ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO

ESCUELA D.E POSTGRADO

TESIS DE GRADO

"Análisis del estado actual de la Compañía de Guerra Electrónica de la 3ra Brigada de Comunicaciones"

AUTORES:

Bachiller. Arévalo Salas Erinna Evelyn
Bachiller. Echeverría Martínez Freddy Jesús

ASESORES:

Mg. Liza Paredes Manrique de Essenwanger
Dra. Diana Amparo Anicama Ormeño

Para optar al grado académico de

MAESTRO EN CIENCIAS MILITARES

Con mención en Planeamiento Estratégico y Toma deDecisiones

LIMA –PERÚ

2021

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO
ESCUELA DE POSTGRADO

DEPARTAMENTO GESTIÓN DE INVESTIGACIÓN

ACTA DE SUSTENTACIÓN DE TESIS No 026 – 2021/ DGI

En la Escuela Superior de Guerra del Ejército - Escuela de Postgrado, a los quince días del mes de marzo del año dos mil veintiuno, siendo las **11:50** horas, se reunió el jurado evaluador conformado por los docentes:

- **Doctor José Luis ANGULO ARGUEDAS** — **Presidente**
- **Maestro José Manuel PALACIOS SANCHEZ** — **Secretario**
- **Maestro José Manolo MAGUIÑA MENDOZA** — **Vocal**

Designados según Resolución de Expedito para Sustentación de Tesis **N° 026-2021/SIE/DGI/ESGE-EPG** del 24 de febrero del 2021, para evaluar la sustentación virtual y defensa de la Tesis de Grado titulada **"ANÁLISIS DEL ESTADO ACTUAL DE LA COMPAÑÍA DE GUERRA ELECTRÓNICA DE LA 3ª BRIGADA DE COMUNICACIONES",** presentado por los Bachilleres **Freddy Jesús ECHEVERRIA MARTINEZ y Erinna Evelyn AREVALO SALAS,** para optar al Grado Académico de Maestro en Ciencias Militares con mención en Planeamiento Estratégico y Toma de decisiones, de acuerdo a lo establecido en el artículo 45º de la Ley Universitaria N° 30220.

Luego de atender la sustentación virtual y defensa de la tesis de grado y realizadas las preguntas de rigor, el jurado acordó concederle la calificación de **APROBADO POR MAYORIA.**
En mérito del cual, el jurado **APRUEBA** (aprueba / no aprueba) que se les otorgue el Grado Académico de Maestro en Ciencias Militares con mención en Planeamiento Estratégico y Toma de decisiones.

Firmado, en Chorrillos a los quince días del mes de marzo de 2021.

Dr. José Luis ANGULO ARGUEDAS	**Mg. José Manuel PALACIOS SÁNCHEZ**	**Mg. José Manolo MAGUIÑA MENDOZA**
PRESIDENTE	**SECRETARIO**	**VOCAL**

Agradecimiento

A Dios todopoderoso por permitirnos estar con nuestros seres queridos, y lograr nuestras metas, por darnos la fortaleza de seguir sin perder el ímpetu y por el apoyo de todos los que de una u otra manera contribuyeron en el desarrollo de la presente investigación.

Dedicatoria

La presente investigación se la dedicamos a nuestros padres y seres queridos, por sus palabras de confianza y su constante apoyo para realizarnos profesionalmente.

Igualmente, se la dedicamos a nuestras hijas, ya que ellas fueron nuestra motivación principal para nunca desistir y poder ser un ejemplo de constancia y dedicación para ellas.

A nuestro Ejército, por darnos la oportunidad de poder contribuir en su engrandecimiento.

Índice

Carátula		I
Acta de sustentación		II
Agradecimiento		III
Dedicatoria		IV
Índice de tablas		VIII
Índice de figuras		IX
Resumen		X
Abstract		XI
Introducción		XII

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1	Descripción de la realidad problemática	15
1.2	Preguntas de investigación	16
1.3	Objetivos Específicos	17
1.4	Justificación y viabilidad	17
1.5	Delimitación de la investigación	18
1.6	Limitación de la investigación	18

CAPITULO II

ESTADO DEL CONOCIMIENTO

2.1	Antecedentes de la investigación	20
2.1.1	Investigaciones nacionales	20
2.1.2	Investigaciones internacionales	23
2.2	Teorías	26
2.3	Marco conceptual	76

CAPITULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1	Enfoque de investigación	92
3.2	Tipo de investigación	92
3.3	Método de investigación	92
3.4	Escenario de estudio	93
3.5	Objeto de estudio	93
3.6	Observable (s) de estudio	93
3.7	Fuentes de información	94
3.8	Técnicas e instrumentos de acopio de información	94
3.8.1	Técnica de acopio de información	94
3.8.2	Instrumentos de acopio de información	94
3.9	Acceso al campo y acopio de información	95
3.9.1	Acceso al campo	95
3.9.2	Acopio de información	95
3.10	Método de análisis de información	96
3.11	Los entrevistados	96

CAPITULO IV

ANÁLISIS Y SÍNTESIS

4.1	Revisión y elaboración de citas	98
4.2	Elaboración de categoría	99
4.3	Elaboración de macro categorías	100
4.4	Triangulación de categorías y macro categorías	101
4.5	Resultados de la triangulación	104

CAPITULO V

DIÁLOGO TEÓRICO – EMPÍRICO 107

Conclusiones 109

Recomendaciones 111

Propuesta para enfrentar la realidad problemática 113

Referencias bibliográficas

Anexos

Anexo 1. Matriz de consistencia
Anexo 2. Instrumentos de acopio de información
Anexo 3. Agenda para recolección de datos cualitativos
Anexo 4. Autorización para acceso de recolección de datos
Anexo 5. Compromiso ético
Anexo 6. Hoja de datos personal
Anexo 7. Autorización para la publicación en el repositorio de la ESGE-EPG
Anexo 8. Turnitin
Anexo 8. CD conteniendo la tesis de grado y la exposición en PDF

Índice de tablas

		Pág
Tabla 1.	Enlaces de comunicaciones	32
Tabla 2.	El jamming en el sistema de comunicaciones	54
Tabla 3.	Implicancias de los objetivos de la localización de emisores	66

Índice de figuras

		Pág
Figura 1.	Actividades de GE	31
Figura 2.	Señales de comunicaciones tácticas	34
Figura 3.	Enlaces data link	35
Figura 4.	Señal de espectro ensanchado	39
Figura 5.	Representación de una señal con salto de frecuencia	41
Figura 6.	Geometría del Jamming	43
Figura 7.	Ataque electrónico data-link de UAV	44
Figura 8.	Localización del transmisor	49
Figura 9.	Tipos de jamming	51
Figura 10.	El jamming de comunicaciones	57
Figura 11.	Equipo de ataque electrónico manpack	61
Figura 12.	Triangulación electrónica.	67
Figura 13	Localización vertical	69
Figura 14	Localización del emisor por medición de distancias múltiples	70
Figura 15.	Localización por diferencia de altitudes	71
Figura 16.	Triangulación de categorías para el objetivo N° 1	101
Figura 17.	Triangulación de categorías para el objetivo N° 2	102

Resumen

El objetivo de la presente investigación, fue analizar el estado actual de la compañía de guerra electrónica, en cuanto a la instrucción y entrenamiento en el tema de doctrina y empleo de la guerra electrónica del personal especialista de la compañía de guerra electrónica, además conocer el estado actual de disponibilidad y operatividad del material de comunicaciones e informática en el tema específico del comando y control de la compañía de guerra electrónica, la metodología empleada fue bajo un enfoque cualitativo, el tipo de investigación fue teórico-empírico, el método empleado fue hermenéutico fenomenológico, el trabajo de campo se realizó mediante las técnicas de análisis documental, observación, y entrevistas, por lo que se obtuvieron las siguientes conclusiones: el estado actual de la instrucción y entrenamiento del personal especialista en el tema de doctrina y empleo de la guerra electrónica es limitado, debido a que la instrucción y entrenamiento solo se realiza de forma teórica, también se concluye que el estado actual de disponibilidad y operatividad del material de comunicaciones e informática en el tema de comando y control de la compañía de guerra electrónica es insuficiente, debido a la limitada cantidad de equipos asignados.

Palabras claves: operaciones de información, adelanto tecnológico, ciberseguridad y ciberguerra.

Abstract

The objective of the present investigation was to analyze the current state of the electronic warfare company, in terms of instruction and training in the subject of doctrine and employment of electronic warfare of the specialist personnel of the electronic warfare company, in addition to know the current state of availability and operability of the communications and computing material on the specific subject of command and control of the electronic warfare company, the methodology used was under a qualitative approach, the type of research was theoretical-empirical. The method used was phenomenological hermeneutical, the field work was carried out through the techniques of documentary analysis, observation, and interviews, for which the following conclusions were obtained: the current state of instruction and training of specialist personnel on the subject of doctrine and use of electronic warfare is limited, because the instruction and training only takes place theoretically, it is also concluded that the current state of availability and operability of the communications and computing material in the command and control issue of the electronic warfare company is insufficient, due to the limited amount of assigned equipment.

Keywords: information operations, technological advancement, cybersecurity and cyberwarfare.

Introducción

Con el transcurrir del tiempo apareció una nueva dimensión en el campo de batalla denominado “espectro electromagnético”, por el cual surgió la preocupación de parte de los comandantes de poder influir significativamente en su completo dominio o control, debido a esa necesidad y del avance tecnológico, las principales potencias militares del mundo comenzaron a fabricar o adquirir equipamiento de guerra electrónica, equipando primero a su armada y aviación debido a su empleo estratégico-operacional, de igual manera se debía equipar a las Fuerzas Tácticas Terrestres encargadas de las operaciones militares, para llevar a cabo esta tarea se crearon las primeras organizaciones con la magnitud de regimiento, batallón o compañía de guerra electrónica, en la actualidad los estados con los que limita nuestro país han adquirido esas capacidades y organizaciones, cada uno de acuerdo a su necesidad, estudiando y desarrollando su propias organizaciones, doctrina y empleo. Debido al problema del diferendo marítimo con el vecino país de Chile en donde se debía esperar el fallo de la Corte Internacional de Justicia de la Haya, las Fuerzas Armadas del Perú en especial el Ejército, empezaron a realizar una planificación con miras a afrontar un probable conflicto necesitando desarrollar capacidades con equipamiento y equipo moderno en guerra electrónica, es por dicha situación que se toma la decisión de crear una unidad de guerra electrónica para la Fuerza Terrestre destinada a operar en el sur del país, debido a lo antes mencionado, con el DS N°018-2009 del 14 de julio del 2009, se crea la “Compañía de Guerra Electrónica Gral. Brigada Pedro Puente Revilla N°113”, orgánica de la 3ra Brigada de Comunicaciones con sede en el distrito de Tiabaya, departamento de Arequipa. Posterior a su creación se forma el comité de guerra electrónica, el cual a través de la formulación de un proyecto de inversión pública que buscaba adquirir las capacidades necesarias en equipos de guerra electrónica. El comité se encontraba integrado por un selecto grupo de oficiales especialistas que en su mayoría eran pertenecientes al arma de comunicaciones. Penosamente y debido a la situación presupuestal, no se destinaron los fondos necesarios para dicha adquisición, motivo por el cual hasta el día de hoy dicha unidad viene realizando funciones administrativas, instrucción y de servicio no acordes con la misión a la que fue creada, ante esta problemática, el objetivo general en la presente investigación fue el de analizar y conocer el estado actual de la compañía de guerra electrónica en la actualidad. La investigación se llevó a cabo mediante un enfoque cualitativo,

hermenéutico-interpretativo, para lo cual la investigación fue distribuida de la siguiente forma: en el Capítulo I "Planteamiento del Problema", en donde se describió la realidad problemática de la investigación, planteando la(s) pregunta(s) de investigación, los objetivos, en el Capítulo II "Estado del Conocimiento", en una primera parte, se hizo mención a las investigaciones anteriores en guerra electrónica y comando y control, estas investigaciones son de carácter internacional y nacional, en donde solo se hizo referencia a los objetivos, el método y las conclusiones, en una segunda parte del estado del conocimiento, se establecieron las teorías necesarias provenientes de los autores más importantes del contexto internacional sobre guerra electrónica y comando y control, en el Capítulo III "Metodología de la Investigación" se explica cómo se emplearon los caminos necesarios para realizar la investigación de tipo cualitativa, debido a ser la metodología más adecuada para responder a las preguntas de investigación, el tipo de investigación elegida fue teórica empírica, debido a que fue necesario realizar un diálogo teórico-empírico durante la investigación, el método empleado, fue el método hermenéutico-fenomenológico, para esta parte es importante precisar que los conocimientos obtenidos en la presente investigación fueron obtenidos en un gran porcentaje de las experiencias del personal que labora o ha venido laborando en esa unidad, es por dicho motivo que el método elegido es el que mejor apoya a la investigación, el escenario de estudio fueron las instalaciones de la compañía de guerra electrónica, ubicado en la 3ra Brigada de Comunicaciones, distrito de Tiabaya, provincia de Arequipa, departamento de Arequipa, las técnicas que se utilizaron fueron tres: entrevista, observación directa y análisis documental, cada una de estas se utilizaron con sus respectivos instrumentos. En el Capítulo IV "Análisis y Síntesis", el cual se desarrolló después del trabajo de campo, se emplearon los métodos de forma manual, en donde se establecieron unidades con sentido propio para posteriormente organizar la información por categorías, siempre buscando en todo momento responder a las preguntas de investigación planteadas. En el capítulo V "Diálogo Teórico-empírico", se confrontaron los resultados obtenidos en el análisis con la construcción de categorías y unidades con sentido procedentes de los autores teóricos que soportan o son la base de esta investigación, para finalmente abordar a las conclusiones y recomendaciones, las mismas que guardan relación con la hipótesis planteada al final de la investigación y que servirán para contribuir con las funciones del CITELE (Ciberdefensa y Telemática del Ejército).

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción de la realidad problemática.

Debido al avance tecnológico, se ha creado una nueva dimensión dentro del campo de batalla, esta dimensión es conocida como el ciberespacio, producto de esta nueva dimensión las naciones empezaron a establecer medidas para poder garantizar la seguridad de las informaciones en esta nueva dimensión, debido al empleo y la importancia que ha adquirido está en el manejo de centrales hidroeléctricas, manejo de sistemas de vigilancia y seguridad, sistemas financieros nacionales, entre otras que forman parte de los activos críticos nacionales. Dentro de este contexto es necesario la aplicación de medidas de ciberseguridad en donde las telecomunicaciones, la inteligencia de señales y la guerra electrónica forman parte de ella como todo o parte según el nivel de ejecución. En el Ejército del Perú se ha creado este año, el órgano de línea Ciberdefensa y Telemática del Ejército (CITELE), este comando cuenta en su organización con los departamentos de ciberseguridad y guerra electrónica, los cuales se vienen implementando y equipando de acuerdo a sus necesidades, el departamento de ciberseguridad en la actualidad viene formulando un proyecto que busque obtener las capacidades necesarias para realizar la protección de los sistemas informáticos en la institución, en el caso del departamento de guerra electrónica a pesar de la importancia con la cuenta para apoyar a la ciberseguridad, no cuenta actualmente con ningún proyecto de implementación que busque obtener capacidades en materia de guerra electrónica, a pesar que existe en la actualidad la compañía de guerra electrónica que fue creada con el DS N°018-2009 del 14 de julio del 2009, orgánica de la 3ra Brigada de Comunicaciones con sede en el distrito de Tiabaya, provincia de Arequipa, departamento de Arequipa, debido al tiempo transcurrido y por no haber sido empleada correctamente, es importante realizar un diagnóstico de la situación actual de dicha unidad, pudiendo encontrarnos con un desfase en instrucción y entrenamiento como en material y equipo. Además tenemos que considerar que actualmente el Ejército del Perú dentro de sus políticas institucionales se encuentra dentro de la etapa de la transformación, en donde se viene apoyando a través de los cambios que se deben realizar en sus respectivas armas y servicios. Con respecto al arma de comunicaciones, es importante plantear la necesidad de poder contar con las capacidades en ciberseguridad, pero antes debemos ejercer una completa administración y dominio del espectro electromagnético, intenciones que fueron rechazadas debido al abandono del proyecto por parte de la institución, esta

problemática también sucede en el aparato estatal, según Contraloría General de la República a través de su página web en la columna semanaeconomica.com, manifiesta que existen un total 1000 obras paralizadas o inconclusas a nivel nacional por un valor de más de S./16,000 millones de soles, por esta razón se busca la presentación de un proyecto de ley para garantizar la continuidad de los proyectos de inversión pública, pudiéndose interpretar que en el estado existe la actitud de no cumplir con la ejecución de los proyectos aprobados, normalmente por falta de fondos o falta de voluntad política, después de un tiempo de paralización en la ejecución del proyecto u obra, es necesario retomar la misma haciendo un previo análisis del estado del proyecto, con la intención de poder recomendar las formas de acción necesarias considerando la vigencia de la tecnología y las necesidades del mundo actual así como generar precedentes para futuras investigaciones. Debido a esto, se decidió analizar el estado actual en el que se encuentra la compañía en mención y de esta forma generar el conocimiento necesario que sirva de base a futuras investigaciones sobre el tema. De no realizar un diagnóstico real y oportuno, surge la posibilidad de que pierda la importancia debida por parte de la institución y no pueda ser considerado dentro del rol fundamental para la defensa y los nuevos roles institucionales como lucha contra el narcotráfico, contrabando, terrorismo y apoyo a la vigilancia de fronteras, otra problemática importante se hace evidente al no contar con el conocimiento en avance tecnológico en el contexto global sobre la tecnología en materia de guerra electrónica, y de ser así, ¿Se estará entrenando al personal especialista en guerra electrónica de forma adecuada? Teniendo en consideración que el activo principal de toda organización es el personal, se debe establecer su nivel de instrucción e entrenamiento y como se encuentra el material de comunicaciones y electrónica que dispone, por ello la presente investigación pretender establecer el estado actual de la compañía de guerra electrónica, centrándonos en la situación actual de su personal y material o equipo que dispone, con la finalidad de que esta investigación sirva como base para proyectos o estudios que busquen mejorar dicha situación.

1.2 Preguntas de Investigación.

¿Cuál es el estado actual de la instrucción y entrenamiento del personal especialista, en el tema específico de doctrina y empleo de guerra electrónica de la compañía de guerra electrónica de la 3ra Brigada de comunicaciones?

¿Cuál es el estado actual de disponibilidad y operatividad del material y equipo en el tema de comando y control que dispone la compañía de guerra electrónica de la 3ra Brigada de comunicaciones?

1.3 Objetivos de la investigación

Analizar el estado actual de la instrucción y entrenamiento del personal especialista, en el tema específico de doctrina y empleo de guerra electrónica de la compañía guerra de electrónica de la 3ra Brigada de comunicaciones.

Conocer el estado actual de disponibilidad y operatividad del material y equipo en el tema de comando y control que dispone la compañía de guerra de electrónica de la 3ra Brigada de comunicaciones.

1.4 Justificación y viabilidad.

La justificación de la presente investigación fue para que el CITELE (Ciberdefensa y Telemática del Ejército) conozca la situación actual de la compañía de guerra electrónica y de esta manera al contar con un diagnóstico real, pueda realizar las acciones necesarias para permitir la integración de la guerra electrónica con la ciberseguridad y así contribuir con la seguridad nacional. El aporte de esta investigación permitió la actualización de los conocimientos teóricos de guerra electrónica, así como la actualización del plan de estudios del curso básico de guerra electrónica, en la búsqueda de asignación presupuestaria y la realización adecuada de los procedimientos administrativos.

La viabilidad de esta investigación estuvo dada por la instrucción, la misma que es una actividad importante en las Fuerzas Armadas. Mantener al personal especializado con los conocimientos actuales y entrenado, permitirá que se cumpla la misión asignada al Ejército, la cual se encuentra contemplada en los roles estratégicos de las Fuerzas Armadas.

1.5 Delimitación de la investigación.

La investigación con respecto a la instrucción y entrenamiento del personal especialista alcanzó hasta los procedimientos del operador para la protección electrónica, los conocimientos básicos de soporte electrónico, ataque electrónico y telecomunicaciones. Con respecto al material y equipo, estos si contaban con los recursos técnicos necesarios anti-soporte y anti-ataque y si contaban con una infraestructura adecuada para realizar un completo ejercicio del comando y control.

1.6 Limitaciones de la investigación.

La presente investigación ha contado con pocos antecedentes sobre el estudio de la realidad de las operaciones de guerra electrónica y situación actual de una unidad de guerra electrónica en nuestra institución, de igual manera acceder a la organización y empleo de otras unidades de guerra electrónica de países extranjeros no fue factible, por el motivo que dicha información de carácter reservado es de suma importancia dentro de una organización militar y está relacionado directamente con la inteligencia de señales que trabaja en el plano estratégico-operacional de las Fuerzas Armadas de los países extranjeros.

CAPÍTULO II
ESTADO DEL CONOCIMIENTO

2.1 Antecedentes de la investigación.

2.1.1 Investigaciones Nacionales.

Gonzales, Goyzueta y Verán. (2017). La tesis cualitativa "*Empleo del personal especialista en guerra electrónica y producción de inteligencia de señales en la IV División de Ejército de la ESGE".* Tuvo como objetivos: Dilucidar la contribución del empleo del personal especialista en guerra electrónica con la producción de inteligencia de señales en la IV División de Ejército, explicar la contribución del contexto de las implicancias de estructura organizacional en el empleo del personal especialista en guerra electrónica con la producción de inteligencia de señales en la IV División de Ejército, analizar la contribución del contexto de significancia teórico-praxis en el empleo del personal especialista en guerra electrónica con la producción de inteligencia de señales en la IV División de Ejército; metodología: Fenomenología, teoría fundamentada e investigación acción. Concluyeron en su trabajo de investigación lo siguiente: la integración de los trabajos entre el personal especialista de guerra electrónica y el personal especialista en inteligencia de señales en la Compañía de Inteligencia N°114 en el VRAEM (Valle de los Ríos Apurímac, Ene y Mantaro), fue óptima debido a que se produjo la integración técnica en recolección de datos, situación que fue beneficiosa para su instrucción y entrenamiento en el campo de la guerra electrónica. Existe una mala administración del personal especialista en GE (Guerra Electrónica) debido a que hay personal que nunca ha trabajado en unidades de este tipo, dándole un empleo no adecuado para su preparación y entrenamiento. En el contexto teórico-praxis: el personal de agentes de inteligencia empleados como operadores de GE, no demostraron el mismo rendimiento que los operadores de comunicaciones, debido a su falta de formación básica como técnicos en telecomunicaciones. De forma general la producción de inteligencia de señales en la zona del VRAEM se incrementó con el empleo de los operadores de GE provenientes de la compañía de guerra electrónica, por lo que se evidenció el beneficio de contar con personal entrenado en GE para actuar en otros escenarios, por último de manera general los autores concluyen en que se debe mantener e incrementar el apoyo de la compañía de guerra electrónica a la Compañía de Inteligencia N° 114 del VRAEM porque es provechoso para el

entrenamiento de los operadores de GE y conveniente para la producción de inteligencia de señales en la IV División de Ejército en las operaciones contraterroristas.

Watson, F. (2015). "*Infodefensa"*. La Dirección de Contrataciones de Material (DIRCOMAT) de la Armada Peruana, a visto por conveniente la contratación de un servicio de asesoría especializado para el desarrollo del proyecto MAGE (Medidas de Apoyo a la Guerra Electrónica) Qhawax, que especifica la elaboración de un actual sistema de guerra electrónica que pueda llevar a cabo la interceptación de señales de radio frecuencia.

Se está desarrollando específicamente para la variante MAGE SMTI Qhawax Mk-01, el cual puede ser programado para la integración dentro de las fragatas misileras tipo LUPO, con las que cuenta la Armada Peruana.

La asesoría se encuentra dividida en cuatro ítems separados. El desarrollo de la ingeniería para el hardware de circuitos de alta frecuencia, así como la medición de microondas en laboratorio y campo para el diseño de sistemas de guerra electrónica.

Marina de Guerra del Perú (2019) *"La Armada del Perú continúa el desarrollo del proyecto Qhawax Mk-II de guerra electrónica"*. La Dirección de Alistamiento Naval requiere de los servicios de un contratista para la elaboración de programas informáticos, acondicionamiento definitivo del proyecto Qhawax MkII y para el acondicionamiento de antenas, receptores y consolas de operadores.

El proyecto Qhawax MkII tiene el objetivo de modernizar los sistemas MAGE de las fragatas LUPO que data de la década de los setenta, mediante la migración a nuevas tecnologías que permiten reducir el número de componentes del sistema, reduce o elimina la obsolescencia tecnológica, mejoras la presentación de la situación táctica, aumenta la capacidad operativa y simplifica los procesos de mantenimiento.

En el conjunto electrónico de la antena se utiliza tecnología DLVA (Detector Log Video Amplifiers) y SDLVA (Successive Detector Log Video Amplifiers) para reducir el número de partes RF (Radio Frecuencia) necesarias para la primera fase de recepción. Se emplea además tecnología FPGA (Field Programmable Gate Array)

para el análisis posterior de las señales detectadas, permitiendo el rápido desarrollo de prototipos, reduce la cantidad de electrónica y aumenta la confiabilidad.
La unidad de detección, elaboración y análisis digital tendrá una capacidad de detección superior al equipo original.

De acuerdo a la Marina de Guerra del Perú (MGP), la antena goniométrica, conformada por seis a ocho antenas tipo espiral de alta ganancia posicionada a 60° una respecto de la otra, detecta las señales de RF (Radio Frecuencia) en un ancho de banda de 1 a 18 Ghz. Las señales detectadas pasan por un detector amplificador logarítmico de video (DLVA) que detecta la envolvente de la señal de entrada de RF y la amplifica, generando dos salidas, la primera con conversión a señal de video y la segunda con la frecuencia detectada.

Cabe resaltar que este módulo tiene protección CW (Continuous Wave) y con la finalidad de evitar problemas derivados por la susceptibilidad electromagnética, se utilizará un prescaler que permitirá dividir 400 veces la frecuencia de salida del DLVA, eliminando la susceptibilidad durante la transmisión de la señal por la bajada de antena hacia el procesador del sistema.

El procesador está conformado por cuatro etapas de procesamiento, de acuerdo al siguiente detalle:

La primera etapa recibe la señal de video y la procesa para que el voltaje se encuentre dentro del rango de entrada requerido por el conversor A/D (Analógico-Digital). Además, recibe la señal de frecuencia para el proceso de identificación.

La segunda etapa es un convertidor A/D que se encargara de la conversión de la señal analógica a digital de los seis canales de antena. La conversión se realiza a alta frecuencia (desde 50nS) para aprovechar todo el ancho de banda disponible.

La tercera etapa es la integración, que tiene la tarea de introducir un umbral que define el nivel mínimo (threshold) que determina la validez de la señal elaborada. Sucesivamente la señal se integra resultando un pulso continuo cuya amplitud está constituida por el promedio de las muestras de la señal que se convierte.

La cuarta etapa correlaciona el video y la frecuencia entre las señales recibidas, organiza las bandas de recepción e identifica la frecuencia. En este punto, la señal de video se correlacionará con la señal de rumbo del girocompás para representar los 360° del horizonte de la unidad.

Finalmente, el "Adapter Video Software" realizara la tarea final para la visualización de los datos enviados a una PC o una consola multifuncional apta que represente el escenario a través de una conexión LAN (Local Área Network) de alta velocidad.

El sistema MAGE actualmente instalado en las fragatas LUPO mantiene una arquitectura conformada por 10 unidades, 7 de estas unidades en el mástil principal y 3 en el C.O.C. Utiliza asimismo guías de onda y cables especiales para bajar las señales de RF hasta la consola principal, necesitando de un continuo mantenimiento dada la gran cantidad de electrónica presente, en adición la consola cuenta con 4 TRC (Tubo de Rayos Catódicos) para la visualización de frecuencia video y análisis de las señales.

El proyecto presentado, representa una evolución de este MAGE, modificando el 90% de la arquitectura actual, sin modificaciones estructurales del mástil, ya que está conformado por una sola antena panorámica con mínima electrónica interna y solo un procesador o consola operativa.

Como en anteriores oportunidades en el desarrollo del proyecto Qhawax se han recabado cotizaciones de las empresas Maestrale S.A.C. y VAESD E.I.R.L.

2.1.2 Investigaciones Internacionales.

Gonzales (2004). En el proyecto previo a la obtención del título de ingeniero en electrónica y telecomunicaciones, "*Estudio y evaluación de las tecnologías aplicadas a la inteligencia de comunicaciones COMINT de la Escuela Politécnica Nacional, Quito - Ecuador".* Concluye en lo siguiente: La inteligencia de comunicaciones (COMINT) consiste en obtener información técnica de comunicaciones, procedente de la escucha de las comunicaciones extranjeras, teniendo la misión de obtener la

superioridad electromagnética en un campo de batalla. De igual manera la autora del proyecto menciona el estudio de la inteligencia de comunicaciones por ser un tema de táctica militar y la importancia que presenta en el contexto internacional, toma un aspecto confidencial, complicado y hasta cierto punto limitado en la búsqueda y obtención de la información, el propio Comando Conjunto de las Fuerzas Armadas de Ecuador cuenta con su propio sistema de COMINT (Inteligencia de Comunicaciones) hasta los 500 MHz y sistemas de perturbación hasta los 300 MHz. Para terminar la autora afirma que en su país no cuenta con un sistema de COMINT integrado, para lo cual requiere primero una entidad que tenga a su cargo entre otras tareas el mantenimiento de gestión del espectro electromagnético.

Según Koch, C. (2014). "*Guerra electrónica e informática en la guerra del mando y control".* Habiendo determinado el siguiente objetivo: comprender como se relaciona la guerra electrónica y la informática con la guerra del mando y control y, en su conjunto, con la guerra de maniobras, concluye que: las operaciones de información está conformado por seis capacidades: OPSEC (Operation Security), MILDEC (Military Deception), PSYOP (Psychological Deception), SO (Security Operation), EW (Electronic warfare) y CNO (Computer Network Operation), todas estas capacidades están íntimamente relacionadas, considerando para el autor que una acción de guerra electrónica o de CNO tiene alcance y repercusiones en OPSEC, MILDEC, PSYOP y SO, debido a esto la necesidad de asegurar el flujo de las informaciones ha dado pie a la creación de mallas capaces de enlazar en forma permanente a quienes requieran de ella, permitiendo la redundancia de los sistemas. Estas mallas están compuestas por nodos y enlaces de comunicaciones, los cuales permiten que la información sea procesada, almacenada y pueda circular por ella, este manejo de la información digital, acceso, uso y protección, negando al adversario el uso de la propia, ha generado un nuevo espacio o dimensión: el espacio virtual. De igual forma estableció la relación entre las actividades de CNO y la EW, el soporte electrónico y la inteligencia de señales se relaciona con la CNE (Computer Network Exploitation), debido a que ambas exploran sus diferentes áreas buscando información que pueda ser explotada de los sistemas adversarios, el ataque electrónico con las CNA (Computer Network Attack), debido a que ambas persiguen atacar a los sistemas adversarios para negar o degradar su funcionamiento o empleo, la protección electrónica y el SIGSEC (Signal Security) se relaciona con las CND

(Computer Network Defense) ya que ambas buscan proteger los sistemas propios de las acciones de operaciones de información del adversario. Por ende la guerra electrónica, la ciberguerra y las C2W (Command and Control Warfare) no se improvisan la tecnología sofisticada es parte de nuestras vidas diarias, tanto civil como militar, el buen uso de los medios empleados por gente capacitada es sinónimo de éxito en las operaciones, como factor multiplicador de la fuerza de combate en las maniobras, la falta de control del espectro electromagnético y del ciberespacio lleva a una fuerza a quedar sin "ojos ni oídos", perder movilidad, incluso al extremo de ser capaz de reaccionar, de obtener inteligencia, de organizar e integrar los medios necesarios para el combate, sincronizar, etc. De lo anterior se puede visualizar que la C2W y la dimensión humana son factores fundamentales en este proceso, debido a la imperiosa necesidad de contar con personal capacitado en C2 (Command and Control) y C2W, de igual forma el autor hace conocer que la guerra electrónica y la CNO avanza a la misma velocidad de los avances tecnológicos, no debiendo ignorar la importancia de este aspecto, finalmente en cumplimiento al objetivo impuesto al inicio del articulo concluye que: la relación entre la guerra electrónica y la informática con la guerra del mando y control y, en su conjunto con la guerra de maniobras está permitiendo el control de la información propia y del adversario haciendo posible el mando y control de las unidades en la guerra de maniobra, manteniendo el ciclo de la planificación propia, degradando la del adversario.

Michavila, B. (1984). "La *guerra electrónica y la electrónica en la guerra".* Habiendo determinado los siguientes objetivos: contribuir en los posible a fomentar la mentalización del personal de las fuerzas armadas en la importancia de la electrónica y en la idea que conviene potenciar los medios (personal y material) en el campo de la electrónica concediéndoles la misma prioridad que los sistemas de armas que apoyan. Concluyendo que: dado que todos los recursos de un ejército, sin duda alguna, el personal es el fundamental, porque el hombre es quien manda, dirige, opera y mantiene, administra los fondos, emplea el tiempo y le imprime dinamismo y personalidad a la fuerza, y solo el ser humano puede lograr que una organización sea eficaz, por ella es conveniente preparar al personal necesario en las fuerzas armadas en este campo de la actividad y colocar a los convenientemente dispuestos en conocimiento y experiencia en los puestos de actuación y sobre todo en los de mando y dirección.

Arellano, J. (2015). "*Interceptación, monitoreo y demodulación NXDN de señales digitales en tiempo real".* Habiendo determinado el siguiente objetivo general: diseñar, simular y evaluar un sistema para la monitorización, interceptación y demodulación de señales digitales NXDN (Next Generation Digital Narrowband) de voz sin encriptar en tiempo real. Como objetivos específicos: Aclarar conceptos y definiciones de Guerra Electrónica (GE) e inteligencia de señales (SIGINT), analizar el estándar NXDN y los diferentes componentes que lo comprenden de manera teórica, diseñar un sistema para la monitorización, interceptación y demodulación de señales digitales NXDN de voz sin encriptar en tiempo real, simular el diseño del sistema para monitorizar, interceptación y demodulación de señales digitales NXDN de voz sin encriptar en tiempo real. Concluyendo que: La guerra electrónica es un arma poderosa que permite control y uso del espectro electromagnético en contra de fuerzas enemigas para la toma inmediata de decisiones en el campo de batalla y se preocupa de las características técnicas de la tecnología a invertir, mientras que la inteligencia de señales es la inteligencia producida al recolectar y analizar la información que se transmite con la tecnología a invertir, además que no depende mucho del tiempo como la anterior, al fijar bien en la definición de interceptación es fácil entender que todo el proceso realizado en el diseño del sistema para la demodulación en tiempo real del estándar NXDN, para ser parte de esta MAE (Medida de Apoyo Electrónico), es decir la demodulación es parte de la interceptación, este diseño es eficiente para realizar la interceptación a transmisión de voz que usen el protocolo NXDN, más no para la transmisión de datos. Además permite obtener en tiempo real la información transmitida, algo muy relevante para la toma decisiones en el frente de batalla.

