemas a las fuerzas de

seguridad.

Las comunicaciones tácticas constituyen un aspecto esencial del funcionamiento de las operaciones fronterizas, especialmente en ubicaciones geográficas complicadas (espacio GEO) que demandan coordinación entre unidades terrestres, activos aéreos y puestos de mando en operaciones de alta área.

La estabilidad continua y la protección de las comunicaciones afectan las posibilidades de éxito de una respuesta. Por lo tanto, mejorar las capacidades relacionadas con la protección electromagnética, la detección del espectro y la seguridad de las comunicaciones es una necesidad tanto para aumentar la eficiencia operativa como para reducir los riesgos causados por el entorno electromagnético.

Igualmente, la integración de capacidades fundamentales de guerra electrónica con herramientas de comunicación táctica puede mejorar la defensa de los enlaces operativos, identificar interferencias y aplicar el control del espectro electromagnético para la seguridad fronteriza.

La comunicación táctica militar es, por lo tanto, un elemento estratégico de las operaciones modernas: asegura el proceso de flujo de información, fortalece el mando y control, y garantiza la posibilidad de mantener la coordinación operativa en entornos complejos y dinámicos.

2.2.5 Seguridad de las comunicaciones (COMSEC)

La seguridad de las comunicaciones, según la doctrina conocida como COMSEC (Seguridad de las Comunicaciones), incluye esfuerzos para proteger la información transmitida a través de sistemas de comunicación del acceso no autorizado, la interceptación, la interferencia o la explotación por parte de la contrainteligencia u otras entidades hostiles.

Es bien sabido que en las operaciones militares o de seguridad modernas

(Departamento de Defensa, 2021), COMSEC proporciona una base para la confidencialidad, integridad y disponibilidad de las comunicaciones tácticas.

En el entorno operativo moderno, la creciente dependencia de los sistemas electrónicos y las redes de comunicación ha provocado una intensificación de los mecanismos de protección, para prevenir amenazas de guerra electrónica, inteligencia de señales e interferencias electromagnéticas.

Según la doctrina militar de EE. UU., la seguridad de las comunicaciones es un componente primordial para mantener la potencia de las capacidades de mando y control en el desarrollo de operaciones tácticas (Jefes del Estado Mayor Conjunto, 2020).

La seguridad de las comunicaciones se relaciona con medios técnicos, físicos y operativos para minimizar las vulnerabilidades en el entorno electromagnético. Tales medidas van desde la encriptación y la gestión de frecuencias hasta la autenticación de usuarios, la protección de hardware y el cumplimiento de obligaciones disciplinarias respecto al uso de comunicaciones tácticas.

COMSEC contiene en uno de sus bloques de construcción importantes la encriptación de información, que permite la encriptación del contenido de la transmisión a través de una serie de algoritmos y claves criptográficas, por lo que los mensajes interceptados pueden ser difíciles de decodificar para un intérprete.

Como afirma la OTAN (2022), los sistemas de encriptación están entre las herramientas utilizadas para asegurar las comunicaciones militares de la manera más efectiva.

El control de frecuencias es otro aspecto de la seguridad de las comunicaciones. Gestionar adecuadamente el espectro

electromagnético evita interferencias, disminuye el impacto de una interferencia, minimiza la exposición y las vulnerabilidades, y permite una mejor organización de los enlaces tácticos en una operación coordinada.

De manera similar, la disciplina de comunicación es también uno de los componentes importantes para salvaguardar el control de la información operativa relevante. Usar procedimientos de radio, códigos operativos y transmisiones de manera correcta y a través de protocolos específicos previene la interceptación y el mal uso por parte del adversario para acceder y malinterpretar información sensible a través de dichos dispositivos o utilizarlos contra la organización.

En las operaciones de defensa contemporáneas, las amenazas a las comunicaciones tácticas han aumentado significativamente como resultado del progreso tecnológico y el acceso a sistemas de comunicación y monitoreo producidos comercialmente.

Radio, satélites, drones y servicios de monitoreo digital son utilizados por organizaciones criminales y operadores irregulares para escuchar sus comunicaciones, observar sus movimientos y realizar operaciones de reconocimiento.

Entre los ataques más severos al entorno electromagnético se encuentran las interferencias intencionales (doctrinalmente denominadas como jamming) que tienen como objetivo los sistemas de comunicación para interferir con ellos saturando las frecuencias utilizadas por los operadores militares involucrados en operaciones de campo y tierra. Esto puede tener repercusiones en la coordinación operativa y en la capacidad de respuesta de las unidades en el terreno (Departamento del Ejército, 2021).

Otra amenaza pertinente es el spoofing o engaño electrónico en el que las señales de navegación o comunicación se fabrican para producir

información falsa o manipular sistemas electrónicos empleados como parte de las operaciones operativas. Estas estrategias constituyen un desafío creciente en los entornos operativos contemporáneos.

Las limitaciones geográficas, la cobertura reducida y la dependencia de los sistemas inalámbricos pueden hacer que las vulnerabilidades de las comunicaciones tácticas aumenten en áreas fronterizas y en situaciones de difícil acceso. Es precisamente por eso que proteger las comunicaciones se convierte en una preocupación estratégica en las operaciones de seguridad fronteriza.

En el caso de operaciones desarrolladas por el Servicio Nacional de Fronteras, el fortalecimiento de medidas relacionadas con seguridad de las comunicaciones permitiría mejorar la protección de enlaces tácticos, reducir vulnerabilidades electromagnéticas y fortalecer la continuidad operacional en áreas de alta complejidad geográfica.

Asimismo, la integración de capacidades básicas de guerra electrónica con procedimientos de COMSEC contribuiría al fortalecimiento de la vigilancia electromagnética y a la detección de posibles amenazas relacionadas con interferencias o uso ilícito del espectro electromagnético.

Esto debería ocurrir solo después de que se conozca el riesgo para la seguridad operativa de las tropas y el éxito de las operaciones; cuando las comunicaciones están comprometidas y los enlaces se pierden o se perturban, esto puede afectar imperceptiblemente las capacidades de despliegue, lo que también podría afectar la información que podrían derivar sobre el entorno en el que están operando.

Por lo tanto, la seguridad de las comunicaciones es un aspecto clave de la seguridad de cualquier operación táctica moderna y militar, protegiendo el acceso y la información para un mando y control de misión en curso.

2.2.6 Operaciones fronterizas

Las operaciones fronterizas comprenden el conjunto de acciones de vigilancia, control, seguridad e interdicción desarrolladas por organismos militares y de seguridad con el propósito de proteger la integridad territorial y garantizar el control de las zonas limítrofes de un Estado. Estas operaciones poseen un carácter estratégico debido a que las fronteras representan espacios vulnerables frente a amenazas transnacionales, actividades ilícitas y movimientos irregulares que pueden afectar la seguridad nacional (Organización de los Estados Americanos [OEA], 2021).

Las operaciones de seguridad desarrolladas en las zonas fronterizas de Panamá se enfrentan actualmente a diversas amenazas, entre ellas el narcotráfico, el tráfico ilícito de migrantes, el contrabando, la minería ilegal y otras actividades vinculadas al crimen organizado transnacional. La mayoría de estas actividades se llevan a cabo en áreas remotas y de difícil acceso, donde las condiciones geográficas adversas, la infraestructura limitada y las restricciones en comunicaciones complican la ejecución de las operaciones.

La experiencia operacional indica que el éxito de las misiones fronterizas depende en gran medida de la capacidad para mantener vigilancia constante, movilidad adecuada de las unidades y coordinación efectiva entre los componentes desplegados en el terreno. En este contexto, las comunicaciones tácticas y el control del entorno electromagnético son factores esenciales para asegurar la continuidad de las operaciones y fortalecer la capacidad de respuesta ante nuevas amenazas (NATO, 2022).

Las áreas selváticas presentan desafíos específicos en cuanto a cobertura de comunicaciones, movilidad y conocimiento de la situación operativa. La vegetación densa, las condiciones climáticas adversas y las dificultades de acceso afectan directamente la propagación de señales

de radio y pueden limitar la coordinación entre las unidades participantes en operaciones fronterizas.

