Facultad del Ejército
Escuela Superior de Guerra
"Tte Grl Luis María Campos"

# TRABAJO FINAL INTEGRADOR

**Título:** "Apoyo de Inteligencia de Señales en el dominio cibernético y electromagnético".

Que para acceder al título de Especialista en Conducción Superior de OOMMTT presenta el Mayor MARIANO MARTÍN MENDILAHATZU PEREZ.

**Director de TFI:** Coronel JUAN CARLOS GUERRA

Ciudad Autónoma de Buenos Aires, 30 de agosto de 2024

## Resumen

El estudio de los conflictos contemporáneos marca la importancia que tienen las actividades de guerra electrónica y las operaciones en el ciberespacio como multiplicador del poder de combate propio.

Como toda operación militar las acciones en los dominios cibernéticos y electromagnéticos requieren del apoyo de la inteligencia, principalmente para evitar la sorpresa.

En este sentido uno de los sistemas que más pude aportar desde el punto de vista de inteligencia a estos dominios es el de Inteligencia de Señales. La integración de los sistemas facilitará la ejecución de operaciones eficaces en múltiples dominios.

Este trabajo buscará determinar los flujos de información necesarios para que los sistemas de guerra electrónica, ciberdefensa e inteligencia de señales operen en forma integrada y mancomunada.

Establecer un canal de comunicaciones directo entre los sistemas será una parte fundamental de esa integración que se complementará con la cooperación del personal para la realización de actividades en común.

***Palabras claves:*** Inteligencia de Señales, Ciberdefensa, Ciberinteligencia, Guerra Electrónica, Comunicaciones.

# INDICE

# Trabajo Final Integrador

## Introducción

La siguiente investigación abordará el apoyo de Inteligencia de Señales en su relación con otros dos importantes sistemas, el de Ciberdefensa y el de Guerra Electrónica. A la luz de las experiencias surgidas en los últimos conflictos, principalmente en Siria, Nagorno Karabaj y Ucrania, se hizo evidente la importancia de la ejecución de operaciones militares multidominio para lo cual la integración de los distintos sistemas de armas es indispensable.

El apoyo de Inteligencia de Señales es esencial en el dominio cibernético y electromagnético para identificar amenazas, determinar intenciones, apoyar las operaciones electrónicas y en el ciberespacio que ejecutarán los elementos en el Teatro de Operaciones. Proporciona a los sistemas de Guerra Electrónica y Ciberdefensa una ventaja crítica al interceptar, analizar y diseminar inteligencia e información extraída de las señales electromagnéticas en todo tiempo y lugar.

En base a estos fundamentos considero de suma importancia la necesidad de analizar, reconocer y establecer flujos de información directos entre los sistemas para integrarlos, con la finalidad de que operen mancomunadamente y acortar el tiempo de respuesta de estos.

## Problema

### *Antecedentes y justificación del problema:*

Desde su aparición en la Guerra Ruso-Japonesa (1904-1905) la guerra electrónica comenzó un proceso de evolución sostenido a través del tiempo. Los medios de guerra electrónica y sus procedimientos de empleo fueron perfeccionándose en relación con el avance de la tecnología. Hoy en día es considerada una actividad esencial para la preservación del comando y control de las operaciones militares. Es por lo que prácticamente la totalidad de las

fuerzas armadas del planeta poseen organizaciones dedicadas a negarle al adversario la superioridad del espectro electromagnético mediante operaciones de guerra electrónica.

Como indica el reglamento Guerra Electrónica para la Acción Militar Conjunta (Estado Mayor Conjunto (EMCO), 2012, pág 7) “la Inteligencia de Guerra Electrónica (IGE) proporciona pautas para la utilización operativa de los medios”. Además, la doctrina conjunta, señala la relación recíproca existente entre el Apoyo de Guerra Electrónica (AGE) y la Inteligencia de Guerra Electrónica la cual provee los datos necesarios para la identificación de las emisiones y la información para la evaluación de las amenazas mientras que AGE aporta a la IGE información y el análisis de las emisiones detectadas a través de la vigilancia del espectro electromagnético.

La Inteligencia de Guerra Electrónica comprende dos actividades principales, la Inteligencia de las Emisiones (INTEM) y la Seguridad de las Emisiones (SEEM). Asimismo, la INTEM comprende las tareas de la inteligencia en el campo de la Guerra Electrónica y como tal, abarca los procesos que se desarrollan para obtener información de las emisiones electrónicas del adversario.

En el Ejército Argentino la actividad de INTEM es responsabilidad del Sistema de Inteligencia de Señales mediante la producción de Inteligencia Electrónica (INTEL) y de Inteligencia de Comunicaciones (INCOM).

Por lo expresado anteriormente, la ejecución de operaciones de guerra electrónica eficaces requiere indudablemente del apoyo de inteligencia de señales. En la actualidad el Ejército cuenta con una Compañía de Inteligencia de Señales la cual forma parte de la Central de Inteligencia Militar.

Esta Subunidad se encarga del estudio y monitoreo del espectro electromagnético centrando su actividad en obtener información de su uso por parte del componente militar de los países de interés.

La doctrina específica hace algunas menciones a la relación recíproca que debe existir entre la guerra electrónica y la inteligencia de señales, pero no establece claramente cómo llevar a cabo la integración de los dos sistemas ni cómo deberá estructurarse el flujo de la información entre ambos. En primer término, en el reglamento Conducción para las Fuerzas Terrestres (Ejército Argentino (EA), 2015, Cap VII pág. 27) se desarrolla el concepto de la guerra electrónica como una operación militar táctica de combate complementaria en donde señala que "el AGE se completa con la inteligencia de emisiones (INTEM), ya sea de comunicaciones (COMINT) o de señales (SIGINT), para obtener el orden de batalla electrónico (OBE) del enemigo".

Continuando el análisis doctrinario, en el reglamento Conceptos Básicos Sobre Sistemas de Comunicaciones, Informática y Guerra Electrónica de la Fuerza (EA, 2016 a) en el capítulo V dedicado a la guerra electrónica indica que en el nivel estratégico durante los periodos de paz la GE será conducida por la Dirección General de Comunicaciones e Informática en permanente y estrecha coordinación con la Dirección General de Inteligencia; la ejecución de las acciones de AGE será a través del subsistema fijo que operarán elementos de la tropa técnica de inteligencia y del arma de Comunicaciones, complementándolas (en caso de necesidad) con acciones llevadas a cabo por el subsistema de campaña que establecerán, operarán y mantendrán elementos de guerra electrónica del arma de Comunicaciones.

El mismo reglamento establece que cuando se instala el Sistema Táctico de Guerra Electrónica (SITAGE) del Componente Terrestre del Teatro de Operaciones (CTTO) desde el Centro de procesamiento de guerra electrónica (CPGE), que es el lugar de trabajo del Oficial de Inteligencia (S2) de la Unidad de GE, se establecerá el flujo de información (enlace por medio de las facilidades de comunicaciones e informática más adecuadas a la situación y a la operación táctica en desarrollo) con el centro integrador de inteligencia (CII) que se encuentre en apoyo al comando del CTTO o de la gran unidad a la cual esté asignado al Batallón de

Guerra Electrónica y Ciberdefensa. En este párrafo se determina un punto de conexión entre un elemento GE y otro de inteligencia, pero el apoyo de inteligencia que puede brindar un CII a un centro de procesamiento de guerra electrónica es muy limitado. Además, durante una operación militar, "el CII será un agrupamiento funcional que operará bajo la supervisión del G-2 al cual asistirá en el cumplimiento de sus responsabilidades" tal como lo aclara el Manual de Inteligencia para el Comandante o Jefe de Elemento (EA, 2008, pág 57).

Llamativamente el reglamento de Inteligencia de Señales (EA, 2016 b) no hace mención alguna al apoyo a las operaciones de guerra electrónica o la relación entre la IGE y el AGE, solo marca las diferencias entre la Inteligencia de Señales y la Guerra Electrónica mediante un pequeño cuadro comparativo.

Como antecedentes adicionales existen algunos trabajos de investigación sobre aspectos particulares de operaciones de guerra electrónica como el de "Concepto general de empleo de elementos de guerra electrónica durante el desarrollo de operaciones defensivas en apoyo a la Gran Unidad de Batalla" realizado por el Mayor FERREYRA (2019), donde el autor plantea cual es la contribución de la GE a la inteligencia táctica y como el ciclo de GE se inserta en el ciclo de producción de inteligencia, sin embargo no desarrolla cómo la inteligencia específica de señales puede apoyar la operaciones de los elementos de GE.

Otro trabajo que menciona la relación de la inteligencia con la guerra electrónica en operaciones es "La influencia de la guerra electrónica en el diseño operacional" realizado por el Mayor CHIAVARO (2018) el cual en sus conclusiones expresa la necesidad de coordinar la ejecución de actividades de Inteligencia Electrónica con los medios de Ejército, Armada y Fuerza Aérea, para incrementar el alcance operacional de las capacidades de guerra electrónica existentes.

Por último, el trabajo final integrador sobre el "Diseño de un órgano director de guerra electrónica en apoyo al comando de nivel operacional" elaborado por el Mayor MARRUPE

PEREYRA (2014), señala en sus conclusiones la necesidad de que dentro de un órgano director de guerra electrónica exista una División Enlaces que tendría la responsabilidad de coordinar con las organizaciones de inteligencia el uso de la GE en el TO.

Por lo mencionado anteriormente entiendo que existe una carencia de previsiones doctrinarias sobre la manera en que una Compañía de Inteligencia de Señales satisface requerimientos o apoye de forma directa con sus productos a un Batallón de Guerra Electrónica y Ciberdefensa.