2.3 Teorías.

2.2.1 Definición de la guerra electrónica

Según, Jarpa, P. (2013) en su obra "*La Guerra Electrónica*" de la Academia Politécnica Militar, define a la guerra electrónica como el completo dominio del ambiente electromagnético, sabiendo que en la actualidad todos los sistemas de telecomunicaciones dependen de su uso, para poder lograr interconectar un sistema de redes que busca dotar a una organización de información completa y en tiempo

real, ahora dentro del proceso de toma de decisiones debemos referirnos al ciclo de comando y control (C2) que es estrechamente dependiente del espectro electromagnético, este ciclo busca utilizar de una forma más efectiva las actividades de vigilancia, adquisición de blancos, las comunicaciones y los sistemas de información. Si estas actividades son neutralizadas, el cerebro de la organización y el personal a su cargo no podrán cumplir con su misión. Por ejemplo sin enlace de comunicaciones el comandante no podrá escuchar, no podrá ordenar y no podrá visualizar. Por lo tanto, estas capacidades para poder conducir el soporte electrónico y el ataque electrónico y dominar el ambiente electromagnético son capacidades valoradas para las fuerzas en la actualidad, cabe redundar en conceptos básicos para entender la teoría que comprende la guerra electrónica (GE), la que dentro de la perspectiva del combate electrónico está definida como el uso del espectro electromagnético (EEM) para degradar o destruir la capacidad de combate de un adversario (incluyendo degradar o negar el uso del EEM así como degradar el desempeño del equipamiento del adversario, su personal e instalaciones) o proteger las capacidades de nuestras fuerzas. La importancia de estas actividades, están puestas en el empleo de las telecomunicaciones y sistemas que transmiten información, para este caso también se indica a los sistemas de armas o vigilancia, motivo por el cual se considera la aplicación de la GE dentro del nivel táctico y el principal blanco de la GE es descubrir la tecnología con la que cuenta el adversario.

2.2.2 Guerra electrónica de comunicaciones y no comunicaciones

Según, Jarpa, P. (2013) en su obra "*La guerra electrónica*" de la Academia Politécnica Militar, explica cómo se divide la guerra electrónica en dos campos principales: GE de comunicaciones y GE de no comunicaciones. En la GE de comunicaciones, su historia data de una antigüedad mayor a comparación con la de no comunicaciones, debido a ser el principal medio de comunicación dentro del campo de batalla en las guerras y conflictos registrados en la historia de la humanidad, específicamente dentro del espectro electromagnético se encuentra enmarcada las bandas de frecuencias que van desde high frecuency (HF) hasta el super high frecuency (SHF). La GE de no comunicaciones tuvo sus inicios en el empleo del sistema de vigilancia aéreo que diseñó Gran Bretaña en la Segunda Guerra Mundial, en donde uno de sus principales componentes fue el radar. El empleo del radar esta misionado a dar la alerta temprana a las fuerzas, en busca de la

protección de las plataformas o instalaciones importantes, dentro del escalonamiento de las fuerzas en un campo de batalla, las frecuencias de trabajo por lo general en este campo militar operan en bandas desde ultra high frecuency (UHF) y superiores. Para las actividades de GE, el adquirir datos del trasmisor enemigo es vital, debido a que estos son explotados con la finalidad de detectar la ubicación de una plataforma o equipamiento y determinar además sus fortalezas y/o capacidades.

2.2.3 División de la Guerra electrónica

Según, Jarpa, P. (2013) en su obra "*La guerra electrónica*" de la Academia Politécnica Militar, explica cómo se clasifica la guerra electrónica en dos campos importantes y en tres actividades principales en las que se basa la GE de comunicaciones y de no comunicaciones, aunque con diferente magnitud de aplicación:

Apoyo Electrónico, conocido como soporte electrónico (SE) en nuestra doctrina o medios de apoyo electrónico en entornos mundiales (MAE), forman parte de las actividades de la GE que involucra operaciones misionadas bajo la responsabilidad de un comandante operacional para obtener información mediante la búsqueda, monitoreo, identificación y localización de emisores electromagnéticos de comunicaciones y no comunicaciones, con la finalidad de obtener la inteligencia necesaria, vigilancia y reconocimiento del campo de batalla, buscando identificar los peligros producto de las operaciones tácticas del enemigo y la identificación del orden de batalla electromagnético del enemigo (OBE). En este (OBE) se determina la ubicación de todas las plataformas electromagnéticas de las unidades militares que conforman el dispositivo de la fuerza militar oponente, además se determinan características del equipamiento, frecuencias, potencia, modulación, polarización, localización y otras informaciones de importancia para posteriormente realizar el ataque electrónico.

Ataque Electrónico, anteriormente denominado contramedidas electrónicas (CME), es un campo de la GE en donde se utiliza la energía electromagnética irradiada con la finalidad de ejercer una acción en contra de las plataformas y puestos de comando que sirven a una arquitectura de mando y control (C2) del adversario, con la intención de atacar dichas ubicaciones buscando degradar o destruir la capacidad de combate

del enemigo. El ataque electrónico comprende la perturbación, el engaño electrónico, la destrucción física y la neutralización. La perturbación es la utilización de grandes cantidades de energía electromagnética para impedir que un equipo de comunicaciones o no comunicaciones reciba las señales necesarias para su empleo. El engaño electrónico se realiza mediante la trasmisión de comunicaciones simuladas o la modificación de las mismas señales del enemigo, buscando generar una confusión en el adversario. La destrucción física se realiza mediante el empleo de los sistemas de armas buscando colapsar las instalaciones físicas de los que se puede considerar como blancos de alto valor (OVE). La neutralización se conoce como el empleo de grandes concentraciones de energía electromagnética para paralizar o degradar permanentemente las posibilidades de las plataformas electromagnéticas del adversario.

Protección Electrónica, anteriormente conocido como medidas de protección electrónica o contra-contra medidas electrónicas (CCME), donde se utilizan medidas destinadas a cuidar al personal, instalaciones y equipamiento de las acciones de soporte electrónico y ataque electrónico propias o del enemigo que minimice, paralice o destruya las posibilidades de GE del adversario.

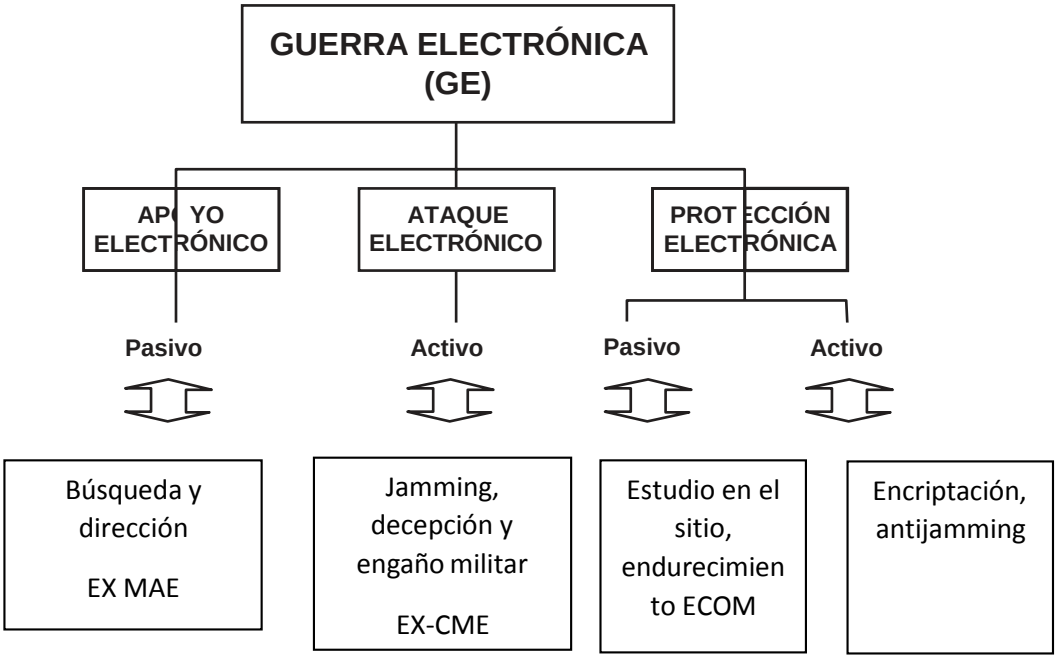
La GE está relacionada con la inteligencia de señales (SIGINT) que está distribuida en dos campos importantes: la inteligencia de comunicaciones (COMINT) y la inteligencia electrónica (ELINT). COMINT consigue las ondas electromagnéticas del campo de las comunicaciones adversarias con la finalidad de extraer conocimiento como una de las fuentes de inteligencia, posteriormente convertirla en información para la toma de decisiones. ELINT consigue las ondas electromagnéticas que no transportan información de parte del adversario con la finalidad de establecer la ubicación de los sistemas de vigilancia y monitoreo del enemigo para de esta manera desarrollar medidas de oposición, es la razón principal por la que los sistemas ELINT siempre obtienen considerables volúmenes de información a través de períodos de tiempo prolongado en provecho de obtener un estudio minucioso de los sistemas rivales. Esta separación de la inteligencia de señales (SIGINT) revela los campos en donde trabaja la GE tanto de comunicaciones y de no comunicaciones, pero su empleo se realiza en el nivel operativo-estratégico. Las diferencias entre la SIGINT y el apoyo electrónico radican en la finalidad de su empleo y a las organizaciones a las que sirven, definitivamente su empleo pasa por

el propósito de lograr la recolección de emisiones adversarias (ya sean de comunicaciones o de no-comunicaciones) con la finalidad de alarmar sobre su existencia rápidamente y disponer el empleo adecuado de las emisiones electromagnéticas hacia los sistemas de armas que están asociados a esas señales. Las emisiones detectadas deben ser bloqueadas (jammer) y su ubicación previamente detectada enviada a un sistema de respuesta como sistemas de armas para aplicar la degradación o destrucción física. Las emisiones detectadas de igual manera pueden ser utilizadas para realizar una alarma situacional, es decir, reconocer y ubicar a las fuerzas enemigas, sistemas de armas o capacidades electromagnéticas. El apoyo electrónico consigue mucha información proveniente de emisiones que buscan respaldar un proceso, haciéndolo más corto, con una gran cantidad de datos obtenidos mediante el empleo de un sistema, de esta manera establecer cuál de los tipos de nodos identificados se encuentran presentes y dónde están ubicados.

La GE además puede ser clasificada como defensa o ataque. El apoyo electrónico y el ataque electrónico buscan realizar acciones de ataque, bajo el criterio que son destinados a ser utilizados para afectar a un adversario y realizar acciones de búsqueda, interceptación, localización, análisis de nodos de comunicaciones y sistemas electrónicos enemigos mediante la perturbación, engaño electrónico y neutralización. El conocimiento de las estrategias en ataque, posibilidades y limitaciones es básico para el empleo efectivo del combate electrónico. La protección electrónica utiliza técnicas que en todo momento buscan proteger a nuestros emisores y cuidar el empleo del espectro electromagnético por parte de nuestros sistemas contra las acciones que buscan atacar a nuestras plataformas y puestos de comando. De igual manera, las técnicas de GE son conocidas como pasivas o activas según su naturaleza. Las actividades pasivas no son identificadas y son utilizadas generalmente en tiempo de paz sin mucha exposición al riesgo. Las medidas activas son identificables y su propagación deber ser regulada en la zona de operaciones y de ser utilizadas en tiempos anteriores a las operaciones deben ser empleadas bajo un férreo control.

Figura 1

Actividades de la Guerra Electrónica.



Nota. El gráfico representa las actividades que forman parte de la guerra electrónica. Tomado de *La guerra electrónica (p.32),* por P. Jarpa, 2013. Instituto Geográfico Militar.

2.2.4 Guerra electrónica de telecomunicaciones

Según, Jarpa, P. (2013) en su obra "*La guerra electrónica*" de la Academia Politécnica Militar, explica como la guerra electrónica actúa sobre las telecomunicaciones, iniciando con las comunicaciones tácticas, las mismas que son utilizadas de forma masiva en el campo de batalla, lo que constituye una importante apreciación en todas las acciones de la GE en el campo de las telecomunicaciones.

Las comunicaciones tácticas por lo general son utilizadas en las bandas militares dentro del rango de frecuencia de HF, VHF y UHF, así mismo se agregar a este tipo de comunicaciones, las emisiones de enlaces fijos punto a punto, satelitales y data links aire-tierra, en la siguiente tabla el escritor de la obra realiza una explicación de las formas de enlaces de comunicaciones de acuerdo al rango, tipo y aplicación militar.

Tabla 1

Enlaces de comunicaciones.

Rango	Tipo de enlace	Aplicación Militar
HF	Superficie punto a punto.	Comunicaciones tácticas de alcance ilimitado para nodos de comunicaciones de superficie.
VHF/UHF	Aire superficie y aire-aire	Comunicaciones tácticas de superficie en línea de vista, sistema de mando y control aéreo.
Microondas	Aire-superficie, repetidores aéreos y satelitales	Data Links aerotransportado, UAV, sistema de mando y control aéreo y de superficie.

Nota. Esta tabla explica las clases de enlaces de acuerdo a su clasificación por categoría de frecuencia en el ámbito militar.

La Naturaleza de las señales de comunicaciones

Las emisiones de comunicaciones contienen datos que van de un lugar hacia otro, por lo que se mueven en una dirección por naturaleza, sin embargo, la mayoría de nodos de comunicaciones actúan como receptores y trasmisores logrando la propagación en una dirección y en ambos sentidos. Esto es importante para los equipos de apoyo electrónico, debido a que por la naturaleza que como se propagan las señales electromagnéticas, solo el trasmisor es detectado. Específicamente las emisiones electromagnéticas del campo de las comunicaciones, presentan una modulación permanente y realizan un periodo de ocupación elevado, relacionado con las señales de radar. Historialmente, las comunicaciones han ocupado un sitio en las bandas HF, VHF y UHF empleando modulaciones AM o FM. Además, con el aumento de en la demanda del empleo de los UAV (vehículo aéreo no tripulado) y las comunicaciones satelitales, las emisiones electromagnéticas del tipo microondas son las más utilizadas. Debido a un tema técnico que específica que a mayor ancho de banda de la señal, la capacidad de poder trasmitir información por unidad de tiempo aumenta. Así mismo al aumentar la frecuencia por razones técnicas la capacidad del ancho de banda que vamos a obtener va ser la más óptima, pero así mismo al emplear emisiones electromagnéticas que comprende desde las microondas hacia algunas otras frecuencias superiores, el empleo de la línea de vista se hace

importante. Seguidamente, se exponen las dos clases de emisiones de comunicaciones fundamentales como una forma de aclarar y conocer las particularidades de las comunicaciones. Dichas señales se encuentran dentro del campo de las comunicaciones tácticas y los enlaces digitales o data links.

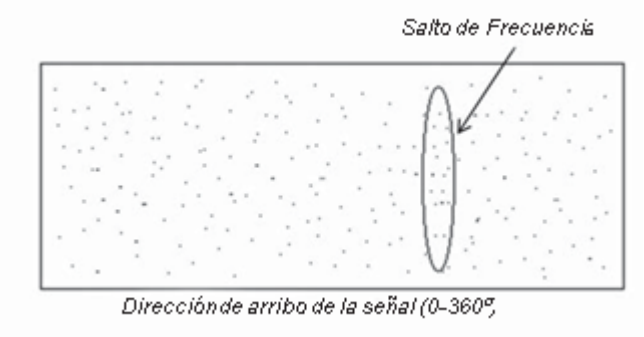
Comunicaciones Tácticas

Las emisiones electromagnéticas del campo de las comunicaciones tácticas se desarrollan como comunicaciones superficie-superficie, aire-superficie y aire-aire. Estas emisiones que se desarrollan en las bandas HF, VHF y UHF, presentan nodos de comunicaciones que utilizan trasmisores y receptores que emplean antenas con una cobertura de 360° en azimut. El uso de antenas tipo látigo es más frecuente en nodos de comunicaciones empleados para comunicaciones de superficie y las antenas tipo dipolo se utiliza comúnmente para estaciones aéreas montado en aeronaves. El uso de antenas isotrópicas permite tener enlaces sin la necesidad de conocer la ubicación del otro extremo del enlace. Una de las características de las antenas isotrópicas es la poca ganancia por lo que es necesario el uso de antenas directivas para lograr en el enlace entre estaciones fijas. Estas antenas proporcionan mayor ganancia y aislamiento de señales no deseadas. Otro aspecto importante en las comunicaciones tácticas es la cantidad de potencia irradiada la que se expresa en uno a varios watts de potencia efectiva irradiada (ERP) y los enlaces en comunicaciones tácticas trabajan sobre escasos kilómetros de distancia. También es importante conocer que los enlaces en HF necesitan una mayor distancia de propagación, debido a su empleo táctico, por lo que será necesario aplicar una ERP mayor por el tipo de propagación ionosfera que utiliza la banda de frecuencia HF. Continuando con las comunicaciones tácticas y utilizando el ejemplo superficie-aire y aire-superficie, las plataformas aéreas utilizan las bandas VHF y UHF presentando medidas extensas que se generan a razón de la comunicación a distancia, las mismas que necesitan de una amplia línea de vista. Los datos enviados mediante una conexión de comunicaciones táctica puede ser voz o data, ambos tipos de información puede ser cargada en formato digital y análogo. La seguridad para la trasmisión de datos se realiza mediante la encriptación de datos, el tipo de enlace debe realizarse en frecuencia fija o protegida de la detección y homming (acompañamiento por fuerza de señal), utilizando otro tipo de técnicas en donde encontramos al “espectro

ensanchado" (spread spectrum), siendo la más conocida en esta clase el salto de frecuencia. Las comunicaciones tácticas por lo general trabajan mediante sistemas del tipo "presiona y habla" (push to talk), es decir que operan a pedido del operador del equipo de comunicaciones, esta situación contempla varios receptores y trasmisores trabajando en la misma frecuencia, con solo una estación control de red comunicándose con los demás nodos a la vez. En condiciones tácticas del empleo de las comunicaciones, las emisiones se comportan intercaladamente con varios ángulos de llegada en la localización de la señal (azimut) y variación en las frecuencias, para esto cada monitor registrara una emisión por cada transmisor. Los enlaces siguientes del mismo nodo de comunicaciones expondrá puntos en la misma frecuencia y ángulo. Una exclusión es la emisión con salto de frecuencia que presenta una cantidad de frecuencias con el mismo ángulo de llegada.

Figura 2

Señales de comunicaciones tácticas



Nota. El gráfico representa las emisiones que intervienen en el tipo de comunicaciones tácticas apreciadas por un conjunto de interceptación de comunicaciones que se mueven dispersamente en frecuencia y ángulo de llegada Tomado de *La guerra electrónica* (p.82), por P. Jarpa, 2013. Instituto Geográfico Militar.

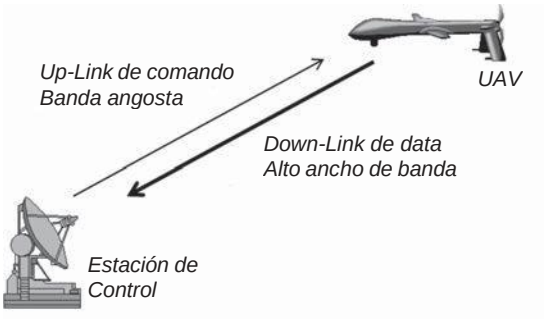
Enlaces de Data Digital (Digital Data Link)

Los enlaces de data transportan información digital en tipo de frecuencia que está dentro del rango de los microondas. Para este tipo de enlace, presentamos un ejemplo típico entre un UAV y una estación de control, según se presenta en la Figura 3, el UAV capta información desde la estación de control y envía la data recolectada a la misma estación. La señal que establece el control (o up-link), por lo general es de

banda estrecha, debido a que la información que tienden a ser enviada por la estación control, es relativamente baja. En el tema de seguridad las emisiones de la estación control hacia el móvil (up-link) emplean señales encriptados y presentando un elevado grado de spread spectrum (para proteger los canales de enlace). Estas medidas logran salvaguardar a la estación de control de las actividades de guerra electrónica que son empleadas por los sistemas enemigos puedan ejecutar, logrando hacer más difícil interferir el control del UAV.

Figura 3

Enlaces data link



Nota. El gráfico representa las comunicaciones entre los UAV y las estaciones de control, son data links digitales típicos. Tomado de *La guerra electrónica* (p.82), por P. Jarpa, 2013. Instituto Geográfico Militar.

Las comunicaciones entre el UAV y la estación de control es conocido como down-link, trasportando la información proveniente de los equipos de vigilancia o comunicaciones del UAV. Referente al tipo de ancho de banda, es técnicamente más amplia que la señal de la estación control debido a la cantidad información que debe ser enviada a la estación control. Los equipos que trasportan los UAV son equipos de captura de imágenes (televisión o forward looking infrared - FLIR) que requiere por lo general grandes cantidades de datos para el enlace radio eléctrico. Estas señales ubicadas dentro de las comunicaciones tácticas utilizan como medidas de seguridad la encriptación y la técnica del tipo spread spectrum. Así mismo, el uso de la banda ancha para la comunicación hace más complicado la cantidad de esparcimiento en frecuencia para poder ser aplicada. Los arreglos de antenas que conforman el up-link presentan un ancho de haz angosto, buscando conseguir la directividad al enlace y

haciéndolas difícil el trabajo de interceptar por parte de sistemas de localización de emisores hostiles. Las antenas del downlink son limitadas en tamaño debido a las acotadas dimensiones del fuselaje del UAV y a consideraciones aerodinámicas. Por esto, las antenas del downlink tienen una ganancia menor y un ancho del haz mayor que las del up-link y son principalmente omnidireccionales.

Enlaces Satelitales

Las comunicaciones satelitales se obtienen mediante emisiones electromagnéticas que trabajan normalmente en bandas de frecuencias del rango de las microondas, comunicando voz y datos a considerables trayectos. La finalidad de los satélites es de dotar acceso a varios clientes al mismo tiempo, por lo consiguiente sus emisiones electromagnéticas deben operar en rangos elevados de mega hertz para poder conseguir un ancho de banda adecuado. Además las empresas civiles y los institutos armados utilizan los satélites para sus comunicaciones atendiendo sus necesidades comerciales y militares. Dentro de estas necesidades comerciales de las empresas civiles contemplan las del servicio de televisión y telefonía, para satisfacer la demanda de la parte militar, se emplean satélites que van a proporcionar generalmente servicios similares con la modificación en temas de formato para las señales que se van a propagar, mostrando variaciones significativas en el tema de la seguridad, haciéndose necesario el empleo de señales encriptadas y pudiéndose agregar técnicas espectro ensanchado contribuyendo a la defensa anti perturbación. Regresando al tema de las comunicaciones tácticas, la experiencia obtenida mediante la práctica nos enseña que las comunicaciones en el rango de frecuencias de la banda en HF son complicadas, debido a que los parámetros sufren modificaciones de acuerdo al día, la estación del año, la localización y las condiciones atmosféricas, de la mano con el tipo de variación solar que modifica la actividad de las capas de la ionósfera. Las comunicaciones en la banda de HF presentan varios tipos de propagaciones pudiendo ser tipo línea vista, onda terrestre u onda espacial. Refiriéndonos al tema de propagación las emisiones electromagnéticas que trabajan en la banda de VHF y UHF no presentan problemas a comparación de las de HF, con desventaja que solo pueden ser empleadas para distancias cortas, pudiéndose emplear con línea de vista y onda terrestre. Para el campo de las microondas se tiene el conocimiento que su propagación requiere definitivamente características rigurosas

de línea vista y por la cantidad de energía que transporta la frecuencia en la que trabaja presenta un ancho de banda adecuado, transportando información de gran volumen a comparación de las señales HF, VHF y UHF. El aspecto de importancia en el tema de la guerra electrónica, es la de centrar el conocimiento en la forma en la que el ataque electrónico pueda realizar acciones en otra de las comunicaciones tácticas, enlaces data link o enlaces satelitales. Por tal motivo, se debe hacer referencia primeramente a las emisiones de espectro ensanchado, posteriormente debatir temas sobre el jamming, las mismas que representan a las señales de baja probabilidad de interceptación (LPI) en el campo de las comunicaciones.

Señales de Baja Probabilidad de Interceptación
(LPI - Low Probability of Intercept)

Según Jarpa, P. (2013) en su obra "*La guerra electrónica*", de la Academia Politécnica Militar indica que algunas emisiones dentro del campo de las comunicaciones y no comunicaciones presentan particularidades que pueden ser explotadas con la finalidad de disminuir los efectos de las actividades de la guerra electrónica del adversario, estas particularidades en el empleo de las emisiones electromagnéticas son conocidas como señales de baja probabilidad de interceptación (LPI). Para lograr explotar estas características en beneficio de la defensa electrónica es necesario aplicar ciertos parámetros como la combinación de antenas de haz angosto, aplicar baja potencia efectiva irradiada y modulación del tipo espectro ensanchado, con la finalidad de hacer dificultosa las actividades de búsqueda, interceptación, monitoreo y localización de la guerra electrónica del adversario.

El empleo de este tipo de señales por parte de los sistemas de mando y control propios busca en todo momento ser una dificultad para los sistemas de guerra electrónica del adversario, disminuyendo su capacidad de localización e interceptación. Para poder cumplir con los parámetros que rigen a las señales de baja probabilidad de interceptación es necesario que los operadores apliquen los conceptos de control de emisión, los mismos que significan el descenso de la potencia de transmisión que permita mantener una comunicación entre estaciones (de comunicaciones o no comunicaciones), manteniendo una adecuada razón S/N. Al emplear esta técnica definitivamente se ha logrado reducir la posibilidad de que las estaciones de monitoreo y localización del adversario logren descubrir la fuente de emisión de la

señal proveniente de nuestros sistemas de comunicaciones. Como siguiente medida para lograr la señal con baja probabilidad de interceptación (LPI) es utilizar antenas que emitan señales electromagnéticas estrechas y direccionadas, que cuenten en sus posibilidad con componentes que logren la supresión de otro tipo de lóbulos como los que emiten las antenas isotrópicas, esas emisiones son conocidas como lóbulos laterales, buscando en todo momento emitir señales de forma directiva hacia la estación donde se quiere establecer el enlace, de esta manera se consigue una vez más dificultar labor de los receptores enemigos. Si la duración de la señal disminuye, contribuye significativamente a mejorar el empleo de las señales de baja intensidad, debido a que los equipos de guerra electrónica del enemigo dispondrán de menos tiempo para encontrar la señal en frecuencia y por ende el ángulo de llegada de la señal, disminuyendo de esta forma el peligro de ser ubicados.

Además para lograr reducir aún más la capacidad de detección de los sistemas de guerra electrónica del adversario tenemos que aplicar la modulación de espectro ensanchado, la misma que divide la energía en toda la banda de frecuencia elegida de un comienzo y empleado lo mínimo de energía para lograr trasportar la información (ancho de banda de información) de la comunicaciones realizada. Realizando esa redistribución de la energía, busca reducir la intensidad de la señal que va a trasportar la información y ganando más ancho de banda en donde se va transportar principalmente el ruido, por lo que los operadores de guerra electrónica del adversario al querer interceptar dicha comunicación van a experimentar una reducción de su relación de S/N.

Señales Spread Spectrum (Espectro Ensanchado)

Según, Jarpa, P. (2013) en su obra "*La guerra electrónica*" de la Academia Politécnica Militar, explica que antes de ingresar al tema de perturbación o también conocido como Jamming de comunicaciones debemos referirnos a el concepto de señales spread spectrum o de baja probabilidad de interceptación (LPI), en el párrafo anterior se hizo una explicación breve sobre este concepto, por lo que volvemos a referirnos a esta técnica como la redistribución de energía sin un patrón definido sobre una cantidad de frecuencias más grande que la debida, con la intención de desplazar la data desde el transmisor al receptor. La cantidad de ancho de banda mínima requerida para una transmisión de comunicaciones es el ancho de banda que

transporta la información y el ancho de banda de transmisión es la frecuencia sobre la cual se distribuye la señal. De esta forma, las señales con baja probabilidad de interceptación es el producto del conjunto de técnicas realizadas sobre las emisiones electromagnéticas de tal forma que resulte casi imposible al adversario conocer nuestra ubicación y en especial poder averiguar información relevante sobre nuestros sistemas de mando y control, dificultando poder explotar la información en beneficio de su inteligencia. Para hacer posible la aplicación esta técnica es necesario disponer de un receptor que pueda volver a juntar la señal que fue transmitida inicialmente y paso a formar parte de un ancho de banda ampliado, por lo que es importante que el receptor este trabajando en armonía con el circuito ensanchador del transmisor, accediendo a que el receptor pueda procesar la señal que fue propagada en forma original y descartando la parte ensanchada de la información. El estado inicial de la señal confrontada con la señal ensanchada se muestra en la Figura 4.

Figura 4

Señal de espectro ensanchado

Nota. El gráfico representa la diferencia entre una señal de transmisión normal con su similar en espectro ensanchado, en donde se puede apreciar la elevada magnitud del ancho de banda y menor intensidad de señal utilizada. Tomado de *La guerra electrónica* (p.86), por P. Jarpa, 2013. Instituto Geográfico Militar.

Para dividir las señales de espectro ensanchado debemos referirnos a dos señales en específico, las señales de salto de frecuencia (frequency hopping) y las señales secuencia directa (direct sequence). Estas frecuencias presentan comportamientos

distintos ante la variación en la distribución de la señal original a un mayor ancho de banda, por lo consiguiente la diferencia en la distribución de potencia, frecuencia y tiempo para cada tipo de modulación, hace posible que se presenten distintas vulnerabilidades que van a ser explotadas por los equipos de perturbación o jamming adversarios.

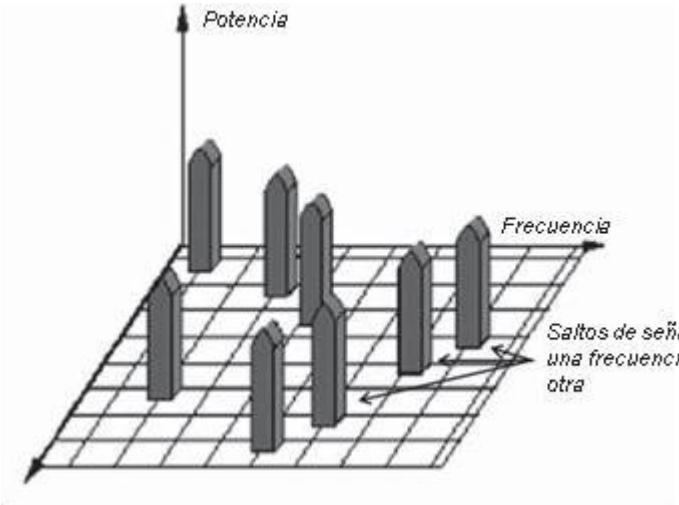
Señales con Salto de Frecuencia (Frequency Hopping - FH)

Según, Jarpa, P. (2013) en su obra "*La guerra electrónica*" de la Academia Politécnica Militar manifiesta que, las emisiones del tipo salto de frecuencia (Frequency Hopping-FH) trasladan la señal portadora con la comunicación, normalmente a frecuencias de transmisión aleatoriamente escogidas. Debido a esta técnica el receptor enemigo nunca pude conocer la secuencia de saltos, debido a que inicialmente los enlaces que son enviados por el receptor busca brincar coordinadamente de frecuencia en frecuencia en todo momento acompañado del trasmisor. El ciclo de saltos se presenta por debajo de los 10 milisegundos y en algunas circunstancias puede ser mucho menor. Tenemos que especificar que la técnica de señal ensanchada puede ser complicada en su aplicación para los enlaces militares, por esa circunstancia la técnica de salto de frecuencia es más considerable para las comunicaciones militares, es también importante precisar que la técnica de salto de frecuencia no es de uso exclusivo de la parte militar, son también empleadas en las comunicaciones civiles en donde son muy bien utilizadas para diferentes tipos de radiocomunicación utilizando un mismo rango de frecuencias y localización logran disminuir notablemente las intromisiones entre usuarios haciendo uso de esta técnica. Las emisiones de salto de frecuencia se encuentran clasificadas como señales baja probabilidad de interceptación (LPI), debido a que por la forma en la que se propagan mediante saltos sucesivos y a una rápida velocidad logra influir sobre el tiempo de ocupación en la frecuencia que de forma aleatoria ha sido seleccionado, ocupando esta durante el menor tiempo posible, haciendo difícil la labor de los equipos de búsqueda e interceptación del adversario, haciendo que su trabajo se torne complicado. Hay que definir que las emisiones de salto de frecuencia es utilizado para proteger el canal de comunicación, comprendiendo que solo su uso es para proteger el enlace entre estaciones de comunicaciones, debido a que existen conocedores que mediante una mala interpretación cometen el error de expresar que

se trata de una técnica de aseguramiento de información, correspondiéndole esa clasificación a la encriptación, lo que busca en todo momento las señales de salto de frecuencias es la protección del canal de transmisión. En la Figura 5 se puede apreciar una gráfica de una señal de salto de frecuencia versus tiempo y potencia.

Figura 5

Salto de frecuencia



Nota. El gráfico es la representación de una señal con salto de frecuencia versus tiempo y potencia. Tomado de *La guerra electrónica* (p.87), por P. Jarpa, 2013. Instituto Geográfico Militar.