Se ha observado que las organizaciones criminales que operan en áreas fronterizas emplean cada vez más radios de comunicación, dispositivos satelitales, sistemas GPS y drones comerciales para coordinar movimientos y mantener enlaces entre sus integrantes. El uso de estas tecnologías incrementa sus capacidades de comunicación, vigilancia y conocimiento del entorno, lo que representa un desafío adicional para las instituciones responsables de la seguridad y protección fronteriza.

Las condiciones actuales de seguridad fronteriza requieren complementar las actividades tradicionales de vigilancia y patrullaje con herramientas tecnológicas que mejoren el monitoreo del espectro electromagnético, refuercen la protección de las comunicaciones y permitan detectar amenazas asociadas al uso de medios electrónicos.

En las operaciones del Servicio Nacional de Fronteras, las comunicaciones tácticas son fundamentales para mantener la coordinación entre puestos de mando, patrullas terrestres, unidades fluviales y medios aéreos. La experiencia operacional demuestra que la continuidad de estos enlaces es indispensable para la conducción de las misiones y la transmisión oportuna de información. No obstante, las características geográficas de las áreas fronterizas de Panamá, especialmente en zonas selváticas y de difícil acceso, generan limitaciones relacionadas con la cobertura de radio, la estabilidad de las comunicaciones y la permanencia de los enlaces operativos. Estas circunstancias hacen necesario fortalecer capacidades asociadas a sistemas de retransmisión, protección de las comunicaciones y vigilancia del espectro electromagnético.

De igual forma, las operaciones fronterizas suelen involucrar la participación coordinada de diferentes unidades y organismos de seguridad, por lo que la interoperabilidad entre sistemas de

comunicación constituye un factor importante para el intercambio de información y la coordinación de esfuerzos operativos. Mantener comunicaciones seguras y continuas contribuye a mejorar la capacidad de respuesta de las unidades desplegadas, particularmente frente a amenazas que aprovechan el conocimiento del terreno y el uso de tecnologías de comunicación para desarrollar actividades ilícitas.

En operaciones desarrolladas en áreas remotas, la pérdida de comunicaciones puede afectar significativamente el mando y control, limitar la capacidad de reacción y comprometer la seguridad del personal desplegado. Por esta razón, las capacidades relacionadas con protección electromagnética y guerra electrónica adquieren una importancia estratégica dentro de los entornos fronterizos modernos.

De igual manera, el fortalecimiento de capacidades básicas de vigilancia electromagnética permitiría mejorar la detección de actividades ilícitas relacionadas con el uso de sistemas de comunicación y tecnologías electrónicas empleadas por actores irregulares dentro de áreas fronterizas.

En consecuencia, las operaciones fronterizas modernas requieren una integración progresiva de capacidades tecnológicas orientadas al fortalecimiento de las comunicaciones tácticas, la protección del espectro electromagnético y la vigilancia electrónica, con el propósito de incrementar la seguridad operacional y mejorar la capacidad de respuesta frente a amenazas transnacionales.

2.2.7 Amenazas híbridas y transnacionales

Las amenazas híbridas y transnacionales constituyen uno de los principales desafíos para las instituciones de seguridad y defensa en el contexto contemporáneo. Estas amenazas se caracterizan por combinar métodos convencionales y no convencionales, así como el empleo simultáneo de recursos tecnológicos, actividades ilícitas y acciones orientadas a afectar la estabilidad y seguridad de los Estados (NATO,

2021).

Las amenazas híbridas se caracterizan por la combinación de diferentes métodos y recursos para alcanzar sus objetivos, lo que dificulta su identificación y neutralización. Una característica fundamental de estas organizaciones es su capacidad de adaptación a las condiciones del entorno, ajustando sus métodos de operación conforme a las medidas de seguridad establecidas por las autoridades. En el contexto fronterizo, las amenazas se manifiestan a través de actividades como el narcotráfico, el tráfico ilícito de migrantes, el contrabando, la ciberdelincuencia, la minería ilegal y otras formas de crimen organizado transnacional.

Las organizaciones criminales transnacionales han adoptado tecnologías avanzadas de comunicación y localización para facilitar la ejecución de actividades ilícitas y optimizar la coordinación entre sus miembros. Entre los recursos más empleados se incluyen radios de comunicación, sistemas satelitales, dispositivos GPS, redes digitales y drones comerciales utilizados para vigilancia, monitoreo y transmisión de información (United Nations Office on Drugs and Crime [UNODC], 2022).

En las zonas fronterizas, el uso del espectro electromagnético representa un factor de interés para las organizaciones criminales, ya que gran parte de sus actividades dependen de sistemas de comunicación que les permiten coordinar desplazamientos, intercambiar información y mantener contacto entre grupos ubicados en diferentes sectores geográficos. Esta situación plantea desafíos adicionales para las instituciones responsables de la seguridad fronteriza, las cuales deben fortalecer su capacidad para monitorear y proteger las comunicaciones.

En el contexto de las amenazas híbridas, los sistemas electrónicos y las redes de comunicación resultan fundamentales, ya que facilitan la coordinación de actividades ilícitas y el intercambio de información entre los actores involucrados. Por esta razón, la doctrina militar

contemporánea reconoce el espectro electromagnético como un espacio estratégico para detectar, rastrear y neutralizar amenazas emergentes en escenarios complejos (Joint Chiefs of Staff, 2020).

En las zonas fronterizas de difícil acceso, las organizaciones dedicadas a actividades ilícitas aprovechan las características del terreno, la limitada cobertura de comunicaciones y las deficiencias de infraestructura para desplazarse con mayor facilidad y eludir la detección por parte de las autoridades. Estas condiciones representan un desafío permanente para las instituciones responsables de la vigilancia y el control fronterizo.

Las áreas selváticas presentan vulnerabilidades que pueden ser explotadas mediante el uso de tecnologías de comunicación y vigilancia.

Uno de los desafíos actuales para las instituciones de seguridad fronteriza es el empleo de drones comerciales por parte de organizaciones criminales. Estos dispositivos permiten observar rutas de acceso, monitorear los movimientos de las fuerzas de seguridad, recopilar información sobre áreas de interés y facilitar actividades ilícitas. Su disponibilidad en el mercado y bajo costo han propiciado su utilización en diversos contextos.

Asimismo, las organizaciones criminales emplean medios de comunicación y tecnologías de localización para coordinar sus operaciones en zonas de difícil acceso. Esta situación exige fortalecer las capacidades de monitoreo de frecuencias, vigilancia del espectro electromagnético y protección de las comunicaciones de las unidades operativas.

En ese orden de ideas, la detección oportuna de amenazas asociadas al uso de tecnologías de comunicación y vigilancia contribuye a mejorar la capacidad de respuesta de las instituciones de seguridad y a proteger los sistemas de comunicaciones tácticas empleados durante las operaciones fronterizas. Por esta razón, la integración de capacidades

de guerra electrónica y vigilancia electromagnética adquiere una importancia estratégica dentro de los escenarios operacionales modernos.

En el caso del Servicio Nacional de Fronteras, las amenazas transnacionales representan un desafío constante debido a la complejidad geográfica de las áreas fronterizas y al empleo creciente de tecnologías de comunicación por parte de actores irregulares.

En ese mismo sentido, la presencia de organizaciones o grupos criminales con capacidad de resiliencia tecnológica exige que las instituciones de seguridad pública, busquen el fortalecimiento escalonado o progresivo de capacidades relacionadas con protección electromagnética, inteligencia de señales y seguridad de las comunicaciones tácticas.

La doctrina de seguridad moderna reconoce que las amenazas híbridas no pueden enfrentarse únicamente mediante medios convencionales, sino que requieren la integración de capacidades tecnológicas, inteligencia operacional y dominio del entorno electromagnético para garantizar operaciones más efectivas y seguras (NATO, 2021).

En virtud de lo anterior, podrías decir que las amenazas híbridas y transnacionales representan un desafío multidimensional para las operaciones fronterizas contemporáneas, evidenciando la necesidad de fortalecer capacidades relacionadas con guerra electrónica, vigilancia tecnológica y protección de las comunicaciones dentro de escenarios operacionales complejos.

2.2.8 Sistemas antidrones y amenazas RF

El avance tecnológico y la masificación de sistemas aéreos no tripulados han transformado significativamente los escenarios de seguridad y defensa contemporáneos. Los drones, también conocidos como UAV (Vehículos Aéreos No Tripulados), son utilizados actualmente en operaciones militares, vigilancia, reconocimiento, monitoreo y transmisión

de información en tiempo real. Sin embargo, el uso creciente de estas tecnologías por parte de organizaciones criminales y actores irregulares ha generado nuevas amenazas relacionadas con el entorno electromagnético y la seguridad operacional (Department of Defense, 2021).