En lo que respecta al apoyo de inteligencia a la compañía de Ciberdefensa que forma parte del Batallón de Guerra Electrónica y Ciberdefensa se presenta un vacío doctrinario aún más profundo, sumado a que actualmente no se dispone un elemento de inteligencia específico que ejecute Ciberinteligencia a nivel Táctico u Operacional.

Para la Inteligencia Militar, uno de los retos fundamentales es el de desarrollar el ciclo de producción de inteligencia completo dentro del dominio cibernético. Solamente hay un elemento encargado de esta tarea en el Ejército Argentino, la División de Ciberinteligencia dependiente de la Dirección de Inteligencia Funcional. Actualmente existe la intención que, sobre la base de la Compañía de Inteligencia de Señales, se forme una organización o fracción que se encargue del apoyo de ciberinteligencia, lo cual está plasmado en el Plan Estratégico del Sistema de Inteligencia del Ejército 2022/2026.

Ante este nuevo escenario cibernético el sistema de inteligencia de señales debe reorganizar su estructura y establecer procesos de trabajo que permitan cumplir con los nuevos desafíos.

Mas allá de la información disponible sobre ciberinteligencia en numerosos sitios en internet, como antecedente principal el trabajo final integrador del Mayor MAIDANA MUR

(2022) que aborda el "Apoyo de la Ciberinteligencia a las Operaciones Militares" es una fuente de consulta obligada. En este trabajo el autor concluye sobre la necesaria conformación de una organización de ciberinteligencia de nivel subunidad dependiente directamente de la Dirección de Inteligencia Operacional que apoye al nivel táctico y operacional.

### *Formulación del problema:*

¿Cuáles son los procesos de trabajo a implementar para la integración del Sistema de Inteligencia de Señales al Sistema de Guerra Electrónica y al Sistema de Ciberdefensa del Ejército Argentino?

## Objetivo

### *Objetivo General:*

Establecer los procesos de trabajo necesarios para integrar los sistemas de Inteligencia de Señales, Guerra Electrónica y Ciberdefensa mediante la determinación de flujos de información directos entre estos.

### *Objetivos particulares:*

Objetivo Particular Nro 1: Describir cada sistema para identificar las actividades y objetivos que posean en común.

Objetivo Particular Nro 2: Describir los flujos de información existentes entre los sistemas para identificar los enlaces necesarios a establecer con la finalidad de abrir canales de comunicación directos entre estos.

**Metodología a emplear**

La metodología que emplearé para realizar la investigación será un método deductivo, un diseño explicativo y utilizando las técnicas de validación a través del análisis bibliográfico, análisis documental y análisis lógico.

# Capítulo 1

# Descripción y Análisis de los Sistemas

## Sección 1: Sistema de Inteligencia de Señales

### Conceptos Generales

La inteligencia de señales conocida también por sus siglas en inglés SIGINT (Signal Intelligence) es una actividad que data de principios del siglo XX, precisamente desde la segunda guerra de los Boers (1899-1902) sobre el actual territorio de Sudáfrica. En esta guerra los Boers capturaron equipos de radios británicos con los cuales podía escuchar las transmisiones militares así obtener valiosa información. Sin embargo, estas acciones de escucha radioeléctrica no se corresponderían al concepto actual de inteligencia de señales que implica una interceptación de la transmisión. La primera interceptación de señales de la historia militar se produjo durante la guerra Ruso-Japonesa (1904-1905) durante la movilización de la flota rusa del Mar Negro. El buque británico HMS Diana apostado en proximidad a Suez interceptó las señales inalámbricas de los equipos telegráficos que ordenaban a la flota rusa su preparación y despliegue para el conflicto. El informe producido por los analistas concluyó que el ritmo de trabajo era extremadamente lento para los estándares británicos, mientras que los intérpretes de la Royal Navy fueron particularmente críticos con el pobre nivel de gramática y ortografía entre los operadores rusos. Como consecuencia de la interceptación y posterior análisis de las señales obtenidas, los británicos pudieron llegar a una conclusión de interés, por

esta razón se considera este hecho el nacimiento de la inteligencia de señales como la conocemos hoy en día. Es importante marcar que en ese mismo conflicto se produjo la primera acción de guerra electrónica ya mencionada en la introducción de este trabajo.

La Inteligencia de Señales mediante el estudio científico técnico del comportamiento del Espectro Electromagnético (EEM) monitorea las emisiones de las fuerzas armadas de los países de interés en distintas bandas de frecuencias.

La producción de la Inteligencia de Señales aporta conocimientos específicos técnicos necesarios para la utilización segura del EEM por propia tropa y, además, sobre el estudio de los factores del Orden de Batalla Electrónico (OBE) del Componente Militar de los países de interés.

**Definición de Inteligencia de Señales**

El reglamento de Inteligencia de Señales define:

*"La Inteligencia de Señales (IS) es la resultante del producto de la búsqueda, detección, evaluación, análisis, integración, interpretación, difusión y uso pertinente de toda la inteligencia resultante, relativa al uso del espectro electromagnético por parte del Componente Militar de los países de interés."* (EA 2016 b)

Para complementar esta definición hay que establecer el significado de señal. El Diccionario para la acción militar conjunta (EMCO, 1998) define a las señales como *"cualquier emisión electromagnética irradiada".*

Una señal es cualquier representación que puede ser interpretada por alguien y en este sentido la Inteligencia de Señales es la encargada de encontrar su significado. Para ello es

indispensable la exploración sistemática y continua sobre todo el espectro electromagnético en búsqueda de la información que poseen las señales a través de la utilización de medios específicamente técnicos de obtención.

**Finalidad**

La finalidad de la Inteligencia de Señales será la de determinar las capacidades, debilidades e intenciones del enemigo en el espectro electromagnético.

Para ello se deberá elaborar la Apreciación de Situación de Inteligencia de Señales (ASIS) el cual es un estudio descriptivo y analítico sobre la información técnica y del OBE de la parte del Espectro electromagnético que quiera analizar.

**Tipo de Inteligencia que produce**

El sistema de Inteligencia de Señales de acuerdo con la especialización requerida de los medios de obtención produce Inteligencia de Emisiones (INTEM). Este tipo de inteligencia es el producto resultante del proceso de la información obtenida mediante medios de detección de emisiones electromagnéticas. La INTEM, está diferenciada en Inteligencia Electrónica (INTEL) e Inteligencia de Comunicaciones (INTCOM).

La INTEL se dedica específicamente a las señales de radar, control de armas guiadas por radar y navegación, telémetros laser, emisiones acústicas, lumínicas, etc. Mientras que, la INTCOM refieren a la inteligencia de las emisiones de comunicaciones y transmisión de datos.

La INTCOM comprende las tareas del Análisis de Tráfico y el Cripto Análisis. El análisis de tráfico es una fuente de obtención de información muy importante, ya que mediante este tipo de análisis se podrá concluir acerca de las intenciones del enemigo, completar el OB

enemigo y su OBE, evaluar el nivel de adiestramiento de los radioperadores enemigos, determinar el nivel de Comando y Control, etc.

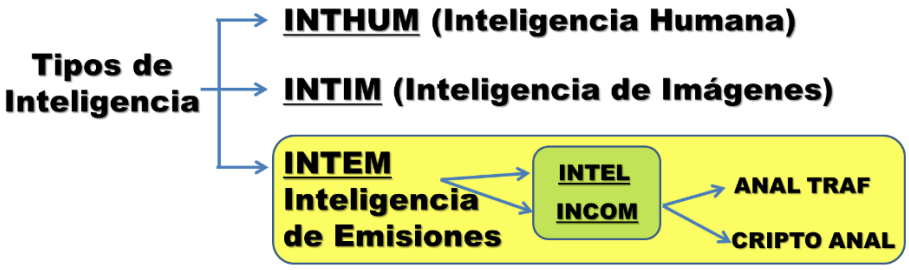


*Gráfico 1: Tipos de Inteligencia (Elaboración propia).*

**Ciclo de Inteligencia de Señales**

Para explicar la inteligencia como un proceso se utiliza como modelo "El Ciclo de Producción de Inteligencia". Este modelo es la representación de las actividades de inteligencia siguiendo una secuencia lógica de pasos y es utilizado de manera global. Si bien, en esencia la secuencia lógica es la misma, cada agencia u organismo utiliza el ciclo con algunos cambios en la cantidad de pasos o fases. Por ejemplo, el Centro Nacional de Inteligencia (CNI) de España utiliza el ciclo de cuatro pasos (dirección, obtención, elaboración y difusión), Central Intelligence Agency (CIA) de los Estados Unidos considera cinco pasos (planificación y dirección; recopilación, procesamiento, análisis y producción; y difusión) mientras que el Centro Nacional de Inteligencia de México prefiere separar el ciclo en seis pasos (Planeación, Recolección, Procesamiento y Análisis; Difusión y Explotación; y Retroalimentación).

En nuestro país y en particular a lo que refiriere a Inteligencia Militar en Ciclo de Inteligencia adoptado es de cuatro pasos (EMCO, 2007):

a) Dirección del Esfuerzo de Obtención.

b) Obtención de la Información.

c) Proceso de la Información.

d) Diseminación y Uso de la Inteligencia.

Basándonos en el ciclo de producción de inteligencia y relacionándolo con las tareas a desarrollar para el apoyo electrónico (búsqueda, interceptación, escucha, localización, análisis, identificación, evaluación y registro) podemos establecer un ciclo de producción de Inteligencia Señales.