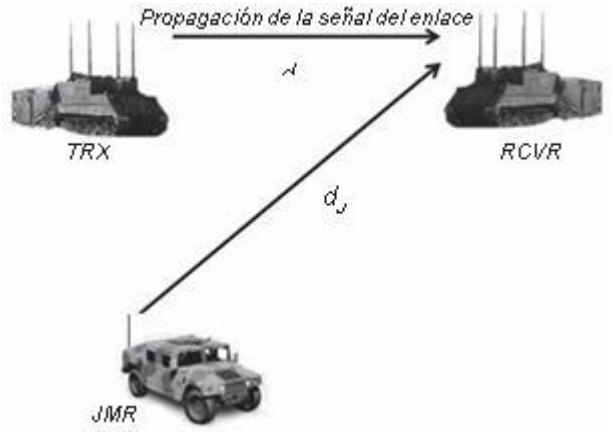
Jamming de Comunicaciones

Según, Jarpa, P. (2013) en su obra "*La guerra electrónica*" de la Academia Politécnica Militar, manifiesta que para realizar actividades de perturbación o también conocidas como jamming a una red de comunicaciones, se debe aplicar una irradiación de energía electromagnética de una potencia superior a la emitida por el trasmisor con la finalidad de evitar la comunicación entre los transceptores (emisor y receptor). Al hacer un análisis sobre la forma de cómo se realizan una actividad de ocultamiento de las emisiones electromagnéticas, podemos apoyarnos en las diferencias que implican estudiar las señales de radar, entonces hablemos de las diferencias primordiales entre ambos tipos de categorías dentro de la administración del espectro electromagnético como los son las ondas del campo de las comunicaciones y no comunicaciones, para el campo de las comunicaciones, a menudo se utiliza una técnica de interferencia basada en un cálculo geométrico para

una actividad de interferencia de señal. En las No comunicaciones, hablando específicamente del radar, para lograr una actividad de interferencia, técnicamente es diferente a lo establecido en el campo de las comunicaciones, debido a que en el tema del radar mantiene al transmisor y receptor en la misma ubicación y en el campo de las comunicaciones, podemos hacer referencia a que mientras un radar tiene tanto el transmisor como el receptor en la misma ubicación (generalmente), en un enlace de comunicaciones las condiciones varían, de acuerdo al empleo, debido a que el radar tiene al transmisor y receptor ubicados en el mismo sitio, situación que varía en el campo de las comunicaciones en donde el transmisor y receptor se encuentran separados en ubicación, buscando interferir netamente al receptor y si nos referimos a temas de ataque electrónico, solo se atacará al receptor. Para esta situación, debemos plantear el caso de un enlace con dos nodos que están en comunicación bidireccional, para que la perturbación o jamming logre tener efectos a ambos nodos, se debe emitir una irradiación electromagnética a un alto nivel de potencia buscando que mantenga una intensidad en ambas posiciones como para lograr una razón J/S superior a 1 en ambas, esta condición es representada en la Figura 6. Por este motivo, el sistema de perturbación o jammer , deben presentar una movilidad táctica para su empleo, evitando siempre mantenerse físicamente en el mismo lugar, mejor dicho debe ser completamente móvil posterior a su tarea de perturbar redes de comunicaciones. Estos jammers operan por lo general en dúo o parejas, en donde una estación transmite mientras el otro se está moviendo. La finalidad es la de lograr un jaiming permanente, evitando siempre la probabilidad de detección.

Figura 6

Geometría del jamming



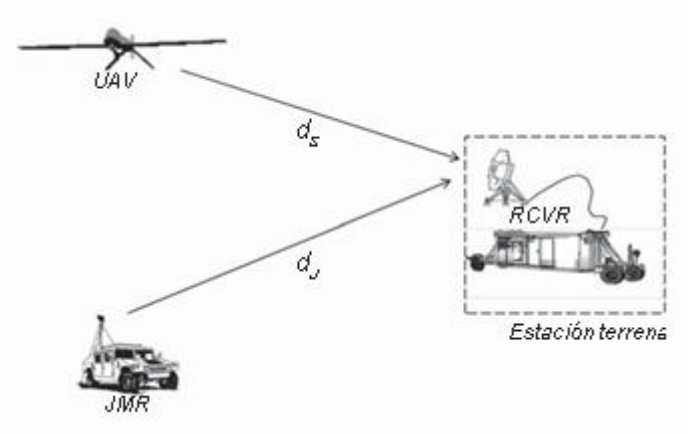
Nota. El gráfico representa la geometría del jamming de comunicaciones, tanto la señal de comunicación como del jamming van en el mismo sentido hacia el receptor. Tomado de *La guerra electrónica* (p.90), por P. Jarpa, 2013. Instituto Geográfico Militar.

El jamming es empleado para disminuir e interrumpir el empleo de nuestro mando y control, pudiendo ser utilizado para atacar sistemas de comunicaciones propios, obviamente para realizar acciones de perturbación o jamming, se debe contar con las informaciones recibidas de los elementos de apoyo electrónico, existe una forma de poder reducir las actividades de apoyo electrónico del adversario mediante el empleo de la perturbación o jamming, esta se realiza cuando los equipos de apoyo electrónico buscan transmitir la información obtenida sobre sus adversarios a sus puestos de mando o instalaciones de mando y control, esta actividad es conocida como enmascaramiento. El empleo de esta actividad de enmascaramiento ayuda al normal desempeño de nuestras redes de comunicaciones, debido a que reduce las actividades o misiones de apoyo electrónico del adversario. En ocasiones se pueden presentar casos en que la comunicación no se presenta un trasmisor o receptor, como puede ser el caso de una misión de vigilancia y reconocimiento llevado a cabo por parte de un vehículo aéreo no tripulado (UAV), en donde su sistema de navegación es la parte encargada de dar dirección al vuelo y el UAV solo se dedica a transmitir la información, como se puede apreciar en la Figura 7. En donde se puede apreciar que

las acciones de jamming se realizan sobre el data-link (o downlink), haciéndonos entender nuevamente que el tema de la interferencia es contra el receptor, que para este ejemplo se trata de una plataforma terrestre.

Figura 7

Ataque electrónico data link UAV.



Nota. El gráfico representa un jammer realizando una acción de perturbación o jamming sobre un data-link de UAV. Esta acción se realiza contra el receptor de la estación terrena. Tomado de *La guerra electrónica* (p.91), por P. Jarpa, 2013. Instituto Geográfico Militar.

Tocando el tema de las señales de radar, debemos centrarnos en las diferencias entre realizar el jamming para un sistema de radiocomunicaciones y un sistema de radares, la principal diferencia es la forma de propagación que utiliza las ondas de radar, las mismas que hacen un viaje de ida y vuelta al blanco, por lo tanto la señal recibida es inversamente proporcional a la distancia al blanco y es determinada por $1/R^4$. Como la potencia del jammer se trasmite solo en un sentido, solo se reduce por el cuadrado de la distancia ($1/R^2$). En jamming de comunicaciones, tanto la potencia de la señal transmitida y la potencia del jammer se reducen por el cuadrado de sus respectivas distancias.

La razón jamming a señal es representada por la siguiente ecuación:

$$\frac{J}{S} = \frac{(ERP)(G)(d^2)}{(ERP)(G)(d^2)}$$

$$\frac{J}{S} = \frac{R_J}{R_S}$$

ERPS es la potencia efectiva irradiada del transmisor; dJ es la distancia del jammer al receptor; dS es la distancia desde el transmisor al receptor; GRJ es la ganancia de la antena receptora hacia el jammer; GR es la ganancia de la antena receptora hacia el transmisor. Esta ecuación puede ser pasada a una notación en decibeles y queda de la siguiente forma:

$$J/S = ERPJ - ERPS + 20\log(dS) - 20\log(dJ) + GRJ - GR$$

Los elementos de esta fórmula son los mismos a los anteriores, pero las ERP se encuentran en unidades de dBm o dBw y las ganancias en dB. En ambas ecuaciones, las ERP son el producto (o suma en la ecuación en dB) de la potencia de salida del transmisor y la ganancia de la antena en la dirección del receptor. En comunicaciones tácticas, donde todos los participantes utilizan transceptores con antenas tipo látigo, la ganancia de la antena del receptor es simétrica en acimut, por lo que la ganancia hacia el jammer será la a misma que la ganancia hacia el transmisor, por lo que ambos términos terminan anulándose en la ecuación. Cuando se interfieren señales de comunicaciones de modulación análoga, es normalmente necesario alcanzar un valor superior a 1 en la razón J/S. Esto es necesario porque un operador en el receptor puede tener la habilidad suficiente como para escuchar la comunicación adaptivamente, es decir puede tener un oído entrenado como para extraer información del enlace a pesar de la existencia de ruido en este. En comunicaciones de voz y video análogo de baja calidad de transmisión, se pueden rellenar los tramos que resulten con mucho ruido siguiendo el contexto del mensaje o la información. Esto es real en comunicaciones militares tácticas, donde la información importante es enviada en formatos muy rígidos. Ejemplo de estos son el lenguaje convenido, el alfabeto fonético y el código Q en el caso de comunicaciones civiles. Cuando se interfieren señales de comunicaciones moduladas digitalmente, el ataque debe lograr que la señal recibida sea ilegible para el demodulador digital del receptor, para eso se puede interferir la sincronización o producir bits erróneos, pero como la sincronización tiende a ser muy robusta, la forma más básica de atacar estos enlaces es incrementando los bits erróneos. En términos generales, la señal recibida no se reduce mucho más por una J/S con valores mayores a uno, si no que bastará que la señal sea ilegible solo una tercera parte del tiempo, así será considerado inútil. Un

ejemplo práctico de cuando ocurre esto es cuando una radio con salto de frecuencia encuentra que una tercera parte de los canales sobre los que salta están ocupados por señales fuertes, así el enlace no se concretará. Esto significa que una señal digital solo necesita ser jammeada a una razón J/S de 0 dB durante una tercera parte del tiempo, mientras que una señal análoga requiere una razón J/S positiva durante el 100% del tiempo.

Jamming contra Señales Spread Spectrum

Según, Jarpa, P. (2013) en su obra "*La guerra electrónica*" de la Academia Politécnica Militar, en el tema del espectro ensanchado nos indica que es necesario explicar los fundamentos de la aplicación de las ecuaciones de jamming, las mismas que se utilizan para todo tipo de señales electromagnéticas, además la diferencia que existe cuando empleamos estas señales con baja probabilidad de interferencia (LPI), encuentra en el empleo del receptor que busca trabajar en coordinación con el transmisor en un espectro que se encuentra completamente ensanchado, logrando de esta forma poder disminuir la efectividad del jamming. En conclusión, la ventaja de la ganancia de procesamiento es la misma que la razón de ensanchamiento (el ancho de banda de transmisión/ el ancho de banda de información).

Jamming contra Señales Frequency Hopping (FH)

Según, Jarpa, P. (2013) en su obra "*La guerra electrónica*" de la Academia Politécnica Militar, hace referencia a los equipos de comunicaciones que dentro de sus características disponen de la posibilidad de poder realizar el salto de frecuencia (FH) se entiende que cuenta con la posibilidad de poder realizar actividades anti-jamming, esta virtud consiste en que el jammer solo tiene conocimiento del rango de salto total y debe dividir su potencia de transmisión sobre la totalidad de ese rango de frecuencias. Para que el trabajo del jamming sea efectivo contra un sistema de comunicaciones, la energía irradiada por el jamming, la misma que es propagada en un ancho de banda angosto, deberá saltar en la misma frecuencia que el receptor se encuentra saltando, la acción explicada tendrá cierto efecto sobre los sistemas de comunicaciones generando la interferencia requerida, pero de todas formas la efectividad del jamming no tendrá los resultados requeridos por lo que se puede

categorizar como un jamming bajo. Por este motivo y con la intención de realizar una mejor acción en el tema de Jamming, se requiere disponer de equipos de jamming sofisticados para interferir señales con salto de frecuencia. En el tema de las emisiones de salto de frecuencia que trabajan en velocidades bajas de salto, la acción que realizan este tipo de jamming solo va a permanecer en una frecuencia por corto período de salto, debido a que el sistema de jamming debe en todo momento conocer la frecuencia de transmisión y aplicar jamming al receptor víctima por el momento suficientemente necesario del período del salto para así evitar una comunicación exitosa. Cómo ya se explicó primero, el porcentaje de interferencia para un jamming que va llevar a cabo una acción sobre las señales digitales, debe ser del 33% del tiempo con una razón de J/S de 0 dB, para lo cual la potencia que va ser aplicar debe ser de tipo moderada. También existen tipos de jammer que interfiere cada salto se frecuencia de forma constante, estos perturbadores son conocidos como "jammer de seguimiento", estos equipos necesitan trabajar con subsistemas receptores y procesadores muy complejos, es necesario conocer que existen este tipo de equipos y que se encuentran disponibles como estado del arte en la tecnología contemporánea y que posibilitan una veloz medición de la frecuencia ubicada, resaltando además la velocidad que presenta para rechazar la posibilidad de poder transmitir información al adversario en cada uno de sus saltos, mediante la aplicación de la potencia necesaria por parte del transmisor del jammer.

Existen diferentes tipos de formas para poder interferir una emisión electromagnética que tiene como medida de protección de canal, al salto de frecuencia, esta acción se realiza mediante la interferencia parcial de la banda de trabajo. Para la aplicación de este método se debe calcular el ancho de banda total de la señal y conocer el nivel de potencia de señal que necesita el receptor durante su entrada, con estos parámetros podemos regular la potencia del jammer y dividirla sobre el total del rango de frecuencias, para esta situación se entiende que el jammer dispone de la potencia suficiente para igualar la potencia de la señal deseada en el receptor con cada uno de los saltos de frecuencias, de igual forma hay que presentar mucha atención al aplicar este tipo de jammer, debido a que pueden conducirnos al fratricidio pudiendo interferir paralelamente enlaces de comunicaciones de las fuerzas propias que se encuentran operando dentro del mismo rango de frecuencias. Existen formas de poder superar estos inconvenientes producidos por la aplicación de este tipo de jammer, la solución pasa por ubicar al jammer los más cerca posible al receptor

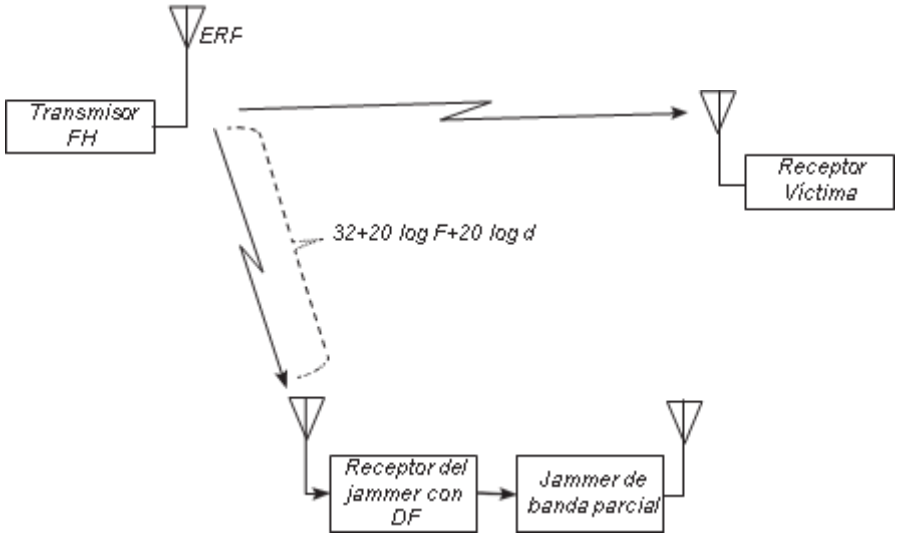
enemigo que se quiere afectar, logrando una interferencia efectiva con un gasto de potencia en lo menos posible y de esta forma cuidar las redes de comunicaciones propias y proteger las comunicaciones amigas. Con lo que respecta a las señales de espectro ensanchado, este tipo de empleo de jammer también son efectivos para producir la interferencia requerida para este tipo de señales con baja propabilidad de interferencia, y de esta forma evitar que se produzca el tránsito de información de forma normal entre los transceptores adversario, pudiéndose apreciar en la Figura 8, si se sabe dónde se encuentra el transmisor que va enviar la comunicación y se conoce a la vez la magnitud de la intensidad de la señal en el receptor del jammer, esto va a dar como resultado el cálculo de la ERP. Para este tipo de ejemplo se comprende que la estación que trasmite tiene una antena isotrópica vertical de un ¼ de onda, la situación es muy distinta cuando los trasmisores utilizan antenas direccionales, pero también existe una solución al respecto. La ERP del transmisor de la señal esperada es la intensidad de la señal (ajustada para la ganancia de la antena del receptor del jammer) ponderada por las pérdidas de propagación según la siguiente fórmula:

$$ERPS = PRJ - GRJ + 32 + 20\log F + 20\log dTJ$$

Donde ERPS es la potencia efectiva irradiada del transmisor de la señal deseada en dBm; PRJ es la potencia recibida en el receptor del jammer en dB; GRJ es la ganancia de la antena receptora del jammer en dB; F es la frecuencia de la señal deseada en MHZ y DTJ es la distancia desde el transmisor de la señal esperada al jammer.

Figura 8

Localizador del transmisor.



Nota. El gráfico representa la localización del transmisor, si este se conoce entonces el receptor del jammer puede determinar la ERP del transmisor desde la potencia de la señal recibida. Tomado de *La guerra electrónica* (p.95), por P. Jarpa, 2013. Instituto Geográfico Militar.

La ERPS determinada puede ser acomodada por disminución atmosférica y cualquier situación física de tipo lluvia y un tema de línea de vista de la antena transmisora si fuera necesario, así mismo la disminución de propagación será el primer factor de las pérdidas. Ahora, si queremos interferir dos estaciones de comunicaciones, mediante una acción de perturbación o jammer, se debe determinar la ubicación exacta del receptor y con dicho cálculo se puede establecer la distancia entre la estación que va trasmitir la información y el receptor que está a la espera del enlace. Para lo que se ha explicado anteriormente, debemos apoyarnos en la fórmula de pérdidas en el espacio libre:

$$LS = 32 + 20\log F + 20\log d$$

Basándonos en la anterior Figura 8, la ERP que era necesaria para poder jammear en enlace de comunicaciones era imprescindible lograr una razón J/S de 0 dB (dónde la señal de perturbación que iba recibir el receptor es similar a la potencia que esperaba

ser obtenida por el receptor enviada por el trasmisor del enlace), esto se pudo lograr debido a la determinación de los datos obtenidos entre el jammer y el receptor víctima, a cualquier frecuencia en el rango de saltos del enlace. Así mismo, para poder lograr efectos sobre las comunicaciones entre los transceptores. Las emisiones electromagnéticas productor de la acción de los jammers logran distribuir la potencia de su acción sobre la totalidad de la banda de frecuencias y así el emisor del jammer logrará establecer la potencia requerida en cada salto. Ahora de ser posible si los efectos del jammer pueden lograr interrumpir un tercio de los canales por donde la señal se transporta aleatoriamente, la acción del jammer es considerada eficiente, así no puede lograr interrumpir todos los canales del ancho de banda.

Señales de Jamming

Según, Jarpa, P. (2013) en su obra *"La guerra electrónica"* de la Academia Politécnica Militar, explica que para poder crear una señal de jamming, se recurre a la modulación sobre la portadora del canal a ser jammeado. Para poder conocer más sobre el tipo de señales de jamming se deben citar las más conocidas como son ruido modulado en frecuencia, ruido modulado en amplitud y morse (CW).

Para interrumpir una comunicación modulada en frecuencia o amplitud, se emplean el ruido modulado en frecuencia, ahora también se debe conocer las características del ancho de banda de la señal de jamming la misma que se produce mediante la unión del ancho de banda de la señal portadora y el indicador de modulación del modulador de frecuencia. Si nos referimos a que va a suceder si una señal de jamming de ruido modulado en frecuencia se emite con una potencia lo sumamente fuerte, sucedería una obstrucción completa del receptor FM, evitando que la señal original sea recibida, caso contrario si nos enfrentamos a una emisión de jamming también de ruido modulado en frecuencia pero débil en potencia, no obstruirá por completo la comunicaciones, solamente incrementara la taza de bits erróneos en la trasferencia de data e aumentara el ruido en los enlaces de voz. El mismo tipo de jamming solo aumentara ruido a las estaciones que trabajan en modulación AM, ocasionando la disminución en la claridad en la señal.

Si se desea afectar a una señal modulada en FM con un tipo de modulación en amplitud, es prácticamente imposible, al menos que la intensidad de la señal de ruido sea muy grande y pueda dañar la comunicación, el impacto de una señal de jamming

de ruido modulado en amplitud sobre una transmisión AM será incrementar el ruido en el receptor.

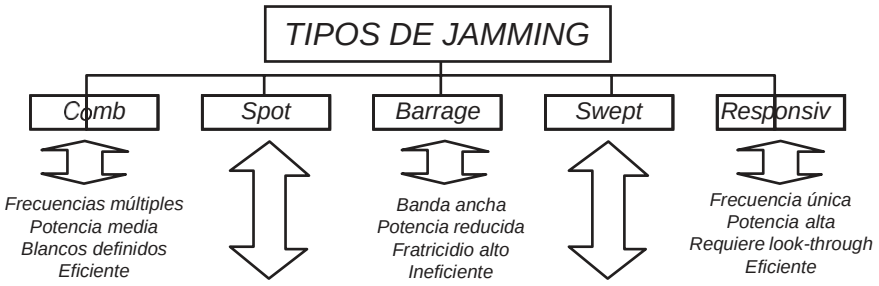
El jamming de CW solo es efectivo contra comunicaciones en modulación de frecuencia y amplitud, debido a que su aplicación solo implica usar una señal portadora, debido a que su nivel de señal es mucho mayor que la misma comunicación, el inconveniente del jamming CW es que es detectable, lo que lo hace más simple para poder superar las técnicas de protección electrónica.

Tipos de Jamming de Comunicaciones

Según, Jarpa, P. (2013) en su obra "*La guerra electrónica"* de la Academia Politécnica Militar, explica los diferentes tipos de jamming de comunicaciones que pueden ser empleados como se puede apreciar en la figura 9.

Figura 9

Tipos de jamming



Nota. El gráfico representa los tipos de jamming existentes en la guerra electronica. Tomado de *La guerra electrónica* (p.97), por P. Jarpa, 2013. Instituto Geográfico Militar.

.

El Spot Jamming

Según, Jarpa, P. (2013) en su obra "*La guerra electrónica*" de la Academia Politécnica Militar, explica la teoría del spot jamming, la misma que se realiza a través de un único canal de comunicaciones y consiste en producir una emisión de jamming mediante un transmisor que transporta la señal desde la banda base o portadora, hasta el canal que será jammeado y se diferencia de un transmisor de comunicaciones únicamente en su potencia de salida que es mayor y una antena que normalmente es directiva, este spot jamming para realizar su cometido, fabrica una

señal que se inicia desde una señal en banda base que normalmente se denomina ruido. Ahora como lo explica el autor anteriormente para aplicar el jammer, se necesita modular la señal irradiada en banda base en amplitud o frecuencia según como se encuentra trabajando el receptor victima que se quiere realizar una interferencia o paralización de sus comunicaciones, empezando por el conocimiento del ancho de banda de la señal que se va aplicar, debiendo ser el mismo ancho de banda del canal del sistema de mando y control víctima, teniendo en consideración que para realizar una acción de jamming, la potencia irradiada por el spot jamming debe ser mayor que la señal que va recibir el receptor víctima, este aparato está dotado de amplificadores de potencia. Para poder cumplir su cometido y dotado de una antena direccional la cual debe ser dirigida a la zona que se ubica el receptor víctima. Ahora en relación a la parte de empleo hay que precisar que utilizamos las antenas direccionales buscando elevar la potencia del jammer hacia el receptor víctima y buscando resta la potencia del mismo jammer evitando el daño colateral en contra de nuestros propios sistemas de comunicaciones, mediante la técnica que hemos precisado se busca obtener la ventaja al concentrar toda la potencia del jamming en un solo canal, lo que aumentara el impacto del jamming sobre un receptor sintonizado a ese canal. Después de haber tomado las medidas contra el daño colateral en nuestras propias, podemos además precisar que minimiza también el fratricidio debido a que las estaciones amigas que utilizan otros canales de comunicaciones no se verán dañadas sus comunicaciones. Refiriéndonos a las desventajas del spot jammer mencionemos que solo puede operar en un solo canal a la vez, y muestra una lentitud para poder cambiar de canal al momento de jammear, además no presenta un método adecuado para cambiar rápidamente el canal, la falta de flexibilidad se ha hecho evidente y una inadecuada forma de poder realizar el control solicitado. Cuando utilizamos el spot jammer, debemos aplicar una acción de interferencia por cortos periodos de tiempo para de estar forma posibilitar el empleo del apoyo electrónico amigo y evaluar su efectividad. Esta técnica puede ser no tomada en cuenta si los sistemas de apoyo electrónico (o COMINT), se encuentran a una distancia considerablemente alejada del jammer de tal forma que su receptor no será víctima de la interferencia provocada por la alta potencia de la señal del jammer.

Barrage Jamming o Jamming de Barrera

Según, Jarpa, P. (2013) en su obra "*La guerra electrónica*" de la Academia Politécnica Militar, explica que una señal de jamming es creada con la finalidad de interrumpir la comunicación de varios canales de comunicaciones, ahora para poder lograr esa acción existen varios tipos de jamming, el jamming de barrera es uno de estos tipos, en donde para poder aplicarlo se necesita la información de las frecuencias utilizadas en toda esa banda donde se va llevar acabo el enlace, la potencia que va utilizar se reparte a lo largo de un cantidad de canales, reduciendo la potencia del jammer en cada uno de los canales, si comparamos este tipo de jammer con el spot jammer vamos a descubrir que su impacto es más reducido. También debemos mencionar la modulación a la que debe ser sometida y el ancho de banda que debe contener, todo esto en banda base como indica la teoría, al igual que el spot jammer el tema de evitar el fratricidio es importante, debido a que colabora con mantener la seguridad y la disciplina, el empleo de una antena direccional buscara dotar de mayor seguridad a las fuerzas propias, reduciendo la propagación a direcciones en donde pueda bloquear comunicaciones amigas, dentro de la clasificación de los tipos de jammer , debemos indicar que un jammer de barrera barrage es más importante que con un spot jammer, a pesar que la potencia de salida en cada canal es más baja que en un spot jammer lo que va a reducir el impacto en las comunicaciones adversarias.

2.2.5 La Protección electrónica

Según, Jarpa, P. (2013) en su obra "La guerra electrónica" de la Academia Politécnica Militar, explica cómo el jamming impacta de diferente forma a los subsistemas de comunicaciones tácticas, lo que depende de las distancias entre el jammer y el blanco y el uso de las técnicas de protección electrónica que el blanco pueda hacer. La efectividad del jamming contra los sistemas de comunicaciones tácticas tiene una dependencia directa de las capacidades y la información generada por los sistemas de apoyo electrónico.

Tabla 2

Jamming de sistemas de comunicaciones tácticas, vulnerabilidades y medidas de protección.

Subsistemas de comunicaciones Tácticas	Vulnerabilidades	Protección
Troncales	Antenas altas	Antenas direccionales, larga distancia entre el receptor y el jammer.
CNR	Antenas Omnidireccionales, distancias cortas.	Salto de frecuencia.
Distribución de data táctica	Antenas omnidireccionales distancias cortas entre el receptor y el jammer.	Fuerte empleo de protección electrónica incluyendo spread sapectrum.
Aerotransportado	Los receptores de los up-links están expuestos.	Los receptores de los down-lins pueden ser protegidos de los jammers en tierra.

Nota. Esta tabla describe las vulnerabilidades y protecciones de cada subsistema de comunicaciones táctico.

Sistema Troncal Táctico

Según, Jarpa, P. (2013) en su obra "*La guerra electrónica*" de la Academia Politécnica Militar, sostiene que los sistemas troncales son más complicados interferir a comparación de los subsistemas de las redes de combate, debido a que su despliegue cumple la necesidad de satisfacer requerimientos operacionales, por lo que no son desplegados tan cerca a la zona de operaciones donde se realizan operaciones de combate. Este sistema troncal se encuentra desplegado mediante una cantidad de estaciones terminales y repetidoras que utilizan antenas direccionales, situación que hace difícil alcanzar los parámetros necesarios para que el jamming sea efectivo. Se puede emplear jammer aerotransportados que mediante el vuelo, logran superar ciertas barreras al respecto de una estación de jammer terrestre, al estar en vuelo y buscar realizar su acción contra un sistema troncal, solo puede interferir el enlace de comunicaciones en una sola dirección, debido que es muy difícil y arriesgado encontrar la ubicación adecuada para poder interferir un radio enlace en ambas direcciones dúplex, debido a que la única opción es la de estar posicionado

directamente en el medio de las dos antenas. Logrando alcanzar un bajo porcentaje de impacto sobre la red de comunicaciones que para ese caso debe estar operando en la banda de los microondas, por lo que si buscamos una administración adecuada de los recursos, no es muy remunerativo desplegar una estación aérea de jammer para poder interrumpir una comunicación en ese tipo de sistema, al menos que mediante esta acción busquemos anular un nodo importante en la comunicaciones adversarios

Jamming de Enlaces Satelitales

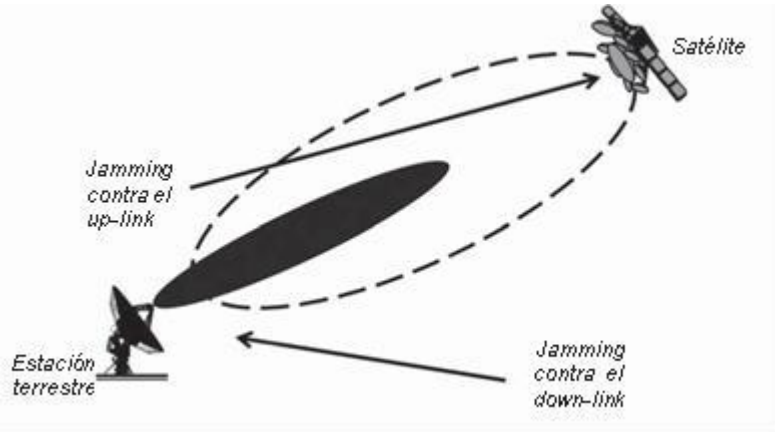
Según, Jarpa, P. (2013) en su obra "*La guerra electrónica*" de la Academia Politécnica Militar, explica que los enlaces troncales satelitales pueden ser interferidos mediante la aplicación del jammer, teniendo en cuenta aspectos tácticos propios de la propagación de este tipo de enlaces, para este tipo de comunicaciones como ha venido explicando el autor, se interfiere al receptor, debemos hacer esta explicación debido a que en las comunicaciones satelitales las estaciones poseen trasmisores y receptores localizados, pudiendo encontrarse separados a muchos kilómetros de distancia, siendo una de sus características los enlaces bidireccionales en donde al conocer la ubicación del transmisor podemos determinar la ubicación del receptor. Conocer estos aspectos es relevantes debido a que la separación entre estaciones hace necesario contar con antenas directivas de jamming en el 100% de los casos. La modulación empleada por lo general es digital, la figura 10 muestra la geometría del jamming de enlaces satelitales en donde se puede interferir el receptor del tramo de subida de la señal (up-link), que se encuentra en el satélite o el receptor del tramo de bajada de la señal (downlink), que se encuentra en la estación terrena. Al interferir el downlink se tiene una terminal satelital que por lo general tiene una antena direccional, por lo que se necesita a distancia cercana a la terminal satelital o aplicar una potencia de jamming elevada para poder aplicar una razón J/S necesaria para perturbar. Se espera generar la potencia suficiente en la perturbación con la intención de crear la cantidad necesaria de bits erróneos en la comunicación que de acuerdo a su modulación se trata de una comunicación digital, en el caso de que la estación de jammer por temas tácticos tenga que ubicarse a una distancia alejada a la estación terrena satelital, deberá aumentar la potencia del jammer para poder tener el efecto esperado. Normalmente, en el tema de la seguridad los enlaces satelitales también utilizan las señales con baja probabilidad de interferencia (LPI), empleando

niveles de espectro ensanchado (spread spectrum) y a su vez cuenta con un sistema de corrección de bits erróneos. Estas medidas de seguridad, aumenta las condiciones que se deben aplicar como es el aumento de potencia requerida para lograr una taza de bits erróneos adecuada para que el jamming cumpla con su cometido. Ahora, el factor a favor para poder aplicar un efectivo jamming para este tipo de comunicaciones, es la característica en la llegada de las emisiones electromagnéticas en los enlaces satelitales, los mismo que a su llegada a la superficie terrestre experimentan bajos niveles de intensidad, debido a las pérdidas de propagación. Considerando los tipos de comunicaciones satelitales muy distintos a las estaciones terrenas, tenemos los casos de los teléfonos satelitales y el GPS, en los cuales también se va aplicar el jamming, en donde para los teléfonos satelitales presentan antenas verticales isotrópicas de propagación omnidireccionales por razones de portabilidad y de uso en las comunicaciones civiles o militares, al utilizar este tipo de antenas experimentan pérdidas de propagación al no contar con un haz dirigido en busca de establecer un enlace con los satélites de órbita baja que debe operar haciendo que el seguimiento de los satélites sea impracticable. Esto tendría como consecuencia que los equipos de jammer puedan apreciar parámetros técnicos de la señal como la ganancia de antena que emite el teléfono hacia el satélite, pero sí de perturbar se refiere el jammer debe usar una antena direccional para optimizar su potencia hacia la localización del receptor (teléfono), la única protección del teléfono satelital similares a las estaciones terrenas satelitales, es la de modulación tipo spread spectrum y corrector de bits erróneos. Refiriéndonos al tema del GPS, el autor explica que no se trata de un sistema de comunicaciones satelital, por el contrario va trabajar como lo hace los equipos de radiodifusión pero dentro de un segmento satelital, siendo importante estudiarlo debido a que se puede indicar como un blanco dentro de la GE. Para poder realizar el jammer a este tipo de señal, se debe conocer primero el valor de la intensidad de señal recibida por el GPS, la misma que debido a las condiciones en la que se realiza es muy baja (en el orden de -150 dBm), ante el conocimiento de la parte técnica del orden de las señales de baja intensidad, se determina que para poder jammear la señal GPS, solo es necesario estar en línea de vista y producir la señal de jamming conveniente. Las emisiones GPS presentan niveles de espectro ensanchado, entre las más conocidas podemos nombrar a la pública conocida como “CA code” y otra de acceso muy restringido conocida como “P code”. Los valores de seguridad en el tema de antijamming para las emisiones del

tipo CA code está dentro de los 40dB, además emplea códigos abiertos, por lo que a pesar de la seguridad que presenta puede ser jammeada con radiaciones de jamming sumamente bajas, por otra parte las emisiones del tipo P code presentan una magnitud agregada de 40dB mayor a la de tipo "CA code" en espectro ensanchado y usan códigos seguros, por lo que para poder jammear una señal de GPS que trabaja con este tipo de seguridad, el jammer debe tener una potencia mayor a los 80 dB y de esta manera lograr la razón J/S adecuada. Entonces, teniendo el conocimiento que los equipos de comunicaciones que forman la estructura principal de un red de comando y control, cuenta con dispositivos del tipo de GPS que proporcionan información de localización, se puede asegurar bajo la teoría revisada que estos dispositivos operan con una señal del tipo P code en el tema de seguridad.

