



**UNIVERSIDAD DE LA DEFENSA NACIONAL**  
**INSTITUTO DE INTELIGENCIA DE LAS FFAA**  
**“Sarg My D. José Antonio ÁLVAREZ DE CONDARCO”**

**“ESPECIALIZACIÓN EN GESTIÓN DE INFORMACIÓN  
MILITAR TERRESTRE”**

**TRABAJO FINAL INTEGRADOR**

**TEMA:** Medidas de Seguridad a nivel GUC, en operaciones defensivas

**AUTOR:** Teniente Primero Daniel Felix Francisco Sampietro

**DIRECTOR:** Mg Coronel (R) Augusto CAYO

**AÑO:** 2022

*“Las ideas expresadas sólo representan la postura personal del autor, por lo que son de su absoluta responsabilidad, no reflejando en consecuencia la opinión del Instituto de Inteligencia de las Fuerzas Armadas y de la Universidad de la Defensa Nacional.”*



## RESUMEN

El permanente avance de la tecnología juntamente con la sociedad impactó sobre la forma de desarrollar la guerra. Así vemos que los combates se producen a la distancia con menor exposición del ser humano, con el desarrollo de armas individuales, de conjunto y de Sistemas de Armas que produjeron un verdadero cambio de paradigma.

La utilización de nuevos aparatos, la operación de computadoras, celulares, tabletas y hasta de televisores inteligentes, hacen que éstos se conviertan en verdaderos Sistemas de Información, todos relacionados y conectados entre sí a través de la Red Internet, datos móviles, wifi, Intranet, etc.

Debido a lo mencionado en el párrafo anterior, los sistemas electrónicos, además de ser una herramienta útil para almacenar información, comunicarse y hacer más dinámicas las tareas, también tornan más vulnerable a nuestra propia organización. Esto se produce por estar conectados a la Red Internet y se acrecienta cuando el personal no tiene desarrollado un gran conocimiento del tema y cuando se carece de un buen sistema de seguridad y encriptación. De esta manera cualquier agente externo puede ingresar a nuestro sistema, siendo difícil su detección oportuna y en algunos casos puede ser indetectable, ocasionando la manipulación de la información por parte de agentes externos que la pueden borrar, capturar o simplemente hacerla funcionar de manera errónea para su beneficio.

A través del presente trabajo, se buscará abordar la importancia que tiene el uso del EEM, disponiendo del personal adecuado, contando con el Hardware y Software necesario y logrando un correcto funcionamiento, mediante la coordinación de los distintos elementos participantes, donde en este caso en particular, serían los Puestos de Comando, los Elementos Logísticos y de otros que ocupan la zona en cuestión. Todos ellos interactuando de manera coordinada y activa.

Se demostrará cómo esto facilita la creación de modelos de las posibles amenazas y su forma de combatir las o de prevenirlas. De manera activa, para detectarlas con el suficiente tiempo para brindarle a los elementos decisores, el espacio y el tiempo suficiente para decidir el mejor modo de acción y evitando de esta forma, la degradación de nuestros sistemas, como así también la detección temprana, minimizando los posibles daños a los elementos logísticos y puestos de comando y lograr una ventaja sobre el enemigo.

**Palabras Clave:** Espectro Electromagnético – Seguridad – Defensa - Amenaza

## ÍNDICE

|                                                                                        |    |
|----------------------------------------------------------------------------------------|----|
| Introducción .....                                                                     | 6  |
| Capítulo I: Empleo de Medidas de Seguridad utilizando el Espectro Electromagnético.... | 9  |
| 1.1 Concepto general .....                                                             | 9  |
| 1.2 Empleo del Espectro Electromagnético en la Guerra Electrónica .....                | 9  |
| 1.2.1 Apoyo de Guerra Electrónica (AGE) .....                                          | 10 |
| 1.2.2. Ataque Electrónico (AE) .....                                                   | 10 |
| 1.2.3 Protección Electrónico (PE) .....                                                | 10 |
| 1.3 Actividades de Guerra Electrónica dentro del Espectro Electromagnético.....        | 10 |
| 1.4. Efecto de la Guerra Electrónica dentro del Espectro Electromagnético.....         | 11 |
| 1.4.1. Control.....                                                                    | 11 |
| 1.4.2 .Detección .....                                                                 | 12 |
| 1.4.3. Negación .....                                                                  | 12 |
| 1.4.4. Engaño .....                                                                    | 12 |
| 1.4.5. Interrupción y Degradación .....                                                | 12 |
| 1.4.6. Protección .....                                                                | 12 |
| 1.4.7. Destrucción .....                                                               | 12 |
| 1.5. Protección Electrónica .....                                                      | 13 |
| 1.5.1. Endurecimiento Electrónico.....                                                 | 13 |
| 1.5.2. Impedimento Electromagnético.....                                               | 13 |
| 1.5.3. Enmascaramiento Electrónico.....                                                | 13 |
| 1.5.4. Reprogramación de Guerra Electrónica.....                                       | 13 |
| 1.5.5. Control de Emisión.....                                                         | 14 |
| 1.5.6. Administración del Espectro Electromagnético.....                               | 14 |
| 1.6. El uso del Espectro Electromagnético en el Sistema de Comando, Control,           |    |
| Comunicaciones, Informática e Inteligencia.....                                        | 14 |
| 1.6.1. Sistema C3I2.....                                                               | 15 |
| 1.7. Ataque Electrónico.....                                                           | 15 |
| 1.7.1 Actividades ofensivas del Ataque Electrónico.....                                | 15 |