En el primer paso el órgano de dirección de inteligencia determina y propone, en primer lugar, los requerimientos de inteligencia a satisfacer que permitan la correcta toma de decisiones y faciliten el planeamiento. A estos requerimientos se les asignará una prioridad para luego con ellos confeccionar el Plan General de Obtención de Señales (PGOS). Este plan es similar en cuanto a su estructura, a cualquier otro utilizado por otro órgano de dirección, la diferencia radica en que el PGOS se apoya en otro documento de trabajo que es el Plan de Obtención Electrónica (POE). El POE tiene la particularidad de "traducir" los requerimientos de inteligencia que son simples interrogantes en frecuencias radioeléctricas concretas donde obtener la información.

En base a los requerimientos de inteligencia, los medios a disposición y la información especifica a obtener se confeccionarán las Órdenes y Pedidos de Obtención a los elementos dependientes o a los escalones superiores y laterales respectivamente. Estas órdenes o pedidos deberán ser muy específicos en las frecuencias a explotar, las actividades a realizar, el servicio y modo de operación y, por último, sobre la forma y la oportunidad de entrega de la información.

El segundo paso se centra en la Obtención de la Información, en donde los medios de obtención de señales ejecutan principalmente las actividades de Búsqueda, Interceptación y

Escucha. Todos los datos y/o información obtenida de utilidad y de acuerdo con lo solicitado en la Orden de Obtención son puestos a disposición de los analistas de señales.

El Proceso de la Información obtenida la realizan los analistas de señales quienes mediante la Localización, Análisis, Identificación, Evaluación y Registro van dando respuesta a los requerimientos del PGOS. Los analistas de señales y del OBE son los que registran la información, procesan esos datos o información para que sean aptos de ser utilizados, la evalúan y valorizan para determinar su pertinencia, confiabilidad y exactitud, la integran con otros datos disponibles y la analizan para determinar su significado, elaborando conclusiones de interés brindando como resultado la inteligencia correspondiente.

La inteligencia producida, los datos y la información obtenida serán registradas en forma escrita en el Diario de Informaciones y luego en forma gráfica sobre la Carta de Situación del Orden de Batalla Electrónico del enemigo (CarSitOBE). Para la elaboración de la carta es necesario el uso del Sistema de Información Geográfica de Inteligencia de Señales (SIG-IS) que es una base de datos geográfica que vincula la información obtenida actual específica a la Inteligencia de Señales con información básica. Además, el órgano de dirección clasifica la información por asunto y los agrupa en temas afines, normalmente por países de interés. Para ello es necesaria la confección de una Carpeta de Trabajo de Inteligencia de Señales que es un documento de trabajo que sienta las bases para la determinación del Orden de Batalla Electrónico. Es importante destacar en este paso y particularmente en la tarea de Registro la necesidad de administrar una base de datos digital eficiente donde se almacenen de forma ordenada los datos obtenidos por los grupos de obtención de señales de manera tal que estén fácilmente disponibles para el uso de los distintos analistas.

Por último, en el paso Diseminación y Uso se transite la inteligencia producida a quienes la necesiten en oportunidad, forma y seguridad adecuada. Para ello se evalúa

principalmente la pertinencia, se determina que elemento o persona tiene la obligación de conocer la inteligencia producida lo que está en directa relación con el uso que le dará a la misma y al cargo o función que desempeña. Para la diseminación se utilizan principalmente los siguientes documentos: Mensaje de información (MI), Informe Periódico de Inteligencia de Señales (IPI), Resumen de Inteligencia de Señales (RIS) e Informe Especial de Inteligencia (IEI); estos serán desarrollados en el próximo apartado.


*Gráfico 2: Ciclo de Producción de Inteligencia de Señales. (Elaboración Propia)*

**Principales Productos de Diseminación**

La Inteligencia/Información de Señales producida se disemina mediante distintos documentos que para su confección deberán respetar algunos aspectos comunes. Ser breves y concisos en lo esencial a diseminar; de nada sirve un extenso desarrollo con información técnica de señales si la resultante del análisis lleva a una conclusión vaga o ambigua que no pueda ser interpretada por el receptor y en consecuencia no pueda ser utilizada. La obtención y análisis de señales requiere el manejo de información y datos netamente técnicos, estos necesariamente deberán ser presentados de manera tal que permita al usuario final

comprenderlos fácilmente, para ello la elaboración de gráficos de red, cuadros comparativos, cartas de situación, fichas de datos técnicos, etc., resultan sumamente útiles.

Los grupos de obtención satisfacen las ordenes de obtención con Partes de Obtención donde vuelcan todos los datos e información solicitada, incluso la información negativa. Si existe algún tipo de información que por sus características amerita una explotación inmediata se confecciona un Mensaje de Información para su diseminación. La información contenida en un Mensaje de Información es de prioridad para su procesamiento por parte de los Analistas de Señales.

Toda la información de importancia sumado a la inteligencia producida en un periodo de tiempo determinado por el órgano de dirección se disemina mediante un Resumen de Inteligencia de Señales (RIS). Este documento debe contener conclusiones breves y, sobre todo, claras sobre la actividad del enemigo en el espectro electromagnético.

En el caso de requerir un informe más detallado y abarcando un periodo más extenso que el RIS, existe otro documento de diseminación denominado Informe Periódico de Inteligencia (IPI). En el IPI las conclusiones deben ser lo más exactas posibles, manteniendo para su justificación una base informativa completa.

Finalmente, para desarrollar un tema particular en profundidad se confecciona un Informe Especial de Inteligencia de Señales. Este tipo de informes tiene múltiples propósitos, su origen generalmente surge de algún aspecto contenido o mencionado en otro documento, del cual se necesite un estudio especifico y en profundidad.

Los distintos documentos serán confeccionados por los operadores y analistas de señales los cuales luego de ser aprobados, estarán en condiciones de ser diseminados a los distintos usuarios manteniendo los criterios de oportunidad, forma y seguridad adecuada.

## Sección II: Sistema de Ciberdefensa del Ejército

### Conceptos Generales

El origen de la ciberdefensa se encuentra en los primeros días de la era de la informática y la tecnología de la información. A medida que las computadoras y las redes de comunicación comenzaron a desarrollarse en la década de 1960 y 1970, se hicieron evidentes las vulnerabilidades y amenazas que podrían surgir en este nuevo espacio digital.

Durante la Guerra Fría, se desarrollaron sistemas de cómputo y comunicación para apoyar las actividades militares y de inteligencia. Esto llevó a la percepción de que los adversarios podrían utilizar la tecnología para espiar o interrumpir las operaciones militares y gubernamentales.

A medida que la tecnología de la información avanzaba, se produjeron algunos de los primeros ataques informáticos notables, como el "gusano MORRIS" en 1988. Estos incidentes despertaron la conciencia sobre la necesidad de proteger los sistemas digitales.

La creación y expansión de Internet en la década de 1990 abrió nuevas oportunidades para la comunicación y el intercambio de información, pero también introdujo una serie de riesgos de Seguridad cibernética y un desafío para la Defensa. Los gobiernos y las organizaciones comenzaron a reconocer la importancia de proteger sus activos en línea.

La ciberdefensa es de vital importancia en la era digital en la que vivimos. En un mundo cada vez más interconectado y dependiente de la tecnología, la seguridad cibernética se ha convertido en un pilar fundamental para la protección de nuestros sistemas, redes y datos. En primer lugar, la ciberdefensa es esencial para salvaguardar la confidencialidad, integridad y disponibilidad de la información tanto en el ámbito civil y militar.

Además, la ciberdefensa desempeña un papel crítico en la defensa y seguridad nacional. Los ciberataques pueden ser utilizados por actores estatales o grupos delictivos para desestabilizar países, interrumpir infraestructuras críticas, o incluso influir en procesos democráticos. Por lo tanto, la ciberdefensa es esencial para proteger la soberanía, la seguridad y la estabilidad de las naciones.

Por último, la ciberdefensa es una responsabilidad compartida que involucra a gobiernos, empresas y ciudadanos. La concienciación y la educación en ciberdefensa son esenciales para fortalecer nuestras defensas y reducir la amenaza de los ciberataques. En un mundo cada vez más conectado, la ciberdefensa es la clave para mantener la confianza en la tecnología y proteger nuestros activos más valiosos.

**Definición de Ciberdefensa**

La ciberdefensa son el conjunto de acciones que se desarrollan en el ciberespacio para prevenir, detectar, identificar, anular, impedir, evitar, contrarrestar, contener o repeler una amenaza o agresión cibernética, sea esta inmediata, latente o potencial, a fin de permitir el empleo del Instrumento Militar de la Nación (EA, 2015).

**Finalidad**

Existen dos diferenciaciones en el sentido de la finalidad buscada, la directa y la indirecta. Ambas se refieren a estrategias y acciones para proteger los sistemas informáticos y las redes contra amenazas cibernéticas, pero poseen enfoques y objetivos distintos.

Ciberdefensa directa, cuya finalidad es la de vigilar y controlar las redes y sistemas en los ámbitos específico y conjunto.

Ciberdefensa indirecta, cuya finalidad es la de disputar el control del ciberespacio necesario para el accionar de las fuerzas militares.

**Particularidades del dominio cibernético**

Para las operaciones militares relacionadas con la Ciberdefensa, se denota al ambiente del ciberespacio como una de las cinco áreas, dominios o dimensiones de operaciones, que es trasversal a los dominios tradicionales: la tierra, el mar, el aire y el espacio, que son a su vez interdependientes. Las actividades en el ciberespacio pueden crear libertad de acción para las actividades en otros dominios, y también crear efectos dentro y a través del ciberespacio. El objetivo central de la integración de los dominios es aprovechar las múltiples capacidades de cada uno para crear efectos únicos y a menudo decisivos.