Los drones comerciales han sido utilizados para actividades ilícitas relacionadas con el tráfico de drogas, vigilancia clandestina, transporte de sustancias ilegales y monitoreo de movimientos operativos de las fuerzas de seguridad en los últimos años. Debido a su bajo costo, facilidad de adquisición y adaptabilidad tecnológica, estos sistemas representan una amenaza emergente dentro de las operaciones fronterizas modernas.

Desde una perspectiva técnica, los drones utilizan enlaces de radiofrecuencia (RF), sistemas de posicionamiento global (GPS) y redes inalámbricas para mantener la comunicación con sus operadores, ejecutar maniobras de navegación y transmitir información. Debido a esta dependencia de medios electrónicos, su funcionamiento se encuentra directamente vinculado al espectro electromagnético, lo que permite su detección, monitoreo o interferencia mediante capacidades asociadas a la guerra electrónica (NATO, 2022).

Resulta imprescindible mencionar que, el empleo de los drones puede abarcar desde la obtención de información sobre áreas de interés, observación de determinadas áreas de operaciones la recopilación de datos y la posible afectación de sistemas de comunicación utilizados por las tropas. Asimismo, estos dispositivos pueden ser empleados para transmitir información en tiempo real a organizaciones criminales que ejecutan sus actividades ilícitas en zonas fronterizas.

En contrapeso a esta situación, resulta importante que los sistemas que utilizados para la detección y neutralización de drones se han convertido en una capacidad de apoyo para las operaciones militares y de

seguridad de todos los estados. Estas herramientas, abarcan capacidades que son integradas por diferentes tecnologías las cuales buscan localizar, identificar y monitorear aeronaves no tripuladas que puedan representar riesgos para las operaciones.

Dentro de las tecnologías que pueden emplearse, están los radares, sensores electroópticos, detectores de radiofrecuencia y sistemas de interferencia electromagnética. La combinación de estos medios facilita la identificación oportuna de drones dentro del área de operaciones y contribuye a mejorar la capacidad de respuesta ante posibles amenazas.

Uno de los métodos más utilizados corresponde al jamming o interferencia electrónica, mediante el cual se interrumpen las señales de comunicación o navegación utilizadas por el dron. Esta técnica puede provocar pérdida de control, retorno automático o aterrizaje forzado del sistema no tripulado (Department of the Army, 2021).

Así mismo, muchos de los sistemas antidrones poseen capacidades de detección de radio frecuencia orientadas a identificar frecuencias utilizadas por drones y localizar la posición aproximada de los operadores. Estas capacidades permiten fortalecer la vigilancia electromagnética y contribuir a operaciones de interdicción y seguridad fronteriza.

En las operaciones de seguridad fronteriza, el uso no autorizado de drones constituye una preocupación para las instituciones encargadas de la vigilancia y el control territorial. Las características geográficas de muchas áreas fronterizas, especialmente aquellas con vegetación densa y acceso limitado, favorecen el empleo de estas aeronaves para realizar actividades de observación, reconocimiento y monitoreo de movimientos operativos.

En la labor diaria del Servicio Nacional de Fronteras, se podrían añadir poco a poco capacidades de alerta temprana y vigilancia al marco

normativo para amenazas aéreas no tripuladas. Esto ayudaría a reforzar la seguridad operativa, ya que permitiría identificar UAV en tiempo real y mejorar la protección de instalaciones, rutas y zonas estratégicas.

Además, si se combinan estas capacidades con herramientas para vigilar el espectro electromagnético y funciones de guerra electrónica, se puede fortalecer la protección de las comunicaciones tácticas y mejorar el control operativo en misiones que se desarrollan en entornos complejos.

Es por lo que, el aumento constante de las amenazas tecnológicas muestra que es necesario mejorar la vigilancia electrónica, el monitoreo de radio frecuencia y la protección del entorno electromagnético. Estas capacidades no solo sirven para mitigar las amenazas actuales, sino también para prepararse para los desafíos tecnológicos del mañana en las operaciones de seguridad fronteriza.

Así, los sistemas anti drones y las capacidades de detección e interferencia de RF son herramientas estratégicas para fortalecer la seguridad y defensa modernas, particularmente cuando estas se ven amenazadas por tecnologías no tripuladas ilícitas que interfieren con la seguridad operativa y el control territorial.

2.3 Términos básicos

2.3.1 Amenaza híbrida

Amenaza que combina medios convencionales y no convencionales, incluyendo acciones criminales, tecnológicas, informativas y operacionales, con la finalidad de afectar la seguridad, estabilidad o capacidad de respuesta de un Estado o institución (NATO, 2021).

2.3.2 Ataque electrónico (EA)

Componente de la guerra electrónica orientado a degradar, neutralizar o interrumpir sistemas electrónicos, comunicaciones, radares o enlaces mediante el empleo de energía electromagnética (Joint Chiefs of Staff, 2020).

2.3.3 C2 / Mando y control

Proceso mediante el cual los mandos ejercen dirección, coordinación y control sobre las unidades desplegadas, apoyándose en sistemas de comunicación, información y procedimientos operacionales (Department of the Army, 2021).

2.3.4 COMINT

La inteligencia de comunicaciones, conocida como COMINT, se refiere a la obtención y análisis de información proveniente de comunicaciones transmitidas por medios electrónicos, tales como radios, enlaces satelitales o redes inalámbricas (Department of Defense, 2021).

2.3.5 COMSEC

La seguridad de las comunicaciones comprende las medidas técnicas, físicas y procedimentales destinadas a proteger la información transmitida frente a interceptación, explotación, interferencia o acceso no autorizado (Department of Defense, 2021).

2.3.6 Dron / UAV

Vehículo aéreo no tripulado empleado para vigilancia, reconocimiento, monitoreo, transmisión de información o ejecución de tareas específicas mediante control remoto o sistemas automatizados (Department of Defense, 2021).

2.3.7 ELINT

La inteligencia electrónica se orienta a la recopilación y análisis de emisiones electromagnéticas no comunicacionales, como radares, sensores y otros sistemas electrónicos utilizados dentro de un entorno operacional (NATO, 2022).

2.3.8 Espectro electromagnético

Conjunto de frecuencias utilizadas para la transmisión de energía, datos y comunicaciones mediante ondas electromagnéticas, siendo fundamental para sistemas de radio, radar, navegación, vigilancia y

enlaces tácticos (Department of Defense, 2020).

2.3.9 Guerra electrónica

Conjunto de acciones militares y tecnológicas orientadas al empleo del espectro electromagnético para detectar, proteger, explotar, interferir o neutralizar sistemas electrónicos y de comunicaciones durante operaciones militares o de seguridad (Joint Chiefs of Staff, 2020).

2.3.10 HF

Banda de alta frecuencia comprendida entre 3 y 30 MHz, utilizada principalmente para comunicaciones de larga distancia, especialmente cuando se requiere propagación más allá de la línea de vista mediante reflexión ionosférica (Federation of American Scientists, 2021).

2.3.11 Interferencia electromagnética

Alteración, degradación o interrupción de una señal electrónica o de comunicación causada por emisiones electromagnéticas, ya sean accidentales, ambientales o deliberadas (Department of Defense, 2020).

2.3.12 Interoperabilidad

Capacidad de diferentes sistemas, unidades o instituciones para operar de manera coordinada, intercambiar información y cumplir objetivos comunes dentro de una operación conjunta o combinada (NATO, 2022).

2.3.13 Jamming

Técnica de interferencia electrónica utilizada para bloquear, degradar o interrumpir señales de comunicación, navegación o control mediante la emisión intencional de energía electromagnética (Department of the Army, 2021).

2.3.14 Protección electrónica (EP)

Componente de la guerra electrónica destinado a proteger los sistemas propios frente a interferencias, ataques electrónicos o acciones que puedan afectar el uso efectivo del espectro electromagnético (Joint Chiefs of Staff, 2020).

2.3.15 Radiofrecuencia (RF)

Rango del espectro electromagnético utilizado para la transmisión inalámbrica de señales de voz, datos, control y navegación en sistemas de comunicación, vigilancia y operación electrónica (Department of Defense, 2020).