|                                                                                       |    |
|---------------------------------------------------------------------------------------|----|
| 1.7.2. Actividades defensivas del Ataque Electrónico.....                             | 16 |
| 1.8. Empleo del apoyo de Guerra Electrónica en las operaciones.....                   | 16 |
| 1.9. Conclusiones parciales del Capítulo I.....                                       | 16 |
| Capítulo II: Vulnerabilidades del uso desmesurado del Espectro Electromagnético ..... | 18 |
| 2.1. Introducción .....                                                               | 18 |
| 2.2. Los Captoreos .....                                                              | 18 |
| 2.3. Características de las Plataformas Captoras .....                                | 20 |
| 2.4. Los Sensores en Plataformas Efectoras .....                                      | 22 |
| 2.5. Conclusiones parciales del Capítulo II.....                                      | 23 |
| Capítulo III: Determinación de los Modelos del Enemigo utilizando el EEM .....        | 25 |
| 3.1 Introducción .....                                                                | 25 |
| 3.2 Modelos del Enemigo .....                                                         | 25 |
| 3.3 Los Diferentes Tipos de Modelos .....                                             | 26 |
| 3.4 Aspectos a tener en cuenta para la creación de Modelos.....                       | 29 |
| 3.4.1 Envoltentes.....                                                                | 29 |
| 3.4.2 Cubrimientos.....                                                               | 29 |
| 3.4.3 Organización.....                                                               | 30 |
| 3.4.4 Distribución en el Terreno.....                                                 |    |
| 3.4.5 Proceso.....                                                                    | 30 |
| 3.4.6 Doctrinas.....                                                                  | 30 |
| 3.5 Conclusiones Parciales del Capítulo III.....                                      | 30 |
| Conclusiones generales .....                                                          | 32 |
| Bibliografía .....                                                                    | 34 |
| Anexo I – Encuesta .....                                                              | 35 |

## INTRODUCCIÓN

El avance de la tecnología viene jugando un papel protagónico en lo que respecta a los conflictos actuales, desde los Sistemas de Armas que se operan a la distancia (misiles teleguiados, aeronaves no tripuladas con sistemas de armas incorporadas, etc), hasta los ataques cibernéticos (ciberataques), de los que se desconoce su origen y quién los generó. Como así también el accionar de Tropas Especiales de Combate.

A partir de lo planteado en el párrafo anterior, surge la necesidad de implementar medidas de seguridad durante la ejecución de operaciones tácticas y el uso activo del Espectro Electromagnético (EEM)<sup>1</sup>.

Con el uso activo del EEM, se busca localizar amenazas y a partir de la obtención de información, poder realizar los respectivos modelos<sup>2</sup> y posteriormente implementar medidas de prevención para que en un futuro no afecten los sistemas propios.

En cambio, en lo referido al uso activo, hace hincapié en la búsqueda y detección de una amenaza con el uso del EEM (radares, software, etc), posibilitando de esta manera la creación de modelos del enemigo u oponente, para que, de esta manera, evite que el enemigo u oponente degrade los sistemas propios, ya que los mismos son la base fundamental para el Comando y Control de las operaciones tácticas, más aún en los combates modernos, desarrollados en el último tiempo.

---

<sup>1</sup>Es el espacio donde interactúan todas las ondas y energías electromagnéticas. Se lo considera infinito, ya que, dentro del mismo se desarrollan los medios de informática, comunicación, sensores, etc.