En el contexto de las operaciones militares relacionadas con la Ciberdefensa, se considera el ciberespacio como una de áreas o dimensiones de operaciones, que coexiste con los dominios tradicionales, a saber, tierra, mar, aire y espacio. Estos dominios tradicionales están interconectados entre sí a través del Espectro Electromagnético. Las actividades realizadas en el ciberespacio pueden influir en la libertad de acción en los otros dominios y también generar efectos dentro del propio ciberespacio y más allá de él. El objetivo fundamental de la integración de estos dominios es aprovechar las diversas capacidades de cada uno de ellos para crear efectos singulares y, en muchas ocasiones, decisivos.

El Ciberespacio se caracteriza por:

a) Ser un entorno único, en el cual el atacante puede encontrarse físicamente en cualquier parte del globo y desde allí actuar en forma remota.

b) Brindar la posibilidad de actuar con un alto grado de anonimato.

c) Poseer multiplicidad de actores operando no sólo elementos estatales o públicos sino también privados.

d) Permitir una confrontación de características asimétricas, anónimas y clandestinas.

e) La constante evolución tecnológica que configura un entorno cada vez más complejo.

f) Permitir a los atacantes operar en forma remota empleando, con o sin conocimiento de otros usuarios, sus propios sistemas, dificultando aún más su identificación, formas de ataque y sus propósitos.

El ciberespacio es un ámbito tanto físico como virtual, en el que se desarrollan actividades de creación, procesamiento, almacenamiento, intercambio y visualización de datos e información digital, a través de redes, software, hardware y firmware de dispositivos electrónicos

**Operaciones en el ciberespacio**

Son operaciones que se planifican y ejecutan en forma contribuyente en el ciberespacio para prevenir, preservar y contrarrestar toda ciberamenaza o ciberincidente que afecte o intente afectar la seguridad de las Infraestructuras Críticas de Información y activos críticos de información del Sistema de Defensa Nacional y de aquellas que sean designadas para su preservación, independientemente del origen de la agresión.

Las operaciones se clasifican en operaciones defensivas, ofensivas y de exploración.

**Operaciones Defensivas de Ciberdefensa.**

Son aquellas operaciones que se desarrollan en el ciberespacio, por parte de los elementos de ciberdefensa cuyo objetivo principal es la protección, preservación y prevención ante ciberataques a los activos de información definidos, sistemas de información, redes de

transmisión de datos, medios de comunicaciones e informática, consideradas Infraestructuras Críticas de Información o Activos Críticos de Información del Sistema de Defensa Nacional o del Instrumento Militar y de aquellas que sean designadas para su preservación.

**Operaciones Ofensivas de Ciberdefensa.**

Son las acciones ejecutadas en el ciberespacio para neutralizar, interrumpir, denegar o degradar el empleo de los sistemas de información del enemigo u oponente, que empleen Tecnologías de Información (TI) o Tecnologías de Operación (TO) y que mediante ciberataques, ciberamenazas o ciberincidentes, afecten o intenten afectar las infraestructuras críticas de información o activo críticos de información de la Defensa Nacional o del Instrumento Militar y sus capacidades, durante el desarrollo de Operaciones Militares.

En el campo Operacional y Táctico la planificación y ejecución de operaciones estarán siempre coordinadas y los efectos buscados sincronizados, con las operaciones militares que se desarrollen en los otros dominios (tierra, mar, aire y espacio), para contribuir al logro de la misión y evitar la superposición de esfuerzos.

**Operaciones de Exploración de Ciberdefensa**

Consiste en operaciones de búsqueda y obtención de información en el ciberespacio, a fin de satisfacer los requerimientos que permita identificar y reconocer la situación de los elementos componentes del ambiente cibernético y de los medios a disposición del enemigo.

Las operaciones de Ciberdefensa normalmente requieren de la ejecución complementaria, y normalmente previa, de operaciones de exploración para la obtención de información sobre el o los objetivos a defender o contraatacar.

Contribuye a realizar una planificación basadas en información e inteligencia para la ejecución de acciones de protección y prevención, mediante la producción de conocimiento e identificación de las vulnerabilidades de nuestros sistemas y/o neutralizar ciberataques o ciberamenazas.

Las operaciones de exploración deben preferentemente evitar el rastreo y servir con información para la producción inteligencia con la finalidad de identificar las vulnerabilidades de los sistemas.

**La Ciberinteligencia**

La ciberinteligencia es el procedimiento de inteligencia realizado en o desde el ciberespacio que, mediante la adquisición, análisis, integración, interpretación de la información se identificará, rastreará y predecirá la capacidad e intenciones de los ciber actores con la finalidad de apoyar la toma de decisiones de las fuerzas.

La ciberinteligencia realiza las siguientes actividades:

a) Patrullaje cibernético que consiste en la búsqueda de información en fuentes abiertas en el ciberespacio;

b) Identificación de ciberamenazas;

c) La determinación de posibles tácticas, procedimientos y técnicas de empleo y comprende los aspectos que resumirán la metodología del accionar de los ciberactores, sintetizando el “cómo” se prevé que estos lleven adelante las ciberamenazas;

d) Proyección de ciberataques consiste en determinar potenciales ataques y los efectos que de ellos se pudieren derivar en un corto-mediano plazo;

e) Simulación de ciberataques para contribuir a la seguridad de la fuerza mediante simulacros de ciberataques de manera similar a los empleados por ciberactores de interés con la finalidad de determinar fortalezas y debilidades;

f) Forensia informática que tiene por finalidad adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y/o soportes informáticos. (Maidana Mur, 2022)

**Requerimientos de Inteligencia**

Para la ejecución de operaciones en el ciberespacio, al igual que en los otros dominios, es fundamental del apoyo de inteligencia para minimizar la incertidumbre y evitar la sorpresa. Como ya se mencioné anteriormente el Ciclo de producción de inteligencia comienza con la formulación de los requerimientos. Estos requerimientos deberán estar dirigidos a plasmar y estructurar los interrogantes que se tuvieran en un Plan de Obtención en el dominio Cibernético (POC).

Los requerimientos de inteligencia estarán orientados a la obtención de información sobre las amenazas, datos técnicos de los equipos enemigos, técnicas y procedimientos, distintos factores del Orden de Batalla Cibernético de interés y principalmente para determinar las capacidades del enemigo que podrían afectar el cumplimiento de nuestra misión.

La información básica del enemigo con la que se deberá contar antes de realizar ante la conformación de un Teatro de Operaciones será:

a) El Orden de Batalla

b) Elementos, fracciones y organizaciones de Guerra Electrónica y Ciberdefensa.

c) Sistemas de Comando y Control.

d) Sistemas de Comunicaciones de Campaña

e) Sistemas de Comunicaciones Territoriales

f) Sistemas Informáticos

g) Sistemas de Radar

h) Etc.

Definidos los requerimientos y luego de ser aprobados y clasificados por el comandante, comienza a funcionar el ciclo de producción de ciberinteligencia.

**Ciclo de Producción de Ciberinteligencia**

El Ciclo de producción de Ciberinteligencia naturalmente se basa en el ciclo básico de inteligencia, pero con algunos cambios. Debido a las características del entorno cibernético el ciclo requiere rapidez en proceso, ya que la información normalmente será válida un corto periodo de tiempo, y un mayor peso en la obtención de información con medios técnicos.

Para conseguir esa rapidez en el procesamiento es necesario contar con herramientas de recolección, análisis y almacenamiento de grandes volúmenes de datos de distintas fuentes. El problema del manejo de grandes cantidades de datos radica en diferenciar cuales de estos son falsos, para resolver esto es necesario además contar con un sistema confiable para la valoración de la fuente y el medio.

El primer paso del ciclo comienza con la formulación de los requerimientos que se estructuran en el Plan de Obtención en el dominio Cibernético (POC), para luego generar las ordenes o pedidos de obtención de información.

La Obtención de Información se ejecuta mediante la operación Exploración en el ciberespacio, cuya importancia será, además de obtener información determinar amenazas y vulnerabilidades.

En el siguiente paso, el proceso de la información obtenida se efectuará con el objeto de determinar principalmente las tácticas y procedimientos de empleo del enemigo. Asimismo, con la información obtenida se podrá completar y actualizar el Orden de Batalla Cibernético del enemigo. La forensia tiene como objetivo extraer datos contenidos en las evidencias de los incidentes, procesarlos, transformarlos en información de utilidad y presentar conclusiones de interés.

En el último paso, la confección de informes detallados sobre la ocurrencia de incidentes y principalmente sobre las amenazas persistentes (APTs) detectadas será de gran utilidad para la planificación y ejecución de operaciones en el ciberespcio.


*Gráfico 3: Ciclo de Producción de Ciberinteligencia (Producción Propia).*

## Sección III: Sistema de Guerra Electrónica.

### Conceptos Generales

La guerra electrónica es fundamental en el campo de combate moderno, ya que las fuerzas dependen en gran medida de sistemas electrónicos y de comunicación para operar. La capacidad de controlar y proteger estos sistemas, así como de afectar a los del enemigo, puede tener un impacto significativo en el resultado de una operación militar. La guerra electrónica es un componente esencial de la guerra actual ya que contribuye a obtener la superioridad en el espectro electromagnético y, por lo tanto, ser un multiplicador del poder de combate.