2.3.16 Retransmisión

Procedimiento técnico mediante el cual una señal recibida es transmitida nuevamente para ampliar cobertura, superar obstáculos geográficos o mantener enlaces entre unidades ubicadas fuera de línea de vista directa (Department of the Army, 2021).

2.3.17 Seguridad operacional

Conjunto de medidas orientadas a proteger al personal, la información, los equipos y las operaciones frente a riesgos, amenazas o vulnerabilidades durante el cumplimiento de una misión (Department of the Army, 2021).

2.3.18 SIGINT

La inteligencia de señales consiste en la obtención, procesamiento y análisis de información proveniente de señales electromagnéticas, incluyendo comunicaciones y emisiones electrónicas (Department of Defense, 2021).

2.3.19 Spoofing

Técnica de engaño electrónico mediante la cual se manipulan señales de comunicación, navegación o posicionamiento con el propósito de generar información falsa o afectar el funcionamiento de sistemas electrónicos (NATO, 2022).

2.3.20 UHF

Banda de ultra alta frecuencia comprendida entre 300 MHz y 3 GHz, utilizada en comunicaciones tácticas, enlaces inalámbricos, sistemas móviles y aplicaciones de corto o mediano alcance (Federation of

American Scientists, 2021).

2.3.21 VHF

Banda de muy alta frecuencia comprendida entre 30 y 300 MHz, empleada comúnmente en comunicaciones tácticas terrestres, sistemas móviles y enlaces operacionales de alcance medio (Federation of American Scientists, 2021).

2.3.22 Vigilancia electromagnética

Actividad orientada al monitoreo, detección y análisis de emisiones dentro del espectro electromagnético con el propósito de identificar amenazas, interferencias o usos no autorizados de sistemas electrónicos (Joint Chiefs of Staff, 2020).

CAPITULO III DESARROLLO DEL TEMA

3.1 Campos de Aplicación

El desarrollo de capacidades básicas de guerra electrónica posee un campo de aplicación amplio dentro de las operaciones modernas de seguridad y defensa, especialmente en escenarios donde las comunicaciones tácticas, el control del espectro electromagnético y la vigilancia tecnológica representan elementos fundamentales para el éxito operacional.

En el ámbito de la seguridad fronteriza, estas capacidades permiten fortalecer la protección de las comunicaciones, incrementar el conocimiento situacional y mejorar la capacidad de respuesta frente a amenazas emergentes relacionadas con el uso ilícito de tecnologías electrónicas.

La doctrina militar moderna reconoce que gran parte de los sistemas utilizados para el mando y control, las comunicaciones, la navegación y la vigilancia dependen del empleo del espectro electromagnético (Joint Chiefs of Staff, 2020). Por esta razón, las capacidades asociadas a la guerra electrónica tienen utilidad en distintos ámbitos operativos, incluyendo operaciones terrestres, aéreas, marítimas y de seguridad fronteriza.

El conocimiento y el monitoreo del entorno electromagnético son especialmente relevantes en zonas de difícil acceso, como la selva y las zonas fronterizas, que afectan las comunicaciones. Muchas agencias operativas han aprendido que la vegetación densa, las irregularidades del terreno y las interferencias también pueden desempeñar un papel en los sistemas de comunicación utilizados por las unidades desplegadas. En este sentido, las capacidades destinadas a facilitar la vigilancia electromagnética y a proporcionar protección de las comunicaciones serán útiles para localizar emisiones de interés, identificar posibles interferencias y reforzar la seguridad de los enlaces tácticos utilizados durante la ejecución de las operaciones.

Por último, como una contribución adicional a las dimensiones de seguridad contemporánea previamente analizadas en los territorios panameños, esta propuesta se dirige al ámbito de las competencias del Servicio Nacional de Fronteras (SENAFRONT), la institución autónoma responsable de la vigilancia y la seguridad de las zonas fronterizas en la República de Panamá. Las características geográficas de estas áreas, combinadas con los requisitos operativos del servicio, generan desafíos continuos en la cobertura de comunicaciones, la movilidad de las unidades y la gestión del entorno electromagnético.

En las zonas fronterizas, las organizaciones dedicadas a actividades ilícitas están usando más tecnología para coordinar sus operaciones y comunicarse. De acuerdo con la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC, 2022), estas organizaciones ya emplean sistemas de comunicación inalámbrica, dispositivos satelitales y drones comerciales para apoyar sus actividades.

Para enfrentar este problema, las capacidades básicas de guerra electrónica ayudan a monitorear las radiofrecuencias, proteger las comunicaciones tácticas e identificar señales importantes en el entorno operativo. También permiten vigilar el espectro electromagnético y detectar actividades relacionadas con el uso indebido de sistemas de comunicación en zonas fronterizas.

La implementación de sistemas antidrones y herramientas para detectar radiofrecuencias ayuda a mejorar la seguridad frente a amenazas de drones usados para reconocimiento, monitoreo y vigilancia encubierta. Según la NATO (2022), las amenazas relacionadas con el uso de drones son uno de los principales desafíos tecnológicos en las operaciones de seguridad actuales.

El campo de aplicación también abarca la protección de sistemas de mando y control (C2), debido a que las comunicaciones tácticas constituyen el principal medio para la coordinación entre unidades terrestres, puestos de mando y medios operacionales desplegados en el área de operaciones.

De igual manera, la implementación progresiva de capacidades de guerra electrónica permitiría fortalecer la interoperabilidad entre unidades y mejorar la capacidad institucional para responder frente a amenazas tecnológicas relacionadas con interferencias, interceptación de señales y vulnerabilidades electromagnéticas.

En hábitats de jungla y áreas con poca cobertura, las capacidades de retransmisión, vigilancia electromagnética y protección de frecuencias ayudan a lograr un nivel mucho más alto de continuidad de las operaciones y una reducción de la probabilidad de pérdida de comunicaciones. (ver anexo D)

Cabe destacar que el campo de aplicación de esta propuesta no se limita exclusivamente al sector militar; más bien, es relevante en operaciones de seguridad pública, control territorial y protección de infraestructuras estratégicas, especialmente en escenarios donde los sistemas electrónicos y las redes de comunicación juegan un papel crucial.

Así, el desarrollo de capacidades básicas de guerra electrónica representa una alternativa viable para fortalecer las operaciones modernas en las fronteras con el objetivo de proteger mejor el entorno electromagnético, asegurar las comunicaciones tácticas y mejorar la capacidad de respuesta ante amenazas tecnológicas emergentes.

3.2 Tipo de aplicación

La propuesta actual proporciona una orientación de aplicación operativa, tecnológica y doctrinal, con énfasis en el fortalecimiento de las capacidades de seguridad fronteriza a través de la evolución incremental de las capacidades básicas de guerra electrónica aplicables al entorno operativo del Servicio Nacional de Fronteras.

Operativamente, la propuesta tiene como objetivo ayudar a mejorar las capacidades de vigilancia, monitoreo y protección de las comunicaciones tácticas que se emplean en el desarrollo de operaciones fronterizas. Estas capacidades permitirían una mejor coordinación de las unidades desplegadas, una mayor conciencia situacional y la minimización de vulnerabilidades relacionadas con el uso del espectro electromagnético dentro del área de operaciones.

Según Joint Chiefs of Staff (2020), las capacidades asociadas a la guerra electrónica forman parte de los elementos que deben considerarse durante la planificación de las operaciones, debido a la dependencia que tienen los sistemas de mando y control, inteligencia y comunicaciones del espectro electromagnético. El adecuado conocimiento y monitoreo de este entorno contribuye a mejorar la toma de decisiones y a fortalecer el empleo de los medios tecnológicos utilizados durante las operaciones.

Desde el punto de vista tecnológico, la propuesta plantea el fortalecimiento gradual de capacidades relacionadas con el monitoreo de radiofrecuencias, la detección de señales y la protección de las comunicaciones utilizadas durante las operaciones. En una etapa inicial, no se considera la adquisición de sistemas complejos de carácter estratégico, sino el desarrollo de capacidades básicas ajustadas a las necesidades operativas y a los recursos disponibles dentro de la institución.