<sup>2</sup>Hace referencia a los procedimientos, tipos de malware o de que manera podría actuar el enemigo sobre los sistemas o el dispositivo.

Estas actividades se encuentran enmarcadas dentro del Ambiente Electromagnético<sup>3</sup>, ya que, el fin que tiene el mismo, es regular todas las actividades de emisiones electromagnéticas.

Se sabe que el uso indiscriminado del EEM, permite por supuesto, un mayor C3I2 pero también acrecienta las propias vulnerabilidades y oportunidades de guerra electrónica que podrían favorecer al enemigo. Sobre esto, es que este trabajo de investigación se va a basar. Estudiando y evidenciando, cómo y a pesar de que las emisiones electromagnéticas son vulnerables cuando se usan de manera continuada, con un buen Comando y Control y la elección de equipos, software y momentos correctos, se puede detectar de manera oportuna e íntegra las amenazas y convertir nuestras debilidades en fortalezas.

Entonces, considerando la dirección que se intenta tomar, establecí como el objetivo general del trabajo, exponer el desarrollo del Espectro Electromagnético, como pilar fundamental de las medidas de seguridad tomadas durante la ejecución de una defensa de zona, particularmente en la zona de retaguardia. Para ello, el ensayo estará estructurado en tres capítulos, que servirán como base para explicar cada uno de los temas necesarios para entender la situación, los cuales se desprenderán de los objetivos específicos señalados a continuación:

- Analizar las medidas de seguridad activas utilizando el EEM, necesarias para preservar los puestos de comando y elementos logísticos de manera independiente al resto de los elementos, para proteger el sostenimiento de las operaciones de la GUC utilizando la Guerra Electrónica (Capítulo I).
- Determinar el uso de los captores y efectores necesarios para el mantenimiento de la seguridad (Capítulo II).

---

<sup>3</sup> "Hace referencia al producto resultante de la potencia y la distribución del tiempo, de emisiones de energía electromagnética radiada o conducida pudiéndose llevar a cabo en diferentes niveles y rangos de frecuencia." (PC - 13 - 50 "Guerra Electrónica para la acción Conjunta", 2012)

- Determinar la creación de los modelos del enemigo u oponente a partir del uso activo del EEM, para la prevención de futuras amenazas (Capítulo III).

Para analizar el problema de nuestra investigación, se empleará el análisis bibliográfico de doctrina y documentación vigentes, clases relacionadas, artículos publicados en Internet y revistas militares en los cuales se plasman conceptos y experiencias en operaciones militares. La investigación será de tipo exploratoria y descriptiva, donde se describirán los conceptos y procedimientos, cómo son y cómo se manifiestan, buscando especificar sus propiedades.

## **CAPÍTULO I**

# **EMPLEO DE MEDIDAS DE SEGURIDAD UTILIZANDO EL ESPECTRO ELECTROMAGNÉTICO**

### **1.1. Concepto General**

En los últimos años, la evolución de la tecnología fue tal, que, en la actualidad los equipos electromagnéticos cada vez son más utilizados, tanto en el ámbito civil como en el militar, con el fin de ejecutar actividades de inteligencia, comunicación, navegación, procesar y almacenar información, etc.

Por ello, aunque la idea de este capítulo será explicar las diferentes formas en que se emplea el EEM para darle seguridad y protección a los propios sistemas y medios, estos dispositivos diariamente en nuestro ámbito laboral, me resulta imprescindible definir qué entendemos como “teléfono inteligente” y mencionar brevemente que los hace tan indispensables para nuestra vida incluyendo su actualización de forma periódica.

### **1.2 Empleo del Espectro Electromagnético en la Guerra Electrónica**

Hoy en día, con la evolución de la tecnológica y por consecuencia, el desarrollo de las operaciones militares, el uso del EEM ha hecho que la Guerra Electrónica ocupe un papel fundamental en las operaciones militares, protegiendo los sistemas, emisiones y transporte de comunicaciones y accionando ofensivamente sobre los sistemas del oponente o enemigo.

Es por ello que el planeamiento de este tipo de operaciones debe planificarse en base a los efectos que el comandante busca producir evitando interferencias, superposiciones y otras consecuencias negativas en el desarrollo de las acciones propias

Su propósito final es el de negar al oponente una ventaja en el EEM, asegurando el empleo efectivo del mismo por parte de nuestras capacidades.