Hoy en día, los dispositivos electromagnéticos están siendo empleados de manera creciente tanto de forma individual como en redes, tanto por entidades civiles como militares. Esto se hace con el propósito de llevar a cabo diversas actividades que incluyen inteligencia, comunicaciones, navegación, procesamiento y almacenamiento de información, así como otras funciones relacionadas.

En consecuencia, las operaciones militares están altamente dependientes de estos equipos para llevarse a cabo. Esto implica el aprovechamiento del espectro electromagnético, que engloba un amplio rango de frecuencias de radiación electromagnética, desde frecuencias cercanas a cero hasta niveles infinitos. Este espectro electromagnético se divide en diversas bandas, que van desde frecuencias de radio hasta rayos X y rayos gamma. El uso del espectro genera un ambiente específico que forma parte del contexto del manejo de la información, conocido como el "Ambiente Electromagnético". (Electromagnetic Environment – EME). (EMCO, 2012)

### Definición de Guerra Electrónica

La Guerra Electrónica es el conjunto de acciones desarrolladas en el ámbito del espectro electromagnético (EEM) que implica el uso de energía electromagnética o dirigida, con el objetivo de determinar y explotar la presencia de actividad enemiga en dicho espectro, neutralizar y/o reducir el empleo de la energía irradiada por el enemigo y asegurar la irradiada por los propios medios. (EA, 2016 a)

**Finalidad**

El objetivo que persigue la Guerra Electrónica es la de reducir o negar a las fuerzas del enemigo la utilización del espectro electromagnético para sus comunicaciones y para los sistemas de armas que necesiten de emisiones electromagnéticas. Además, asegurar el empleo efectivo del EEM por parte de las propias fuerzas. (EA, 2016 a)

En otras palabras, la finalidad de la Guerra Electrónica es la de obtener la superioridad en el dominio electromagnético.

**Particularidades del dominio electromagnético**.

El espectro electromagnético es el rango completo de todas las frecuencias posibles de radiación electromagnética. La radiación electromagnética se propaga en forma de ondas electromagnéticas y no requiere un medio material para moverse, lo que significa que puede viajar a través del vacío del espacio.

El espectro electromagnético se organiza típicamente en diversas regiones o bandas, cada una asociada con un rango específico de frecuencias y longitudes de onda. (EA, 2016)

<u>Características del Ambiente Electromagnético:</u>

El Ambiente Electromagnético (Electromagnetic Enviornment – EME) hace referencia al producto resultante de la potencia y la distribución de tiempo, de emisiones de energía electromagnética radiada o conducida, pudiéndose llevar a cabo en diferentes niveles y rangos de frecuencia. Situación en la que los medios, sistemas o plataformas propias, pueden encontrarse mientras ejecutan misiones dentro del ambiente operacional y verse afectada su Capacidad Operativa. Esto se lo denomina efectos del Ambiente Electromagnético (Electromagnetic Environment Effects - E). (EMCO, 2012)

Características del EEM:

a) Bandas de Frecuencias: El espectro electromagnético abarca un amplio rango de frecuencias, desde frecuencias muy bajas (como las ondas de radio) hasta frecuencias muy altas (como los rayos gamma y los rayos X). Esto significa que incluye todo tipo de radiación electromagnética, desde la más suave y de baja energía hasta la más intensa y de alta energía.
b) Longitudes de Onda Variadas: Las diferentes regiones del espectro electromagnético se caracterizan por longitudes de onda variables. Las ondas de radio tienen longitudes de onda más largas, mientras que las radiaciones ionizantes, como los rayos gamma, tienen longitudes de onda extremadamente cortas.
c) Comportamiento Ondulatorio y Corpuscular: La radiación electromagnética puede exhibir tanto comportamiento ondulatorio como corpuscular. Esto significa que puede propagarse como ondas y partículas, dependiendo del contexto y la observación. Por ejemplo, en ciertas circunstancias, la luz se comporta como una onda, mientras que en otras puede considerarse como partículas llamadas fotones.
d) Velocidad de la Luz: La velocidad de la luz en el vacío es constante y es de aproximadamente 299.792,458 metros por segundo. Esta velocidad es la misma para

todas las radiaciones electromagnéticas en el vacío, independientemente de su frecuencia o longitud de onda.

e) Interacción con la Materia: Diferentes regiones del espectro electromagnético interactúan de manera diferente con la materia. Por ejemplo, las ondas de radio y las microondas son absorbidas y reflejadas por objetos metálicos, mientras que los rayos X y los rayos gamma tienen la capacidad de ionizar átomos y moléculas, lo que puede causar daño biológico.

f) Aplicaciones Variadas: Las diferentes regiones del espectro electromagnético se utilizan en una amplia variedad de aplicaciones tecnológicas y científicas. Por ejemplo, las ondas de radio se utilizan en telecomunicaciones, las microondas en hornos y radares, la luz visible en la visión humana y la fotografía, y los rayos X en medicina y control de calidad industrial.

En resumen, el espectro electromagnético es un concepto que engloba todas las formas de radiación electromagnética y es fundamental para las aplicaciones científicas, tecnológicas y de comunicación en nuestra vida cotidiana. Por ende, su uso no es exclusivo a ningún ámbito. Las emisiones electromagnéticas civiles y militares comparten el mismo espacio, existen incontables señales recorriendo este dominio permanentemente. En consecuencia, el control, administración y uso del EEM resulta de vital importancia para las operaciones militares modernas y serán una fuente de información medular para los sistemas de inteligencia militar.

**Acciones de Guerra Electrónica**

Por la finalidad de las acciones se definen en Apoyo de guerra electrónica (AGE), Ataque electrónico (AE) y Protección electrónica (PE).

Apoyo de guerra electrónica:

Es aquella parte de la guerra electrónica que incluye las acciones para obtener información de la energía presente en el medio ambiente, mediante la búsqueda, interceptación, escucha, localización, análisis, identificación, evaluación y registro de las características de las emisiones detectadas, intencionales o no; con la finalidad de contribuir al inmediato reconocimiento y seguimiento de amenazas presentes en el EEM y proporcionar bases para la planificación y conducción de futuras operaciones.(EA, 2016 a)

Ataque Electrónico:

El ataque electrónico (AE) comprende el empleo de energía electromagnética para prevenir o reducir el uso efectivo del espectro electromagnético por parte del enemigo, con la finalidad de afectar negativamente sus sistemas de comunicaciones, sistemas de comunicaciones especiales (radares, sensores, etc.) y sistemas de armas que requieren de emisiones electromagnéticas para su funcionamiento, mediante la ejecución de acciones de interferencia o de engaño. (EA,2016 a)

Protección electrónica:

Consiste en todas aquellas acciones realizadas para proteger al personal, instalaciones y equipamientos de cualquier efecto producido por el uso del espectro electromagnético (EEM) por parte de la Fuerza e impedir o reducir la efectividad de las acciones de guerra electrónica (GE) que ejecute el enemigo con la finalidad de degradar, neutralizar o destruir la capacidad de combate propia. (EA, 2016 a)

**Requerimientos de Inteligencia**

La guerra electrónica se tendrá que nutrir de información e inteligencia principalmente de INTEM para cumplir con su misión. Los interrogantes básicos serán orientados al enemigo

para completar y actualizar la información sobre los factores del Orden de Batalla Electrónico que son de vital importancia para el planeamiento y conducción de operaciones en este dominio.

En este punto el Sistema de Inteligencia de Señales puede hacer un gran aporte ya que normalmente contará con información básica y actual sobre el OBE producto de su permanente producción de inteligencia tanto en tiempo de paz como en la guerra.

El sistema de Guerra Electrónica necesita conocer las amenazas electromagnéticas que se presentan en el Teatro de Operaciones. Las amenazas serán todos los medios del enemigo que mediante la emisión o recepción de energía electromagnética permitan la ejecución de actividades guerra electrónica; los medios de Comando, Control, Comunicaciones e Inteligencia; los sistemas de guiado y detección de los distintos sistemas de armas; y los medios de reconocimiento y vigilancia electrónicos enemigos.

**Ciclo de Producción de Inteligencia de Guerra Electrónica**

La inteligencia de Guerra Electrónica (IGE) se encuentra definida en el reglamento GE para la Acción Militar Conjunta (EMCO, 2012) como "*el producto resultante de la colección, evaluación, análisis, integración, interpretación y difusión a quien se determine de toda la información disponible relativa al uso de los espectros electromagnético por parte del enemigo o potencial adversario, o al uso que de dichos espectros se hace en un área de operaciones potencialmente significativa desde el punto de vista de la Guerra Electrónica."*

Al igual que la Inteligencia de Señales y la Ciberinteligencia, la IGE tiene su propio ciclo de producción. Este ciclo es similar al de inteligencia de señales debido a que comparte las actividades de guerra electrónica para la obtención y proceso de la información.