Estas capacidades facilitarían una mejor respuesta institucional al uso de radios de comunicación, dispositivos satelitales y drones utilizados por organizaciones

criminales a lo largo de la frontera. Este tipo de organizaciones recurre cada vez más a tecnologías comerciales para la coordinación de actividades ilícitas y las comunicaciones entre sus miembros (Oficina de las Naciones Unidas contra la Droga y el Delito [UNODC], 2022).

En términos de doctrina, el plan tiene como objetivo fortalecer los procesos de seguridad de la información en las comunicaciones, el control del espectro electromagnético y la protección de los sistemas utilizados en las operaciones. Se llevan a cabo enfoques similares para reforzar la COMSEC y la disciplina en las comunicaciones con el fin de reducir los riesgos asociados con la detección, el bloqueo (jamming) y el uso del espectro electromagnético por entidades hostiles.

Otro elemento clave de la propuesta se basa en integrar funciones para identificar y rastrear posibles amenazas provenientes de drones que ingresen en zonas fronterizas. Proporcionamos estas herramientas para proteger mejor las distintas instalaciones, puestos de mando y otros lugares de interés utilizados durante el desarrollo de las operaciones.

También enfatizamos que la propuesta es progresiva y puede adaptarse, con respecto a la capacidad institucional ya disponible y la necesidad de reforzar gradualmente el aspecto tecnológico de la guerra electrónica dentro de las operaciones fronterizas.

Además, el desarrollo de tales capacidades podría servir como un puente para mejorar la interoperabilidad entre diferentes unidades operativas y entidades de seguridad, facilitando una comunicación y coordinación más efectivas de las operaciones en situaciones complejas.

Como señala Department of the Army (2021), las capacidades relacionadas con guerra electrónica y protección de comunicaciones deben desarrollarse de manera escalonada y acorde a las necesidades operacionales de cada institución, priorizando inicialmente la protección del entorno electromagnético y la continuidad de las comunicaciones tácticas.

Así, el tipo de aplicación de esta propuesta está orientado al fortalecimiento operativo, tecnológico y doctrinal de las operaciones fronterizas, a través del mejoramiento progresivo de las capacidades electrónicas básicas que permitirían establecer la seguridad operativa y mejorar la capacidad de respuesta a las nuevas amenazas tecnológicas que surgen en un área.

3.3 Diagnóstico

El entorno operativo contemporáneo presenta desafíos crecientes relacionados con el uso del espectro electromagnético, las comunicaciones tácticas y el empleo de tecnologías electrónicas por parte de actores irregulares y organizaciones criminales transnacionales.

En este contexto, las operaciones fronterizas requieren capacidades destinadas a fortalecer la vigilancia tecnológica, proteger las comunicaciones y controlar el entorno electromagnético como parte integral de la seguridad operativa.

Las operaciones en zonas fronterizas se llevan a cabo en entornos geográficos complejos en los que la densidad de la vegetación y las elevaciones del terreno, las condiciones meteorológicas y la limitada infraestructura tecnológica influyen directamente en la eficacia de las comunicaciones tácticas y la coordinación operativa.

En la doctrina militar moderna, las comunicaciones son uno de los ingredientes principales para garantizar el mando y control en cualquier operación de seguridad y defensa. La continuidad en las comunicaciones es un requisito básico para las operaciones, porque sin ella, los enlaces pueden interrumpirse o degradarse y, por lo tanto, se ve afectada la coordinación y el intercambio de información entre las unidades desplegadas (Department of the Army 2021).

La interoperabilidad en las operaciones del servicio fronterizo nacional depende de sistemas de radio HF, VHF y UHF para conectar patrullas terrestres, puestos de mando, medios fluviales y unidades aéreas. La experiencia operativa ha demostrado que estos enlaces deben ser continuos, o se perderá el control

operativo y los riesgos no se atenderán a tiempo.

Sin embargo, las características geográficas de las zonas fronterizas, en particular en las regiones selváticas y en sectores de difícil acceso, tienen un impacto decisivo en la cobertura y la estabilidad con respecto a las comunicaciones. Los obstáculos para la propagación de la señal, como la vegetación densa, la topografía local del terreno y la infraestructura cercana, pueden afectar las señales, haciendo casi imposible mantener permanentemente trayectorias conectadas entre unidades desplegadas.

Las organizaciones criminales en estas zonas fronterizas incluso utilizan radios comerciales, dispositivos satelitales y drones. Esto vuelve a crear un desafío para las instituciones encargadas de la seguridad y la vigilancia fronterizas, ya que estas tecnologías se utilizan para mantener las comunicaciones, coordinar los movimientos y obtener información sobre el entorno.

Según la Oficina de las Naciones Unidas contra la Droga y el Delito, las herramientas electrónicas ya están ampliamente disponibles y han incrementado las capacidades tecnológicas de las organizaciones criminales transnacionales, representando una amenaza creciente para las instituciones encargadas de la seguridad fronteriza (UNODC, 2022).

Un segundo aspecto se refiere a las vulnerabilidades en relación con el espectro electromagnético y la seguridad de las comunicaciones tácticas. La falta de herramientas diseñadas para el monitoreo de frecuencias de radio, detectar interferencias y monitorear el entorno electromagnético puede limitar la capacidad de la institución para identificar de manera oportuna las prácticas asociadas al mal uso de las tecnologías electrónicas por parte de actores adversos.

Asimismo, las operaciones en zonas selváticas tienen dificultades para mantener enlaces estables entre las unidades desplegadas. Factores como la vegetación densa, la topografía del terreno y las limitaciones de cobertura pueden afectar la propagación de las señales y reducir el alcance efectivo de los sistemas de

comunicación utilizados durante las operaciones.

Afirma NATO (2022) que, las interferencias electromagnéticas, el empleo de drones y la explotación del espectro electromagnético constituyen desafíos presentes en los escenarios operativos actuales, especialmente en actividades relacionadas con la seguridad y vigilancia territorial. En este contexto, la ausencia de capacidades básicas de guerra electrónica restringe las posibilidades de realizar actividades de monitoreo, detección de señales de interés y protección de las comunicaciones tácticas.

Asimismo, la evolución de las tecnologías utilizadas por organizaciones criminales plantea la necesidad de continuar fortaleciendo capacidades doctrinales, operativas y tecnológicas relacionadas con la protección de las comunicaciones y el conocimiento del entorno electromagnético.

Otro elemento identificado dentro del diagnóstico corresponde a la necesidad de fortalecer la capacitación especializada del personal en áreas relacionadas con guerra electrónica, vigilancia RF, protección electromagnética y amenazas tecnológicas emergentes.

Joint Chiefs of Staff (2020) señala que las capacidades de guerra electrónica no dependen únicamente de sistemas tecnológicos, sino también de personal capacitado, doctrina operativa y procedimientos adecuados orientados a garantizar el uso eficiente del entorno electromagnético.

En consecuencia, el diagnóstico realizado evidencia la existencia de desafíos operacionales y tecnológicos relacionados con cobertura de comunicaciones, vigilancia electromagnética, amenazas RF y protección del espectro electromagnético dentro de las operaciones fronterizas modernas.

Por consiguiente, se identifica la necesidad de desarrollar progresivamente capacidades básicas de guerra electrónica orientadas al fortalecimiento de las comunicaciones tácticas, la vigilancia tecnológica y la protección del entorno operacional dentro de las operaciones desarrolladas en áreas fronterizas.

3.4 Propuesta de innovación

El entorno operacional contemporáneo exige que las instituciones encargadas de la seguridad fronteriza fortalezcan progresivamente sus capacidades tecnológicas y operacionales para enfrentar amenazas relacionadas con el uso ilícito del espectro electromagnético, sistemas de comunicación y tecnologías emergentes utilizadas por actores irregulares y organizaciones criminales transnacionales.

En este contexto, la presente propuesta de innovación se orienta al desarrollo progresivo de capacidades básicas de guerra electrónica aplicables a las operaciones fronterizas del Servicio Nacional de Fronteras, con la finalidad de fortalecer la seguridad de las comunicaciones tácticas, mejorar la vigilancia electromagnética e incrementar la capacidad de respuesta frente a amenazas tecnológicas emergentes.

La propuesta posee un enfoque operativo, tecnológico y doctrinal, orientado a complementar las capacidades existentes de comunicaciones tácticas mediante herramientas básicas de monitoreo RF, protección electromagnética y vigilancia tecnológica adaptadas al entorno operacional institucional. (ver anexo C)

Según Joint Chiefs of Staff (2020), las capacidades de guerra electrónica modernas deben desarrollarse de manera integrada y progresiva, priorizando inicialmente la protección de las comunicaciones y el fortalecimiento del conocimiento situacional dentro del entorno electromagnético.