Figura 10

Jamming de comunicaciones.



Nota. El gráfico representa porque el jamming de comunicaciones satelitales, depende fuertemente de la geometría del escenario para el jamming. Tomado de *La guerra electrónica* (p.110), por P. Jarpa, 2013. Instituto Geográfico Militar.

Si buscamos realizar alguna actividad de ataque electrónico como interferir una señal satelital, tenemos que tener en cuenta la geometría que se forma desde la ubicación de la estación de jammer, el receptor satelital y el trasmisor, desde la ubicación de la estación del jammer no es difícil darse cuenta que para interferir el enlace de subida del sistema satelital es geométricamente menos complicado que hacerlo con el enlace de bajada. Esto se realiza debido a que el transponer satelital en su situación de receptor presenta su antena apuntando a la tierra y emite una señal hacia la tierra

denominada pisada satelital, que cubre gran parte de la superficie terrestre, la estación de jammer para esa circunstancia puede estar ubicado desde cualquier área que este dentro del 45% de la zona formada por la pisada satelital y de igual forma poder lograr su accionar de ataque electrónico contra el lóbulo principal. Dentro de este tipo de propagación que tiene los enlaces satelitales tenemos que nombrar nuevamente a las técnicas de seguridad como lo son spread spectrum y de corrección de bits erróneos, otro caso importante es referirnos a la señal de bajada que por características de los equipos de segmento satelital utiliza antena de haz angosto, que sucedería si el equipo de jammer no puede estar dentro del área que hemos indicado como pisada satelital, para este caso en busca de que el equipo de jammer logre superar la falta de acceso a gran parte del lóbulo de irradiación debido al empleo de antenas direccionales y las posibilidades de antijamming del enlace de subida. El aspecto más importante que se debe considerar es el problema en superar las pérdidas de propagación al momento interferir el enlace de subida, debido principalmente a la gran separación que presenta interferir a un trasponder satelital que está ubicado en una órbita alrededor del planeta, teniendo en este caso la estación de jammer aplicar una potencia mucho mayor que la de la estación en tierra que cumple funciones de trasmisor para de esta manera generar una cantidad necesaria por la razón J/S, el factor de seguridad antijamming y el aislamiento de la antena si corresponde.

Subsistemas de Redes de Radios de Combate (CNR)

Según, Jarpa, P. (2013) en su obra "*La guerra electrónica*" de la Academia Politécnica Militar, explica que una gran cantidad los equipos de jamming tácticos se preocupan en afectar a los subsistemas de las redes de radio de combate (CNR), debido a su empleo táctico, el mismo que siempre busca estar muy cerca de la línea de contacto en la zona de operaciones y además emplean emplean una propagación a los 360° debido al uso de antenas isotrópicas. La aplicación del jamming a este tipo de redes tácticas de comunicaciones, normalmente es dirigida a todas las estaciones que conforman una red, a otras estaciones en especial dentro de un área determinada o a una sola estación si se necesita. La finalidad de su accionar es la de evitar el enlace de comunicaciones no permitido la recepción de informaciones o forzar a una red encriptada a trabajar en un modo que atente contra su seguridad, permitiendo que los sistemas de apoyo electrónico o soporte electrónico puede generar la información

que necesitan para su beneficio, esta actividad es desarrollada de forma dificultosa por parte de las estaciones de jammer, debido a las técnicas de salto de frecuencia con la que cuentas los equipos de comunicaciones.

En el tema de empleo táctico de los jammers es necesario hablar de la movilidad con la que deben de contar con respecto a apoyo a una fuerza en particular, porque el sistema de jammers está montado sobre un vehículo en este caso va poseer una movilidad pero dicha movilidad puede ser limitada debido a los diferentes empleos que pueden tener la fuerza terrestre dentro de un campo de batalla. Si nos referimos al apoyo de jammer a una brigada mecanizada, necesariamente el jammer deberá estar montado en un vehículo con orugas para poder tener la misma movilidad o superior que la fuerza apoyada, volviendo al tema de la propagación, existen limitación para todo equipo que trasmite señales radioeléctricas en tierra debido a la curvatura del terreno, especialmente en la banda de frecuencias del VHF hacia arriba. Esta circunstancia también afecta a los perturbadores que trabajan en estas bandas de frecuencias. Esta situación de la curvatura de la tierra puede ser utilizada de forma provechosa, debido que ante un ataque electrónico de tipo jammer ante una estación de una red de comunicaciones se puede utilizar el terreno para poder ocultar el ataque del resto de las estaciones de la red, esta técnica se conoce como apantallamiento., esto acompañado de los detalle con llevan a despliegue de las antenas de jammer cuando un vehículo está en movimiento, algunos requieren que el vehículo este detenido y despliegue un mástil, la parte provechosa en el despliegue del mástil es la reducción en las pérdidas de propagación debido a la mayor altura de la antena y el consecuente aumento del rango de alcance. Un equipo de jammer comunicaciones militar tiene la posibilidad de atacar electrónicamente, mínimo una banda militar completa, por ejemplo, la banda HF desde los 2MHZ hasta los 30 MHz, o la banda VHF que va desde los 30MHZ hasta los 300 MHz. En la actualidad existen otros sistemas con la capacidad de atacar bandas de forma más amplia, pudiendo cubrir desde los 100 KHz hasta 1 GHz, teniendo además, la capacidad de actuar sobre varios canales a la misma vez, haciendo posible perturbar diferentes canales en una misma unidad de tiempo. Si hablamos de potencia con la que puede contar un jammer montado en un vehículo va desde 1KW hasta los 10KW, teniendo como fuente de energía a un banco de baterías o un generador fuera de la configuración del vehículo. En la configuración de una plataforma terrestre que opera como jammer, puede venir estas equipado con posibilidades que le permitan realizar apoyo electrónico, esto es

posible porque se le agrega en la parte modular de la plataforma terrestre , equipos de apoyo electrónico, buscando de esta forma obtener informaciones del momento que pueden ser explotadas por observadores avanzados, los mismos que pueden emplear para varios cometidos como la localización o tal vez destrucción física entregando esta información a los sistemas de apoyo de fuego, este equipo de apoyo electrónico debe operar sobre la misma frecuencia del jammer, pudiendo operar con receptores de ambas bandas, angostas o anchas, dependiendo lo que la situación táctica demande. Definitivamente cuando el jammer este en una condición de realizar su acción de ataque electrónico, el receptor de apoyo electrónico que trabaja en la misma estación de jammer, podrá explotar la información de las emisiones electromagnéticas que detecte en ese momento. Anteriormente el autor hizo referencia a los jammers en plataformas vehiculares, diferenciando a los vehiculares con ciertas condiciones para apoyar a brigadas mecanizadas, queda claro que las necesidad de empleo de estos jammers está sujeta a la necesidad táctica que se tiene que apoyar, por esto también debemos nombrar a los jammers portables, que por sus características son de poco peso con la intención de que sean operadores y cargados por soldados a pie, esta dotación de equipo obviamente está destinada a fuerzas que puedan emplear infantería a pie, si en caso todavía estuviera en sus organizaciones o también es el caso de las fuerzas especiales. La gran ventaja en estos equipos de jammer trasportable es la posibilidad de poder acercarlos en provecho de atacar receptores victimas que se ubiquen en áreas que no puedan ser accesible por vehículos motorizados o mecanizados, presentando la desventaja que no cuentan con la potencia suficiente que te puede brindar una configuración vehicular, esta desventaja nos lleva tener que buscar acercar siempre el equipo de jammer portátil lo más cerca posible al blanco electromagnético. Por razones técnicas y tácticas este equipo portátil trabaja con antenas cortas en longitud, por lo que definitivamente favorece la perdida en la emisión irradiada por el jammer al momento de aplicarle una perturbación al receptor. La configuración portátil hace difícil su empleo y transporte en condiciones no adecuadas para el desplazamiento a pie de las fuerzas, además no ofrece cubiertas adecuadas para poder darle supervivencia a las fuerzas, por lo que es necesario el empleo de árboles y todo tipo de características naturales con la intención de ofrecer elevación adicional para favorecer al empleo táctico del jammer. En lo referente a la capacidad del jammer portable para poder actuar sobre porciones del espectro electromagnético, es similar a las del jammer vehicular u otros

que trabajan en diferentes plataformas, igual que la capacidad de poder afectar diferentes tipos de canales de comunicaciones, la gran diferencia está relacionada con el tema de la potencia, siendo la potencia que puede emplear el jammer transportable desde 20 W hasta 100, el peso total es de máximo o15 kg, teniendo como limitación la autonomía de sus baterías, las mismas que solo puede asegurar algunas horas de duración. Además esta versión portable puede contar con un receptor de apoyo electrónico o soporte electrónico de banda angosta. En la figura 11 se puede visualizar las magnitudes de un equipo jammer manpack.

Figura 11

Equipo de ataque electrónico manpack

,

Nota. El gráfico representa una silueta de un soldado de infantería portando un jammer manpack. Tomado de *La guerra electrónica* (p.113), por P. Jarpa, 2013. Instituto Geográfico Militar.

También existen jammers aerotransportados que pueden ser empleados en plataformas aéreas como UAV, helicópteros o aeronaves de ala fija. Teniendo en cuenta el riesgo de la aplicación de la potencia del jammer puede afectar los sistemas de navegación de las aeronaves que se comportan como plataforma. La principal posibilidad de este tipo de jammers, es la de superar las limitaciones de la curvatura de la tierra, las mismas que afectan el desempeño de los jammers que operan en tierra, pero de igual manera pierden la capacidad de usar el terreno en otros aspectos como la de poder realizar un enmascaramiento en su ataque electrónico, al poder atacar un receptor y mediante la cubierta del terreno no afectar las demás estaciones de la red. Los jammers que operan en plataformas aerotransportadas de última generación en

versión de ala fija, tienen la posibilidad de poder actuar en el espectro electromagnético desde la banda más baja para las comunicaciones militares en el rango de HF hasta los 2GHZ, pudiendo actuar sobre las señales de equipos que trasmiten información y sobre los radares. Con respecto a su potencia, la configuración trasportable aérea, hace que pueda tener una buena capacidad con respecto a la potencia de salida, la misma que puede llegar hasta 1KW, pudiendo operar desde que se encuentran en el aire, debido a que la potencia está amarrada con los generadores de la aeronave, pudiendo atacar muchos canales de comunicación durante el vuelo. Además existen otras versiones de jammers aéreos que pertenecen a la clasificación de jammers táctico o mejor conocidos como UAV, teniendo como principal fortaleza su mayor capacidad de altitud en sus operaciones. Este tipo de jammers, obtiene la potencia necesaria para su vuelo y aplicar su jammer, de sus propias baterías. Existen otro tipo de aeronaves que pueden trasportar los jammers, pero este tipo de aeronaves con de capacidad mediana, lo que impide poder tener una capacidad elevada debido al peso del material y equipo. De igual forma como se explicó en las configuraciones anteriores de jammer, también puede estar acompañada de receptores de apoyo electrónico, contribuyendo a la labor de los sistemas de guerra electrónica propios, con la limitación de que este tipo de localizadores se vuelven vulnerables debido a la altura donde se encuentran realizando su accionar, esta deficiencia se ve aumentada debido al empleo de antenas omnidireccionales en este tipo de receptores. Por lo dicho hasta este punto, para realizar un jammer electrónico en este tipo de plataforma aéreas se necesita solo un transmisor, caso contrario para las plataformas terrestres que debido a las dificultades del terreno y la dificultad de desplegar las antenas, necesita de mínimo dos estaciones para poder realizar su ataque electrónico, además esta plataforma aérea como parte de un sistema requiere de elementos encargados de las actividades de mantenimiento y reabastecimiento en donde para esa tarea debe tener como mínimo hasta tres plataformas , teniendo la particularidad de que durante el reabastecimiento del vuelo, el transmisor de jammer no puede realizar ataques electrónicos. Antes de realizar un ataque electrónico aéreo, existe un trabajo de despliegue en donde para la cobertura, se requiere una operación al mismo tiempo en donde deberán intervenir un mínimo de dos plataformas de ataque electrónico de configuración aerotransportadas o de superficie, para frecuencias VHF y superiores, aunque esta capacidad se obtendrá de una mejor manera cuando se asignen misiones de jammer aéreas desde el nivel

operacional en donde esta asignación se llevara a cabo con un mínimo de dos jammers basados en tierra o tres plataformas de jammer aerotransportados. La capacidad necesaria será mayor a la de un canal, lo que se puede lograr destacando jammers del tipo multicanal o equipamiento jammer extra. Esta dialéctica se lograra teniendo como mínimo de tres jammers aerotransportados o dos jammers fijados en tierra lo que se necesita en el nivel operativo, cantidad que puede aumentar si en caso se requiere poder alcanzar la capacidad de exceso en esa capacidad, sin embargo, en el campo de batalla moderno, se puede emplear una cantidad exorbitada de jammers de acuerdo a la necesidad táctica que se pueda presentar y a la necesidad de la fuerza apoyada, es el resultado del compromiso de proveer una estructura de fuerza adecuada. Es importante mencionar que en este tipo de estudio, solo se están considerando las plataformas jammer en el sentido que deben realizar el ataque electrónico, bajo la situación en la que va realizar su acción lejos o en una posición que no genere daño alguno, por tal motivo no se están considerando posibilidades para poder protegerse de las amenazas que se puedan presentar producto de la acción del enemigo. Como se explicó en las anteriores configuraciones de equipos jammer, esta versión en plataformas aéreas, también deben actuar con su respectivo apoyo electrónico para poder tener el soporte de informaciones necesarios para afinar o mejorar las acciones de ataque electrónico, este acompañamiento puede formar parte de un sistema o ser un equipo aparte. El emplear las capacidades ataque electrónico y apoyo electrónico por separado, contribuye a limitar la flexibilidad y las condiciones positivas para poder atender a otras misiones de combate electrónico (apoyo y ataque electrónico), lo que hace reducen las capacidades de poder apoyar a la fuerza en su conjunto. Por lo general, se atiende la necesidad de actuar con una fuerza integrada por equipos de ataque electrónico que tienen su propia posibilidad de vigilancia, la que es incrementada, cuando se presente la situación, agregando equipos de soporte electrónico. Es claro que para la teoría explicada hasta este momento, definimos que el rol del ataque electrónico se puede desarrollar en operaciones convencionales hasta niveles operacionales, en el caso de otro tipo de operaciones que tengan una disposición táctica más extensa, se requiere un mayor número de sistemas de ataque electrónico, debido a los problemas que presenta siempre las características del terreno con las emisiones electromagnéticas. Al referirnos sobre el apoyo del ataque electrónico en niveles operacionales, se debe establecer sistemas que en magnitud estén en condiciones de apoyar dentro de ese

nivel, en donde el apoyo electrónico que se necesita para cumplir esas misiones, deben establecer la geometría necesaria, para eso siempre es necesario como mínimo tres dispositivos electrónicos, encargados de realizar la búsqueda y localización de señales electromagnéticas, como en el caso de los receptores electrónicos de apoyo que realizan localización de llegada de señal (DF - Direction Finder), se necesita para cumplir la localización de forma precisa dos estaciones o tres. En el caso del nivel operativo, se estima suficiente contar con un número de seis unidades y para el caso de plataformas aerotransportadas, este número se puede reducir a cuatro. Las actividades del apoyo electrónico como son la búsqueda, monitoreo, interceptación y localización DF, puede ser realizados con un único receptor, que debe ser de la tecnología adecuada a la época, es el caso de los receptores digitales que presente una velocidad propia de la tecnología en mención, estas actividades con la adición de la tecnología proporcionan a las funciones de búsqueda, interceptación y DF la velocidad necesaria en busca de aumentar el apoyo electrónico contra las cada vez más cortas señales, que cambian tan rápidamente en el campo de batalla.

Radio Localización de Emisores

Según, Jarpa, P. (2013) en su obra "*La guerra electrónica*" de la Academia Politécnica Militar, explica conceptos básicos en el tema de los emisores y receptores que van desde el nivel operacional hasta el nivel táctico, en donde para poder ejercer el control adecuado deben inevitablemente enviar señales electromagnéticas hacia elementos militares que se encuentren posicionados en sectores o aéreas preparadas para poder conducir las operaciones militares, independientemente del tipo de elemento que se encuentre ubicado para realizar su actividad como pueden ser del tipo de blindados, infantería a pie, aeronaves y/u otros, que tienen la misión de reportarse o simplemente entregar información útil a sus unidades y puestos de mando, ejecutando su misión y cerrar el ciclo de comando y control (C2). En este tema de formar redes y nodos de comunicaciones rescata la importancia de la seguridad ante la guerra electrónica adversaria, debido a que las estaciones de comunicaciones a simple vista pueden ser visibles para los elementos de vigilancia y reconocimiento o pueden volverse invisibles mediante la mimetización en el terreno, ante la niebla o accidentes geográficos, situación que no se presenta de la misma manera ante las emisiones electromagnéticas que son las mismas que pueden delatar

la ubicación de las mismas ante un mal empleo de las medidas de seguridad, situación que es aprovechada por las estaciones de apoyo electrónico y el empleo de estaciones de jammer. Del trabajo de las estaciones de apoyo electrónico se puede determinar la ubicación. Un análisis inmediato de las señales transmitidas desde su ubicación permite identificar a las fuerzas desplegadas, pudiendo ser estas del tipo de unidades terrestres, aéreas o navales, para este tipo de acciones se deben realizar medidas de protección con la finalidad de evitar la localización, identificación y movimiento de las tropas, evitando la posibilidad de que el orden de batalla propio sea develado por parte de la fuerza oponente, del conocimiento de estas informaciones van a determinar la entrega de la información que permitirá establecer la ubicación de blancos y perfeccionando la configuración de sensores ópticos de búsqueda. Todo lo precisado anteriormente expresa la posibilidad esencial de la GE y la SIGINT de poder ubicar fuentes de trasmisión de información de emisión enemigas, que normalmente son llamadas como Direction Finding (DF). La necesidad de poder ubicar a los emisores electrónicos antagonistas parte de un requerimiento de los equipos de inteligencia de señales y GE debido que necesitan ubicar señales electromagnéticas para cubrir necesidades de información para la planificación a nivel estratégico, ahora el tema de la precisión para la ubicación depende del alcance real de los sistemas de armas que se utilizan para destruir los objetivos sistematizados por la información que se determinó en la ubicación geográfica de cada estación y esa precisión está sujeta a la necesidad de conocer la situación táctica que se está desarrollando en ese momento. El conocimiento obtenido es la base para conocer el OEB, que se plasma en archivos con variedad de formatos en donde se encuentra la ubicación en precisión, data completa, en relación a las clases y números de sistemas electrónicos disponibles en la composición del enemigo y que será empleado con la finalidad de degradar a las fuerzas propias. En muchas circunstancias la calidad de la resolución obtenida es más importante que la simple ubicación geográfica de sus nodos. Se conoce como resolución al grado en el que se determina un direction finding (DF) mediante el conocimiento de la cantidad de emisores que se encuentran dentro del margen de operatividad que trabajan los equipos. En conclusión, los equipos que buscan data para poder obtener la información suficiente para poder contar con la información suficiente para obtener el OEB, requiere la cantidad necesaria de resolución para localizar emisores que se encuentren trabajando dentro

de un sistema de mando y control, discriminarlos, obtener parámetros y comunicar este conocimiento para que sea inscrito en el OEB.

Tabla 3

Detalles sobre los objetivos de la ubicación de emisores.

Objetivo	Valor	Exactitud requerida
Orden electrónico de batalla (OBE)	Ubicación de la clase de estaciones relacionadas con los sistemas de mando y control y batallones sabiendo la magnitud de las tropas del enemigo, situación y misión.	Medida= 1km
Localización de sensores de armas (autoprotección)	Otorga el conocimiento de la potencia del jamming o maniobrar para reducir las amenazas.	Baja un ángulo general y un rango =5 km.
Localización de sensores de armas (autoprotección)	Permite detener amenazas contra otro tipo de adversarios.	Media =1km
Localización de instalaciones adversarias.	Permite la búsqueda y reconocimiento y seguimiento de señales por medio de dispositivos del tipo homming.	Media-5km
Localización de blancos de precisión.	Permite el ataque directo por bombas inertes o artillería.	Alta=100m

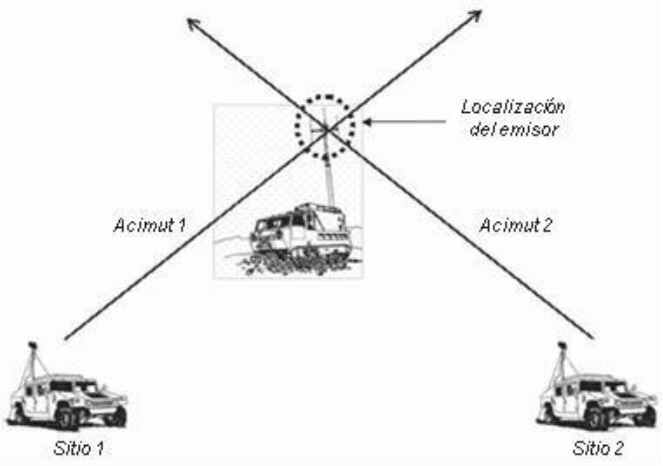
Nota. Esta tabla muestra la exactitud requerida por cada uno de los objetivos con su respectivo valor.

La constante forma de técnicas para ocultar señales a través de diferencia de sus datos en la información, las mismas que se utilizan en el salto de frecuencia y la frecuencia aleatoria de repetición de pulsos, han logrado que localizar a las estaciones adversarias se convierta en la posibilidad más relevante para los equipos DF hasta el día de hoy. El método empleado como pulsos o los saltos de señales en la trasmisión

de datos en su ubicación es la forma más conocida de determinar que esas señales son provenientes de la misma emisora y es la forma más conocida o común de poder reunir la información necesaria para reconocer y tener una exactitud de conocer a que amenaza se pueden enfrentar. Para lograr ubicar a los emisores adversarios se deben emplear una o varias técnicas de localización que pasaremos a explicar brevemente, después de haber logrado establecer resultados producto de una técnica se pueden combinar con otras técnicas para aclarar las dudas o afinar los resultados. Cuando ubicamos a un emisor entre la intersección de dos líneas formadas por el ángulo de llegada de cada una de las estaciones de localización es conocida como triangulación. El ángulo de llegada se forma por las líneas que se interceptan, ambas líneas corresponden al azimut desde dónde la señal es tomada de dos estaciones de apoyo electrónico diferentes, según se puede ver en la figura 12. Además de poder conocer el ángulo de llegada de las señales electromagnéticas es importante determinar tres dimensiones, las dos primeras son el azimut de llegada de dos estaciones y la tercera es la elevación del arribo de la señal, para eso es necesario contar con otra estación que será la tercera de interceptación, de tal forma que la localización se realiza bajo la técnica de ubicación mediante tres líneas, donde esa línea se comporta como la que va a dar una exactitud de la localización, debido a que si se genera un error en una de las líneas de llegada se va producir un grave error.

Figura 12

Triangulación electrónica

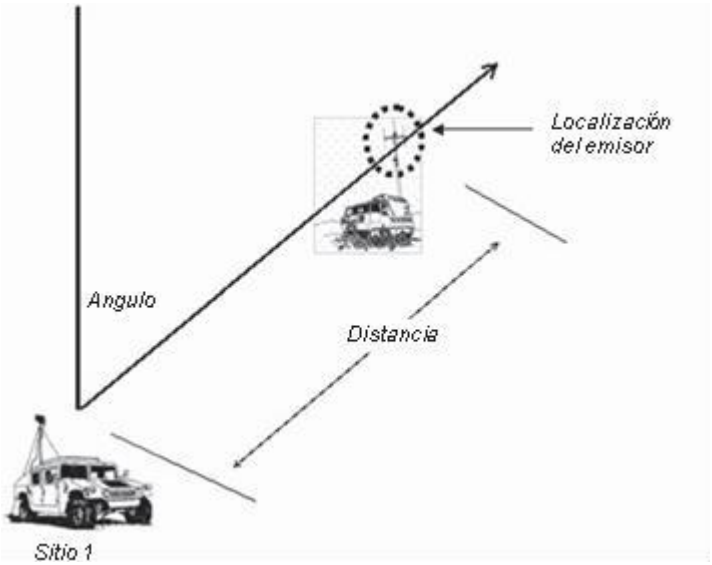


Nota. El gráfico representa que la triangulación implica tomar medidas del ángulo de arribo de la señal (acimut), desde más de un sitio, por uno o más sistemas interceptores. Tomado de *La guerra electrónica* (p.119), por P. Jarpa, 2013. Instituto Geográfico Militar.

Para explicar la segunda técnica, debemos precisar que en este método solo existe de acuerdo a una necesidad táctica, esta técnica se materializa mediante el empleo de una sola estación de apoyo electrónico la cual solo va tener que registrar únicamente la medición del ángulo y la distancia entre el interceptor y la estación emisora. Esta técnica es muy similar a la forma de empleo de los radares, ya que mediante la emisión de una señal puede obtener patrones de ángulo y distancia mediante la variación de la señal al tocar el objeto o blanco que desea determinar. Estos radares para la aplicación en los equipos de GE y SIGINT utilizan el procedimiento conocido como pasivos, son los que el autor explico en el párrafo anterior, estas estaciones de ubicación desde un punto determinado desde un planeamiento operacional-táctico, normalmente sirven en lugares no muy cercanos a la zona de combate, desde donde lograran determinar distancias mediante la interceptación de emisiones, normalmente de bandas de frecuencias del tipo de comunicaciones, específicamente en el rango de del HF ver figura 13, logrando identificar el ángulo de elevación de la señal, que proviene del resultado del fenómeno que produce en las capas de la atmosfera, específicamente en la ionosfera, este fenómeno técnica se lleva acabo debido a un periodo constante de refracciones sucesivas de una porción de la onda electromagnética que ha realizado un propagación mediante la onda espacial o también conocida como onda ionosfera, mediante la medición de la señal obtenida a través de este fenómeno se obtiene el ángulo de llegada. Por otro lado, en el campo de las no-comunicaciones, se presenta el empleo de las plataformas aéreas, en el cual los radares conocidos como Radares Warning Receivers (RWR), buscan conocer parámetros técnicos de este tipo de señales como, la potencia de la señal recibida y establecer la distancia al radar (cuya potencia ya es conocida). Esta técnica, para ubicar emisores mediante una sola estación de apoyo electrónico para la banda de comunicaciones y no-comunicaciones, es conocida por su baja efectividad en ubicación de los trasmisores adversarios.

Figura 13

Localización vertical



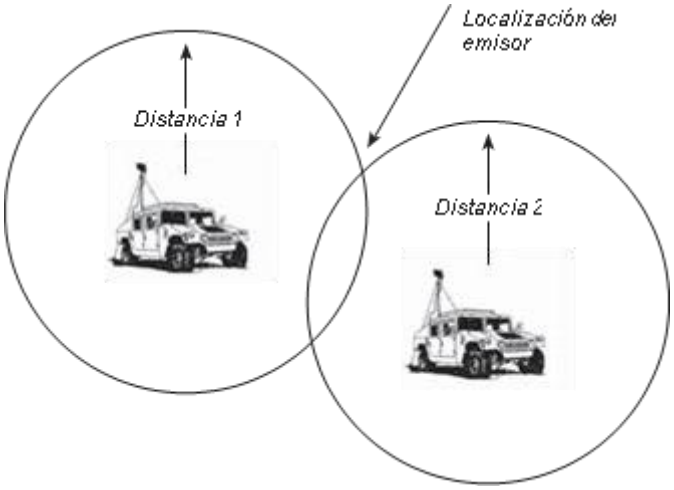
Nota. El gráfico representa la técnica de la localización vertical. Para esta técnica (medición de ángulo y distancia desde solo un sitio de interceptación), el receptor de apoyo electrónico determina la distancia en base a la intensidad de la señal que lleva a captar procedente de la ionosfera. Tomado de *La guerra electrónica* (p.120), por P. Jarpa, 2013. Instituto Geográfico Militar.

Cabe señalar que al comienzo de la explicación sobre la triangulación, el autor especificó que existían tres técnicas, la tercera técnica corresponde a la localización que se realiza mediante la bifurcación de dos arcos de radios (ver figura 14). Debido a la utilización de esta técnica se produce una problema para la GE y la SIGINT, las que utilizan estos procedimientos para poder obtener el OBE, debido a que la localización que se realiza mediante la interceptación en dos puntos distintos, se presenta una problemática ¿cuál de estos es la localización del emisor? Para resolver dicho problema se utiliza forzosamente otra técnica que complemente la que estamos explicando buscando despejar la ambigüedad. Ahora para poder medir el espacio entre la estación de apoyo electrónico y el trasmisor enemigo no cooperativo, se hace dificultoso debido a la forma de comportamiento de sus emisiones, las mismas que se comportan de forma pasiva y sin exactitud, debiendo emplear equipos que busquen medir la diferencia del tiempo de llegada de las emisiones, las que me van a dar una

ubicación con mejores datos de precisión en la ubicación, presentando variaciones de magnitud insignificantes.

Figura 14

Localización por medición de distancias.



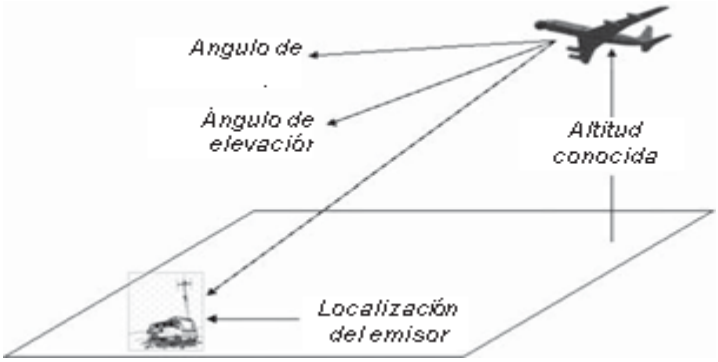
Nota. El gráfico representa la localización por medios de distancias. Para la técnica representada mediante la figura, el receptor de apoyo electrónico realiza su localización mediante la interceptación en los arcos que se producen debido a los campos eléctricos que están confluyendo de la emisión de las comunicaciones adversarias, debido a que lo datos que se van a obtener no son precisos es necesario el apoyo de otra técnica. Tomado de *La guerra electrónica* (p.121), por P. Jarpa, 2013. Instituto Geográfico Militar.

La cuarta técnica está relacionada al empleo operacional-estratégico que implica la utilización de la SIGINT, en este caso emplea vehículos aéreos, en donde va a entregar los datos necesarios en base a tres parámetros, el primero es el ángulo en el que se encuentra la aeronave con respecto al horizonte, el segundo el ángulo de llegada de la señal electromagnética y como tercer parámetro es la altura en la que se encuentra el vehículo aéreo, en base a estos parámetros se puede hallar la distancia y el azimut en el que se encuentra el trasmisor enemigo, logrando afinar el DF del receptor de apoyo electrónico. Un ejemplo apropiado del empleo de esta técnica de ubicación es el despliegue de aeronaves equipados con instrumentos de navegación inercial, que trabaja en armonía con la computadora del sistema de interceptación en

el manejo de las informaciones, que al realizar el análisis entrega la elevación del sitio en un mapa digital (ver Figura 15).

Figura 15

Localización por diferencia de altitudes.



Nota. El gráfico representa la localización por diferencia de altitudes. Si la computadora tiene conocimiento de los valores de la altitud entre el vehículo aéreo que está en el aire y el transmisor electromagnético, la medición de los ángulos de elevación y acimut determinarán la posición del emisor. Tomado de *La guerra electrónica* (p.122), por P. Jarpa, 2013. Instituto Geográfico Militar.

Para el último método de empleo de la localización, el autor se refiere a un sistema de ubicación montado sobre una plataforma que se encuentra en movimiento, en donde se realiza una medición múltiple de ángulos, esta técnica realiza la obtención de los parámetros midiendo los ángulos de llegada de las emisiones electromagnéticas provenientes de distintas ubicaciones, lo dificultoso de esta técnica es que demanda gran cantidad de tiempo y movimientos, debido a que las mediciones deben tener un distanciamiento de 90°, obligando que el receptor de apoyo electrónico que por lo general para este tipo de movimiento se encuentra emplazado en una plataforma aérea, deberá viajar una vez y media aproximadamente a la distancia del transmisor adversario, debido a que ante una variación en la ubicación de la estación enemiga conllevaría a anular las mediciones establecidas anteriormente, por lo que esta técnica es la más complicada en la localización.