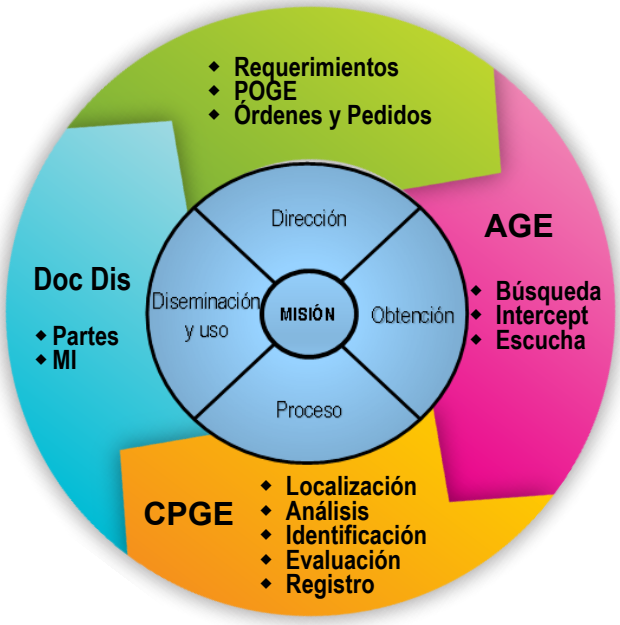


*Gráfico 4: Ciclo de Producción de Guerra Electrónica (Elaboración propia).*

El ciclo de producción de inteligencia GE comienza con los requerimientos analizados el apartado anterior. Estos requerimientos estructuran el Plan de Obtención de Guerra Electrónica (POGE) que servirá para elaborar los pedidos y órdenes de obtención a los medios de Apoyo de Guerra Electrónica. Las actividades de apoyo las realizarán los medios de campaña, como así también, las instalaciones fijas que, mediante la búsqueda, interceptación y escucha obtendrán información en el EEM.

El proceso de la información obtenida se realizará en el Centro de Procesamiento de Guerra Electrónica (CPGE), lugar de trabajo del Oficial de Inteligencia del elemento de GE que este operando.

Normalmente la diseminación de la información se hará a través de partes y mensajes de información.

## Sección IV: Comparación de los Sistemas

### Factores de comparación

Para comparar los sistemas analizados e identificar actividades y objetivos en común resulta necesario determinar qué factores utilizar.

Esta determinación arbitraria está orientada a evaluar y obtener conclusiones que contribuyan a la posible solución problema de investigación planteado. Algunos de los factores seleccionados fueron desarrollados en el presente trabajo y otros son extraídos de la doctrina consultada.

Los factores de comparación que utilizaré son:

a) Nivel de la Conducción
b) Empleo
c) Finalidad
d) Tipo de actividad
e) Alcance en el tiempo
f) Órgano responsable de su ejecución
g) Actividades y tareas principales
h) Requerimientos de Inteligencia
i) Ciclo de Producción de Inteligencia

### Comparación

Con la finalidad de realizar una ordenada comparación de los factores seleccionados y presentar la información de forma clara y concisa elaboré un cuadro comparativo.

| Factores | IS | CD | GE |
|---|---|---|---|
| **Nivel de la Conducción** | Estratégico Militar | Estratégico Militar / Operacional / Táctico | Estratégico Militar /Operacional / Táctico |
| **Empleo** | Estratégico Militar / Operacional / Táctico | Estratégico Militar / Operacional / Táctico | Operacional / Táctico |
| **Finalidad** | Determinar Capacidades, Debilidades e Intenciones del Eno | Disputar el control del ciberespacio necesario para el accionar de las fuerzas militares. | Reducir o negar el uso de EEM al Eno y asegurar su empleo por parte de las propias Fuerzas |
| **Dominio** | EEM | Ciberespacio | EEM |
| **Tipo de actividad** | Pasiva | Activa - Pasiva | Activa - Pasiva |
| **Alcance en tiempo** | Permanente | Permanente | Operaciones Militares |
| **Órgano responsable** | Inteligencia Militar | Elementos de Ciberdefensa | Elementos de Guerra Electrónica |
| **Actividades y tareas** | AGE | Op (s) Def, Op(s) Ofen y Explo | AGE, AE y PE |
| **Requerimientos** | Datos técnicos<br>Bandas de frecuencia | Amenazas cibernéticas<br>OB Ciber | Amenazas electromagnéticas<br>OBE |
| **Ciclo de Producción** | Basado en las actividades de AGE | Basado en las actividades de ciberinteligencia | Basado en las actividades de AGE |

*Gráfico 5: Cuadro de Comparación de Sistemas (Elaboración Propia).*

**Principales Similitudes y diferencias**

Claramente el sistema de IS posee varias similitudes con el sistema de GE, en particular porque comparten el dominio donde realizan sus actividades principales. Además, estas actividades son los mismas con la diferencia que el proceso de trabajo tiene otra finalidad. Por el lado del sistema de CD, si bien las actividades son en esencia diferentes a los otros sistemas presenta la misma finalidad que la GE en el dominio que le es propio.

En relación con el alcance en el tiempo la IS y la CD son permanentes mientras que la GE actúa cuando se realizan operaciones militares, por ello es sumamente importante la producción de inteligencia de señales especifica que nutra de información a los elementos de GE durante la paz.

Queda claro que el sistema de IS necesita principalmente conocer la frecuencia de donde obtener la información, y no solo eso, también otros parámetros técnicos que permiten

la interceptación de las señales. Por esta razón, los requerimientos de inteligencia propios de la IS estarán orientados a los datos técnicos y firmas electromagnéticas para poder realizar su función. En cambio, tanto la CD como la GE requieren conocer las amenazas a enfrentar, de esta manera actualizar el Orden de Batalla para el planeamiento y ejecución de sus operaciones y/o actividades.

**Conclusiones Parciales**

A la luz de lo analizado el sistema de Inteligencia de Señales representa un importante apoyo para las operaciones en el ciberespacio y especialmente en el espectro electromagnético. Indudablemente para cualquier tipo de operación el apoyo de inteligencia resulta primordial, más aún cuando se opera en dominios tan particulares.

Tanto las operaciones de Guerra Electrónica como las de Ciberdefensa son multiplicadoras del poder de combate propio, además brindan la posibilidad de degradar las capacidades del enemigo mediante la afectación de su comando y control, la interferencia de sus comunicaciones, el engaño de sensores, la dilación en la toma de decisiones, etc.

Resultado de la comparación de los sistemas desde el punto de vista inteligencia claramente surge que los sistemas afines y complementarios son el de Inteligencia de Señales y el de Guerra Electrónica principalmente por el espacio en donde operan y sus actividades concurrentes. Sin embargo, la Inteligencia de Señales sin operar dentro del ciberespacio puede aportar un apoyo sustancial al Sistema de Ciberdefensa.

En el campo de combate moderno existe una innumerable cantidad de equipos y dispositivos que emiten ondas electromagnéticas normalmente para comunicarse o mantener un enlace entre ellos. Estas señales que viajan por el espectro electromagnético transportan

paquetes o tramas de datos. Estos datos cargan con información muy valiosa para la identificación de amenazas, intenciones y características de los equipos utilizados. Por esta razón, la integración de los sistemas resulta sumamente necesario.

La saturación de señales en el espectro consecuencia de la masificación de dispositivos móviles y de enlaces basados en tecnología inalámbrica imponen, en primer lugar, la necesidad de contar con equipos de detección con una gran capacidad de almacenamiento de datos, además, poseer herramientas para el análisis y procesamiento de grandes volúmenes de información y, por último, lo más importante, analistas altamente capacitados para evaluar e interpretar la información con poco tiempo disponible y elaborar conclusiones claras, precisas y concretas.

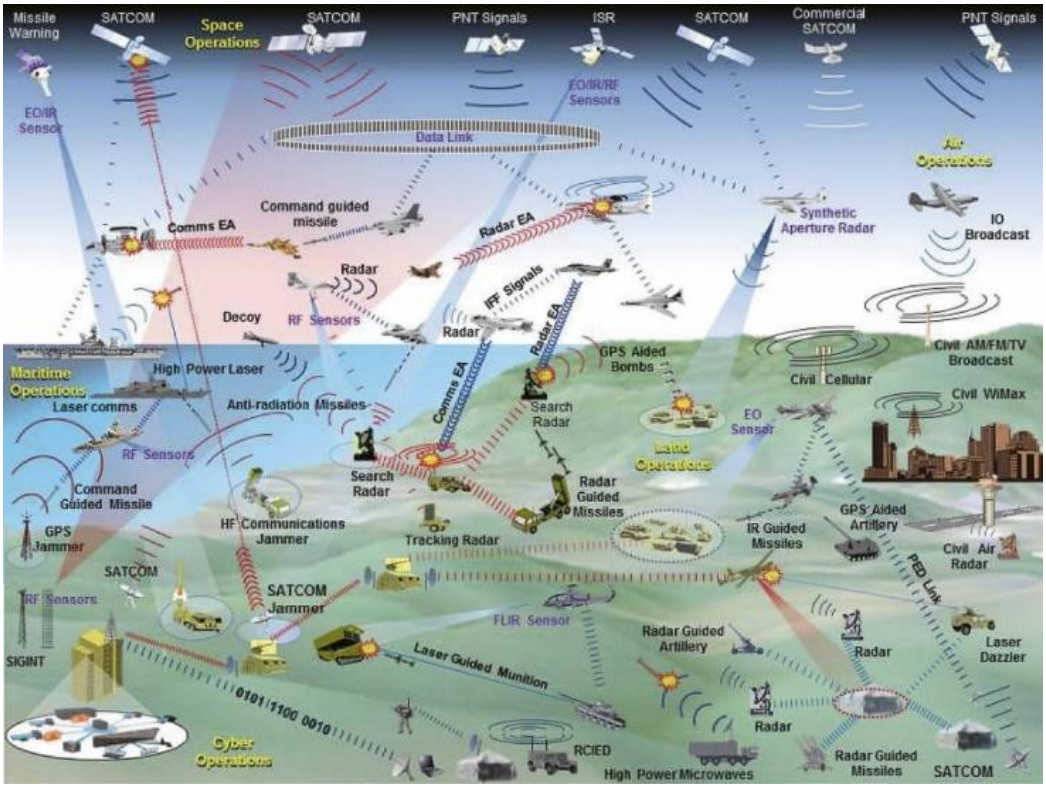


*Gráfico 6: Saturación del EEM (Imagen del Departamento de Defensa de Estados Unidos)*

# Capítulo 2

# Flujos de Información

## Sección I: Flujos de Información del Sistema de Inteligencia de Señales

Entendiendo que la IS es conducida desde el nivel estratégico militar, pero el empleo de los productos de inteligencia elaborados sirve, además, a los niveles operacional y táctico, es medular unificar criterios para el establecimiento de canales de comunicación.