La GE<sup>4</sup> se divide en tres partes:

- 1.2.1 Apoyo de Guerra Electrónica (AGE):** Acciones para la obtención de 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, con el fin de contribuir al inmediato reconocimiento y seguimiento de amenazas presentes en el EEM” (PC-13-50, 2012, pág. 3).
- 1.2.2. Ataque Electrónico (AE):** “Consiste en el uso de la energía electromagnética, energía dirigida o armas anti-radiación para atacar al personal, instalaciones y equipamiento con la intención de degradar, neutralizar o destruir la capacidad de combate del enemigo” (PC-13-50, 2012, pág. 3).
- 1.2.3. Protección Electrónica (PE):** Son todas las acciones destinadas a proteger al personal, instalaciones y equipamientos del efecto que produce el uso del EEM por parte de propia fuerza, o del oponente/enemigo que amenace, degrade, neutralice o destruya la capacidad de combate propia.

Las tres divisiones de la GE, mencionadas anteriormente, evidencia que sus acciones dentro del EEM, van desde la detección de una amenaza y su acción para rechazarla, hasta el ataque a los sistemas, personal, equipamiento e instalaciones del enemigo u oponente, siendo un pilar fundamental para el desarrollo de las operaciones, teniendo en cuenta que el uso de las misma, se va a dar en base a las prioridades que le asigne el comandante en ese momento en particular.

### **1.3. Actividades de Guerra Electrónica dentro del Espectro Electromagnético.**

Las actividades de Guerra Electrónica fueron desarrolladas para explotar oportunidades y vulnerabilidades dentro del EEM, a través de las emisiones, transporte de datos, equipos, etc.

---

<sup>4</sup> Guerra Electrónica.

Por esta razón, con el paso del tiempo, el desarrollo de estas actividades, fueron evolucionando, en lo que respecta al equipo y tácticas que se emplean. Siendo, estas actividades fundamentales para la protección y control del EEM de las amenazas enemigas.

Las actividades de GE son: Contramedidas, Compatibilidad Electromagnética, Engaño Electromagnético, Endurecimiento Electromagnético, Impedimento Electromagnético, Intrusión Electromagnética, Inferencia Electromagnética, Enmascaramiento Electrónico, Investigación Electrónica, Reconocimiento Electrónico, Inteligencia, Electrónica, Seguridad Electrónica, Reprogramación de Guerra Electrónica, Control de Emisión, Administración del Espectro Electromagnético, Modos de reserva para tiempos de Guerra.

Todas las actividades mencionadas en el párrafo, son de carácter ofensivo y defensivo, teniendo en cuenta, que van a estar direccionadas en la intención del Comandante en base a como quiera emplearlas para el desarrollo de las operaciones y poder lograr el efecto deseado.

#### **1.4. Efectos de la Guerra Electrónica dentro del Espectro Electromagnético.**

Las actividades de GE dentro del EEM, son variadas, pudiendo ser, ofensivas o defensivas, dependiendo siempre de la intención que tenga el comandante, respecto a la operación a realizar. Estas actividades, se ejecutarán con la finalidad de lograr un efecto en particular.

Los efectos que pueden producir las actividades de GE con el uso del EEM son:

- 1.4.1. Control:** para lograr el control del EEM, se debe administrar y coordinar el uso de los sistemas de armas propios, mientras se degradan los del enemigo. De esta manera se limitará el uso del EEM por parte del adversario, mientras que se asegura el uso del mismo por parte de propia fuerza, permitiendo al comandante una actualización precisa de la situación en el área de operación.