2.2.6 La ciberguerra con la guerra electrónica

Según, Jarpa, P. (2013) en su obra "*La guerra electrónica*" de la Academia Politécnica Militar, sustenta la relación entre la ciberguerra y la GE. Empezando con los especialistas en GE a nivel global es una facción pequeña, pero altamente preparada y equipada tecnológica, que debido a esa necesidad tecnológica ha impulsado la integración con sistemas existentes y promoviendo proyectos ingeniosos basados en la experiencia y la necesidad, basados en las posibilidades de mantener siempre el dominio sobre el EEM (Espectro Electromagnético), en donde dichas fuerzas involucradas siempre en realizar procesos en operaciones como lo son: planificación, ejecución y control en apoyo a las operaciones tácticas buscan dar a las fuerzas militares el incremento de la potencia combativa en busca del cumplimiento de su misión, estas fuerzas militares utilizan y emplean el EEM, este dominio va desde el empleo de las comunicaciones por parte de combatientes a pie como la infantería, hasta el empleo de los sistemas sofisticados que utilizan bandas del EEM que llegan hasta los rayos laser, no teniendo el reconocimiento de la importancia de su actividad, por lo que se debe tener presente que la GE lucha dentro del EEM para tener el control este tipo de lucha espectral, no apreciada, no siempre presente en los reconocimientos de los medios y de ejercicios al nivel táctico y operativo, obviamente por lo incompresible de su ciencia y la mínima cantidad de personas que lo dominan. Es lógico pensar que es lo que se necesita para que el ciberespacio, ese requerimiento es el establecimiento de las telecomunicaciones, bajo el dominio y la protección de la GE, de no existir esas condiciones, nunca se producirían las condiciones para que se desarrolle la ciberseguridad sin problemas. En el tema de lo cotidiano y popular por el gran empleo de las masas, tenemos que referirnos a la práctica de las redes informáticas, en donde es fácil referirnos a temas que son experimentados por los ciudadano normales y a menudo se vuelve un tema que se puede escuchar a diario en las más populares primeras planas de la prensa como es el robo de información y los delincuentes informáticos que roban y hackean cuentas bancarias se entienden que deben estar sumamente protegidas y que comparten información de una base de datos, debido al tema tan conocido y que es parte de la vida diaria es donde la ciberguerra se hace más notoria porque tiene cobertura civil y mediática (por ejemplo: el colectivo Anonymous, el caso wikileaks

y otros), que expone esta actividad a los noticieros y los medios en general, ante esta realidad se presentan los ataques a nivel internacional a los gobiernos de las principales naciones, respecto a esto último es que se debe tener presente lo ocurrido en Estonia el año 2007, ocasión en que por una decisión política que afectó a la Comunidad Rusa residente, Estonia enfrentó una parálisis casi total de una parte altamente sensible de su infraestructura crítica, debido a un ciberataque masivo que bloqueó todas las páginas web del gobierno (se debe imaginar el registro civil e impuestos internos fuera de servicio, justo los días de declaración de renta), también todos los medios de comunicación quedaron desconectados imposibilitándoles informar lo que ocurría, bloqueo total del servicio bancario vía web e inutilización total de la red de cajeros automáticos y finalmente un ataque sistemático a los sitios web de las universidades más importantes, todo esto duró poco más de un mes.

Entonces, el acelerado desarrollo tecnológico global incluye las TICS (Tecnologías de la Información y la Comunicación), sistemas definidos por software, tecnologías en red y el repunte exponencial del desarrollo de la tecnología de circuitos integrados, los que en su conjunto están impactando fuertemente el entorno de amenazas tanto para la GE como para la ciberseguridad y el tipo de soluciones que se pueden desarrollar contra esas amenazas. Paralelamente, se debe observar la homogenización de la tecnología que busca la compatibilidad de los sistemas en su interconectividad y formatos de soporte de información. Por esto, tanto la GE y la ciberseguridad se enfrentarán a un panorama de amenazas variables, diversas y de rápida ocurrencia y evolución. Hoy, los sistemas modernos ya son vulnerables a los ciberataques, porque tecnológicamente estos son predominantemente definidos por software, con lo que las posibilidades de ataques también se incrementarán.

Entonces, en el campo de batalla digital existe ahora una relación que obligará a la coordinación de las operaciones de GE con las llevadas a cabo por la ciberguerra, cuando al menos estas se lleven a cabo en contra de los sistemas de comando y control (C2), sin perder de vista que ambas son ejecutadas para lograr la superioridad en el gran paraguas de la guerra de la información.

Finalmente, la guerra no se ganará simplemente por tener una ventaja tecnológica, sino por cómo se integra y utiliza la tecnología.

2.2.7 Sistemas de mando y control

Según, Michavila. (1984). en su obra "*La Guerra Electrónica y la Electrónica en la Guerra*", establece el concepto de sistema de mando y control como la combinación

de personal, instalaciones, equipos, técnicas y procedimientos utilizados por un comandante para ejercer la función de mando, control y coordinación permanente en las Fuerzas Armadas. Este sistema proporciona la información y los datos necesarios convenientemente procesados y presentados con la finalidad de difundirlas con prontitud, seguridad, exactitud y reserva. Las funciones y los sistemas deben ir estrechamente relacionados para ejercer las funciones de mando debiendo existir una cadena de telecomunicaciones sin rotura alguna desde el alto mando hasta los escalones subordinados, este sistema de telecomunicaciones debe utilizar los canales militares o alquilando los civiles si en caso fuera necesario, o construyendo los necesarios de acuerdo a la situación, debido al avance tecnológico y la escasez de tiempo en las operaciones los sistemas de telecomunicaciones deben contar con la capacidad de replicar instantáneamente mediante el uso de fuerzas o armas presentes en los demás sistemas del campo de batalla, por tal motivo los sistemas de mando y control que están apoyados en los sistemas de telecomunicaciones deben contar con las siguientes características a fin de cuidar su eficiencia, estas características son: personal preparado, calificado y puesto al día en estudios y en el ejercicio profesional en sus distintos niveles, por lo que el autor se refiere en todo momento que el personal es el elemento primordial del sistema, ahora con respecto al equipamiento de los sistemas de mando y control, deberán ser los adecuados en calidad, cantidad, características y configuración, manteniendo en todo momento técnicas y procedimientos perfectamente establecidos.

2.2.7.1 Historia de los sistemas de mando y control

En la guerra Árabe-Israelí de 1973, fue de suma importancia para los árabes anular las funciones de mando y control de las fuerzas israelíes, por lo que pudieron paralizar todas sus operaciones militares mediante acciones de perturbación durante un tiempo prolongado durante el conflicto, esto tuvo un gran impacto en las futuras decisiones de los jefes políticos y militares del país de Israel debido a que ese nuevo concepto de mando, control y comunicaciones, les obligo a mantener un equipamiento permanente en materia de telecomunicaciones y preparar a su personal de acuerdo al avance de la tecnología, así mismo debido a este conflicto aparecieron técnicas que hasta en la actualidad se vienen empleando como son: salto de frecuencia, comunicaciones satelitales mediante antenas direccionales, equipos de

HF adaptables que puedan compensar todo tipo de perturbación, contar con sistemas de distribución de información táctica como los aviones de alerta E-3 AWACS, un sistema de comunicaciones de alerta contra bombardeos a la zona interior de su territorio. Se puede apreciar que el autor hace toda una descripción de las capacidades militares con las que cuentan los sistemas de mando y control a través de la historia y que en la actualidad se mantienen en vigencia con tecnologías de vanguardia.

2.2.7.2 Sistemas de mando y control para el Ejército de Tierra.

Las unidades del Ejército de Tierra, utilizan los sistemas de mando y control para diversos usos: enlace, observación, telemetría, dirección de tiro, etc. El enlace principalmente se apoyó en los sistemas de telecomunicaciones y en especial en la comunicación por radio formando redes fijas y móviles, paras las redes fijas o semifijas se usan los enlaces microondas junto con las instalaciones alámbricas, para las comunicaciones móviles se despliegan sistemas de radio en HF, VHF y UHF con técnicas de encriptación y salto de frecuencia, en ese momento el autor hace referencia que se vienen empleando de hace tiempo atrás un sistema de mando y control por parte del ejército americano denominado el PLRS (posición, localización, reporte y sistema) con la finalidad de poder comunicarse y saber en tiempo real donde se encuentran sus unidades, el mismo que ha sido diseñado con la finalidad de solucionar un problema constante del campo de batalla, mantener informado en todo momento al comandante de la situación real de sus unidades con el debido secreto y seguridad, de tal manera que el comandante pueda tomar las decisiones basadas en las informaciones en tiempo real, los equipos pueden ser de diferentes plataformas de acuerdo a la necesidad; portátiles vehiculares, transportables, aéreos, etc. Las unidades maestras son transportadas en camiones o helicópteros, todas las informaciones se pueden visualizar en varias pantallas ubicadas en las unidades maestras o puestos de comando, como ayuda a la detección se deben utilizar sistemas de radares para detectar aeronaves, vehículos y personal hostil, esto se puede complementar con equipos de detección térmica, amplificadores, de imágenes y sensores sísmicos formando redes de protección mediante una vigilancia completa y continua que buscan evitar sorpresas en el campo de batalla. Así mismo los sistemas de mando y control según el autor deben contar con sistemas de dirección de armas con la ayuda del radar, rayos laser y rayos infrarrojos, los mismos que son empleados

para defensa antiaérea, anticarro, vehículos blindados y destrucción de reductos protegidos donde se necesita gran precisión para el disparo.

2.2.7.3 Interoperabilidad de los sistemas de mando y control

Según, Guerrero. (2006). En su obra "*Evolución de los Sistemas de Mando y Control"*, hace referencia a este tema de importancia en los sistemas de mando y control conocidos como interoperabilidad, en donde define dicho concepto en base a los estándares de la OTAN conocidos como *"*la capacidad que tienen los sistemas, unidades o fuerzas para suministrar y/o aceptar los servicios de otros sistemas, unidades o fuerzas y usar dichos servicios para operar conjuntamente de una forma efectiva". De igual forma establece que los sistemas que no presenten estas características serán desplazados por los sistemas interoperables que por su actualización tecnológica habitualmente son usados por organizaciones de corte internacional.

Evidentemente, y al margen de que los sistemas de cada país sean más o menos modernos, incorporen más o menos nuevas tecnologías, el elemento crítico en las operaciones reales es la interoperabilidad entre los sistemas multinacionales. Por tanto una conclusión obvia es que hay que seguir trabajando en mejorar cómo se resuelve esa interoperabilidad.

2.3 Marco conceptual.

a.a Adquisición (Adq)

Es el proceso de vigilancia del espectro electromagnético, identificación y explotación de blancos electrónicos del oponente. Comprende la busca de interceptación, el monitoreo y la localización electrónica. Los sistemas de adquisición, cuando instalados en plataformas aéreas (aeronaves o helicópteros), aumentan la capacidad de interceptación. Doctrina general de guerra electrónica (2008) ME 11-16.

a.b Agilidad de frecuencia (Agi Fre)

Es la capacidad de un radar en cambiar su frecuencia de transmisión a cada pulso o grupo de pulsos transmitidos, conforme un algoritmo preestablecido. Doctrina general de guerra electrónica (2008) ME 11-16.

a.c Análisis (Anl)

También conocida como análisis de Guerra Electrónica (GE), es el proceso aplicado por la Inteligencia de Señal (Intg Sñl) y por la GE de verificación de los resultados obtenidos por la adquisición de datos y localización electrónica con el objetivo de dar a conocer informaciones sobre blancos electrónicos necesarios para la actualización de una base de datos o para el desarrollo inmediato de las operaciones de combate. Doctrina general de guerra electrónica (2008) ME 11-16.

a.d Análisis de amenaza (Anl Ame)

Descomposición de las partes constitutivas de la estructura organizacional del enemigo de manera que facilita el conocimiento de su poder de combate. Doctrina general de guerra electrónica (2008) ME 11-16.

a.e Ataque Electrónico (AE)

Es la actividad de GE que tiene la finalidad impedir o reducir el uso efectivo del espectro electromagnético por el enemigo, bien como para destruir, neutralizar o degradar su capacidad de combate, usando energía electromagnética o armamento que emplee la emisión del propio blanco para su guiado. Es importante considerar que los ataques que usan las emisiones no voluntarias, como los misiles infrarrojos y los guiados por TV no son entendidos, actualmente, como AE. Doctrina general de guerra electrónica (2008) ME 11-16.

b.a Banda de Infrarrojo

Parte del espectro de frecuencias situada entre el límite superior de las ondas de radio y el límite inferior de la luz visible (300 a 300.000 GHz). Doctrina general de guerra electrónica (2008) ME 11-16.

b.b Barrido (Brdo)

Acción de recorrer una porción del espectro de frecuencias, a partir de una frecuencia inicial, con incremento preestablecido, hasta una frecuencia final. Doctrina general de guerra electrónica (2008) ME 11-16.

b.c Base de Datos (BD)

Es la reunión de todos los datos relacionados a los equipos de comunicaciones y no-comunicaciones civiles y militares nacionales y de los probables enemigos. Es dividida en Base de Datos de Señal (BD Sñl), Base de Datos de Referencia (BD Ref) y Base de Datos de Trabajo (BD Trab). Doctrina general de guerra electrónica (2008) ME 11-16.

b.d Búsqueda Electrónica.

Es la búsqueda del espectro electromagnético o de partes de él, con el fin de determinar la existencia, fuentes y características pertinentes a partir de radiaciones electromagnéticas. Doctrina general de guerra electrónica (2008) ME 11-16.

c.a Campo de Comunicaciones

Es la porción del espectro en que operan los equipos utilizados para el tránsito de informaciones (radiotransmisores y receptores en general). Doctrina general de guerra electrónica (2008) ME 11-16.

c.b Campo de No-Comunicaciones

Es la parte del espectro en que operan los equipos utilizados para producir informaciones, como los radares de vigilancia; sensores remotos; sistemas electrónicos de guiado de misiles, sensores infrarrojos, telémetro láser y sistemas electrónicos de ayudas de navegación. Doctrina general de guerra electrónica (2008) ME 11-16.

c.c COGE

Centro de Operaciones de Guerra Electrónica. Doctrina general de guerra electrónica (2008) ME 11-16.

c.d CCN

Centro de Coordinación Nacional. Doctrina general de guerra electrónica (2008) ME 11-16.

c.e CCR

Centro de Coordinación Regional. Doctrina general de guerra electrónica (2008) ME 11-16.

c.f "CHAFF" (Sin traducción, por ser término universal)

Pueden ser de metal, cintas, laminillas metálicas, fibra de vidrio metálica o cable perturbadores de diferentes dimensiones. Son cortados en la dimensión de aproximadamente mitad de la longitud de onda, de acuerdo a la frecuencia en que opera el radar blanco. El material más empleado es fibra de vidrio con revestimiento de aluminio. Puede ser usado para perturbar o para generar blancos falsos al radar objetivo. Doctrina general de guerra electrónica (2008) ME 11-16.

c.g CITELE

Ciberdefensa y Telemática del Ejército, órgano de línea de acuerdo a la organización del Ejército del Perú, creado el 28 de octubre del 2018.

d.a Datos del equipo (D Eq)

Conjunto de informaciones capaces de caracterizar un equipo electrónico. Ejemplo: ancho de banda, número de canales, modos de operación (Voz, CW y otros), fabricante/modelo, tipos de antena, tipo de instalación, tipo de equipo

(radar, radio, fax, telemetría, de infrarrojo, procesamiento de datos y Otros). Doctrina general de guerra electrónica (2008) ME 11-16.

d.b Datos de Puesto

Conjunto de informaciones capaz de caracterizar un puesto, como, por ejemplo: finalidad (comunicaciones, control de tiro, auxilio a navegación, reconocimiento, localización electrónica, etc.), empleo (tipo de red radio y escalón), indicativo y otras. Doctrina general de guerra electrónica (2008) ME 11-16.

d.c Datos característicos de la emisión

Conjunto de mediciones capaces de caracterizar una emisión electromagnética. Ejemplo: frecuencia, intensidad, ancho de banda, modulación, desvío de frecuencia y otras. Doctrina general de guerra electrónica (2008) ME 11-16.

d.d Decepción Electrónica

Ver Engaño Electrónico. Doctrina general de guerra electrónica (2008) ME 11-16.

d.e "Decoys" (Sin traducción, por ser término universal)

Son dispositivos usados para crear blancos falsos o para que un pequeño blanco incremente una gran señal eco, dificultando, de esta manera, la evaluación de la amenaza. Ejemplos: reflectores angulares, nubes de "chaff" y otros. Doctrina general de guerra electrónica (2008) ME 11-16.

d.f Detección (Det)

Acción de percibir o establecer contacto a través de equipos electrónicos con el emisor de energía electromagnético procurado. Doctrina general de guerra electrónica (2008) ME 11-16.

d.g Distorsión

Es un cambio indeseable en forma de onda de la señal original. Puede presentarse en la amplitud, en la frecuencia o fase original y en la forma de ondas. Doctrina general de guerra electrónica (2008) ME 11-16.

e.a Emisión (Emi)

Irradiación producida o acción de producir irradiación, por un sistema transmisor de energía electromagnética. Doctrina general de guerra electrónica (2008) ME 11-16.

e.b Emisión de Comunicaciones (Emi Com)

Irradiación electromagnética producida por equipo de comunicaciones. Doctrina general de guerra electrónica (2008) ME 11-16.

e.c Emisión de No-Comunicaciones (Emi NCom)

Irradiación electromagnética producida por equipo de No-Comunicaciones. Doctrina general de guerra electrónica (2008) ME 11-16.

e.d Equipo Electrónico (Eq Elt)

En sentido amplio, es todo aquel dispositivo formado de componentes electrónicos, pudiendo ser pasivo (no necesita de fuente de energía) o activo (aquel que precisa ser alimentado por alguna forma de energía). Doctrina general de guerra electrónica (2008) ME 11-16.

e.e Equipos de No-Comunicaciones (Eq NCom)

Son aquellos destinados, particularmente, a producir informaciones como radares, sensores infrarrojos, intensificadores de luz y diversos equipos con aplicaciones del láser. Doctrina general de guerra electrónica (2008) ME 11-16.

e.f Estado de Alerta (E Alr)

Medida de coordinación establecida para la GE, que traduce a probabilidad de ocurrencia de perturbación en nuestros sistemas de comunicaciones y no-comunicaciones. Es establecido por el centro de operaciones de GE. Doctrina general de guerra electrónica (2008) ME 11-16.

e.g "EXPENDABLES" (Sin traducción, por ser término universal)

Transmisores de pequeño porte, normalmente descartables, dejados en zona de acción del enemigo o lanzados por medio de aeronaves o proyectiles de artillería, con la finalidad que actúen como perturbadores. Doctrina general de guerra electrónica (2008) ME 11-16.

e.h EEM

Espectro Electro Magnético.

f.a Frecuencia de Repetición de Pulso (FRP)

Es la cantidad de pulsos transmitidos por un radar en un segundo, medida en pulsos por segundo (PPS). Doctrina general de guerra electrónica (2008) ME 11-16.

g.a Guerra electrónica (GE)

Actividad militar encargada de realizar acciones electromagnéticas, para conseguir el dominio del espectro electromagnético. Doctrina general de guerra electrónica (2008) ME 11-16.

h.a Huella Electrónica del Emisor (“Finger Prints”) (HEE)

Es la técnica de identificación de un emisor especifico, basada en parámetros únicos que asocian la emisión a un determinado equipo, puesto o localización. Doctrina general de guerra electrónica (2008) ME 11-16.

i.a Información de Señal (Infm Sñl)

Es el conocimiento sobre blancos electrónicos del enemigo, necesario al desenvolvimiento inmediato de las operaciones de combate, resultante de un análisis sumario de las conclusiones o de las informaciones obtenidas por la adquisición y localización electrónica. Doctrina general de guerra electrónica (2008) ME 11-16.

i.b Integración (Integ)

Acción de colocar una unidad o sección temporariamente subordinada a una unidad o fuerza de constitución variable. Doctrina general de guerra electrónica (2008) ME 11-16.

i.c Inteligencia Electrónica (Intg Elec)

También conocida como Inteligencia de No-Comunicaciones (Intg NCom), es la actividad de colección y procesamiento técnico de informaciones derivadas de radiaciones electromagnéticas, excluidas aquellas destinadas a las comunicaciones, las provocadas por detonaciones nucleares y las emanadas de fuentes radioactivas, para crear la base de datos de los emisores de no-comunicaciones del oponente, asociándolos a UU, SSUU, GUC, equipos de Com, etc. Doctrina general de guerra electrónica (2008) ME 11-16.

i.d Interferencia (Interf)

Es la existencia de irradiación no voluntaria (no-intencional) de energía electromagnética en frecuencia utilizada por nosotros que dificultan la recepción de emisiones de nuestro interés. La interferencia puede ser de tres tipos: de origen natural (tempestades eléctricas, erupciones del sol, ruido de estática y disturbios en el medio de propagación); artificial (proximidad de mecanismos eléctricos) y mutua (proximidad de sistemas de comunicaciones o no-comunicaciones). Doctrina general de guerra electrónica (2008) ME 11-16.

i.e Intrusión (Intr)

Tentativa de entrar en una red de comunicaciones de las fuerzas oponentes, con la finalidad de obtener informaciones o causar confusión. Doctrina general de guerra electrónica (2008) ME 11-16.

j.a Jammer

Un jammer o bloqueador de señal es un dispositivo que genera ondas capaces de bloquear diferentes señales y frecuencias de comunicación como GPRS, Wifi, 3G, 4G, entre otras. Efectivamente, los sistemas de rastreo satelital funcionan en su mayoría a través de comunicación celular (GPRS).

j.b Jamming

El término jamming no posee una traducción acertada que englobe todo el concepto. En su más puro significado, jamming se define como aquella actividad que afecta la línea de tiempo en alguna comunicación. Es decir, logra que la información no llegue al receptor en el momento que debía de hacerlo.

l.a Línea Base (LB)

Línea formada por los puestos de localización electrónica que están distanciados entre sí. Doctrina general de guerra electrónica (2008) ME 11-16.

l.b Línea de Vista (L Vis)

Es la capacidad que posee un dispositivo transmisor o receptor de "ver" el otro, siguiendo una ruta de señal directa e incesante. Ejemplo: la luz de una linterna (dispositivo transmisor) vista por los ojos de una persona (dispositivo receptor). Análogamente, para que se dé entre una antena transmisora y receptora debe existir una ruta directa e incesante, se puede decir que hay línea de vista entre las antenas. Doctrina general de guerra electrónica (2008) ME 11-16.

l.c Localización Electrónica (Loc Elt)

Es el proceso de determinación, por medios electrónicos, de la ubicación de una fuente emisora de energía electromagnética. Doctrina general de guerra electrónica (2008) ME 11-16.

o.a Monitoreo.

Es el acto de escuchar las comunicaciones propias o de del enemigo. La primera es realizada con el propósito de mantener y/o mejorar las MPE, la segunda es para obtener informaciones del oponente. Doctrina general de guerra electrónica (2008) ME 11-16.

o.a Orden de Batalla Electrónica (OBE)

Documento en forma de un orden de operaciones, calco, imagen de vídeo o sus combinaciones, conteniendo datos, tales como: probable localización de los emisores de energía del enemigo y datos característicos de las emisiones, así como a localización de nuestros medios de GE. Doctrina general de guerra electrónica (2008) ME 11-16.

o.b Orden de Batalla Electrónica del Enemigo (OBEE)

Es la OBE sin la localización de los medios de GE amigos. Doctrina general de guerra electrónica (2008) ME 11-16.

p.a Perturbación (Pert)

Es la radiación, re-radiación o reflexión deliberada de la energía electromagnética, con el propósito de impedir u obstaculizar el empleo de los dispositivos, equipos o sistemas electrónicos enemigos. Doctrina general de guerra electrónica (2008) ME 11-16.

p.b Plataforma Aérea (Plf Aer)

Aeronave controlada remotamente o no, capaz de recibir equipamientos con misiones específicas. Ejemplo: equipos de GE, cámaras de video, sensores infrarrojo, etc. Doctrina general de guerra electrónica (2008) ME 11-16.

p.c Plataforma Flotante (Plf Flo).

Embarcación capaz de recibir equipamientos con misiones específicas. Doctrina general de guerra electrónica (2008) ME 11-16.

p.d Plataforma Terrestre (Plf Ter)

Vehículo en condiciones de recibir equipamientos con misiones específicas. Doctrina general de guerra electrónica (2008) ME -16.

p.e Posición Alterna (Pos Altr)

Sitio ocupado por un puesto de GE, previamente establecido, con la finalidad de permitir la continuidad del apoyo a la operación. Doctrina general de guerra electrónica (2008) ME 11-16.

p.f Posición Temporal (Pos Tempr)

Sitio ocupado por un puesto de GE antes de su empleo en una operación considerada. Su elección, en principio, depende del estudio en la carta. Doctrina general de guerra electrónica (2008) ME 11-16.

p.g Posición de Operación (Pos Opn)

Sitio ocupado por un puesto de GE en la fase inicial de la operación. Doctrina general de guerra electrónica (2008) ME 11-16.

p.h Protección Electrónica (PE)

División (actividad) de GE que tiene por misión asegurar la utilización eficiente del espectro electromagnético por nuestras fuerzas, no importando si el oponente

tiene o no equipos de GE. Doctrina general de guerra electrónica (2008) ME 11-16.

p.i Puesto de Perturbación (P Pert) o Perturbador (Pert)

Instalación o vehículo, compuestos por personal y equipamientos, destinados a la ejecución de la acción de perturbación sobre emisores electromagnéticos. Doctrina general de guerra electrónica (2008) ME 11-16.

p.j Puesto de Localización Electrónica (P Loc Elt)

Instalación o vehículo (aéreo, naval o terrestre), compuestos por personal y equipamientos, destinados a la ejecución de la acción de localización electrónica de emisores electromagnéticos. Doctrina general de guerra electrónica (2008) ME 11-16.

r.a Radar de Búsqueda (Rd Búsq)

Radar que normalmente opera entre 3,00 a 6,00 GHz y casi siempre está integrado a un sistema de armas, con la finalidad de detectar e identificar cualquier aeronave, helicóptero o vehículo en un sector del espacio con la debida antecedencia, aproximadamente hasta 50 km. Doctrina general de guerra electrónica (2008) ME 11-16.

r.b Radar de Guiado de Armas o de Acompañamiento (Rd Gd Ar)

Radar que normalmente opera en faja de frecuencia superiores a 5,00 GHz y que tiene la finalidad de acompañar un determinado vector hostil y proveer para la unidad de tiro informaciones precisas, permitiendo el ataque y la destrucción de dicho vector hasta una distancia aproximada de 30 km. Son también llamados de radares de tiro. Doctrina general de guerra electrónica (2008) ME 11-16.

r.c Radar de Identificación Amigo o Enemigo

Radar que tiene la finalidad de identificar plataformas amigas, equipadas con transmisores especiales de señales de código. Este equipamiento es más

conocido como Radar IFF o Radar Secundario, pues normalmente es asociado a un radar de vigilancia o de búsqueda. Mayormente realiza la transmisión de la pregunta código en la frecuencia de 1030 MHz y recibe la respuesta de las aeronaves en la frecuencia de 1090MHz de aeronaves hasta aproximadamente 500 km. Las aeronaves que no contesten las preguntas codificadas del radar serán consideradas como enemigas. Doctrina general de guerra electrónica (2008) ME 11-16.

r.d Radar de Vigilancia Terrestre (Rd Vig Ter)

Radar que opera normalmente entre 8,00 a 12,00 GHz o entre 14,00 a 17,00 GHz, que proviene de la expresión inglesa "*Ground Surveillance Radar*" (GSR), también nombrado radar de vigilancia del campo de batalla, debido la traducción de "B*attlefield Surveillance Radar*" (BSR). Es caracterizado por ser un sistema activo que utiliza la onda electromagnética para la vigilancia, detección, localización y clasificación de blancos terrestres, helicópteros en vuelo o suspendido, aeronaves y vehículos aéreos no tripulados (VANT) volando a baja altitud y para ajuste de disparos de morteros y de baterías de artillería amigas. Doctrina general de guerra electrónica (2008) ME 11-16.

r.e Radio de Acción de Perturbación (R Ac Pert)

Radio del círculo dentro del cual equipamientos receptores de determinadas características podrán sufrir los efectos de la acción de perturbación. Doctrina general de guerra electrónica (2008) ME 11-16.

r.f Registro (Regt)

Es el almacenamiento del contenido de la emisión electromagnética, hecho a través de grabación, impresión o cualquier otro proceso que proporcione guardar la información. Doctrina general de guerra electrónica (2008) ME 11-16.

r.g Repetidor (Rpt)

Consiste en una superficie reflectora que recibe y repite la señal transmitida. Puede ser pasivo o activo. Si es pasivo, la señal no sufre amplificación. Doctrina general de guerra electrónica (2008) ME 11-16.

r.h Refuerzo de GE (R/GE)

Apoyo prestado por elemento de GE a otro elemento de GE, aumentándole la eficacia. Doctrina general de guerra electrónica (2008) ME 11-16.

r.i ROPE (Sin traducción, por ser término universal)

Es una variación de "CHAFF" en forma de anillos largos de laminillas metálicas o malla de alambre destinado a producir una respuesta eficaz a los radares de alta frecuencia. Doctrina general de guerra electrónica (2008) ME 11-16.

s.a Sensor

Dispositivo formado por células sensibles que detecta variaciones en una magnitud física y las convierte en señales útiles para un sistema de medida o control, como el sensor acústico y de temperatura, para permitir la generación de datos e informaciones relacionadas a producción del conocimiento de determinado oponente o región de operaciones. Doctrina general de guerra electrónica (2008) ME 11-16.

s.b Sensor Infrarrojo (Sen Infrj)

Dispositivo sensible as frecuencias superiores a 300 GHz (faja del infrarrojo). Doctrina general de guerra electrónica (2008) ME 11-16.

s.c Señal Perturbadora (Sñl Pert)

Señal transmitida intencionalmente con el objeto de impedir, reducir o perturbar la recepción de señal de interés. Doctrina general de guerra electrónica (2008) ME 11-16. Doctrina general de guerra electrónica (2008) ME 11-16.

s.d Sistema de Armas (Sist Ar)

Sistemas normalmente compuestos de armamento, sensores, medios de comunicaciones, procesadores automáticos, dispositivos de telemetría, rastreo, C2 de armas, integrados y bajo comando de un centro de control, para destrucción o neutralización de amenaza. Doctrina general de guerra electrónica (2008) ME 11-16.

t.a Técnica de Triangulación (Tec Triang)

Es la técnica que permite la obtención de triángulos a través de la intersección de, como mínimo, tres direcciones, marcadas sobre una carta con finalidad de levantar áreas probables de localización de la fuente emisora. Doctrina general de guerra electrónica (2008) ME 11-16.

t.b Tiempo Real

Para guerra electrónica, tiempo real significa tiempo instantáneo, es decir, un equipo detecta una emisión en tiempo real cuando esta emisión ha sido interceptada en el exacto momento de su transmisión. Sin embargo, también tiene el significado relacionado al principio de la oportunidad, es decir, el operador del equipamiento es que define cuál es su tiempo real. Es también el caso cuando él necesite de una información dentro de un tiempo hábil de cinco minutos y consiga atender este plazo, fue obtenida una información en tiempo real. Doctrina general de guerra electrónica (2008) ME 11-16.

v.a Vehículo Aéreo No-Tripulado (VANT)

Vehículo de pequeño porte, construido con material de difícil detección, piloteado remotamente, usando alas fijas o rotativas, y empleado para sobrevolar el blanco o área de interés con el objetivo de obtener, principalmente, informaciones a través de sus sistemas de sensores electrónicos de Com y de No Com. Doctrina general de guerra electrónica (2008) ME 11-16.

CAPITULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Enfoque de investigación.

El enfoque de esta investigación fue un enfoque cualitativo, debido a que se construyó el conocimiento basado en las vivencias y actuaciones directas de los investigadores, los que fueron testigos de la baja efectividad del apoyo de la compañía de guerra electrónica en el plan de operaciones "Escudo del Sur". Los autores Blasco y Pérez (2007:25) señalan que la investigación cualitativa estudia la realidad en su contexto natural y como sucede, sacando e interpretando fenómenos de acuerdo con las personas implicadas.

3.2 Tipo de Investigación.

El tipo de investigación realizada fue teórica empírica, debido a que busca solucionar un problema, por lo cual procedimos a encontrar primero la estructura categorial de la realidad en la que se encontraba actualmente la compañía de guerra electrónica, para posteriormente contrastarla con los autores teóricos que hemos identificado. Este tipo de investigación ha sido tomada como referencia del libro ¿Cómo hacer una investigación cualitativa? Xavier Vargas Beal (2011), en la pág. 106, en donde se detalla para el autor los tipos de investigaciones existentes, siendo para el tipo de investigación elegida, la investigación teórica empírica la más adecuada.

3.3 Método de investigación.

El método de investigación que se utilizó fue el método hermenéutico fenomenológico. Hermenéutico debido a que se buscó interpretar la realidad en base al análisis de documentos y textos propios de la unidad en estudio, fenomenológico debido a que se buscó interpretar los fenómenos tal y cual como se presentan dentro del mundo interior de las personas, las mismas que fueron el personal especialista que laboran en la compañía de guerra electrónica. Para asentar mejor este concepto vamos a apoyarnos en el autor Xavier Vargas Beal (2011), en su obra ¿Cómo hacer una investigación cualitativa? En la pág 31, en donde se refiere al método hermenéutico como el método que sirve para aproximarse a cualquier texto, sea éste histórico, periodístico teórico, discursivo, transcripción de entrevistas, etc. El método

fenomenológico fue definido en la misma obra en la pág. 33, detallando que tiene que ver con el mundo interior de las personas.

3.4 Escenario de estudio.

El escenario de estudio donde se realizó la investigación, fueron las instalaciones de la compañía de guerra electrónica, ubicada en la 3ra Brigada de Comunicaciones en el distrito de Tiabaya, provincia de Arequipa, departamento de Arequipa. Fue importante definir el lugar exacto donde se llevó a cabo el trabajo de campo debido a que contribuyó para el acceso a las fuentes de información u observables de estudio.

3.5 Objeto de estudio.

El objeto de estudio conceptual determinado fue el estado actual de la instrucción y entrenamiento del personal especialista en guerra electrónica y el estado actual del material de comunicaciones y GE que dispone. Conocer el estado actual de la instrucción y entrenamiento del personal especialista en guerra electrónica, nos permitió conocer como se viene administrando y gestionando las bases del conocimiento de esta dimensión importante del campo de batalla. Según, Vargas Beal. (2011). en la pág. 77, establece el objeto de estudio puede ser empírico si la investigación es empírica, pero puede ser, y de hecho lo es en la mayoría de veces, un objeto conceptual si la investigación es teórica o teórica empírica. Por objeto de estudio conceptual debe entenderse el recorte del campo del conocimiento y del campo especifico mismo que es necesario hacer para poder centrar la construcción del conocimiento y poder así orientar permanentemente el trabajo de búsqueda teórico o teórico empírico.

3.6 Observables de estudio.

Los observables de estudio para la presente tesis fueron:
En instrucción y entrenamiento.

- Rendimiento en el campo.
- Conocimientos en telecomunicaciones.
- Preparación del personal en doctrina de GE.

- Preparación del personal en el empleo de la GE.

Material y equipo de comunicaciones.

- Nivel de operatividad.
- Cantidad de material y equipo
- Nivel de conservación
- Clase de mantenimiento
- Capacidad de mando y control

3.7 Fuentes de información.

Las fuentes de información primaria para este trabajo de investigación fueron tres:

- Personal de oficiales y técnicos suboficiales especialistas en guerra electrónica.
- Documentos: la memoria anual de la unidad, cuadro de organización y equipo, programa de instrucción y entrenamiento (PIE).
- Observación: las actividades de instrucción y entrenamiento del personal en los campos de instrucción de la unidad y los talleres o almacenes de mantenimiento.