A nivel Componente Terrestre del Teatro de Operaciones (CTTO) se deberán establecer los canales necesarios para que el flujo de la información recorra los distintos niveles de la conducción de forma fluida, ininterrumpida y segura.

Los elementos de IS producirán inteligencia desde sus instalaciones fijas. La obtención de información será desde sus plantas de obtención de señales y se servirán de la información que se obtenga en el campo de combate. Además, mediante pedidos de información conseguirán inteligencia producida por los otros Componentes del Teatro de Operaciones.

Hoy los flujos de información establecidos hacia el nivel superior pasan en primer lugar por la Central de Inteligencia Militar (CIM), la cual es cabeza de dos sistemas, el Sistema de Inteligencia Territorial y el sistema de Inteligencia de Proyección. A su vez, la Central a través de la Dirección General de Inteligencia (DGI) puede mantener canales de comunicación abiertos con las otras Fuerzas Armadas y con la Dirección Nacional de Inteligencia Estratégica Militar (DNIEM). En este sentido la integración del sistema de inteligencia de señales del Ejército con los sistemas afines de la Fuerza Aérea y la Armada se materializa a través primero de la CIM para luego pasar por la Dirección General de Inteligencia.

El sistema de IS está contemplado como parte integrante del Subsistema de Guerra Electrónica del Ejército (SUGE). Este subsistema forma parte del Sistema Único de Comunicaciones e Informática (SUCOMI) que es el conjunto coordinado e integrado de personal especialmente capacitado y facilidades de comunicaciones, informática, guerra electrónica y ciberdefensa del Ejército. (EA, 2016 a).

El SUGE está conformado por dos estructuras, una estructura territorial y una de campaña. La estructura territorial es el Sistema a estratégico de guerra electrónica (SIEGE) que está conformado por elementos de comunicaciones y de inteligencia, organizados, equipados, instruidos y adiestrados para desarrollar apoyo de guerra electrónica (AGE) y protección electrónica (PE) que ejecutarán sus tareas desde estaciones o plantas establecidas en forma permanente y estarán capacitados para operar ininterrumpidamente.

El SIEGE obtiene información de utilidad para el nivel Estratégico Militar y eventualmente para el nivel Operacional y Táctico en caso de conflicto o guerra. Naturalmente el sistema de IS junto con las estaciones fijas de GE integra la estructura territorial aportando sus productos al SUGE para la ejecución de distintas acciones de AGE, AE y PE. La estructura de campaña se conformará sobre la base de fracciones móviles aptas para operar en proximidades del enemigo las cuales materializan el Sistema Táctico de Guerra Electrónica (SITAGE) de las Fuerzas Terrestres del Teatro de Operaciones. (EA, 2016 a).

Ante la conformación de un TO el punto de enlace entre el sistema de IS y el SUGE será el Centro Integrador de Inteligencia (CII) de la unidad de la tropa técnica que este en apoyo al CTTO. El CPGE de la unidad de GE en apoyo al CTTO deberá contar con un enlace

permanente con el CII, ya que todo pedido de información será canalizado y enviado a través del canal técnico de inteligencia.

## Sección II: Flujos de Información del Sistema de Ciberdefensa

El Sistema Militar de Ciberdefensa se caracteriza por tener una estructura jerárquica y vertical. Su componente estratégico está encabezado por la Subsecretaría de Ciberdefensa, que supervisa el nivel estratégico operacional materializado en el Comando Conjunto de Ciberdefensa. Este último, a su vez, ejerce el control funcional sobre el nivel táctico, que comprende la Dirección de Ciberdefensa de cada Fuerza y las unidades subordinadas a las Direcciones Generales de Comunicaciones e Informática de cada fuerza respectiva.

Las Direcciones de Ciberdefensa de cada Fuerza Armada, al conformarse un Teatro de Operaciones, serán puestas a disposición del Comando Conjunto de Ciberdefensa, quien ejercerá el comando operacional de estas.

La Dirección de Ciberdefensa y los elementos de Ciberdefensa del Ejército forman el sistema de Ciberdefensa que actuará en el nivel Táctico apoyando las operaciones del CTTO.

Un elemento de CD desplegado en el TO cuenta con un Centro de Procesamiento de Ciberdefensa (CPCD) con similares funciones del CPGE, incluso puede que el mismo centro se encargue del procesamiento de la información de ambos sistemas (CPGECD).

Las operaciones son planificadas y dirigidas desde el Centro de Operaciones de Ciberdefensa (COC) que contará con un enlace directo al CPCD. Al mismo tiempo, el CPCD tendrá su enlace con el CII del CTTO por donde pasarán los flujos de información entre ambos.

Por otro lado, la actividad de Ciberinteligencia debe apoyar al Sistema de Ciberdefensa ya que es un área concurrente para la producción de Inteligencia a fin de poder definir, calificar y cuantificar las ciberamenazas reales y potenciales, permitiendo complementariamente la readecuación de las políticas de seguridad y la determinación de estándares de comportamiento seguro, en la generación de nuevas reglas y métricas de los sistemas de monitoreo y alarma del Sistema de Ciberdefensa, en la prevención ante ciberataques. La División de Ciberinteligencia del Ejército en una parte del Departamento Proyección dependiente de la Dirección de Inteligencia Funcional.

La División de Ciberinteligencia que estará en apoyo del Sistema de Ciberdefensa del Ejército podrá ser el punto de enlace entre el sistema de IS y el de CD. Si bien aún no se dispone de un elemento con medios móvil responsable de realizar la actividad de ciberinteligencia desplegado en el TO para satisfacer los requerimientos de inteligencia a nivel táctico, existe la posibilidad de ejecutar las actividades desde instalaciones fijas siempre que se cuente con un canal de comunicación apto y seguro por donde fluya la información.

Resulta trascendental el uso del canal técnico de inteligencia, por el cual diligenciar, órdenes y pedidos de información, documentos de diseminación, partes, paquetes o tramas de datos, etc; desde las instalaciones fijas de inteligencia hacia el CII que se encuentre desplegado en el terreno. El CII será la puerta de entrada del Sistema de Inteligencia de Señales y de la División de Ciber Inteligencia al TO.

Otra vez es primordial que el CII en apoyo al CTTO cuente con capacidades de gestionar información especifica de IS, GE y CD con celeridad. Por ello es necesario instalar, operar y mantener los medios de comunicaciones particulares de Inteligencia integrados con los medios del Arma de Comunicaciones para permitir el flujo de información seguro, ágil y constante entre los sistemas.

## Sección III: Flujos de Información del Sistema de Guerra Electrónica

Durante períodos de paz, la responsabilidad de dirigir las operaciones de guerra electrónica, con el fin de prevenir incidentes con implicaciones internacionales, lograr la cooperación conjunta, fomentar el intercambio de información, reducir los costos, establecer procedimientos y definir los requisitos de protección electrónica para sistemas de comunicación, sistemas de armas y equipos encargados de las misiones de apoyo de guerra electrónica (AGE) y ataque electrónico (AE) en apoyo de operaciones tácticas, recae en el nivel estratégico militar desde el ámbito conjunto.

Como ya se explicó en la Sección I existen DOS (2) sistemas de apoyo de guerra electrónica integrados, uno es el sistema estratégico de guerra electrónica (SIEGE) y otro sistema es el denominado sistema táctico de guerra electrónica (SITAGE) para apoyar las operaciones tácticas del componente terrestre del teatro de operaciones (CTTO). Estos dos sistemas componen el SUGE.

En el Ejército Argentino, la GE será conducida por la Dirección General de Comunicaciones e Informática en permanente y estrecha coordinación con la Dirección General de Inteligencia; la ejecución de las acciones de apoyo de guerra electrónica (AGE) será a través del subsistema fijo que operarán elementos de la tropa técnica de inteligencia y del arma de Comunicaciones, complementándolas (en caso de necesidad) con acciones llevadas a cabo por el subsistema de campaña que establecerán, operarán y mantendrán elementos de guerra electrónica del arma de Comunicaciones. (EA, 2016 a)

Durante el desarrollo de operaciones tácticas, SITAGE en apoyo del CTTO será establecido, operado y mantenido por elementos del arma de Comunicaciones siendo

conducidos por el comando del componente, con el asesoramiento y asistencia del departamento comunicaciones, informática y guerra electrónica (Dpto CIGE) de ese comando.

Las acciones que ejecutará el SITAGE se integrarán en las que se desarrollan desde el subsistema fijo de guerra electrónica y para ello se requiere de un sistema de comunicaciones particular que enlace los distintos medios a fin tener una conducción centralizada.

Como ya se mencionó en la Sección I, el CPGE juega un papel fundamental en la gestión y diligencia de la información hacia y/o desde el TO. Desde el CPGE, se establecerá el flujo de información por medio de las facilidades de comunicaciones e informática más adecuadas a la situación y a la operación táctica en desarrollo con el CII que se encuentre en apoyo al comando del CTTO. Eventualmente se establecerá, también, un canal de información con el puesto comando del CTTO.