La presente propuesta no contempla el desarrollo inmediato de sistemas estratégicos complejos, sino la implementación gradual de capacidades básicas que permitan fortalecer las operaciones fronterizas y reducir vulnerabilidades relacionadas con interferencias, monitoreo ilícito de comunicaciones y amenazas tecnológicas asociadas al uso del espectro electromagnético.

3.4.1 Objetivo de la propuesta

Proponer el desarrollo progresivo de capacidades básicas de guerra electrónica orientadas al fortalecimiento de las comunicaciones tácticas, la vigilancia electromagnética y la seguridad operacional dentro de las operaciones fronterizas desarrolladas por el Servicio Nacional de Fronteras.

3.4.2 Descripción simple de la propuesta

La propuesta consiste en el fortalecimiento gradual de capacidades relacionadas con monitoreo del espectro electromagnético, protección de comunicaciones tácticas y vigilancia tecnológica, mediante la integración de herramientas básicas de guerra electrónica dentro de las operaciones fronterizas.

En el ámbito operacional, la propuesta contempla el fortalecimiento de las comunicaciones tácticas mediante la integración de procedimientos orientados a mejorar la protección de enlaces operacionales y reducir vulnerabilidades relacionadas con interferencias y explotación del espectro electromagnético.

Asimismo, se propone el fortalecimiento de procedimientos de COMSEC orientados a mejorar la seguridad de las comunicaciones utilizadas durante operaciones tácticas, incluyendo control de frecuencias, disciplina de comunicaciones y aplicación de medidas básicas de protección electromagnética.

Desde el punto de vista tecnológico, la propuesta contempla la incorporación progresiva de herramientas básicas de monitoreo RF y vigilancia electromagnética orientadas a detectar señales sospechosas, identificar posibles interferencias y fortalecer el conocimiento situacional dentro del entorno operacional.

De igual manera, se propone el desarrollo inicial de capacidades antidrones orientadas a detectar amenazas aéreas no tripuladas que puedan afectar la seguridad operacional o ser utilizadas para vigilancia ilícita dentro de áreas fronterizas.

De acuerdo con NATO (2022), las capacidades destinadas a la detección de drones y a la vigilancia del espectro electromagnético han adquirido una mayor relevancia dentro de los entornos de seguridad y defensa debido al empleo cada vez más frecuente de tecnologías comerciales por parte de organizaciones criminales y otros actores irregulares.

Otros aspectos de la propuesta contemplan reforzar la interoperabilidad entre las unidades operativas individuales mediante la implementación de procedimientos que permitan a las fuerzas de seguridad pública en los puestos de mando y aquellos puestos avanzados de vigilancias, coordinarse con patrullas terrestres, unidades móviles y medios de apoyo desplegados en el área de operaciones. Se produce un intercambio adecuado de información cuando estos componentes se comunican correctamente y, por lo tanto, ayudan a que las misiones asignadas se desarrollen de manera eficiente.

Resulta importante mencionar que, dentro de la propuesta la capacitación del personal en áreas vinculadas al seguimiento de radiofrecuencias y la protección de las comunicaciones, la supervisión del espectro electromagnético y la identificación de amenazas tecnológicas. Es importante mencionar lo señalado por el Department of the Army (2021), el desarrollo de capacidades asociadas a la guerra electrónica no depende únicamente de la disponibilidad de equipos y sistemas tecnológicos, sino también de la formación del personal y de la aplicación de procedimientos adecuados para su empleo.

La propuesta también contempla el fortalecimiento de los conocimientos y habilidades necesarios para operar en entornos donde las condiciones

geográficas y las limitaciones de cobertura afectan el desempeño de las comunicaciones. Esta necesidad resulta especialmente relevante en áreas fronterizas y zonas selváticas, donde la continuidad de los enlaces constituye un factor importante para la coordinación de las operaciones.

De igual forma, la incorporación gradual de herramientas relacionadas con la retransmisión de señales, el monitoreo de radiofrecuencias y la vigilancia del entorno electromagnético puede contribuir a mejorar la cobertura de las comunicaciones y facilitar el intercambio de información entre las unidades desplegadas. La propuesta se concibe como una medida de apoyo orientada al fortalecimiento de capacidades ya existentes y a la adaptación institucional frente a los cambios tecnológicos que inciden en el entorno operativo.

Asimismo, reforzar estos atributos contribuirá a mejorar los procesos de mando y control, incrementar la interoperabilidad entre diversos elementos operativos y mitigar los efectos producidos por la degradación o la pérdida de comunicaciones tácticas durante la ejecución de la misión.

Esta propuesta describe un plan incremental en el que las capacidades de comunicaciones, el monitoreo del espectro electromagnético y las herramientas tecnológicas relacionadas con las operaciones fronterizas irían aumentando con el tiempo como parte de una cartera integral. Siendo el propósito principal de contribuir al fortalecimiento de la capacidad institucional para enfrentar los desafíos que presentan las nuevas amenazas tecnológicas, considerando las características operativas y geográficas propias de las áreas bajo responsabilidad del Servicio Nacional de Fronteras.

CONCLUSIONES

La evolución de las amenazas presentes en las zonas fronterizas y el empleo cada vez más frecuente de tecnologías de comunicación y vigilancia han incrementado la importancia del espectro electromagnético dentro de las operaciones de seguridad y defensa. En este contexto, las capacidades asociadas a la guerra electrónica constituyen una herramienta de apoyo para la protección de las comunicaciones, el monitoreo del entorno electromagnético y el fortalecimiento de la capacidad de respuesta ante situaciones que puedan afectar el desarrollo de las operaciones.

En el caso de las operaciones fronterizas, estas capacidades pueden contribuir a mejorar el conocimiento de la situación operativa, proteger los enlaces de comunicación utilizados por las unidades desplegadas y reducir los riesgos asociados a interferencias o al uso indebido de tecnologías electrónicas por parte de actores adversos.

El análisis realizado durante el proceso de investigación confirmó que las operaciones a través de fronteras como selvas y lugares inaccesibles plantean barreras significativas de cobertura de comunicación, propagación de señales y tecnología que socavan la cohesión operativa junto con la coordinación entre las unidades en el sitio. T

También se identificó el uso de radios comerciales, dispositivos satelitales y drones por parte de organizaciones criminales transnacionales como una amenaza emergente para las operaciones de seguridad fronteriza, ya que tales tecnologías permiten a sus organizaciones llevar a cabo actividades de vigilancia ilícita, coordinar operaciones y monitorear el movimiento de movimientos institucionales.

Por otro lado, la capacidad de vigilancia electromagnética, monitoreo de RF y protección avanzada de las comunicaciones tácticas han demostrado tener una importancia estratégica hoy en día, particularmente dada la aparición de amenazas híbridas y tecnológicas.

Este trabajo mostró que, con el paso hacia la implementación de capacidades básicas de guerra electrónica, tales capacidades ayudarían en gran medida a mejorar las operaciones fronterizas, particularmente en lo que respecta a la protección de las comunicaciones, la vigilancia tecnológica y la seguridad operativa del Servicio Nacional de Fronteras.

Además, el punto de que el desarrollo de una capacidad básica de guerra electrónica no consiste exclusivamente en la adquisición de equipos basados en tecnología, sino también en el fortalecimiento doctrinal y la capacitación de personal especializado, y procedimientos para la aplicación efectiva y segura del espectro electromagnético. Un enfoque práctico y una solución proactiva para complementar las capacidades institucionales existentes a través de la creación de herramientas fundamentales para la protección EM, COMSEC y RF, adaptadas a las condiciones operativas fronterizas, se crea una propuesta a través del proceso de investigación.

Finalmente, el estudio encontró que un fortalecimiento progresivo de las capacidades en el tema de la guerra electrónica fue efectivo como una solución alternativa para mejorar la seguridad operativa, mejorar las comunicaciones tácticas y aumentar la capacidad de respuesta ante amenazas tecnológicas emergentes en las operaciones fronterizas modernas.