3.8 Técnica e instrumento de acopio de información

3.8.1 Técnica de acopio de información

Las técnicas empleadas para el presente trabajo de investigación fueron las técnicas de entrevista, observación directa de campo e indagación documental estas técnicas fueron realizadas posteriormente al planteamiento de las preguntas de investigación, el método, los observables y las fuentes de información.

3.8.2 Instrumento.

Los instrumentos aplicados para el levantamiento de campo fueron: la guía de entrevista, ficha de registro de observación y ficha de registro documental, estos instrumentos son los que corresponden a cada técnica seleccionada en el ítem anterior, los mismos que son los apropiados para este tipo de investigación cualitativa, según, Vargas Beal (2011) en la pág. 63, especifica, para la técnica de entrevista corresponde: el guion con todas preguntas por hacer y formatos específicos

de registro, para la técnica de indagación documental corresponde según el autor: relación de documentos buscados y ruta de sitios virtuales o reales donde se pueden encontrar y para la ficha de registro de observación de campo todos los aspectos que se van a observar en relación a instrucción y material.

3.9 Acceso al campo y acopio de información.

3.9.1 Acceso al campo.

Las mediciones fueron realizadas en el sitio, en las instalaciones de la compañía de guerra electrónica ubicada en la 3ra Brigada de comunicaciones; en el distrito de Tiabaya, provincia de Arequipa, departamento de Arequipa, para lo cual se formuló la autorización correspondiente para poder tener el acceso al campo y se realizaron las coordinaciones necesarias con el comandante de dicha unidad, no se consideró que exista problema alguno para realizar esta investigación de campo. Según lo que corresponde para el paradigma hermenéutico-fenomenológico, se trabajó en base a los experimentales de campo, debido a que las fuentes constituyen principalmente el lugar, objeto, documento y personas, siendo importante tener que trabajar en el sitio para poder hacer un correcto trabajo de campo, según, Vargas Beal. (2011). en la pág. 44 y 45 de su guía práctica, manifiesta que para un trabajo de investigación de carácter hermenéutico fenomenológico se debe realizar experimentales de campo: estas son mediciones manipuladas de muy diverso tipo realizadas en sitio, es decir, en lugar donde las cosas que desean ser medidas ocurren.

3.9.2 Acopio de información.

En lo que respecta al acopio de información, este se realizó en el campo, paralelamente al levantamiento en campo, realizando simultáneamente el traspaso de la información en limpio, organizándola de la mejor manera en dispositivos electrónicos y físicos que tengan la capacidad suficiente para poder almacenar la totalidad de los datos obtenidos y en forma ordenada. El realizar el acopio de información de esta forma, nos permitió poder ahorrar tiempo en la investigación y asegurarnos de que ninguna información se pierda, siendo aprovechada completamente en beneficio de la investigación, según Vargas Beal. (2011). en la

pág. 66 y 67, manifiesta: recomendamos trabajar en el laboratorio y/o campo, tratando en la medida de lo posible, de hacerlo en “limpio”, es decir, no pensando en que después habrá tiempo para organizar la información, esta debe ir quedando desde su levantamiento mismo ya catalogada de la mejor forma posible.

3.10 Método de análisis de información.

Después de haber realizado el levantamiento de campo, se procedió a realizar el análisis de la información, lo que fue apoyado en el método de análisis manual, el mismo que busca obtener citas, categorías y macro categorías con la finalidad de obtener la realidad empírica develada. Posteriormente en base a cada instrumento se realizó la triangulación de los resultados obtenidos con el fin de dar respuestas a nuestra pregunta de investigación. Según Vargas Beal. (2011) en la pág. 68, establece en esta parte del trabajo de investigación, la misma que va ser motivo del informe final de investigación, establece lo siguiente: en donde se obtiene para algunos autores la estructura de la realidad, esto es conocido también como especie de esquemas, mapa diagrama, etc., construido a partir de los datos procesados y que en su conjunto permite dar cuenta de las partes, de sus relaciones entre si y de ellas con el todo.

3.11 Los entrevistados.

Los entrevistados fueron escogidos debido a su amplio conocimiento en el campo de las comunicaciones y la guerra electrónica, así como a haber realizado cursos y capacitaciones en el extranjero, además de haber realizado el programa básico de guerra electrónica. Presentan estudios de maestría en telecomunicaciones en universidades del extranjero debido haber sido becados por la institución, estos conocimientos los convierten en expertos en el tema en investigación.

CAPITULO IV

ANÁLISIS Y SÍNTESIS

4.1 Revisión y elaboración de citas

Después de haber realizado el trabajo de campo mediante las técnicas como la entrevista, el análisis documental y la observación directa, se procedió a realizar una revisión completa de la información obtenida, elaborando citas en cada párrafo de la información, las mismas que procederé a enunciar por técnica respectivamente empezando por la técnica de entrevista:

- Capacidad para desempeñarse como instructores de guerra electrónica solo en la teoría.
- Conocimiento teórico y práctica limitada del plan de engaño.
- Necesidad del apoyo de la Compañía de Inteligencia N°114 para el entrenamiento del personal.
- Realización de la fase de instrucción y entrenamiento de forma limitada.
- Falta de instructores para las capacitaciones de GE.
- El entrenamiento de protección se realiza con los limitados medios de comunicaciones.
- Practicas teóricas en la carta y una práctica anual en los campos de instrucción.
- Obtención de conocimientos básicos en GE y especialmente de protección en forma teórica al término de la instrucción.
- Capacidad de dar opiniones de planeamiento y opiniones técnicas al final de la instrucción, únicamente de forma teórica.
- Limitada asignación de personal de todas las especialidades necesarias.
- Limitada cantidad de especialistas en GE.
- Falta de integración con la ciberseguridad
- Ausencia de especialistas en ciberseguridad.
- Falta de continuidad de los cursos básicos de GE.
- Limitada cantidad de equipos de comunicaciones, comando y control.
- Falta de interés en el comando para la gestión en la adquisición de equipos de GE.
- Material de comunicaciones con medidas anti soporte y anti ataque en AJ.
- Equipos de comunicaciones con variedad en modos de trabajo.

Ahora vamos a enunciar las citas que corresponde a la técnica de análisis documental, de acuerdo al siguiente detalle:

- Empleo y practica de redes de engaño en el campo.
- Realización de ejercicios prácticos en el campo una (01) vez al año.
- Ausencia y falta de continuidad de los cursos básicos de GE.
- Avance tecnológico que junto a la ausencia de material y equipo, afectan la situación actual.
- Realización de prácticas de protección electrónica en el campo de forma limitada.
- Necesidad de material de comunicaciones.
- Se dispone del 40% y 7% de Oficiales y Técnicos según el COEQ (Cuadro de organización y equipo).
- Se dispone del 10% y 20% de material de comunicaciones y computo según COEQ.

Continuando con la elaboración de citas, corresponde a enunciar las citas de la observación directa:

- Limitada cantidad de ambientes para la instrucción.
- Limitada cantidad de campos de instrucción.
- Poca cantidad de ayudas y material para la instrucción
- Dispone de programas de instrucción y capacitación solo teóricos.
- Los instruidos al final sin competencias completas en GE.
- Ausencia de conocimientos básicos de Telecomunicaciones.

4.2 Elaboración de categorías

Después de haber realizado las citas y continuando con la elaboración del análisis hermenéutico fenomenológico con la finalidad de crear unidades con sentido, se procedió a ordenar la información en categorías, las mismas que se desarrollaron según la metodología elegida para la misma, comenzando con las categorías correspondientes a la entrevista:

- Fase especializada de GE con limitaciones en material e instructores.
- Instrucción teórica con limitada practica en el campo.
- Capacidades y opiniones de forma teórica.
- Limitada cantidad de personal especialista en GE.

- Desconocimiento y falta de integración con la ciberseguridad.
- Falta de equipamiento de GE y continuidad en los cursos básicos de Guerra electrónica.
- Limitada cantidad de medios anti soporte y anti ataque.

Para la elaboración de las categorías procedentes del análisis documental se empleó la misma metodología que para las categorías anteriores, procediendo a describir las siguientes:

- Ejercicio de redes de engaño y protección electrónica en el campo una (01) vez al año, en forma limitada.
- Ausencia de material que aumenta el desfase tecnológico en instrucción y empleo.
- Limitada asignación de personal especialista en GE, medios de comunicaciones y cómputo.

Para las categorías elaboradas de las citas que salieron de la observación directa, de igual forma se empleó la misma metodología, procediendo a encontrar las siguientes categorías:

- Limitada condiciones de infraestructura para la instrucción y entrenamiento.
- Dispone de programas anuales solo teóricos
- Personal capacitado sin las competencias necesarias en telecomunicaciones y GE.

4.3 Elaboración de macro categorías.

Para la elaboración de estas macro categorías se tomó en cuenta la cantidad de categorías que todavía se disponen, las mismas que para realizar un análisis más exacto eran numerosas, por lo consiguiente se decidió darle una perspectiva más precisa a este método, elaborando las siguientes macro categorías que corresponden a la técnica de entrevista:

- Instrucción limitada en instructores y medios, conducida generalmente de forma teórica.
- Limitado personal especialista en GE y ciberseguridad.
- Ausencia de conocimientos de telecomunicaciones.
- Material de comunicaciones insuficiente para el C2.
- Necesidad de apoyo de Compañía de Inteligencia N° 114 para el entrenamiento.

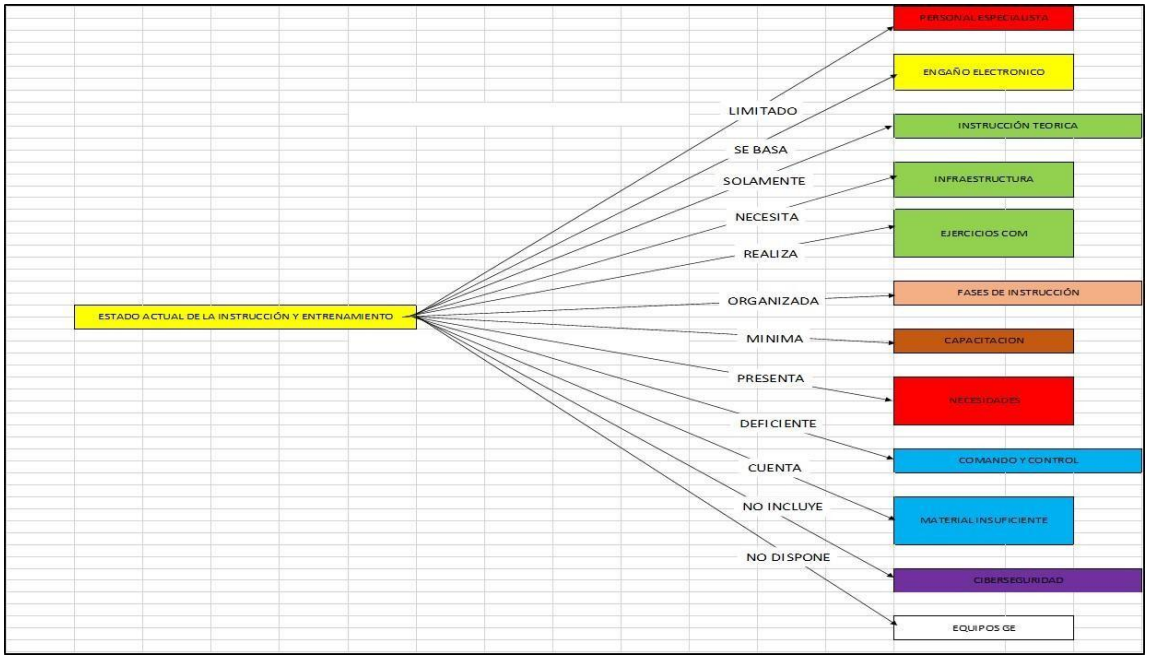
Para las demás técnicas empleadas, los investigadores no consideraron necesario realizar la elaboración de las macro categorías debido a que se dispone de la cantidad necesaria para poder realizar la triangulación de categorías y macro categorías.

4.4 Triangulación de categorías y macro categorías.

Con la finalidad de poder obtener la realidad develada y poder realizar el dialogo teórico empírico, se procedió a realizar la triangulación de categorías y macro categorías, las mismas que se representa en las figuras siguientes:

Figura 16

Triangulación de categorías para el objetivo N°1



Nota. El gráfico representa el proceso de triangulación de categorías para desarrollar el objetivo N° 1.

Figura 17

Triangulación de categorías para el objetivo N° 2.

Nota. El gráfico representa el proceso de triangulación de categorías para desarrollar el objetivo N° 2.

Por lo que se procedió a formular la triangulación, la misma que fue de tipo interpretativo con la única finalidad de poder hallar la realidad develada de nuestra investigación. En las figuras (16) apreciamos la agrupación por técnicas, obtenida mediante la agrupación de redes semánticas, las mismas que buscan responder la pregunta de investigación N°1; ¿Cuál es el estado actual de instrucción y entrenamiento en el tema específico de doctrina y empleo de la guerra electrónica del personal especialista de la compañía de guerra electrónica de la 3ra brigada de comunicaciones? Procediendo agrupar por redes semánticas, se buscó obtener la relación que existen entre cada categoría y macro categoría, teniendo en cuenta a que técnica pertenece, relacionando las categorías y macro categorías a cada una de las redes semánticas, empezando con la red semántica de entrevista: la limitada cantidad de material que aumenta el desfase tecnológico, la poca infraestructura, las condiciones solo teóricas para llevar acabo la instrucción, la falta de equipos de GE, la falta de continuidad de los cursos básicos de GE, los limitados conocimientos en el tema de las telecomunicaciones, son aspectos que impactan significativamente en

la instrucción y entrenamiento, continuando con la triangulación y al realizar la misma evaluación para la red semántica de análisis documental sobre las categorías siguientes: instrucción limitada por falta de instructores y medios conducida generalmente de forma teórica junto con los programas de instrucción anuales solo teóricos, los instruidos sin competencias completas y los ejercicios de redes de engaño y protección electrónica en el campo que son realizadas una sola vez al año, entendemos que la instrucción es insuficiente, solo limitándonos a capacitar personal especialista con capacidades y conocimientos teóricos.

Para finalizar el último análisis de la red semántica de observación, que presenta las categorías siguientes: Limitada asignación de personal especialista en GE, medios de comunicaciones, GE y computo, limitado personal existente especialista en GE y ciberseguridad y una instrucción limitada en instructores y medios, origina que volvamos a obtener como resultado de la triangulación que la instrucción y entrenamiento del personal especialista en GE solo se realice de forma teórica, esta deducción relacionada con la ausencia de equipos de GE y la limitada cantidad de material de comunicaciones y computo, origina que también podamos discernir que el estado actual de la compañía de guerra electrónica es limitada en medios para poder cumplir su misión.

De igual forma en la figura N°17 apreciamos la agrupación por técnicas, obtenida mediante la agrupación de redes semánticas, las mismas que buscan responder la pregunta de investigación N°2; ¿Cuál es el estado actual de disponibilidad y operatividad del material y equipo de comunicaciones en el tema específico de comando y control que dispone la compañía de guerra electrónica de la 3ra brigada de comunicaciones? Procediendo de igual manera como en el análisis anterior a agrupar por redes semánticas, buscando obtener la relación que existen entre cada categoría y macro categoría, teniendo en cuenta a que técnica pertenecen, relacionando las categorías y macro categorías a cada una de las redes semánticas, empezando con la red semántica de entrevista: ausencia de una estructura de comando y control y ausencia de interoperabilidad, continuando con la triangulación y realizando el análisis de la red semántica de observación directa tenemos las siguientes categorías: ausencia de estructura de comando y control, limitada cantidad de personal operador y ausencia de interoperabilidad en cada uno de sus equipos de comunicaciones, para terminar, analizaremos la red semántica de indagación

documental, la misma que cuenta con las categorías siguientes: ausencia de estructura de comando y control, ausencia de material y equipos suficientes y ausencia de interoperabilidad, por lo que se entiende principalmente que la compañía de guerra electrónica carece principalmente de infraestructura adecuada en comando y control, interoperabilidad, situación que no le permitiría trabajar con otros elementos de las Fuerzas Armadas y limitada cantidad de personal de operadores especialistas en GE.

Finalmente como hallazgo de la investigación podemos nombrar la necesidad de continuar contando con el apoyo en la instrucción y capacitación del personal por parte de la Compañía de Inteligencia N°114 perteneciente a la IV DE, debido a que fue suspendida por motivos administrativos, situación que se registra en los antecedentes nacionales de la presente tesis.

4.5 Resultado de la triangulación.

El resultado de la triangulación se conoce como realidad develada, la que buscamos para poder dar respuesta a las preguntas de investigación planteadas, buscando alcanzar los objetivos establecidos en el planteamiento del problema, los mismos que especifican lo siguiente:

Objetivo N°1: Entender el estado actual de instrucción y entrenamiento en el tema específico de doctrina y empleo de guerra electrónica que cuenta el personal especialista de la compañía de guerra electrónica de la 3ra Brigada de Comunicaciones.

Teniendo dicho objetivo vamos a detallar la realidad develada para el objetivo N° 1, el estado actual de instrucción y entrenamiento en el tema específico de doctrina y empleo de guerra electrónica con el que cuenta el personal especialista, es limitado, debido a que la ausencia de material de GE y la limitada cantidad de equipos de comunicaciones, hacen que esta actividad solo se realice en forma teórica, contando con algunas prácticas en tema de engaño electrónico y protección electrónica una vez al año, las mismas que no son suficientes para considerar las actividades de instrucción y entrenamiento como las más adecuadas, además cobra importancia la falta de instructores de GE, debido a la falta de continuidad del curso básico de GE impartido por la escuela de comunicaciones del COEDE (Comando de Educación y Doctrina del Ejército), por lo que se debe plantear su retorno con una actualización en su plan de estudios.

Objetivo N°2: Conocer el estado actual de disponibilidad y operatividad del material y equipo de comunicaciones que dispone la compañía de guerra electrónica.

Teniendo dicho objetivo vamos a detallar la realidad develada para el objetivo N° 2, el estado actual de disponibilidad y operatividad del material y equipo de comunicaciones en el tema de comando y control que dispone la compañía de guerra electrónica de la 3ra Brigada de comunicaciones es insuficiente, debido a la ausencia de equipos de comunicaciones y computo, a esto le agregamos la falta de interoperabilidad, la ausencia de una estructura de comando y control, situación que afectan directamente al entrenamiento del personal y al cumplimiento de la misión de esa unidad.

CAPÍTULO V

DIALOGO TEÓRICO - EMPÍRICO

5.1 Dialogo teórico - empírico para el objetivo N°1

De acuerdo a la realidad develada para cada objetivo de la investigación, se realizó el dialogo teórico-empírico, con el siguiente objetivo:

Objetivo N°1: Entender el estado actual de instrucción y entrenamiento en el tema específico de doctrina y empleo de guerra electrónica que cuenta el personal especialista de la compañía de guerra electrónica de la 3ra Brigada de comunicaciones.

La realidad develada empírica para este objetivo fue la siguiente: el estado actual de instrucción y entrenamiento en el tema específico de doctrina y empleo de guerra electrónica con el que cuenta el personal especialista, es limitado, debido a que la ausencia de material GE y la limitada cantidad de equipos de comunicaciones, hacen que esta actividad solo se realice en forma teórica, contando con algunas prácticas en tema de engaño electrónico y protección electrónica una vez al año, las misma que no son suficientes para considerarlo óptimo, cobra importancia la falta de instructores de GE, debido a la falta de continuidad del curso básico de GE impartido por la escuela de comunicaciones del COEDE.

Según la realidad teórica develada mediante la categorización de las unidades con sentido propio que se plantearon en el estado de conocimiento según la obra de Jarpa (2013). "*Guerra Electrónica*", donde se buscó contribuir a responder a la primera pregunta de investigación ¿Cuál es el estado actual del personal especialista de guerra electrónica en el tema de doctrina y empleo de guerra electrónica? Encontramos los siguientes resultados, el personal especialista debe tener los conocimientos de guerra de mando y control, propagación de ondas electromagnéticas, telecomunicaciones para ser empleados en el apoyo electrónico y ataque electrónico, técnicas de jamming, localización electrónica, tácticas de ataque electrónico, conocimientos del campo de batalla digital y la integración de la tecnologías de GE y ciberseguridad, conocimientos que no se evidenciaron en la realidad empírica develada.

5.2 Dialogo teórico - empírico para objetivo N°2

Para el objetivo N°2: Conocer el estado actual de disponibilidad y operatividad del material y equipo en el tema de comando y control que dispone la Compañía de Guerra de Electrónica.

Debemos de igual manera describir la realidad empírica develada para este objetivo que fue la siguiente: el estado actual de disponibilidad y operatividad del material y equipo en el tema de comando y control que dispone la compañía de guerra electrónica de la 3ra Brigada de comunicaciones es insuficiente, debido a la ausencia de sistemas de comunicaciones con la capacidad tecnológica e interoperabilidad necesaria, se evidencia que la poca disponibilidad de equipos de comunicaciones y computo que afectan directamente al entrenamiento del personal especialista y al cumplimiento de la misión de esa unidad.

Según la realidad teórica develada mediante la categorización de las unidades con sentido propio que se plantearon en el estado de conocimiento según la obra de Michavila (1984) "*La guerra electrónica y la electrónica en la guerra*" (2006) que nos habla de la importancia de la evolución de los sistemas de mando y control, donde se buscó contribuir a responder la segunda pregunta de investigación ¿Conocer el estado actual de disponibilidad y operatividad del material y equipo en el tema de comando y control que dispone la compañía de guerra de electrónica. Encontramos los siguientes resultados, los sistemas de mando y control deben contar con un sistema basado en una infraestructura de telecomunicaciones con la capacidad de poder almacenar y procesar datos, así mismo deberá mantener estos sistemas de telecomunicaciones de acuerdo al avance tecnológico y al personal que lo opera en todo momento capacitado y entrenado, deberá incluir equipos de comunicaciones con características de seguridad en capacidad de unirse al sistema de acuerdo a necesidad de empleo, contando con capacidades tácticas multiplataforma (personal, vehículos transportables, etc.) contando con servicios adicionales de vigilancia así como mantener en todo momento la interoperabilidad con otros sistemas, esta realidad teórica no coincide con la realidad empírica por lo que se le considera insuficiente.

CONCLUSIONES

Para la presente tesis establecimos las siguientes conclusiones que en su mayoría guardan similitud con la realidad develada, la misma que fue refrendada y mejorada en el dialogo teórico - empírico, concluyendo en lo siguiente:

- El estado actual de instrucción y entrenamiento del personal especialista en materia de doctrina y empleo de la compañía de guerra electrónica es limitado y solo teórico, debido a la falta de equipos de GE y la limitada cantidad de equipos de comunicaciones y computo, de igual forma la falta de oficiales, técnicos y suboficiales especialista en GE, debido a la suspensión del curso básico de GE el cual era dictado por la Escuela de Comunicaciones del Ejército.

- Es importante que las escuelas de formación y capacitación de los oficiales, técnicos y suboficiales del arma de comunicaciones capaciten al personal en el uso de TICS (Telecomunicaciones, redes y conectividad) con el fin de poder tener los conocimientos necesarios para operar los equipos de GE y los sistemas de mando y control.

- El estado actual de disponibilidad y operatividad de equipos de comunicaciones y GE de la compañía de guerra electrónica es insuficiente, debido a la falta de un sistema de telecomunicaciones con características de seguridad, flexibilidad e interoperabilidad.

- El apoyo de la Compañía de Inteligencia N°114 de la IV DE es importante para entrenar al personal especialista en GE hasta que el Ejército del Perú adopte una solución.

- El curso básico de GE es importante para poder contar con mayor cantidad de oficiales, técnicos y suboficiales especialistas en GE que podrán desempeñarse como instructores y operadores de los futuros sistemas que se deben adquirir.

- Debido al periodo de ausencia en el desarrollo del curso básico de GE, se debe formular un plan de estudios actualizado buscando mantener al día los conocimientos a impartir, buscando como perfil de egreso las competencias en la guerra del mando y control.

- La integración de la GE, la ciberseguridad y las telecomunicaciones es necesaria debido a que son los principales protagonistas de la guerra del mando y control.

- El desarrollo de las actividades de engaño electrónico y protección electrónica que viene realizando la compañía de guerra electrónica como parte de su instrucción y entrenamiento, es importante debido a que brinda capacidades en ataque electrónico y protección con los equipos de comunicaciones que actualmente se dispone, ayudando a dar solución a la problemática de forma parcial brindando el apoyo de combate necesario a las fuerzas desplegadas en el campo de batalla.

RECOMENDACIONES

Para esta tesis recomendamos lo siguiente:

- La actualización del proyecto de inversión pública “Kuelap”, el mismo que obtuvo la viabilidad en el año 2012, pero por tema de tiempo en formulación y desfase tecnológico debe ser actualizada en el menor tiempo posible.

- Planificar la realización de manera continua de los cursos básicos de Guerra electrónica para oficiales, técnicos y suboficiales, de igual forma proponer un curso superior para oficiales superiores, debido a que los campos de acción de la GE van desde lo táctico hasta lo operacional y lo estratégico.

- Recomendar al comando del Ejército la adquisición de un sistema de telecomunicaciones que busque integrar a todas las unidades y reparticiones del Ejército y dejar de lado la adquisición de equipos de comunicaciones en forma individual.

- Recomendar a la Escuela de Comunicaciones la actualización del plan de estudios del curso básico de GE, buscando obtener como perfil de egreso las competencias en la guerra del mando y control.

- Recomendar al COPERE (Comando de Personal del Ejército) que el personal egresado de los cursos de capacitación en GE, sean cambiados de colocación a la compañía de guerra electrónica o unidades similares con la intención de asegurar la cantidad de instructores y operadores para darle sostenimiento de personal al sistema.

- Coordinar con el Comando del Ejército, para obtener nuevamente el apoyo para temas de entrenamiento de la Compañía de Inteligencia N°114 de la IV DE, la única unidad en el Ejército del Perú que cuenta con equipamiento de GE.

Propuestas para enfrentar la realidad Problemática

Después de haber descrito las recomendaciones, presentamos las siguientes propuestas de solución, que van a contribuir junto con los resultados de la tesis a mejorar la problemática planteada:

La actualización del PIP "Kuelap" o la formulación de un proyecto nuevo, se debe realizar bajo la conformación de un comité, dirigido por Ciberseguridad y Telemática del Ejercito (CITELE), el mismo que debe convocar a tiempo completo el personal necesario para laborar los perfiles técnicos necesarios para su formulación.

El CITELE en coordinación con el COEDE debe solicitar misiones de oficiales de ejércitos extranjeros expertos en GE, para que pueda estructurar todo el programa de capacitación de los cursos básicos de GE, en caso no se pueda realizar esta propuesta, convocar a la mayoría de oficiales con curso básico de GE a necesidad y pedido de la ECOME para que se pueda realizar permanentemente el curso básico de guerra electrónica con un tiempo mínimo de 6 meses con sus respectivas practicas operativas en unidades y ambientes que poseen todas la infraestructura y medios de GE para poder culminar su preparación.

Actualizar el plan de estudios del programa básico de Guerra Electrónica en coordinación con la Escuela de Comunicaciones, buscando obtener como perfil de egreso las competencias en la guerra del mando y control.

Solicitar al SCOME (Servicio de Comunicaciones del Ejército) la adquisición de un sistema de telecomunicaciones con las capacidades necesarias para integrar los equipos de comunicaciones y cómputo de la compañía de guerra electrónica pueda incrementar su capacidad de comando y control.

Referencias Bibliográficas

- Vargas, X. (2011). **¿Cómo hacer una investigación cualitativa?** Una guía práctica,para saber que es la investigación en general y como hacerla, con énfasis en las etapas de la investigación cualitativa. (9na ed) México. Editorial ETXETA.
- Ejército del Perú. (2008). **M 11-16 Doctrina general de guerra electrónica**. Perú
- Ejército del Perú. (2008). **ME 11-105 Empleo táctico de guerra electrónica**. Perú
- Izcara, S. P. (2014). **Manual de investigación cualitativa.** México, D.F. Editorial Fontamara.
- Jarpa, P. (2013). **Guerra Electrónica.** Trabajo presentado en la Academia Politécnica Militar. Chile.
- Michavila, P. (1984). **La guerra electrónica y la electrónica en la guerra**. Boletín de Información N° 171-V. Trabajo presentado en el Centro Superior de Estudios de la Defensa Nacional. España.
- Barreto, J. (2018). **La defensa nacional y la estrategia militar de la seguridad cibernética**. Trabajo presentado en la Escuela superior de guerra conjunta de las fuerzas armadas. Argentina.
- Cubeiro, E. (2001). **Los sistemas de mando y control: una visión histórica-prospectiva.** Boletín de Información, ISSN 0213-6864, Nº 271. España.
- Tanenbaum, A. y Wetherall, D. (2012). **Redes de computadoras**. (5ta ed). México. Editorial Pearson educación.
- Ejército del Aire de España. (2010). **Tecnologías y sistemas de C4ISR el impacto de la tecnología aeroespacial, 1-22.** Politécnica de Madrid. España: https://docplayer.es/44903101-Tecnologias-y-sistemas-c4isr-el-impacto-de-la-tecnologia-aeroespacial.html.

- Ratti, A.O. (2011). **Interoperabilidad de los sistemas de comunicaciones en apoyo al comando y control en el nivel estratégico operacional, (1-57).** Trabajo final de licenciatura presentado en la Escuela Superior de Guerra. Argentina.

ANEXO 1

MATRIZ DE CONSISTENCIA

Anexo 1: Matriz de consistencia(Enfoque cualitativo)

Título: Análisis del estado actual de la compañía de guerra electrónica.

Preguntas de investigación	Objetivos	Justificación	Observables	Metodología
¿Cuál es el estado actual de la instrucción y entrenamiento del personal especialista, en el tema Específico de doctrina y empleo de guerra electrónica de la compañía de guerra electrónica de la 3ra Brigada de comunicaciones?	Entender el estado actual de la Instrucción y entrenamiento del personal especialista, en el tema específico de doctrina y empleo de guerra electrónica de la compañía de guerra electrónica de la 3ra Brigada de comunicaciones.	Es para que el CITELE Conozca la situación actual de la compañía de guerra electrónica y de esta manera al contar con un diagnostico real pueda realizar las acciones necesarias para permitir la integración de la guerra electrónica con la ciberseguridad y de esta manera contribuir con la seguridad nacional.	Instrucción y entrenamiento: - Rendimiento en el campo. - Conocimientos en telecomunicaciones - Preparación del personal endoctrina de GE. - Preparación del personal en elempleo de la GE.	Hermenéutico Fenomenológico
¿Cuál es el estado actual de disponibilidad y operatividad del material y equipo en el tema de Comando y control que dispone la compañía de guerra electrónica?	Conocer elestado actual de disponibilidad y operatividad del material y equipo en el tema de Comando y control que dispone la compañía de guerra electrónica.	El SCOME conozca la situación de equipamiento en materia de comando y control y pueda asignar sistemas y equipos de comunicacioness.	Material y equipo de comunicaciones: Nivel de operatividad. Cantidad de material y equipo. Nivel de conservación.	Hermenéutico Fenomenológico

ANEXO 2

INSTRUMENTOS DE ACOPIO Y RECOLECCION DE DATOS

GUÍA DE ENTREVISTA

Buenos días/tardes, expresamos nuestro agradecimiento por el tiempo y la atención presentada para poder realizar esta entrevista, cuya información y comentarios que nos sean proporcionados serán muy valiosos para profundizar la presente investigación. Marque con un aspa la o las respuestas que considere importantes, así como responda brevemente las preguntas.

Entrevistado:

Grado Académico:

D.N.I. /C.I.P.:

Lugar – fecha:

Experiencia: oficial de instrucción y entrenamiento de la compañía de guerra electrónica.

INSTRUCCIÓN Y ENTRENAMIENTO

Rendimiento en el campo

1. ¿Cuántas veces al año se dirige el personal al campo a realizar la parte práctica de lainstrucción y entrenamiento?

2. ¿Cómo mide el rendimiento del personal en el campo?

3. ¿Cómo es el rendimiento de dicho personal?

Preparación del personal en doctrina de GE.

4. ¿Cómo se llevan a cabo las actividades de instrucción en guerra electrónica y se tieneen cuenta el conocimiento en ciberseguridad?

5. ¿Cuáles son los módulos de instrucción en los que se encuentran divida la capacitación del personal?

6. ¿Cuáles son las capacidades con las que deben de contar los especialistas en guerra electrónica y el personal no especialista, al final del módulo de instrucción y entrenamiento en guerra electrónica. ?

Preparación del personal en empleo de GE.

7. ¿Cómo es la participación de la guerra electrónica en apoyo a las operaciones deciberseguridad en la compañía de guerra electrónica?

8. ¿Dispone de algún apoyo exterior para poder realizar capacitaciones al personalespecialista en GE?

9. ¿Cómo se realizan los entrenamientos de engaño electrónico y de guerra electrónicadel personal de la compañía de guerra electrónica?

Conocimientos en telecomunicaciones.

10. ¿El personal de instructores cuenta con los conocimientos actuales en el campo de las telecomunicaciones, guerra del mando y control, propagación de ondas electromagnéticas?

MATERIAL Y EQUIPO DE COMUNICACIONES.

Nivel de operatividad.

11. ¿Cuál es el estado de operatividad de la unidad en material de comunicaciones?

12. ¿Cuáles son las medidas anti soporte y anti ataque con las que cuenta este materialde comunicaciones?

Cantidad de material y equipo.

13. ¿Cuál es el material de comunicaciones con el que cuenta la compañía de guerraelectrónica?

14. ¿La cantidad de material de comunicaciones es la suficiente para establecer elcomando y control entre sus elementos? ¿Por qué?

15. ¿Se imparte instrucción de técnicas de jamming y apoyo electrónico al personal dela compañía de guerra electrónica?

Nivel de operatividad.

16. ¿Cuál es el nivel de conservación del material y equipo de comunicaciones?

ENTREVISTA N°1

Buenos días/tardes, expresamos nuestro agradecimiento por el tiempo y la atención presentada para poder realizar esta entrevista, cuya información y comentarios que nos sean proporcionados serán muy valiosos para profundizar la presente investigación. Marque con un aspa la o las respuestas que considere importantes, así como responda brevemente las preguntas.