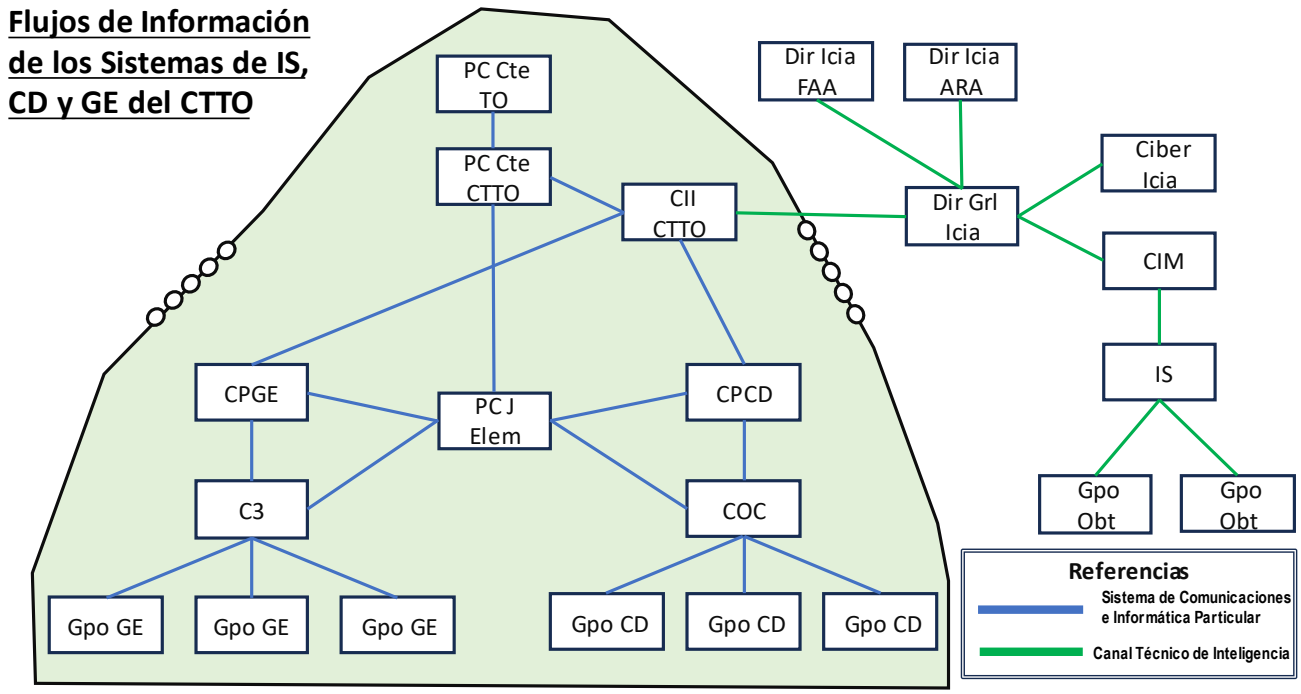


*Gráfico 7: Flujos de Información de los Sistemas (Elaboración propia)*

## Conclusiones Parciales

La información oportuna y precisa es esencial para la toma de decisiones en todos los niveles de la conducción. Los flujos de información proporcionan la base para evaluar situaciones, identificar problemas y encontrar soluciones, en otras palabras, resultan indispensable para una detallada planificación.

En el Teatro de Operaciones, la toma de decisiones rápida y precisa es esencial. Los flujos de información proporcionan a los decisores (Cte(s) y JJ) datos actualizados sobre la situación, la ubicación del enemigo, los recursos disponibles y otros factores relevantes para la toma de decisiones a nivel táctico.

La obtención de información para la producción de inteligencia es fundamental para ejecutar cualquier tipo de operación. Los flujos de información permanentes y seguros permiten el desarrollo del ciclo de producción inteligencia de forma continua y en oportunidad.

En este sentido, el aporte de la Inteligencia de Señales a los elementos que integran los Sistemas de Guerra Electrónica y Ciberdefensa en apoyo al CTTO será muy importante. Asimismo, la información obtenida por los medios desplegados en el terreno de GE y de CD serán de suma utilidad para la producción de inteligencia de señales.

Establecer un flujo de información directo entre los sistemas permite la celeridad de transmisión de partes, documentos de diseminación, mensajes, archivos, datos, sumamente necesario para acortar los tiempos del ciclo de producción de inteligencia, poseer más cantidad y mejores en calidad elementos de juicio para un rápido asesoramiento y de esta manera incidir positivamente en el ciclo OODA (observar, orientar, decidir y actuar).

## Conclusiones Finales

En el desarrollo del presente trabajo se analizó en profundidad los sistemas de Inteligencia de Señales, Guerra Electrónica y Ciberdefensa con el foco puesto en las actividades de inteligencia. El análisis de los ciclos de producción de inteligencia en los tres sistemas resulta muy útil para entender las necesidades de información que deben satisfacer.

Queda claro que existe la necesidad de que estos sistemas actúen en forma integrada y mancomunada, la GE y la CD ejecutando sus operaciones con el apoyo de la IS y la Ciber Icia. En los conflictos de la actualidad es claro que las operaciones se ejecutan en múltiples dominios, de esos dominios los transversales a los demás resultan ser el ciberespacio y el EEM, en esto reside la importancia de lograr establecer los procesos de trabajo necesario para la integración de los sistemas que actúan en y desde estos ámbitos.

La manera de establecer un flujo de información directo entre los sistemas es abrir nuevos canales de comunicación. Estos canales se materializan en enlaces con equipos de comunicación específicos que formen una red particular e integren los sistemas. Estos equipos deberán contar, además de las medidas de seguridad propias de los equipos modernos, con la posibilidad de transmitir datos a gran velocidad.

Lo ideal es poder acceder a las bases de datos de los distintos sistemas en forma remota para contar con información básica de GE, CD o IS en forma permanente evitando tener que solicitarla por los canales formales lo que implica pérdida de tiempo en la elaboración y envío del pedido de información.

Resultado del análisis de los flujos de información realizado en el Capítulo 2, una posible solución al problema planteado es la de establecer un enlace permanente entre los

CPGE y CPCD con el elemento de Inteligencia de Señales, más precisamente con la fracción que se desempeñe como Control del Sistema.

Otra solución es la de reforzar al CII CTTO con el personal y equipos con aptitud para intervenir y ser parte del flujo de información entre los sistemas. Normalmente un CII no cuenta con analistas dedicados a las actividades cibernéticas o electrónicas, por ello es indispensable reforzar al CII con personal capacitado para entender los requerimientos, saber diligenciarlos y de ser posible satisfacerlos.

Por último, cabe mencionar que ninguna de estas propuestas será posible si el personal integrante de cada sistema no está dispuesto a trabajar en equipo y a brindar la información obtenida ni la inteligencia producida sin restricciones justificadas. La dependencia orgánica de los sistemas (IS-DGI, GE-DGCI, CD-DCEA) impone una separación de hecho en las relaciones de comando que resultarán difíciles de modificar en el corto plazo. La forma más sencilla de eliminar cualquier tipo de recelo o desconfianza entre los integrantes de los tres sistemas es comenzar a trabajar en pequeños proyectos o en ejercicios de forma integrada.

La guerra moderna impone nuevos desafíos que las Fuerzas Armadas y en particular el Ejército Argentino tiene que afrontar, uno de ellos es poder influir de forma efectiva en los distintos dominios y en diferentes dimensiones. Una buena opción es la de desarrollar sus capacidades en el ciberespacio y en el EEM, ya que estos son transversales a todos los dominios.

## Bibliografía

Chiavaro, G. D. (2018). Trabajo Final Integrador. *La influencia de la guerra electrónica en el diseño operacional*. Buenos Aires, Argentina.

De Arcangelis, M. (1983), Historia de la Guerra Electrónica, España, Editorial San Martín.

Ejército Argentino. (2008). *Manual de Inteligencia para el Comandante o Jefe de Elemento.* Buenos Aires: Departamento Doctrina.

Ejército Argentino. (2008). *Inteligencia Táctica*. Buenos Aires: Departamento Doctrina.

Ejército Argentino. (2015). *Conducción para las Fuerzas Terrestres.* Buenos Aires: Departamento Doctrina.

Ejército Argentino. (2016 b). *Inteligencia de Señales*. Buenos Aires: Departamento Doctrina.

Ejército Argentino. (2016 a). *Conceptos Básicos sobre Sistema de Comunicaciones, Informática y Guerra Electrónica de la Fuerza*. Buenos Aires: Departamento Doctrina.

Estado Mayor Conjunto de las Fuerzas Armadas. (1998). *Diccionario para la Acción Militar Conjunta*. Buenos Aires: Departamento Doctrina.

Estado Mayor Conjunto de las Fuerzas Armadas. (2007). *Inteligencia para la Acción Militar Conjunta*. Buenos Aires: Departamento Doctrina.

Estado Mayor Conjunto de las Fuerzas Armadas. (2012). *Guerra Electrónica para la Acción Militar Conjunta*. Buenos Aires: Departamento Doctrina.

Ferreyra, A. A. (2019). Trabajo Final Integrador. *Concepto general de empleo de elementos de guerra electrónica durante el desarrollo de operaciones defensivas en apoyo a la Gran Unidad de Batalla*. Buenos Aires, Argentina.

Marrupe Pereyra, A. I. (2014). Trabajo Final Integrador. *Diseño de un órgano director de guerra electrónica en apoyo al comando de nivel operacional*. Buenos Aires, Argentina.

Maidana Mur, J. A. (2022). Trabajo Final Integrador. *Apoyo de la Ciberinteligencia a las Operaciones Militares.* Buenos Aires, Argentina.