- 1.4.2. Detección:** monitoreo activo y pasivo del Ambiente Operacional para detectar amenazas electromagnéticas. La detección, permite el aprovechamiento y explotación efectiva, asignación de blancos y una correcta defensa y protección de los fuerzas. Deben poseer la capacidad de detectar todo tipo de interferencia y caracterizarla, tratándose de interferencias hostiles o no.
- 1.4.3. Negación:** control de la información que recibe del adversario a través del EEM, evitando la intromisión a información clasificada o a los sistemas de propia fuerza.
- 1.4.4. Engaño:** tiene el fin de inducir al adversario a tomar conclusiones erróneas de la información que se proporciona, manipulando el ciclo de toma de decisión del adversario, haciendo dificultoso la idea de una realidad objetiva.
- 1.4.5. Interrupción y Degradación:** tiene el fin de interferir por medio de la Interferencia Electrónica, Engaño Electrónico e Intrusión Electrónica a través del EEM, evitando que el enemigo haga uso del mismo, limitando sus capacidades de combate. De esta manera aumentará la incertidumbre del enemigo, logrando una ventaja significativa.
- 1.4.6. Protección:** consiste en asegurar el uso del EEM por propias fuerzas, por medio de tácticas y procedimientos, como así también, garantizar que las actividades conjuntas de GE no degraden los sistemas de inteligencia y comunicación propios. Esto se logra por medio del endurecimiento electrónico, control de emisiones, administración de frecuencias, y el empleo de otros medios para impedir el uso del EEM por parte del adversario y contraatacar en caso de una posible intrusión del mismo en nuestros sistemas.
- 1.4.7. Destrucción:** consiste en eliminar los sistemas de blancos del enemigo, por medio del EEM, realizando ataques electrónicos sobre sus sistemas y equipos, disminuyéndole sus capacidades, generando una debilidad en el enemigo, pudiendo transformarla en una vulnerabilidad aplicando el modo de acción sobre la misma, siendo una notable ventaja para la propia fuerza.

Estos efectos, como se mencionó anteriormente, se darán en base a la operación a realizar, y la intención que tenga el comandante sobre la misma, sobre el modo de acción a ejecutar, dándole diferentes capacidades de GE a ejecutar en el EEM, otorgándole al comandante diferentes opciones para alcanzar sus objetivos.

Todas las actividades y efectos mencionados en este capítulo, son variados con el fin de darle al comandante diferentes capacidades.

### **1.5 Protección Electrónica.**

La Protección electrónica, son aquellas actividades destinadas a proteger, personal, equipos e instalaciones del uso del EEM por parte de las fuerzas adversarias o de propias fuerzas, que degrade, neutralice o destruya la capacidad de combate propia.

Para cumplir con las finalidad de las actividades mencionadas en el párrafo anterior se deben considerar los siguientes procedimientos o actividades:

**1.5.1. Endurecimiento Electromagnético:** son acciones con el fin de proteger al personal, equipos e instalaciones de efectos no deseados de energía electromagnética.

**1.5.2. Impedimento Electromagnético:** Es una alteración electromagnética que interrumpa el normal funcionamiento de los sistemas y equipos electrónicos.

**1.5.3. Enmascaramiento Electrónico:** Proteger emisiones de comunicaciones y sistemas electrónicos, evitando el apoyo de guerra electrónico (AGE) y la Inteligencia de Emisiones (INTEM) por parte del adversario.

**1.5.4. Reprogramación de Guerra Electrónica:** Es la alteración de los sistemas de GE, sensores, blancos y tácticas y procedimientos utilizados para validar cambios en el

equipamiento, tácticas y Ambiente Electromagnético. Su finalidad es la de mejorar el rendimiento y efectividad de los equipos y sistemas electromagnéticos.

**1.5.5. Control de Emisión:** tiene la finalidad de controlar el uso de emisiones electromagnéticas, optimizando la efectividad del comando y control (C2) e incrementar la seguridad de las operaciones. También, tiene la tarea de realizar engaño a las transmisiones que pueda interceptar el adversario o pueda interferir en los sistemas con el fin obtener acceso a información clasificada.

**1.5.6. Administración del Espectro Electromagnético:** Consiste en el planeamiento y coordinación a través de procedimientos y técnicas.

## **1.6. El uso del Espectro Electromagnético en el Comando, Control, Comunicaciones, Informática e Inteligencia.**

Los sistemas de comando y control tienen la finalidad de facilitar la conducción del Comandante. Los mismos, con el correr del tiempo, han ido evolucionando, aumentando su complejidad en base a los avances tecnológicos, necesitando herramientas más eficaces y versátiles.

Para la coordinación y desarrollo de esas herramientas, es esencial el uso correcto y eficiente del EEM, de manera tal, de poder transportar gran volumen de información y comunicaciones, como así también, realizar acciones ofensivas y defensivas, con el fin de apoyar y proteger el desarrollo eficiente de las operaciones.

Entonces, se puede decir, que los sistemas de comando y control, son una interdependencia entre los sensores de vigilancia y reconocimiento, sistemas de comunicaciones y procesamiento de datos, personal designado a las actividades de conducción y sus órganos de asesoramiento. Los cuales obtienen información, la procesan (registro, valorización, análisis, integración e interpretación) generando conclusiones (Inteligencia), para su posterior diseminación a los elementos que necesiten dicho producto, principalmente

destinado al asesoramiento para la toma de decisión. El Ejército Argentino, tiene el “concepto” de Comando, Control, Comunicaciones, Informática, e Inteligencia (C3 I2).