Entrevistado: CAP COM MORALES DEL PINO

Edson.Grado Académico: Bachiller

D.N.I. /C.I.P.: 41030465/122315100

Lugar – fecha: Tiabaya, 27 de agosto del 2019.

Experiencia: oficial de instrucción y entrenamiento de la compañía de guerra electrónica.

1. ¿La cantidad de personal especialista en comunicaciones y guerra electrónica es lanecesaria para el cumplimiento de su misión?

   Repuesta: La cantidad de personal que se dispone todos los años no es la suficiente,debido a que la asignación de técnicos y suboficiales cada vez es menor y algunos de ellos son destacados al cuartel general de la brigada de comunicaciones, de igual manera cada vez hay menos personal especialista en guerra electrónica debido a quela escuela de comunicaciones que era la encargada de realizar el curso básico de guerra electrónica, ya no viene realizando esta capacitación.

2. ¿Cómo se llevan a cabo las actividades de instrucción en guerra electrónica y se tieneen cuenta el conocimiento en ciberseguridad?

   Repuesta: Se vienen realizando de acuerdo a los programas de instrucción y entrenamiento, en coordinación con el G-3 instrucción, miembro del estado mayor de la 3ra brigada de comunicaciones encargado de verificar la instrucción y la capacitación del personal, no se ha considerado la instrucción en lo que respecta a ciberseguridad. Por el motivo que recién el comando del ejército se viene ordenando en dicho tema, asignando responsabilidades y estableciendo programas, un hecho

con respecto a ese tema es la creación del COTELE con las direcciones de ciberseguridad y guerra electrónica.

3. ¿Cuáles son los módulos de instrucción en los que se encuentran divida la capacitación del personal?

   Repuesta: Dentro de la instrucción del personal de oficiales, técnicos y suboficiales, existe la fase de auto preparación, en donde se monitorea su aprendizaje con las pruebas de auto preparación que se remiten periódicamente al G-3 instrucción de la brigada, paralelamente, debido a que la compañía es una unidad de alta especialización, dentro de la fase especializados se programa la instrucción al personal de técnicos y suboficiales especialistas en guerra electrónica y a todo el personal del arma de comunicaciones, de igual forma se realiza un curso para todo el personal de la brigada de comunicaciones, con poca asistencia del personal debido a que las actividades administrativas, de oficina y de servicio son prioridad ante la instrucción.

4. ¿Cuáles son las capacidades con las que deben de contar los especialistas en guerra electrónica y el personal no especialista, al final del módulo de instrucción y entrenamiento en guerra electrónica?

   Repuesta: El personal especialista debe recordar y poner en práctica todos los conocimientos adquiridos durante su programa básico de guerra electrónica, adquiriendo la riqueza técnica para poder dar opiniones y asesorar al comando sobre el tema, la habilidad para poder plantear soluciones técnicas en el caso de los técnicos y suboficiales, y soluciones tácticas en el caso de los oficiales, en caso del personal no especialista deber contar con los conocimientos básicos y ser expertos en lo relacionado a la protección electrónica.

5. ¿Cómo es la participación de la guerra electrónica en apoyo a las operaciones de ciberseguridad en la compañía de guerra electrónica?

   Repuesta: A pesar de tener el conocimiento que es un tema muy importante, en la actualidad no se viene realizando ningún trabajo o capacitación que permita apoyar

e integrar esta actividad, debido a que no se cuenta con material de guerra electrónicay no se cuenta con personal especialista en ciberseguridad en la unidad.

6. ¿Cómo se realizan los entrenamientos de engaño electrónico y de guerra electrónicadel personal de la compañía de guerra electrónica?

   Repuesta: Se realiza en un primer momento en la carta de operaciones y mediante situaciones particulares, empleando temas bases sobre la situación en donde se debentomar decisiones tácticas de empleo de la compañía, este tipo de entrenamiento es para los oficiales, para el personal subalterno especialista también se realiza mediante situaciones particulares, pero con la diferencia que deben tomar decisiones técnicas de acuerdo a la doctrina actual, para el personal de operadores, se realizan entrenamientos de protección electrónica con material de comunicaciones en los campos de instrucción que dispone la unidad, todos estos entrenamientos se realizande mejor forma en la maniobra anual que se realiza en el campo Trelles, región Locumba.

7. ¿Cuál es el material de comunicaciones con el que cuenta la compañía de guerraelectrónica?

   Repuesta: Cuenta con equipos de radio HF-6000 y VHF-9000, Tácter de campaña, teléfonos de campaña, centrales telefónicas, navegadores satelitales GPS y grupos electrógenos de 5 kw.

8. ¿Cuál es el estado de operatividad de la unidad en material de comunicaciones?

   Repuesta: De acuerdo al COEQ aprobado para la compañía de guerra electrónica, actualmente solo cuenta con el 20% de operatividad en material de comunicaciones y electrónica.

9. ¿Cuáles son las medidas anti soporte y anti ataque con las que cuenta este materialde comunicaciones?

Repuesta: Los equipos de radio HF y VHF con los que cuenta la unidad, cuentan con salto de frecuencia AJ con ECCM/COMSEC, y en modo de operaciones cuentacon los modos de AUTOCALL y ALE.

10. ¿La cantidad de material de comunicaciones es la suficiente para establecer el comando y control entre sus elementos? ¿Por qué?

    Respuesta: No, debido a que la cantidad de material de comunicaciones inalámbrico y computadoras de campaña (Tácter-31) no es la suficiente, no se puede establecer el comando y control entre todas las secciones de la compañía de guerra electrónica.

11. ¿Cuentan en la actualidad con equipos de guerra electrónica para realizar actividadesde soporte y ataque electrónico? ¿Cuál es la causa?

    Respuesta: No, actualmente no contamos con el material de guerra electrónica parapoder cumplir la misión para la que fue creada la unidad, tengo entendido que hubo un proyecto de inversión pública denominado "KUELAP" para equipar a toda la unidad, pero este no se pudo realizar por temas presupuestales a nivel MINDEF.

12. ¿Dispone de algún apoyo exterior para poder realizar capacitaciones al personal especialista en GE?

    Respuesta: Actualmente no contamos con el apoyo de ninguna otra unidad a nivel nacional, anteriormente enviábamos a nuestro personal de especialistas y operadoresa la Compañía de Inteligencia N°114 del VRAEM, ya que esta unidad se encuentra equipada, con material y equipos para realizar inteligencia de señales y COMINT.

13. ¿El personal de instructores cuenta con los conocimientos actuales en el campo de las telecomunicaciones, guerra del mando y control, propagación de ondas electromagnéticas?

Respuesta: Actualmente los conocimientos que dispone el personal de instructores son los adquiridos durante su etapa de formación y militar, los mismos que no han sido actualizados de acuerdo a los avances tecnológicos en materia de tecnologías dela información y comunicaciones.

14. ¿Se imparte instrucción de técnicas de jamming y apoyo electrónico al personal dela compañía de guerra electrónica?

Respuesta: Si, pero solo se imparten de forma teórica, debido a la falta de equipamiento en GE.

ENTREVISTA N°2

Buenos días/tardes, expresamos nuestro agradecimiento por el tiempo y la atención presentada para poder realizar esta entrevista, cuya información y comentarios que nos sean proporcionados serán muy valiosos para profundizar la presente investigación. Marque con un aspa la o las respuestas que considere importantes, así como responda brevemente las preguntas.

Entrevistado: TTE COM ZELADA QUINTANILLA

BrissetGrado Académico: Bachiller

D.N.I. /C.I.P: 70555555/400652600

Lugar – fecha: Tiabaya, 27 de agosto del 2019.

Experiencia: comandante de sección, curso básico de guerra electrónica.

1. ¿La cantidad de personal especialista en comunicaciones y guerra electrónica es lanecesaria para las labores de instrucción y entrenamiento?

   Repuesta: La cantidad de personal que dispone actualmente la unidad es insuficiente, afectando las actividades de instrucción y entrenamiento, debido a que no se cuenta con la cantidad suficiente de instructores para llevar acabo la preparación del personal a nivel de la unidad o nivel brigada.

2. ¿Cómo se llevan a cabo las actividades de instrucción en guerra electrónica y setiene en cuenta el conocimiento en ciberseguridad?

   Repuesta: Se realiza de acuerdo a la programación realizada por el oficial S-3 de la unidad, normalmente divida en módulos, ciertos módulos son de única competencia para oficiales, técnicos y suboficiales especialistas en guerra electrónica y del arma de comunicaciones y otros módulos son de estricto cumplimiento para el personal de tropa. No se cuenta con la capacitación en ciberseguridad y su importancia debido a que los programas de instrucción y entrenamiento que provienen del escalón superior no lo incluyen dentro de los módulos, de igual forma no se cuenta con el personal especialista en ciberseguridad.

3. ¿Cuáles son los módulos de instrucción en los que se encuentran divida la capacitación del personal?

   Repuesta: Módulo de auto preparación para el personal de oficiales, técnicos y suboficiales, paralelamente se realiza durante un periodo de dos a tres meses el módulo especializado en guerra electrónica con la finalidad de recordar, poner en práctica y actualizar los conocimientos del personal especialista en guerra electrónica, para el personal del arma de comunicaciones es el momento en el que ellos deben de aprender los conocimientos básicos de la guerra electrónica y en especial todo lo relacionado a la protección electrónica.

4. ¿Cuáles son las capacidades con las que deben de contar los especialistas en guerraelectrónica y el personal no especialista, al final del módulo de instrucción y entrenamiento en guerra electrónica?

   Repuesta: Para el personal especialista debe contar con la capacidad de poder dar opiniones técnicas para poder asesorar al comando en lo referente a temas de guerra electrónica, habilidad para poder plantear soluciones ante problemas del tipo técnico y táctico, para el personal no especialista disponer de los conocimientos básicos en materia de guerra electrónica y ser experto en protección electrónica.

5. ¿Cómo es la participación de la guerra electrónica en apoyo a las operaciones de ciberseguridad en la compañía de guerra electrónica?

   Repuesta: a pesar de tener el conocimiento de que es un tema muy importante, en la actualidad no se viene realizando ningún trabajo o capacitación que permita apoyar e integrar esta actividad, debido a que no se cuenta con material de guerra electrónica y no se cuenta con personal especialista en ciberseguridad en la unidad.

6. ¿Cómo se realizan los entrenamientos de engaño electrónico y de guerra electrónicadel personal de la compañía de guerra electrónica?

Repuesta: Se realizan en la sala de operaciones de la unidad, mediante situacionesparticulares a las que se dan soluciones en la carta o en el campo de instrucción y entrenamiento de la compañía, estas prácticas han tenido como sustento el programa de instrucción desarrollado con anterioridad, para posteriormente realizar un entrenamiento a nivel división de ejército en el campo Trelles de la región Locumbaen donde se ponen en práctica todo lo aprendido en el año. Con respecto a engaño electrónico se realiza engaño electrónico manipulativo, siguiendo lineamientos de un plan de engaño electrónico elaborado años atrás para la III DE.

7. ¿Cuál es el material de comunicaciones con el que cuenta la compañía de guerraelectrónica?

Repuesta: Cuenta principalmente con equipos de radio de la marca Tadiran, VHF 930,710 y HF 620, al igual que computadoras de campaña Tácter-31, como material de última adquisición, como material de campaña con antigüedad se cuenta con teléfono de campaña y centrales telefónicas.

8. ¿Cuál es el estado de operatividad de la unidad en material de comunicaciones?

Repuesta: De acuerdo al COEQ con el que cuenta la unidad, se podría especificar que se dispone de un 25% en lo que cuenta a la capacidad operativa en comunicaciones.

9. ¿Cuáles son las medidas anti soporte y anti ataque con las que cuenta este materialde comunicaciones?

Repuesta: Los equipos de radio en la banda de frecuencia de HF y VHF cuentan principalmente con el modo de trabajo en AJ (anti-jaming) y con la selección de potencia entre 5,10 y 20 watts, de igual forma el modo de trabajo en ALE y AUTOCALL.

10. ¿La cantidad de material de comunicaciones es la suficiente para establecer elcomando y control entre sus elementos? ¿Por qué?

Respuesta: La cantidad de material de comunicaciones no es la suficiente debido a que la compañía de guerra electrónica tiene muchas necesidades de comunicacionesdebido a su organización.

11. ¿Cuentan en la actualidad con equipos de guerra electrónica para realizar actividades de soporte y ataque electrónico? ¿Cuál es la causa?

Respuesta: No cuenta con material de guerra electrónica debido a que no se llevó a cabo la adquisición en su oportunidad, tengo entendido por temas de presupuesto, hasta la fecha no se ha mostrado el interés en el tema para poder reformular los proyectos y buscar adquirir capacidades que van ser muy importantes para el ejército.

12. ¿Dispone de algún apoyo exterior para poder realizar capacitaciones al personal especialista en GE?

Respuesta: Anteriormente contábamos con el apoyo de la CIA INTG 114 del VRAEM, para realizar la parte práctica que necesita nuestro personal especialista, debido a que esta unidad está equipada en inteligencia de señales. En mi opinión debería volverse a retomar este tipo de entrenamiento que es muy valioso para la experiencia del personal, que se dejó de realizar por temas de índole administrativo.

13. ¿El personal de instructores cuenta con los conocimientos actuales en el campo de las telecomunicaciones, guerra del mando y control, propagación de ondas electromagnéticas?

Respuesta: Actualmente los conocimientos que dispone el personal de instructores son los adquiridos durante su etapa de formación y militar, los mismos que no han sido actualizados de acuerdo a los avances tecnológicos en materia de tecnologías de la información y comunicaciones, pero la mayoría de conocimientos solo de forma teórica.

14. ¿Se imparte instrucción de técnicas de jamming y apoyo electrónico al personal dela compañía de guerra electrónica?

Respuesta: Si, pero solo se imparten de forma teórica, debido a la falta de equipamiento en GE.

ENTREVISTA N°3

Buenos días/tardes, expresamos nuestro agradecimiento por el tiempo y la atención presentada para poder realizar esta entrevista, cuya información y comentarios que nos sean proporcionados serán muy valiosos para profundizar la presente investigación. Marque con un aspa la o las respuestas que considere importantes, así como responda brevemente las preguntas.

Entrevistado: TTE COM SAYAN SANCHEZ

LuisGrado Académico: Bachiller

D.N.I. /C.I.P.: 70126578

Lugar – fecha: Tiabaya, 27 de agosto del

2019.Experiencia: Comandante de sección.

1. ¿La cantidad de personal especialista en comunicaciones y guerra electrónica es lanecesaria para las labores de instrucción y entrenamiento?

   Repuesta: La cantidad de personal con la que cuenta la compañía de guerra electrónica no es la adecuada, viéndose afectada las actividades de instrucción y entrenamiento, no se puede disponer de suficientes instructores y de acuerdo al COEQ de personal no se puede realizar una adecuada organización de la unidad.

2. ¿Cómo se llevan a cabo las actividades de instrucción en guerra electrónica y setiene en cuenta el conocimiento en ciberseguridad?

   Repuesta: Se realizan de acuerdo a la programación anual de instrucción, cumpliendo en todo momento la progresión semanal, esta se realiza en la sala de operaciones de la unidad, bajo el control del oficial S-3, mediante el modulo especializado para el personal de oficiales, técnicos y suboficiales especialistas y el personal no especialista que normalmente se centran en el aprendizaje de la protección electrónica. No se tiene en cuenta el conocimiento de ciberseguridad, debido a que no se cuentan con ningún elemento especialista en ese campo.

3. ¿Cuáles son los módulos de instrucción en los que se encuentran divida la capacitación del personal?

   Repuesta: Para el personal de oficiales, técnicos y suboficiales, su instrucción se realiza en el módulo de auto preparación, de igual forma se llevaba a cabo un módulo especializado en donde se enseñan todos los conocimientos básicos de guerra electrónica como son: soporte electrónico, ataque electrónico y ataque electrónico para el personal especialista y no especialista, igualmente se desarrolla un curso para el personal especialista de la unidad que se encuentra destacado en elcuartel general de la brigada.

4. ¿Cuáles son las capacidades con las que deben de contar los especialistas en guerraelectrónica y el personal no especialista, al final del módulo de instrucción y entrenamiento en guerra electrónica?

   Repuesta: El personal especialista debe estar en condiciones de poder desempeñarse como instructor de guerra electrónica ante el déficit de personal especialista, poder asesor en temas de índole técnico y táctico en guerra electrónica, el personal no especialista centrado particularmente en temas de protección electrónica y con algunos conocimientos básicos en guerra electrónica.

5. ¿Cómo es la participación de la guerra electrónica en apoyo a las operaciones de ciberseguridad en la compañía de guerra electrónica?

   Repuesta: La guerra electrónica y la ciberseguridad son interdependientes en el campo de la guerra de informaciones, actualmente no se realiza ninguna preparaciónen ese campo, debido a que no se cuenta con personal especialista en dicho campo.

6. ¿Cómo se realizan los entrenamientos de engaño electrónico y de guerra electrónicadel personal de la compañía de guerra electrónica?

Repuesta: Lo que respecta a engaño electrónico, se entrena en engaño electrónico manipulativo, mediante la elaboración de IOC (Instrucciones Operativas de Comunicaciones), falsas y libretos de comunicación ficticios, por lo que se aprende técnicas de decepción electrónica, los otros temas referentes a la instrucción se practican en la sala de operaciones de la unidad o en los campos de instrucción y entrenamiento, para después a fin de año dirigirnos al campo Trelles, donde se realiza un entrenamiento en el terreno a cargo de la III DE.

7. ¿Cuál es el material de comunicaciones con el que cuenta la compañía de guerraelectrónica?

Repuesta: Cuenta principalmente con equipos de radio de la marca Tadiran, VHF 930,710 y HF 620, al igual que computadoras de campaña Tácter-31, como material de última adquisición, como material de campaña con antigüedad se cuentan con telefonía de campaña y centrales telefónicas.

8. ¿Cuál es el estado de operatividad de la unidad en material de comunicaciones?

Repuesta: De acuerdo al COEQ con el que cuenta la unidad, se podría especificar que se dispone de un 15% en lo que cuenta a la capacidad operativa en comunicaciones.

9. ¿Cuáles son las medidas anti soporte y anti ataque con las que cuenta este materialde comunicaciones?

Repuesta: Los equipos de radio en la banda de frecuencia de HF y VHF cuentan principalmente con el modo de trabajo en AJ (anti-jaming) y con la selección de potencia entre 5, 10 y 20 watts, de igual forma el modo de trabajo en ALE y AUTOCALL.

10. ¿La cantidad de material de comunicaciones es la suficiente para establecer elcomando y control entre sus elementos? ¿Por qué?

Respuesta: La cantidad de material de comunicaciones con la que cuenta la compañía es insuficiente para poder satisfacer las necesidades de comunicaciones, de igual forma cuando se realizan los entrenamientos en el terreno, es necesario solicitar material en calidad de préstamo para poder cubrir nuestra necesidad en materia de entrenamiento. Todo esto debido a que su organización contempla variassecciones.

11. ¿Cuentan en la actualidad con equipos de guerra electrónica para realizar actividades de soporte y ataque electrónico? ¿Cuál es la causa?

Respuesta: No se cuenta con material de guerra electrónica debido a que no se llevó a cabo la adquisición en su oportunidad tengo entendido por temas de presupuesto, hasta la fecha no se ha mostrado el interés en el tema para poder reformular los proyectos y buscar que adquirir capacidades que van ser muy importantes para el ejército.

12. ¿Dispone de algún apoyo exterior para poder realizar capacitaciones al personal especialista en GE?

Respuesta: Anteriormente contábamos con el apoyo de la CIA INTG 114 del VRAEM, para realizar la parte práctica que necesita nuestro personal especialista, debido a que esta unidad está equipada en inteligencia de señales. En mi opinión debería volverse a retomar este tipo de entrenamiento que es muy valioso para la experiencia del personal, que se dejó de realizar por temas de índole administrativo.

13. ¿El personal de instructores cuenta con los conocimientos actuales en el campo de las telecomunicaciones, guerra del mando y control, propagación de ondas electromagnéticas?

Respuesta: Actualmente los conocimientos que dispone el personal de instructores, fueron adquiridos durante su etapa de formación y militar, los mismos que no han sido actualizados de acuerdo a los avances tecnológicos en materia de tecnologías de la información y comunicaciones.

14. ¿Se imparte instrucción de técnicas de jamming y apoyo electrónico al personal dela compañía de guerra electrónica?

Respuesta: Si, pero solo se imparten de forma teórica, debido a la falta de equipamiento en GE.

FICHA DE REGISTRO DOCUMENTAL

Datos de la aplicación

Nombre de la unidad: Compañía de guerra electrónica.

Nombre de los investigadores: MY COM Freddy Echeverría Martínez,
MY COM Erinna Arévalo Salas.

Documentos revisados:

DOCUMENTOS	TIENE		SE REVISO	
	SI	NO	SI	NO
MEMORIA ANUAL	**x**		**x**	
COEQ DE LA UNIDAD	**x**		**x**	

Aspectos por verificar:

MEMORIA ANUAL

1. Todas las actividades de instrucción que haya realizado la unidad, específicamentelas relacionadas con el S-3.(Instrucción y Operaciones)
2. Todas actividades de entrenamiento y maniobras en el campo que haya realizado launidad.
3. Formulación y actualización de planes que se hayan realizado en la unidad.
4. Conclusiones y recomendaciones del campo de estado mayor de instrucción y entrenamiento.
5. Conclusiones y recomendaciones del campo funcional de planes y operaciones de launidad.
6. Conclusiones y recomendaciones del campo funcional de logística.
7. Conclusiones y recomendaciones del campo funcional de personal.

COEQ

1. Cantidad de personal asignado.
2. Cantidad de equipos de comunicaciones y electrónica asignados.

ASPECTOS VERIFICADOS

1. INSTRUCCIÓN Y ENTRENAMIENTO

27 ABR -18 La CIA GE, se desplazó con personal y material (COMUNICACIONES) a la Región Pampas San José con la finalidad de presentar al Sr Comandante General de la 3ra Brigada de comunicaciones el despliegue de los medios para el plan de engaño electrónico contemplado dentro del plan de acción inmediata y a su vez presenciar la exposición de la empresa Judía IAI exposición del sistema de comando y control para el proyecto "CAHUIDE".

23 MAY-18 Se desplegó material y equipo de comunicaciones a las instalaciones del COREMOV; en el mencionado lugar se hizo un ejercicio de comunicaciones ante la presencia del Sr Crl Com Inspector de la 3ª BRIG COM sobre redes de engaño en HF y VHF.

19-23 NOV-18 de acuerdo a la DVA Nº 001/III DE/3ª BRIG COM/C-1/05.00.00 Nov 2018, del 19 al 23 de NOV 2018, se realizó el ejercicio de entrenamiento conjunto a nivel III DE en la Rg LOCUMBA, corredor de la costa y Rg CHALLAPALCA, corredor de la sierra, correspondiente al ejercicio de entrenamiento en el terreno a nivel III DE como parte del componente terrestre AF-2018; en la cual la CIA GE tuvo la misión de instalar redes de engaño para asegurar la supervivencia de los PC en el corredor de la costa, asimismo proteger electrónicamente las comunicaciones, de que los batallones aseguren el enlace de sus GUB; siendo inspeccionado en el campo (LOCUMBA) por el Sr. CRL Inspector de la III DE Crl Com ICOCHEA, manifestando la FELICITACION correspondiente a los integrantes que conformaban las redes de engaño y por ente al Sr My Com Cmdte de la CIA GE.

a. CONCLUSIONES

1) La instrucción del curso de guerra electrónica para el personal de oficiales,técnicos y sub oficiales que no tiene la especialidad, se llevó a cabo en forma normal.

2) Se deben mantener las instrucciones de actualización de guerra electrónicaal personal de unidad, debido al avance de la tecnología.

b. RECOMENDACIONES

Se mantengan las instrucciones de actualización en guerra electrónica a todo el personal de la unidad, debido a que el avance de la tecnología hace que losconocimientos necesiten ser actualizados constantemente.

2. PLANES Y OPERACIONES

a. FRENTE EXTERNO

1) Se realizó el ejercicio de entrenamiento conjunto a nivel III DE en Rg LOCUMBA por el corredor de la Costa y Rg CHALLAPALCA por el corredor de la cierra, correspondiente al ejercicio de entrenamiento en el terreno a nivel III DE como parte del componente terrestre AF-2013.

2) La CIA GE tuvo la misión de instalar redes de engaño para asegurar la supervivencia de los PC (Puestos de Comando) en el corredor de la costa.

3) La CIA GE protegió electrónicamente las comunicaciones, logrando de que los batallones aseguren el enlace de sus GUB; siendo inspeccionada esta operación en el campo (LOCUMBA) por el Sr. CRL Inspector de la III DE.

b. FRENTE INTERNO

1) El 220800 May 2018, la INSPECTORIA de la 3ª BRIG COM, inspeccionó a la CIA GE; en donde se desplegó personal, material y equipo al COREMOV.

2) En esta región se hizo un ejercicio de comunicaciones ante la presencia del Sr Crl Com Inspector de la 3ª BRIG COM y su comitiva; para lo cual

se explicó cómo se conformaron las redes de engaño en HF y VHF para elengaño electrónico, la 1era red con el puesto de comando falso de la III DE en HF, la cual transmitiría información falsa en claro, secreto y AJ de igual manera se utilizó el equipo de radio AN/GRA-39 para la seguridad de los operadores, para las redes en VHF se estableció el mismo procedimiento de trabajo pero simulando más estaciones que vendrían a ser los puestos de comando ficticios de las GUC que son los elementos demaniobra en el corredor de la costa.

c. CONCLUSIONES

1) El personal de oficiales, técnicos y suboficiales ha logrado los diferentes objetivos y metas trazadas, teniendo como resultado calificaciones optimas, felicitaciones y críticas positivas por el comando.
2) En el campo de planes y operaciones, se ha logrado que el personal de oficiales, técnicos y sub oficiales y tropa conozca su función dentro de losdiferentes planes así como la misión de la compañía.

d. RECOMENDACIONES

1) Se recomienda que se asigne un campo de instrucción a la unidad para poder llevar a cabo de mejor manera la instrucción y entrenamiento del personal.
2) Se recomienda que se asigne el material de comunicaciones y material diverso necesario, vistas las necesidades en los diferentes ejercicios de comunicaciones.

3. LOGISTICA

a. CONCLUSIONES

SERVICIO LOGISTICO DE COMUNICACIONES

La CIA GE, tiene como misión asignada por el comando, realizar redes de engaño en HF y VHF para el engaño electrónico tanto para el corredor de la costa y el corredor de la sierra (la 1era red con el puesto de comando falso de la III DE en HF); el cual transmitiría información falsa en claro, secreto y AJde igual manera se utilizaría los equipos de radio AN/GRA-39 para la seguridad de los operadores, para las redes en VHF se establecería el mismo procedimiento de trabajo pero simulando más estaciones que vendrían a ser los puestos de comando ficticios de las GUC que son los elementos de maniobra, se recomienda el completamiento del siguiente material de comunicaciones:

- Se necesita equipos de radio HF (PRC-6020, VRC-6200V y VRC-6200F) y equipos de radio VHF (PRC-930, VRC-950 versión vehicular, VRC-950Versión Base), CANT: 08 por c/Equipo.
- Se necesita antenas especiales HTDA-8020 para los equipos de radio HF PRC-6020.
- Se necesita equipos de radio AN/GRA 39, para realizar la integración de los equipos de radio HF y VHF, CANT: 08 por c/Equipo.
- Se necesita baterías BA-30 de 3 voltios marca DURACELL para los equipos de radio AN/GRA 39.
- Se necesita baterías TNC 2188 y baterías LITHIUM-ION TLI-9380E TADIRAN, CANT: 16 por c/batería.
- Se necesita amplificadores de potencia, que permitirán dar mayor alcance a la comunicación inalámbrica.
- Se necesita cable de campaña WD-1/TT, aproximadamente 08 millas.
- Se necesita equipo de herramientas e instrumentos, para realizar el mantenimiento preventivo de 1er y 2do Elon, para los equipos de HF y VHF.
- Se necesita carretes y desenrrolladores para el tendido de línea.
- Se necesita baterías recargables TRB-1264 LITHIUM-ION DF 10.8 VDC 4.0 A-H, para el terminal táctico de datos versión MANPACK.
- Se necesita cables de conexión (Cable CX-8972 de 1.5 mts), para terminal táctico de datos versión Manpack, que permitirán realizar la integración conlos Equipos de radio HF.

- Se necesita cables de conexión (Cable CX-5455 de 2.00 mts), para el terminal táctico de datos versión Manpack, que permitirán realizar la integración con los equipos de radio VHF.
- Se necesita grupos electrógenos de 1.5 Kw y 3.5 Kw.
- Se necesita transformador de 220/500W y 220/1000W.
- Se necesita panel solar para carga de baterías TNC 2188 Power Pack 4.

b. RECOMENDACIONES

1) SERVICIO LOGISTICO DE COMUNICACIONES

Que la SELOG (Sección Logística) de la 3ª Brigada de Comunicaciones realice la gestión al escalón superior para la asignación de material y equipos de radio, para realizar el despliegue y funcionamiento del plan deengaño electrónico.

2) PERSONAL

Se recomienda el completamiento del personal de oficiales, técnicos y sub oficiales, que de preferencia que sean especialistas en GE para poder realizar una serie de trabajos por parte de la compañía.

3) CUADRO DE ORGANIZACIÓN Y EQUIPO (COEQ)

a) PERSONAL

Según los datos del COEQ en lo que respecta a personal, la compañía de guerra electrónica debería contar con 16 oficiales y 164 técnicos y suboficiales entre especialistas en guerra electrónica y otras especialidades, de acuerdo a la memoria anual, solo se cuenta con 6 oficiales lo que representa el 40%, técnicos y suboficiales solo cuenta con 11 lo que representa el 7% de su personal.

b) LOGISTICA

Según el COEQ de material y equipo de comunicaciones y GE, la compañía de guerra electrónica en cada una de sus secciones debe estar equipada con el material de guerra electrónica que le corresponde, lo que hasta la fecha no ha sido adquirido por parte de

la institución. En lo que respecta a comunicaciones en el COEQ figura que debe de contar con 10 radios C/P UHF , 10 radios B/P FM, 10 radios C/V FM, 5 equipos C/P FM base, 10 equipos C/P BLU, 10 equipos C/V BLU, 5 equipos C/P BLU base, 15 tácter 31k, de lo cual solo dispone de 03 equipos B/P BLU, 03 equipos B/P FM y 03 tácter 31k lo que representa el 10% en equipos de comunicaciones y el 20% en tácter 31k.

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO
Escuela de Postgrado
VII Maestría en Ciencias Militares

FICHA DE OBSERVACION DE INSTRUCCIÓN Y MATERIAL

Nombre del Instructor: STTE COM MEZA QUISPE Juan.

Nombre del Jefe de Unidad: MY COM BERLANGA LOAYZA Jorge.

Tiempo de observación: 60 minutos

Fecha de la observación: 27 de agosto 2019.

Parte Técnico Pedagógico

Instrucciones: Según las observaciones visualizadas al momento de realizar la observación en el campo de instrucción.

INSTRUCCION:

No	DESCRIPCION	SI	NO	OBS
1	El instructor a cargo de la capacitación del curso de guerra electrónica posee y demuestra tener los conocimientos, la metodología y la experiencia necesaria y adecuada para lograr que sus instruidos alcancen un buen nivel de instrucción		x	Dispone de instructores que no son dela especialidad
2	La unidad dispone de ambientes adecuados e implementados para realizar la preparación teórica de los fundamentos básicos de Guerra Electrónica.		x	Ambientes inadecuados
3	La unidad dispone de campos de instrucción adecuados para desarrollar la parte teórica de manera práctica.		X	No dispone de campos de instrucción
4	La unidad dispone de ayudas y material de apoyo a la instrucción para el mejor desarrollo de las asignaturas.		X	No dispone de ayudas adecuadas
5	La unidad cuenta con el programa de instrucción y entrenamiento (PIE) correspondiente a toda la fase especializada que llevan a cabo los instruidos de guerra electrónica, de igual manera disponen de notas del instructor, que certifican la buena conducción de la asignatura.	X		Dispone de documentación de instrucción
6	Al final de la instrucción, el personal demuestra capacidad para poder resolver las situaciones problemáticas impuestas por el instructor, dando soluciones prácticas de acuerdo a lo aprendido durante la asignatura.		x	Capacidades limitadas

MATERIAL

No	DESCRIPCION	SI	NO	OBS
1	El material y equipo de comunicaciones con el que cuenta la compañía de guerra electrónica es el suficiente para poder administrar sus redes de comando y control para el cumplimiento de la misión asignada.		x	Cantidad de material insuficiente
2	El material y equipo con el que cuenta la compañía de guerra electrónica, es de última tecnología en materia de seguridad y transmisión de datos.	X		Con características básicas.
3	Dispone de material y equipos de guerra electrónica.		x	No adquirido
4	Se realiza el mantenimiento de 1er y 2do Elon del material y equipo de comunicación de acuerdo a los programas de mantenimiento preventivo.	x		No herramientas y personal mantenimiento
5	La unidad dispone de ambientes y almacenes adecuados que garanticen la buena conservación del material de comunicaciones.		x	Sin características suficientes
6	La unidad dispone de personal capacitado en mantenimiento (Mecánicos de comunicaciones) que pueda brindar el soporte necesario para la conservación del material.	x		Limitado, sin capacidad de empleo

ANEXO 3

VALIDACION DE INSTRUMENTOS

FICHA DE DATOS PERSONALES DEL VALIDADOR EXTERNO

1. Apellidos y nombres del informante (Experto):
   LAZO ACOSTA, Karina del Pilar……
2. DNI: 06807309……
3. Grado Académico: MAGISTER EN CIENCIAS MILITARES……
4. Profesión: Oficial del Ejército del Perú……..….
5. Especialidad: Comunicaciones……
6. Colegiatura:……..……Código:……..
7. Institución donde labora: 1RA BRIFFEE-CIA COM61…….
8. Cargo que desempeña: Comandante de PPUU…….
9. Denominación del Instrumento:
   Guía de entrevista…… …….
10. Autor del instrumento:
    ECHEVERRIA MARTINEZ, Freddy……
11. Programa Maestría:
    VII MAESTRIA EN CIENCIAS MILITARES……..

Chorrillos, 22 de setiembre de 2020.