RECOMENDACIONES

- Se recomienda que gradualmente desarrollemos capacidades para la vigilancia electromagnética y la defensa de las comunicaciones tácticas dentro de las operaciones fronterizas, comenzando con herramientas básicas de monitoreo de RF y procedimientos de seguridad en las comunicaciones.
- También se considera necesario promover programas de capacitación especializada dirigidos al personal involucrado en comunicaciones y operaciones, sobre temas relacionados con la guerra electrónica, la protección electromagnética, las amenazas de RF y los sistemas antidrones.
- Para reducir las vulnerabilidades en las operaciones tácticas, se recomienda mejorar los procedimientos de COMSEC y la disciplina en las comunicaciones en relación con la interceptación de señales, la interferencia y la explotación del espectro electromagnético. Asimismo, se sugiere promover el desarrollo progresivo de capacidades básicas antidrones dirigidas a detectar amenazas aéreas no tripuladas utilizadas para la vigilancia ilícita y el monitoreo operativo en áreas fronterizas.
- También se sugiere mejorar la interoperabilidad entre las unidades operativas y los sistemas de comunicación mediante procedimientos que mejoren la coordinación y la continuidad de las comunicaciones en áreas de cobertura limitada. Se considera conveniente promover la investigación futura relacionada con la guerra electrónica, la vigilancia electromagnética y la protección del espectro electromagnético aplicadas a las operaciones de seguridad fronteriza, debido a la constante evolución de las amenazas tecnológicas y la importancia estratégica del entorno electromagnético en los escenarios modernos de seguridad y defensa.
- Por último, se recomienda considerar la guerra electrónica como un componente complementario dentro de las capacidades modernas de seguridad fronteriza, principalmente dirigido a fortalecer las comunicaciones tácticas, la vigilancia tecnológica y la seguridad operativa institucional.

REFERENCIAS BIBLIOGRÁFICAS

Department of Defense. (2020). *Operaciones del espectro electromagnético*. Departamento de Defensa de los Estados Unidos.

Department of Defense. (2020). *Sistemas y operaciones de comunicaciones militares*. Departamento de Defensa de los Estados Unidos.

Department of Defense. (2021). *Operaciones de seguridad de las comunicaciones*. Departamento de Defensa de los Estados Unidos.

Department of Defense. (2021). *Estrategia contra sistemas de aeronaves no tripuladas*. Departamento de Defensa de los Estados Unidos.

Department of Defense. (2021). *Operaciones de inteligencia de señales*. Departamento de Defensa de los Estados Unidos.

Department of the Army. (2021). *Guerra electrónica y protección de las comunicaciones*. Dirección de Publicaciones del Ejército de los Estados Unidos.

Department of the Army. (2021). *Guerra electrónica y operaciones contra sistemas aéreos no tripulados*. Dirección de Publicaciones del Ejército de los Estados Unidos.

Department of the Army. (2021). *Operaciones de guerra electrónica*. Dirección de Publicaciones del Ejército de los Estados Unidos.

Department of the Army. (2021). *Operaciones de comunicaciones tácticas*. Dirección de Publicaciones del Ejército de los Estados Unidos.

Federation of American Scientists. (2021). *Espectro de radiofrecuencia y comunicaciones militares*. https://fas.org

Joint Chiefs of Staff. (2020). *Publicación conjunta 3-85: Guerra electrónica*. Departamento de Defensa de los Estados Unidos.

Mark M. Lowenthal. (2022). *Inteligencia: De los secretos a la política* (9.ª ed.). CQ Press.

NATO. (2021). *Amenazas híbridas y desafíos modernos de seguridad*. Organización del Tratado del Atlántico Norte.

NATO. (2022). *Doctrina de seguridad fronteriza y comunicaciones operacionales*. Organización del Tratado del Atlántico Norte.

NATO. (2022). *Doctrina de sistemas de comunicaciones e información*. Organización del Tratado del Atlántico Norte.

NATO. (2022). *Doctrina y procedimientos de seguridad de las*

comunicaciones. Organización del Tratado del Atlántico Norte.

NATO. (2022). *Sistemas contra drones y seguridad electromagnética*. Organización del Tratado del Atlántico Norte.

NATO. (2022). *Doctrina de guerra electrónica e inteligencia de señales*. Organización del Tratado del Atlántico Norte.

NATO. (2022). *Política y doctrina de guerra electrónica*. Organización del Tratado del Atlántico Norte.

NATO. (2022). *Operaciones del espectro electromagnético en la guerra moderna*. Organización del Tratado del Atlántico Norte.

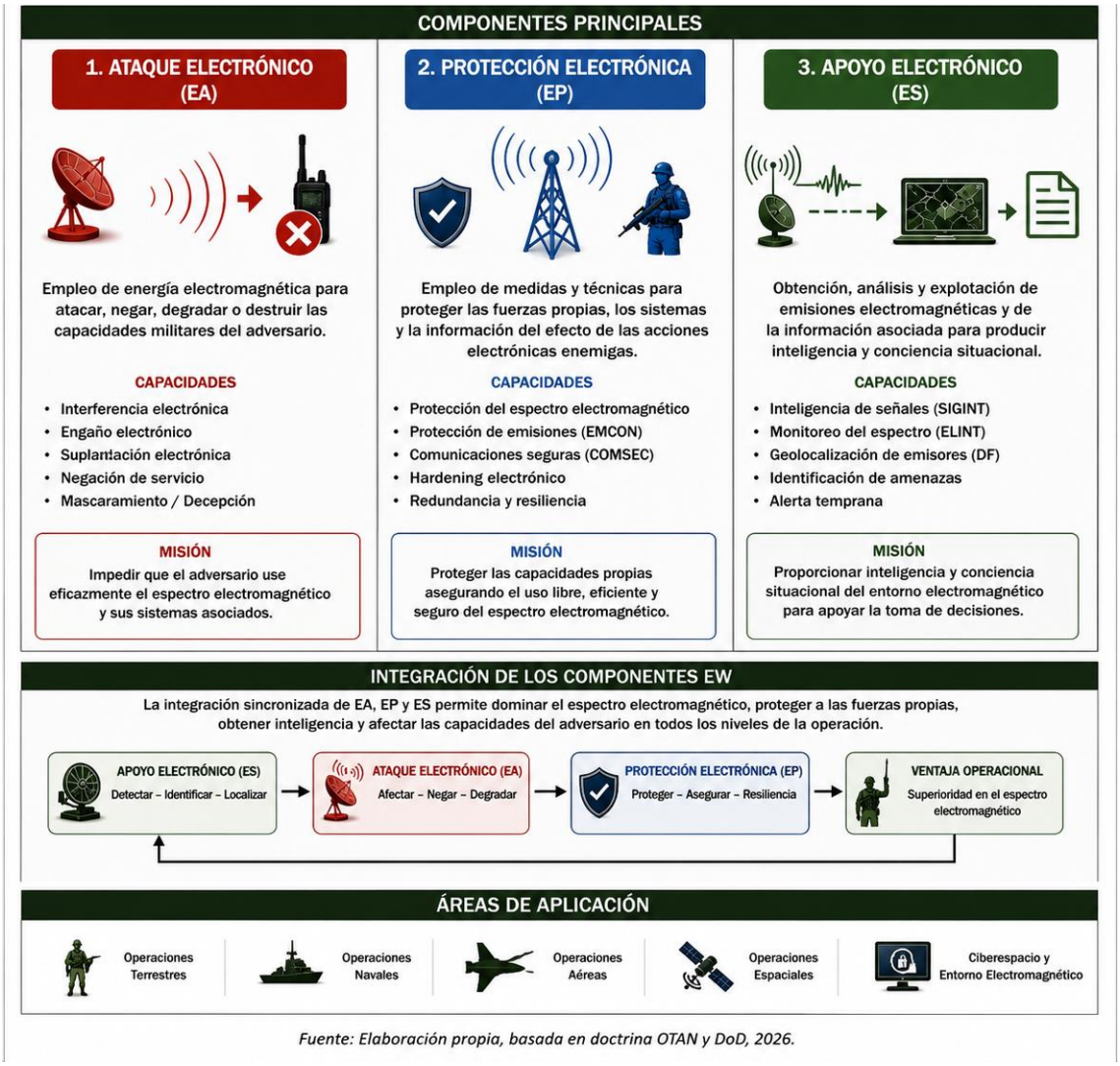
Organización de los Estados Americanos. (2021). *Seguridad multidimensional y amenazas transnacionales en las fronteras*. OEA.