#### **1.6.1. Sistema C3I2**

Es un conjunto de medios humanos, sistemas y equipos tecnológicos coordinados, de forma tal de, ejecutar técnicas y procedimientos posibilitando al Comandante y su órgano de asesoramiento, la rápida apreciación de situación, la toma de decisiones, comunicación, mantener actualizada la situación del terreno, condiciones meteorológicas y enemigo en tiempo real o casi real.

#### **1.7. Ataque Electrónico**

Consiste en el uso la energía electromagnética, para ataque del equipo, sistemas, personal e instalaciones para degradar, neutralizar o destruir la capacidad de combate del enemigo.

Son acciones para negar el uso del EEM por parte del enemigo, con el fin de evitar que degrade sistemas, equipos y materiales electromagnéticos, como así también, incidir en los mismos para poder capturar, degradar o destruir información de alto valor.

##### **1.7.1. Actividades ofensivas del Ataque Electrónico:**

- Interferencia de los sistemas de comunicaciones.
- Interferencia de los sistemas de radar.
- Interferencia de los sistemas de armas que emplean emisiones electromagnéticas.
- Engaño de los sistemas de comunicación que emiten ondas electromagnéticas.
- Engaño a los sistemas de Inteligencia, vigilancia y Reconocimiento del enemigo.
- Empleo de armas dirigidas para inhabilitar los sistemas del enemigo.

### **1.7.2. Actividades defensivas del Ataque Electrónico:**

- Empleo de señuelos.
- Uso de sistemas de contramedida de energía dirigida infrarroja.
- Empleo de sistemas contra explosivos improvisados y radio controlados.

### **1.8. Empleo del Apoyo de Guerra Electrónica en las operaciones defensivas de la GUC<sup>5</sup>.**

Las actividades, procedimientos y técnicas de GE podrán ser empleadas en los niveles Estratégico, Operacional y Táctico.

En lo que respecta al Nivel Táctico, más precisamente en el apoyo a las operaciones defensivas, serán empleados para el apoyo directo al comandante y a sus sistemas de armas, procurando la protección de los sistemas informáticos, equipos, materiales, instalaciones y cualquier actividad que se desarrolle dentro del Ambiente Electromagnético.

El empleo de la GE en las operaciones defensivas se realizará de acuerdo a lo siguiente:

- Se utilizará únicamente el tiempo que dure la guerra.
- Constituye operaciones complementarias.
- Servirá al comando del componente terrestre de la GUC.
- Establecerá, operará y mantendrá el sistema táctico de guerra electrónica.
- Ejecutará Apoyo de Guerra Electrónica, Ataque Electrónico y Protección Electrónico.
- Todas las tropas deberán realizar operaciones de PE.

### **1.9. Conclusiones parciales del Capítulo I**

Las operaciones militares han ido evolucionando, desde que se combatía en la trinchera, mediante un combate casi estático y poco profundo, siguiendo por la implementación de armas automáticas. Luego se priorizó la maniobra y los sistemas de

---

<sup>5</sup> Gran Unidad de Combate.

armas combinadas, hasta el día de hoy que se puede ver que los combates pueden ser entre dos fuerzas regulares o entre dos irregulares, en los cuales, se ha ido implementando el EEM por medio de los sistemas informáticos, sensores, medios de adquisición de blancos, GPS, etc.

La evolución de las tecnologías, han tenido un impacto significativo en los combates, ya que, ha modificado la forma de combatir a lo largo de los años, abriendo nuevos horizontes en cada una de sus áreas siendo el EEM un nuevo ambiente. Allí es donde se suceden gran parte de las actividades que realizan los combatientes.

Debido a esta nueva forma de combatir, el Ejército Argentino, con el fin de apoyar y proteger sus medios, equipos, personal e instalaciones, ha dado lugar al desarrollo de la Guerra Electrónica, siendo la misma, la de manejar las actividades del EEM y proteger de las acciones del enemigo. También, realizar acciones ofensivas para degradar los sistemas electrónicos, equipos, información y materiales del enemigo, tomando una ventaja sobre éste. También se encarga de asesorar al decisor o comandante en lo que respecta al C3I2

La gran evolución de las tecnologías, que a lo largo del tiempo que fue modificando la manera de combatir y la aparición del Ambiente Electromagnético donde funcionan estas tecnologías, las cuales son controladas por los medios de GE, permite concluir que, las actividades de protección electrónica y ataque electrónico deben estar destinados a apoyar y proteger los puestos comandos y elementos logísticos, siendo los blancos principales del enemigo ya que si son destruidos afectarían el sostenimiento y el C3I2 de la propia tropa. Todo eso aplicado en la Zona de Retaguardia, durante la ejecución de una Defensa de Zona por parte de una Brigada Mecanizada.