Karina del Pilar LAZO ACOSTA
Magister

ESCUELA SUPERIOR DE GUERRA DEL

EJÉRCITOESCUELA DE

POSTGRADO

Apellido y Nombre del Experto informante	Cargo o Institución donde labora	Nombre del instrumento	Autor del Instrumento
LAZO ACOSTA, Karina del Pilar.	1ra BRIFFE-CIA COM 61	Entrevista de opinión.	ECHEVERRIA MARTINEZ Freddy AREVALO SALAS Erinna.

Título de la Investigación: Análisis del estado actual de la compañía de guerra electrónica de la 3ra Brigada de Comunicaciones.

I. ASPECTOS DE EVALUACION

CRITERIOS	INDICADORES	DEFICIENTE 00-20%				REGULAR 21-40%				BUENO 41-60%				MUY BUENO 61-80%				EXCELENTE 81-100%			
		0	6	11	16	21	28	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje apropiado																			95	
2. OBJETIVO	Está expresado en Capacidades observables																			95	
3. ACTUALIDAD	Adecuado a la identificación del conocimiento de las variables de investigación																			94	
4. ORGANIZACIÓN	Existe una organización lógica enel instrumento																			95	
5. SUFICIENCIA	Comprende los aspectos en cantidad Y calidad con respecto a las variables de investigación																			95	
6. INTENCIONALIDAD	Adecuado para valorar aspectos de las variables de investigación																			95	
7. CONSISTENCIA	Basado en aspectos teóricos de conocimiento																			95	
8. COHERENCIA	Existe coherencia entre los índices e va y las dimensiones																			94	
9. METODOLOGÍA	La estrategia responde al propósito de la investigación																			94	
10. PERTINENCIA	El inventario es aplicable																			95	

II. OPINIÓN DE APLICACIÓN:

Favorable y aplicable al contexto actual de aislamiento social…….

III. OPINIÓN DE APLICACIÓN:

Instrumento válido y aplicable……

IV. PROMEDIO DE VALORACIÓN: 94.80

LUGAR Y FECHA	DNI	FIRMA DEL EXPERTO INFORMANTE	N" DE TELÉFONO
Chorrillos, 22 de setiembre de 2020	06807309		998000456

ESCUELA SUPERIOR DE GUERRA DEL

EJÉRCITOESCUELA DE

POSTGRADO

TÍTULO DE LA INVESTIGACIÓN:
Análisis del estado actual de la Compañía de Guerra Electrónica de la 3ra Brigada de Comunicaciones.

I. DATOS DEL EXPERTO:

a. Apellidos y nombres : LAZO ACOSTA Karina del Pilar
b. Grado académico-profesión : Magister en Ciencias Militares
c. D.N.I. 06807309
d. N° de teléfono 998
e. Lugar y fecha : Ch[illegible] del 2020.
f. Firma :

II. **DATOS DEL INSTRUMENTO DE EVALUACIÓN** (entrevista)

a. Autor(es) del instrumento : ECHEVERRIA MARTINEZ Freddy/AREVALO SALAS Erinna.
b. Institución a la que pertenece: EJÉRCITO DEL PERÚ, ESGE-EPG.
c. Método de investigación : HERMENEUTICO FENOMENOLOGICO
d. Tipo de entrevista : EMPIRICO

III. ASPECTOS DE EVALUACIÓN

N°	Criterios	Indicadores	Valoración De: O a 1
01	Diseño	Convocatoria: Lugar – tiempo. Contenidos: Propuesta de temas- preguntas – respuestas.	0.90
02	Organización	Selección: informantes – representación de temas – tipo de respuesta – número de entrevistas.	0.95
03	Estructuración	Guía de entrevista : Dirección a seguir - Objetivos - N° de preguntas según tipo de entrevista Contexto de los datos: Conocer experiencias del entrevistado Tema propios : Aspectos que interesen	1.00
04	Secuencial	Con relación a variables – dimensiones e indicadores. Sigue un orden lógico y pre-requisitorial.	0.98
05	Conectividad	Conjuga el tipo de pregunta con el objetivo de investigación y se armoniza con las experiencias que esperan ser revaloradas en el cuestionario.	1.00
06	Intencionalidad	Adecuado para valorar aspectos desconocidos y/o modificados de las variables de investigación.	1.00
07	Actualidad	Existe coherencia entre resultados alcanzados con la realidad por conocer en el marco de doctrina, leyes, teorías vigentes.	0.97
08	Contrastación de otros Resultados	Han sido formuladas las preguntas, conociéndose los resultados alcanzados por otro instrumento para comparar la hipótesis de investigación.	0.95
09	Orientación a solución de problemas	Se concatenan las preguntas para alcanzar criterios, juicios, conceptos que ayuden a solucionar el problema de investigación planteado.	0.96
10	Análisis e interpretación	Se ha adecuado algún instrumento o herramienta para verter los resultados de la entrevista y analizarlos /interpretarlos.	0.95

III. RESULTADO DE VALORACIÓN:

96.60%

Aspectos para la valoración
- Valida por 05 expertos de la ESGE-EPG
- Debe aplicarse la prueba de la "V" de Aiken
- Resultado mínimo aprobatorio: 0.85 u 85%
- La validación solo se hará hasta dos decimales que terminen en cero o en cinco. Ejemplo: 0.60; 0.75

V. OPINIÓN DE APLICACIÓN

El instrumento de evaluación cumple con todos los criterios que deben considerarse en su formulación.
Es aplicable

FICHA DE DATOS PERSONALES DEL VALIDADOR EXTERNO

1. Apellidos y nombres del informante (Experto):
   ESTELA RENGIFO Cristobal .....……
2. DNI: 40086186……
3. Grado Académico: MAGISTER EN CIENCIAS MILITARES……
4. Profesión: Oficial del Ejército del Perú……..….
5. Especialidad: Comunicaciones……
6. Colegiatura:……..……Código:……..
7. Institución donde labora: 3I BRIG. INF-BCT 79
8. Cargo que desempeña: S-3…….
9. Denominación del Instrumento:
   Guía de entrevista……. …….
10. Autor del instrumento:
    ECHEVERRIA MARTINEZ, Freddy……
11. Programa Maestría:
    VII MAESTRIA EN CIENCIAS MILITARES……..

Chorrillos, 22 de setiembre de 2020.

Cristóbal ESTELA RENGIFO
Magister

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO

ESCUELA DE POSTGRADO

Apellido y Nombre del Experto informante	Cargo o Institución donde labora	Nombre del instrumento	Autor del Instrumento
ESTELA RENGIFO Cristobal	31 brigada infantería-BCT 79	Entrevista de opinión.	ECHEVERRIA MARTINEZ Freddy AREVALO SALAS Erinna.

Título de la Investigación: Análisis del estado actual de la compañía de guerra electrónica de la 3ra Brigada de comunicaciones.

I. ASPECTOS DE EVALUACION

CRITERIOS	INDICADORES	DEFICIENTE 00-20%				REGULAR 21-40%				BUENO 41-60%				MUY BUENO 61-80%				EXCELENTE 81-100%			
		0	6	11	16	21	28	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje apropiado																			95	
2. OBJETIVO	Está expresado en Capacidades observables																			95	
3. ACTUALIDAD	Adecuado a la identificación del conocimiento de las variables de investigación																			94	
4. ORGANIZACIÓN	Existe una organización lógica enel instrumento																			95	
5. SUFICIENCIA	Comprende los aspectos en cantidad Y calidad con respecto a las variables de investigación																			95	
6. INTENCIONALIDAD	Adecuado para valorar aspectos de las variables de investigación																			95	
7. CONSISTENCIA	Basado en aspectos teóricos de conocimiento																			95	
8. COHERENCIA	Existe coherencia entre los índices e indicadores y las dimensiones																			94	
9. METODOLOGÍA	La estrategia responde al propósito de la investigación																			94	
10. PERTINENCIA	El inventario es aplicable																			95	

II. OPINIÓN DE APLICACIÓN:

Favorable y aplicable al contexto actual de aislamiento social……..

III. OPINIÓN DE APLICACIÓN:

Instrumento válido y aplicable……

IV. PROMEDIO DE VALORACIÓN: 94.80

LUGAR Y FECHA	DNI	FIRMA DEL EXPERTO INFORMANTE	N" DE TELÉFONO
Chorrillos, 22 de setiembre de 2020	40086186		943932105

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO

ESCUELA DE POSTGRADO

TÍTULO DE LA INVESTIGACIÓN:
Análisis del estado actual de la Compañía de Guerra Electrónica de la 3ra Brigada de Comunicaciones.

II. DATOS DEL EXPERTO:

a. Apellidos y nombres : ESTELA RENGIFO Cristobal.
b. Grado académico-profesión : Magister en Ciencias Militares
c. D.N.I. 40086186
d. N° de teléfono 943932105
e. Lugar y fecha : Chorrillos, 22 de Setiembre del 2020.
f. Firma :

IV. **DATOS DEL INSTRUMENTO DE EVALUACIÓN** (entrevista)

a. Autor(es) del instrumento : ECHEVERRIA MARTINEZ Freddy/AREVALO SALAS Erinna.
b. Institución a la que pertenece: EJÉRCITO DEL PERÚ, ESGE-EPG.
c. Método de investigación : HERMENEUTICO FENOMENOLÓGICO
d. Tipo de entrevista : EMPIRICO

III. ASPECTOS DE EVALUACIÓN

N°	Criterios	Indicadores	Valoración De: O a 1
01	Diseño	Convocatoria: Lugar – tiempo. Contenidos: Propuesta de temas- preguntas – respuestas.	0.90
02	Organización	Selección: informantes – representación de temas – tipo de respuesta – número de entrevistas.	0.95
03	Estructuración	Guía de entrevista : Dirección a seguir - Objetivos - N° de preguntas según tipo de entrevista Contexto de los datos: Conocer experiencias del entrevistado Tema propios : Aspectos que interesen	1.00
04	Secuencial	Con relación a variables – dimensiones e indicadores. Sigue un orden lógico y pre-requisitorial.	0.98
05	Conectividad	Conjuga el tipo de pregunta con el objetivo de investigación y se armoniza con las experiencias que esperan ser revaloradas en el cuestionario.	1.00
06	Intencionalidad	Adecuado para valorar aspectos desconocidos y/o modificados de las variables de investigación.	1.00
07	Actualidad	Existe coherencia entre resultados alcanzados con la realidad por conocer en el marco de doctrina, leyes, teorías vigentes.	0.97
08	Contrastación de otros Resultados	Han sido formuladas las preguntas, conociéndose los resultados alcanzados por otro instrumento para comparar la hipótesis de investigación.	0.95
09	Orientación a solución de problemas	Se concatenan las preguntas para alcanzar criterios, juicios, conceptos que ayuden a solucionar el problema de investigación planteado.	0.96
10	Análisis e interpretación	Se ha adecuado algún instrumento o herramienta para verter los resultados de la entrevista y analizarlos /interpretarlos.	0.95

V. RESULTADO DE VALORACIÓN:

96.60%

Aspectos para la valoración

- Valida por 05 expertos de la ESGE-EPG
- Debe aplicarse la prueba de la "V" de Aiken
- Resultado mínimo aprobatorio: 0.85 u 85%
- La validación solo se hará hasta dos decimales que terminen en cero o en cinco. Ejemplo: 0.60; 0.75

V. OPINIÓN DE APLICACIÓN

El instrumento de evaluación cumple con todos los criterios que deben considerarse en su formulación.
Es aplicable

FICHA DE DATOS PERSONALES DEL VALIDADOR EXTERNO

1. Apellidos y nombres del informante (Experto):
   ALANOCA SANCHEZ Jefferson.....……
2. DNI: 40422376……
3. Grado Académico: MAGISTER EN CIENCIAS MILITARES……
4. Profesión: Oficial del Ejército del Perú……..….
5. Especialidad: Comunicaciones……
6. Colegiatura:……..……Código:……..
7. Institución donde labora: COEDE-ESC MG…….
8. Cargo que desempeña: DEDUC.…….
9. Denominación del Instrumento:
   Guía de entrevista……. …….
10. Autor del instrumento:
    ECHEVERRIA MARTINEZ, Freddy……
11. Programa Maestría:
    VII MAESTRIA EN CIENCIAS MILITARES……..

Chorrillos, 22 de setiembre de 2020.

Jefferson ALANOCA SANCHEZ
Magister

ESCUELA SUPERIOR DE GUERRA DEL

EJÉRCITOESCUELA DE

POSTGRADO

Apellido y Nombre del Experto informante	Cargo o Institución donde labora	Nombre del instrumento	Autor del Instrumento
ALANOCA SANCHEZ Jefferson	1ra BRIFFE-ESC MG	Entrevista de opinión.	ECHEVERRIA MARTINEZ Freddy AREVALO SALAS Erinna.

Título de la Investigación: Análisis del estado actual de la Compañía de Guerra Electrónica de la 3ra Brigada de comunicaciones.

II. ASPECTOS DE EVALUACION

CRITERIOS	INDICADORES	DEFICIENTE 00-20%				REGULAR 21-40%				BUENO 41-60%				MUY BUENO 61-80%				EXCELENTE 81-100%			
		0	6	11	16	21	28	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje apropiado																			95	
2. OBJETIVO	Está expresado en Capacidades observables																			95	
3. ACTUALIDAD	Adecuado a la identificación del conocimiento de las variables de investigación																			94	
4. ORGANIZACIÓN	Existe una organización lógica enel instrumento																			95	
5. SUFICIENCIA	Comprende los aspectos en cantidad Y calidad con respecto a las variables de investigación																			95	
6. INTENCIONALIDAD	Adecuado para valorar aspectos de las variables de investigación																			95	
7. CONSISTENCIA	Basado en aspectos teóricos de conocimiento																			95	
8. COHERENCIA	Existe coherencia entre los índices e indicadores y las dimensiones																			94	
9. METODOLOGÍA	La estrategia responde al propósito de la investigación																			94	
10. PERTINENCIA	El inventario es aplicable																			95	

III. OPINIÓN DE APLICACIÓN:

Favorable y aplicable al contexto actual de aislamiento social……..

IV. OPINIÓN DE APLICACIÓN:

Instrumento válido y aplicable……

IV. PROMEDIO DE VALORACIÓN: 94.80

LUGAR Y FECHA	DNI	FIRMA DEL EXPERTO INFORMANTE	N" DE TELÉFONO
Chorrillos, 22 de setiembre de 2020	40422376		937286574

ESCUELA SUPERIOR DE GUERRA DEL

EJÉRCITOESCUELA DE

POSTGRADO

TÍTULO DE LA INVESTIGACIÓN:
Análisis del estado actual de la compañía de guerra electrónica de la 3ra Brigada de comunicaciones.

III. DATOS DEL EXPERTO:

a. Apellidos y nombres : ALANOCA SANCHEZ Jefferson
b. Grado académico-profesión : Magister en Ciencias Militares
c. D.N.I. 40422376
d. N° de teléfono 937286574
e. Lugar y fecha : Chorrillos, 22 de Setiembre del 2020.
f. Firma :

VI. **DATOS DEL INSTRUMENTO DE EVALUACIÓN** (entrevista)

a. Autor(es) del instrumento : ECHEVERRIA MARTINEZ Freddy/AREVALO SALAS Erinna.
b. Institución a la que pertenece: EJÉRCITO DEL PERÚ, ESGE-EPG.
c. Método de investigación : HERMENEUTICO FENOMENOLOGICO
d. Tipo de entrevista : EMPIRICO

III. ASPECTOS DE EVALUACIÓN

N°	Criterios	Indicadores	Valoración De: O a 1
01	Diseño	Convocatoria: Lugar – tiempo. Contenidos: Propuesta de temas- preguntas – respuestas.	0.90
02	Organización	Selección: informantes – representación de temas – tipo de respuesta – número de entrevistas.	0.95
03	Estructuración	Guía de entrevista : Dirección a seguir - Objetivos - N° de preguntas según tipo de entrevista Contexto de los datos: Conocer experiencias del entrevistado Tema propios : Aspectos que interesen	1.00
04	Secuencial	Con relación a variables – dimensiones e indicadores. Sigue un orden lógico y pre-requisitorial.	0.98
05	Conectividad	Conjuga el tipo de pregunta con el objetivo de investigación y se armoniza con las experiencias que esperan ser revaloradas en el cuestionario.	1.00
06	Intencionalidad	Adecuado para valorar aspectos desconocidos y/o modificados de las variables de investigación.	1.00
07	Actualidad	Existe coherencia entre resultados alcanzados con la realidad por conocer en el marco de doctrina, leyes, teorías vigentes.	0.97
08	Contrastación de otros Resultados	Han sido formuladas las preguntas, conociéndose los resultados alcanzados por otro instrumento para comparar la hipótesis de investigación.	0.95
09	Orientación a solución de problemas	Se concatenan las preguntas para alcanzar criterios, juicios, conceptos que ayuden a solucionar el problema de investigación planteado.	0.96
10	Análisis e interpretación	Se ha adecuado algún instrumento o herramienta para verter los resultados de la entrevista y analizarlos /interpretarlos.	0.95

VII. RESULTADO DE VALORACIÓN:

96.60%

Aspectos para la valoración

- Valida por 05 expertos de la ESGE-EPG
- Debe aplicarse la prueba de la "V" de Aiken
- Resultado mínimo aprobatorio: 0.85 u 85%
- La validación solo se hará hasta dos decimales que terminen en cero o en cinco. Ejemplo: 0.60; 0.75

V. OPINIÓN DE APLICACIÓN

El instrumento de evaluación cumple con todos los criterios que deben considerarse en su formulación.
Es aplicable

ANEXO 4

AUTORIZACION PARA EL ACCESO DE RECOLECCION DE DATOS

PERÚ | Ministerio de Defensa | Ejército del Perú | Comando de Educación y Doctrina del Ejército

"Año del Bicentenario del Perú: 200 años de Independencia"

Oficio Nº 080/U-8.g.1/27.00

Chorrillos, 18 de Junio del 2021.

Señor : General de Brigada
Rivera Machuca John Edgar
Comandante General del Agrupamiento José Olaya.-**Tiabaya**

Asunto : Solicita brindar facilidades al personal que se indica.

Ref. : a. Reglamento de investigación de la ESGE-EPG.
b. Reglamento para la obtención del grado de maestro de ciencias militares.

Tengo el agrado de dirigirme a usted en relación al documento de la referencia, para solicitarle se digne disponer a quien corresponda brindar las facilidades para el acceso a las instalaciones de la compañía de guerra electrónica N°113 al Tte Crl EP ECHEVERRIA MARTINEZ Freddy Jesús identificado con CIP Nº 121291500 y DNI Nº 40048592 y la My EP AREVALO SALAS Erina Evelyn identificada con CIP Nº 400103600 DNI Nº 43337338 oficiales investigadores de esta casa de estudio que realizaron la investigación titulada "ANALISIS DEL ESTADO ACTUAL DE LA COMPAÑÍA DE GUERRA ELECTRONICA DE LA 3RA BRIGADA DE COMUNICACIONES.

Es propicia la oportunidad para renovarle los sentimientos de especial consideración y estima personal.

Dios guarde a Ud.

ESCUELA SUPERIOR DE GUERRA - DIRECCIÓN -

O – 214452665 - A+
LUIS ALBERTO ROJO ALZAMORA
General de Brigada
DIRECTOR
ESGE-ESCUELA DE POSTGRADO

DISTRIBUCIÓN:
- Agrupamiento JO.....01
- Archivo 01/02

PERÚ | Ministerio de Defensa | Ejército del Perú | Comando de Educación y Doctrina del Ejército

"Año del Bicentenario del Perú: 200 años de Independencia"

Chorrillos, 20 de Junio del 2021.

Oficio N° 001/U-8.g.1/27.00

Señor : Gral Brig Director de la ESGE-EPG.-**CHORRILLOS.**

Asunto : Autoriza brindar facilidades a los oficiales que se indican.

Ref. : a. Reglamento de investigación de la ESGE-EPG.
b. Reglamento para la obtención del grado de maestro de ciencias militares.

Tengo el Honor de dirigirme a usted en relación al documento de la referencia, para brindar autorización de acceso a nuestras instalaciones y a nuestro personal de la Compañía de Guerra Electrónica a los siguientes oficiales: Tte Crl EP ECHEVERRIA MARTINEZ Freddy Jesús identificado con CIP N° 121291500 y DNI N° 40048592 y la My EP AREVALO SALAS Erina Evelyn identificada con CIP N° 400103600 DNI N° 43337338 oficiales investigadores de su caso de estudio que realizaron la investigación titulada "ANÁLISIS DEL ESTADO ACTUAL DE LA COMPAÑÍA DE GUERRA ELECTRÓNICA DEL AGRUPAMIENTO DE COMUNICACIONES "JOSÉ OLAYA".

Es propicia la oportunidad para renovarle los sentimientos de especial consideración y estima personal.

Dios guarde a Ud.

AGRUPAMIENTO JOSE OLAYA COMANDANCIA

O – 2015947666 - A+
JOHN EDGAR RIVERA MACHUCA
General de Brigada
CMDTE GRAL DEL AGRUPAMIENTO JOSE OLAYA

DISTRIBUCIÓN:
- ESGE-EPG.....01
- Archivo 01
- Investigador.....01/03

"EL COEDE ES EL EJEMPLO DEL EJÉRCITO"

ANEXO 5

COMPROMISO ETICO

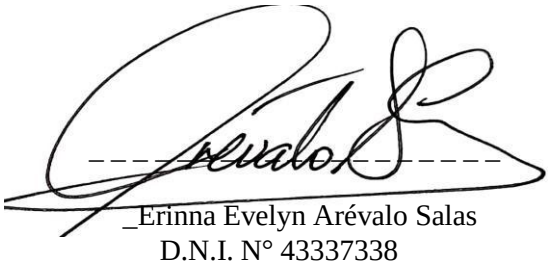
Declaración Jurada de Autoría

Mediante el presente documento, Yo, Erinna Evelyn Arévalo Salas, identificada con Documento Nacional de Identidad N° 43337338, con domicilio real en Calle Las Amapolas 204. Dpto 402., en el distrito de Surquillo, provincia de Lima, departamentode Lima, egresada de la VII Maestría de Ciencias Militares de la Escuela Superior de Guerra-Escuela de Postgrado (ESGE) declaro bajo juramento que:

Soy el autor de la investigación titulada Análisis del estado actual de la Compañíade Guerra Electrónica de la 3ra Brigada de comunicaciones que presento a los 19 días de noviembres del año 2019, ante esta institución con fines de optar el grado académicode Maestro en Ciencias Militares.

Dicha investigación no ha sido presentada ni publicada anteriormente por ningún otro investigador ni por el suscrito, para optar otro grado académico ni título profesional alguno. Declaro que se ha citado debidamente toda idea, texto, figura, fórmulas, tablas u otros que corresponde al suscrito u a otro en respeto irrestricto a los derechos del autor. Declaro conocer y me someto al marco legal y normativo vigente relacionado a dicha responsabilidad.

Declaro bajo juramento que los datos e información presentada pertenecen a la realidad estudiada, que no han sido falseados, adulterados, duplicadas ni copiados. Que no he cometido fraude científico, plagio o vicios de autoría; en caso contrario, eximo de toda responsabilidad a la Escuela Superior de Guerra - Escuela de Postgrado y me declarocomo el único responsable.



_Erinna Evelyn Arévalo Salas
D.N.I. N° 43337338

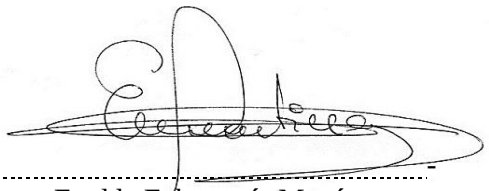
Declaración Jurada de Autoría

Mediante el presente documento, Yo, Freddy Echeverría Martínez, identificada con Documento Nacional de Identidad N° 40048592, con domicilio villa militar este , calle maría parado de bellido 483 en el distrito de Chorrillos, provincia de Lima, departamento de Lima, egresada de la VII Maestría de Ciencias Militares de la Escuela Superior de Guerra-Escuela de Postgrado (ESGE) declaro bajo juramento que:

Soy el autor de la investigación titulada Análisis del estado actual de la Compañíade Guerra Electrónica de la 3ra Brigada de comunicaciones que presento a los 19 días de noviembres del año 2019, ante esta institución con fines de optar el grado académicode Maestro en Ciencias Militares.

Dicha investigación no ha sido presentada ni publicada anteriormente por ningún otro investigador ni por el suscrito, para optar otro grado académico ni título profesional alguno. Declaro que se ha citado debidamente toda idea, texto, figura, fórmulas, tablas u otros que corresponde al suscrito u a otro en respeto irrestricto a los derechos del autor. Declaro conocer y me someto al marco legal y normativo vigente relacionado a dicha responsabilidad.

Declaro bajo juramento que los datos e información presentada pertenecen a la realidad estudiada, que no han sido falseados, adulterados, duplicadas ni copiados. Que no he cometido fraude científico, plagio o vicios de autoría; en caso contrario, eximo de toda responsabilidad a la Escuela Superior de Guerra - Escuela de Postgrado y me declarocomo el único responsable.



Freddy Echeverría Martínez

D.N.I. N° 40048592

ANEXO 6

HOJA DE DATOS PERSONALES

HOJA DE DATOS PERSONALES

GRADO : TTE CRL COM

NOMBRE COMPLETO : FREDDY JESÚS

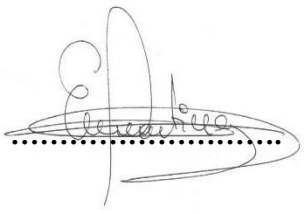
APELLIDOS : ECHEVERRIA MARTINEZ

EMAIL : fecheverriam@esge.edu.pe

DIRECCION : Calle María parado de Bellido 483-Chorrillos

CELULAR : 955502888

FIRMA : ……



HOJA DE DATOS PERSONALES

GRADO : MY COM

NOMBRE COMPLETO : ERINNA EVELIN

APELLIDOS : AREVALO SALAS

EMAIL : earevalos@hotmail.com

DIRECCION : Av Los Faiasanes 535. Dpto 406. Urb la campiña chorrilloa

CELULAR : 958541858

FIRMA : 

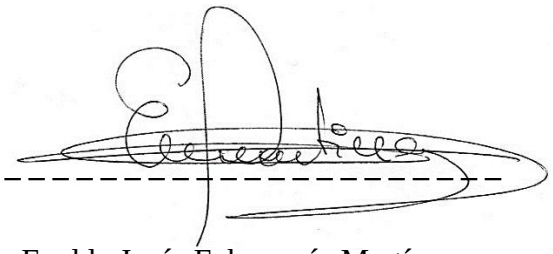
ANEXO 7

AUTORIZACION PARA PUBLICACION EN EL REPOSITORIO DE LA ESGE-EPG

Autorización de publicación

A través del presente documento autorizo a la Escuela Superior de Guerra del Ejercito del Perú – Escuela de Posgrado, la publicación del texto completo o parcial de la tesis de grado titulada "Análisis del estado actual de la compañía de guerra electrónica dela 3ra Brigada de Comunicaciones" , presentada para optar al grado de Magister en Ciencias Militares en el Repositorio Institucional y en el Repositorio Nacional de Tesis (Renati) de la Sunedu, de conformidad al marco legal y normativo vigente. La tesis se mantendrá permanente e indefinidamente en el Repositorio para beneficio de la comunidad académica y de la sociedad. En tal sentido autorizo gratuitamente y en régimen de no exclusividad los derechos estrictamente necesarios para hacer efectiva la publicación, de tal forma que el acceso al mismo sea libre y gratuito, permitiendo su consulta e impresión, pero no su modificación. La tesis puede ser distribuida, copiada y exhibida con fines académicos siempre que se indique la autoría y no se podrán realizar obras derivadas de la misma.

15 de Noviembre del 2019



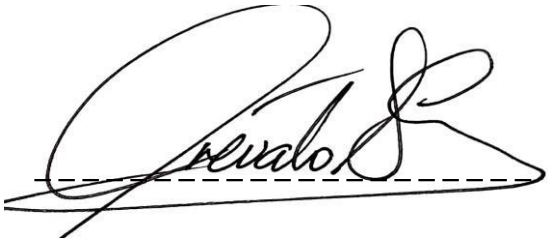
Freddy Jesús Echeverría Martínez

D.N.I. N° 40048592

Autorización de publicación

A través del presente documento autorizo a la Escuela Superior de Guerra del Ejercito del Perú – Escuela de Posgrado, la publicación del texto completo o parcial de la tesis de grado titulada "Análisis del estado actual de la compañía de guerra electrónica dela 3ra Brigada de Comunicaciones" , presentada para optar al grado de Magister en Ciencias Militares en el Repositorio Institucional y en el Repositorio Nacional de Tesis (Renati) de la Sunedu, de conformidad al marco legal y normativo vigente. La tesis se mantendrá permanente e indefinidamente en el Repositorio para beneficio de la comunidad académica y de la sociedad. En tal sentido autorizo gratuitamente y en régimen de no exclusividad los derechos estrictamente necesarios para hacer efectiva la publicación, de tal forma que el acceso al mismo sea libre y gratuito, permitiendo su consulta e impresión, pero no su modificación. La tesis puede ser distribuida, copiada y exhibida con fines académicos siempre que se indique la autoría y no se podrán realizar obras derivadas de la misma.

15 de Noviembre del 2019

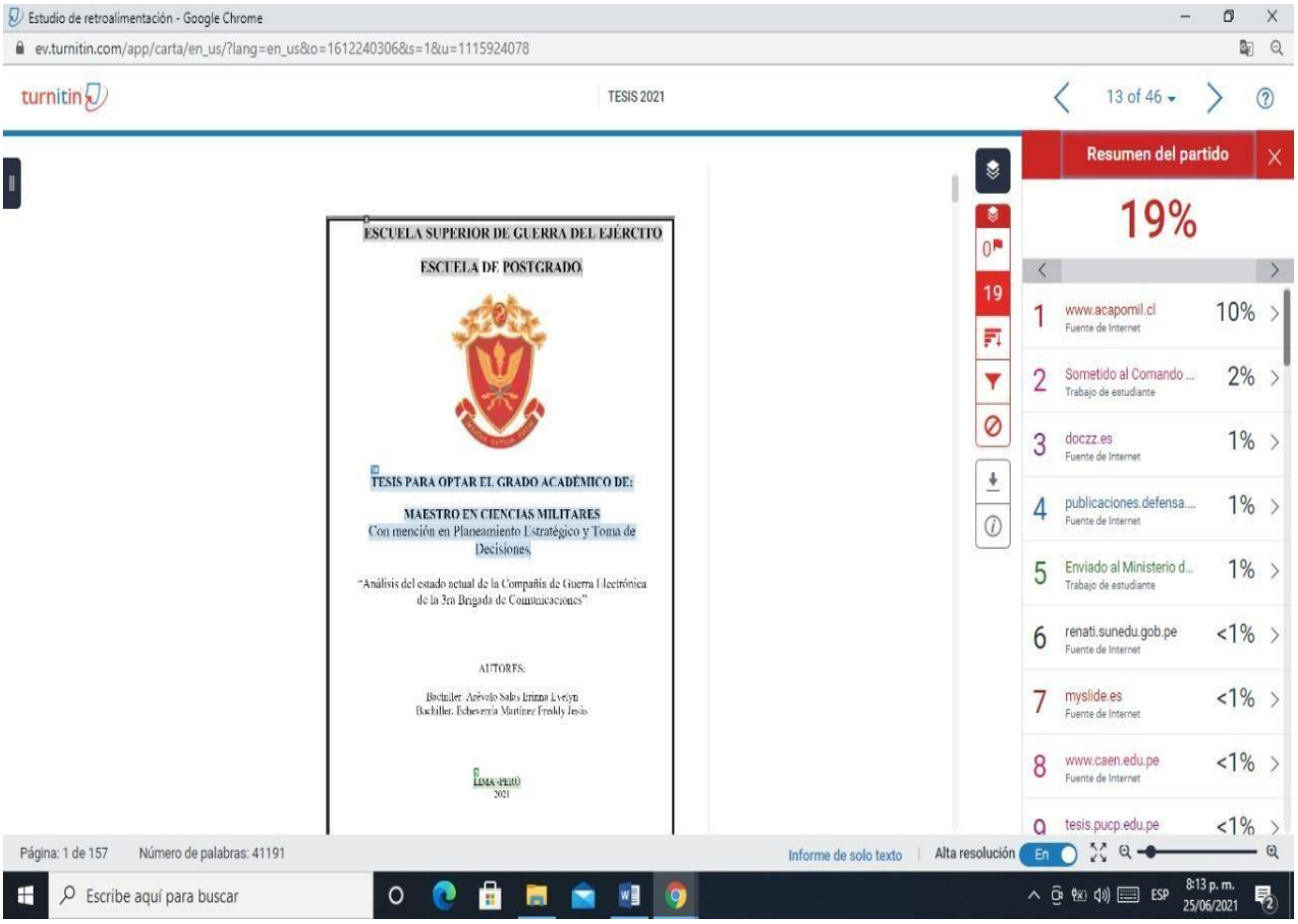


Erina Evelyn Arévalo Salas

D.N.I. N° 40048592

ANEXO 8

TURNITIN


Estudio de retroalimentación - Google Chrome
ev.turnitin.com/app/carta/en_us/?lang=en_us&o=1612240306&s=1&u=1115924078
turnitin
TESIS 2021
13 of 46
Resumen del partido
19%
1 www.acapomil.cl Fuente de Internet 10%
2 Sometido al Comando ... Trabajo de estudiante 2%
3 doczz.es Fuente de Internet 1%
4 publicaciones.defensa.... Fuente de Internet 1%
5 Enviado al Ministerio d... Trabajo de estudiante 1%
6 renati.sunedu.gob.pe Fuente de Internet <1%
7 myslide.es Fuente de Internet <1%
8 www.caen.edu.pe Fuente de Internet <1%
9 tesis.pucp.edu.pe <1%
ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO
ESCUELA DE POSTGRADO
TESIS PARA OPTAR EL GRADO ACADÉMICO DE:
MAESTRO EN CIENCIAS MILITARES
Con mención en Planeamiento Estratégico y Toma de Decisiones
"Análisis del estado actual de la Compañía de Guerra Electrónica de la 3ra Brigada de Comunicaciones"
AUTORES:
Bachiller Arévalo Solis Iriana Evelyn
Bachiller Echeverría Martínez Freddy Jesús
LIMA-PERÚ
2021
Página: 1 de 157
Número de palabras: 41191
Informe de solo texto
Alta resolución
En
Escribe aquí para buscar
ESP
8:13 p. m.
25/06/2021

ANEXO 8

CD CONTENIENDO LA TESIS Y LAEXPOSICION