Winn Schwartau. (2018). *Guerra de la información: Ciberterrorismo y guerra electrónica*. Thunder's Mouth Press.

United Nations Office on Drugs and Crime. (2022). *Crimen organizado transnacional y tecnologías emergentes*. Naciones Unidas.

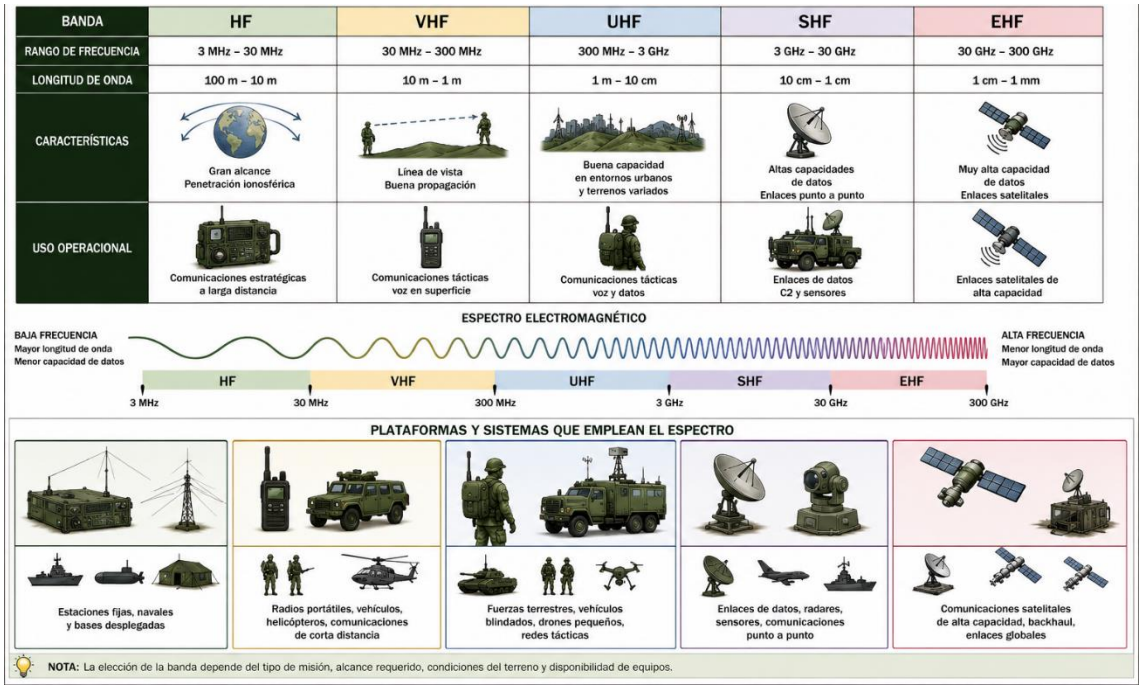
ANEXOS

Anexo A. Componentes de la Guerra Electrónica



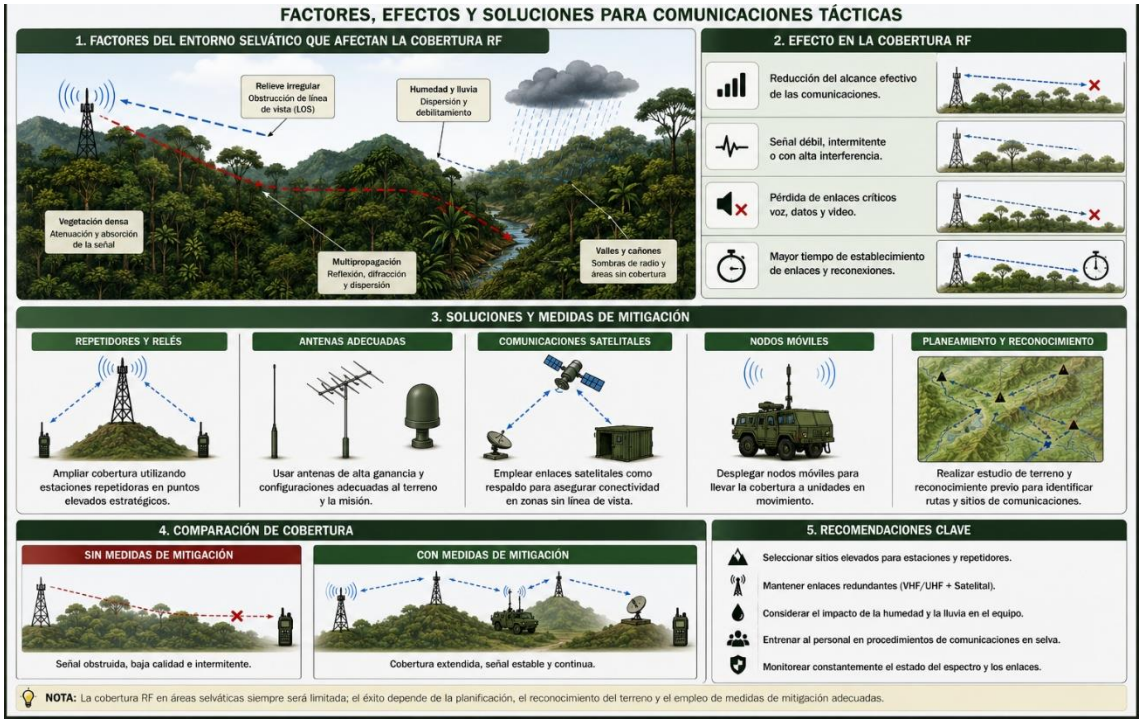
Fuente: Elaboración propia, basada en doctrina OTAN y DoD, 2026.

Anexo B. Bandas del Espectro Electromagnético



Anexo C. Arquitectura de comunicaciones tácticas

Anexo D. Cobertura RF en áreas selvática



Anexo E. Amenazas tecnológicas en las operaciones fronterizas

ESCUELA MILITAR DE CHORRILLOS CORONEL FRANCISCO BOLOGNESI

"Alma Mater del Ejército del Perú"

ANEXO 01: INFORME PROFESIONAL PARA OPTAR

EL TÍTULO PROFESIONAL DE LICENCIADO EN CIENCIAS MILITARES

1. DATOS PERSONALES:

1.01	Apellidos y Nombres	MORALES VÁSQUEZ MARTIN
1.02	Grado y Arma / Servicio	TENIENTE COMUNICACIONES
1.03	Situación Militar	ACTIVO
1.04	CIP	88771307
1.05	DNI	XXXXXX
1.06	Celular y/o RPM	+507 61283524
1.07	Correo Electrónico	mmoralesv1102@gmail.com

2. ESTUDIOS EN LA ESCUELA MILITAR DE CHORRILLOS:

2.01	Fecha_ ingreso de la EMCH	22 MARZO 2014
2.02	Fecha_ egreso EMCH	11 DICIEMBRE 2018
2.04	Fecha de alta como Oficial	01 ENERO 2019
2.05	Años_ experiencia de Oficial	7AÑOS
2.06	Idiomas	ESPAÑOL

3. SERVICIOS PRESTADOS EN EL EJÉRCITO

Nº	**Año**	**Lugar**	**Unidad / Dependencia**	**Puesto Desempeñado**
3.01				

4. ESTUDIOS EN EL EJÉRCITO DEL PERÚ

Nº	Año	Dependencia y Período	Denominación	Diploma / Certificación
-----	------	--------	---------	-----

5. ESTUDIOS DE NIVEL UNIVERSITARIO

Nº	Año	Universidad y Período	Bachiller - Licenciado
5.01	2025	UNIVERSIDAD DE PANAMÁ	TÉCNICO EN SEGURIDAD NACIONAL Y FRONTERAS

6. ESTUDIOS DE POSTGRADO UNIVERSITARIO

Nº	Año	Universidad y Período	Grado Académico (Maestro – Doctor)
-----	------	--------	---------

7. ESTUDIOS DE ESPECIALIZACIÓN

Nº	Año	Dependencia y Período	Diploma o Certificado
-----	------	--------	---------

8. ESTUDIOS EN EL EXTRANJERO

N°	Año	País	Institución Educativa	Grado / Título / Diploma / Certificado
8.01	2014-2018	Perú	EMCH	Bachiller en Ciencias Militares

FIRMA

_____

POSTFIRMA