## CAPÍTULO II

### EL USO DE CAPTORES Y EFECTORES PARA EL MANTENIMIENTO DE LA SEGURIDAD

#### 2.1. Introducción

Las actividades que se describieron en el Capítulo I, hacen referencia al asesoramiento, apoyo y protección del Ambiente Electromagnético durante las operaciones mediante la Guerra Electrónica

La Guerra Electrónica, realiza las tareas de Apoyo Electrónico, Ataque Electrónico y Protección Electrónica. Para realizar estas actividades, se necesitan variados tipos de sensores, sistemas, medios, equipos, materiales e instalaciones.

En el presente capítulo, se desarrollará el uso de esos sensores, sistemas, medios, equipos, materiales e instalaciones, desde el punto de vista de la protección electrónica (Detectores). Y del Ataque Electrónico teniendo que desempeñarse como un sistema integrado para el rápido proceso de la información y diseminación a los decisores o comandantes, de manera tal que puedan tomar una decisión antes que el enemigo, logrando una ventaja sobre el mismo.

#### 2.2. Los Captorees

“Como Captorees debemos considerar todos aquellos medios que brindan información, sean sensores u otras fuentes” (Sistema de la Información, 2017, pág. 20).

Si bien, a veces nos alcanza con una fuente de información, siempre se busca explotar todos los medios de detección para confirmar la misma, los sensores, son aquellos a los que más se recurren, debido a su alcance y a su corto tiempo en registrar y transmitir la información.

“En cuanto a los sensores, actualmente existe una enorme variedad, desde los más complejos, hasta los anteojos de luz residual del infante. Desde los que tienen un alcance de 400km, hasta los que solo llegan a los 400mts. Desde los diseñados específicamente para obtener información que ayude al comando y control, hasta los integrados en un sistema de armas para su aplicación directa contra blancos” (El Sistema de Información, 2019, pág. 21).

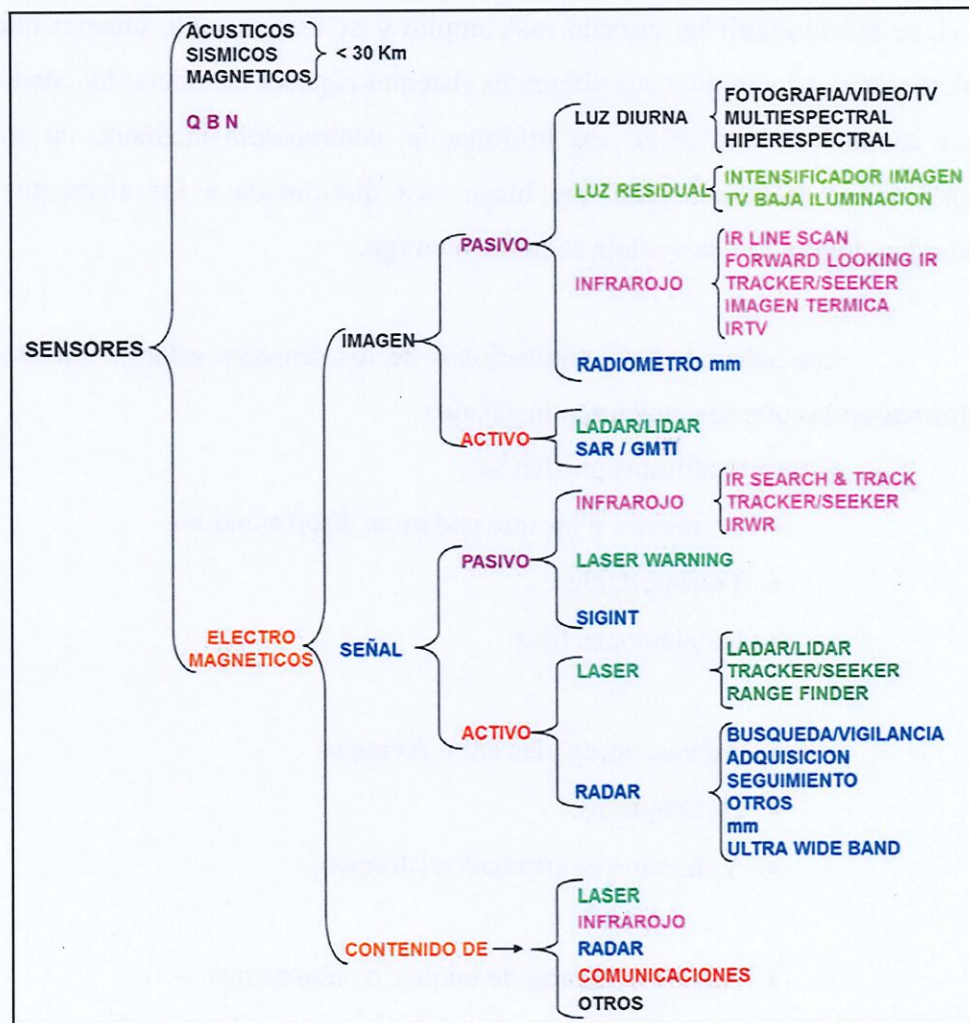
Todos estos sensores, sea cual sea la plataforma donde se encuentren, son aquellos que brindan la información para una correcta toma de decisiones, buscando de los mismos la oportunidad y la máxima integridad posible.

Los sensores son aquellos que nos darán la materia prima, la base de todo el proceso, debido a que estos datos primeramente se transformarán en información. Luego cuando llegue esa información al decisor, tendrá un conocimiento real de la situación, el terreno y el enemigo. Esta información deberá ser transmitida con el tiempo y el espacio suficiente para lograr una real ventaja por sobre el enemigo.

Todos los sensores que se utilizan en los Teatros de Operaciones para la búsqueda de una amenaza y la detección de la misma, basan su funcionamiento en el uso del Espectro Electromagnético cubriendo amplias zonas de acción.

Estos sensores, si bien cumplen con la función de detección y aviso, no buscan una amenaza en particular, sino que su funcionamiento se basa en los tipos de presión o magnitud del cuerpo o masa que corta la señal que emanan, esto hace que en algunos casos no sean tan exactos, o poco exactos prestándose a confusiones a la hora de identificar una amenaza encontrada.

Por otro lado, estos sensores, se encuentran relacionados entre sí, conectados a una plataforma repetidora de señal, en la cual, una vez que capta un elemento, transmite esa información a la plataforma mencionada anteriormente, la misma envía dicha información al operador de esos sensores, que se encuentra más a retaguardia. Posteriormente, el operador de los sensores, envía esa información a los puestos comandos, donde se procesa dicha información.



Sensores – Libro “El Sistema de la Información”

### 2.3. Características de las Plataformas Captoras.

En lo que respecta a las plataformas captoras, primeramente se deben conocer las capacidades y limitaciones de esas plataformas, ya sea, propia tropa, para saber hasta donde y en que tiempo puedo obtener la información del enemigo, como así también, la forma en que pueden ser vulnerados los propios sistemas; y del enemigo, para saber con que medios de detección cuenta, la forma de vulnerar dichos medios y poder tener una ventaja sobre el mismo.

El Objetivo de las plataformas es que con los sistemas de sensores combinados entre sí, se pueda cubrir un espacio más amplio y de esta manera, obtener información más completa sobre el enemigo y sus diferentes sistemas capaces de afectar los medios logísticos y puestos comandos. Para luego esa información centralizarla mediante un software en los sistemas, y ser procesada para que luego, sea diseminada a los elementos decisores en oportunidad, logrando una ventaja sobre el enemigo.

Las capacidades y limitaciones de los sensores estarán sujetas en parte a las plataformas en las que se encuentren instalados.

Estas plataformas pueden ser:

- Terrestres, a las que podemos discriminar en:
  - Transportables.
  - Instalaciones fijas.
- Aéreas, agrupadas en: o Aviones.
- Helicópteros.
- Vehículos no tripulados (drones).
- Navales, a bordo de buques o submarinos.
- Satelitales, que pueden ser plataformas: o Propias.
- De países amigos.
- De terceros. (Sistema de la Información , 2017, págs. 150-151)

La clasificación que se mencionó en la cita anterior, hace referencia, que, en base al medio en el que se encuentran operando, brindará una apreciación de las posibilidades de uso, dependiendo de los aspectos militares del terreno<sup>6</sup>, altitud, tiempo, espacio y características propias del enemigo.

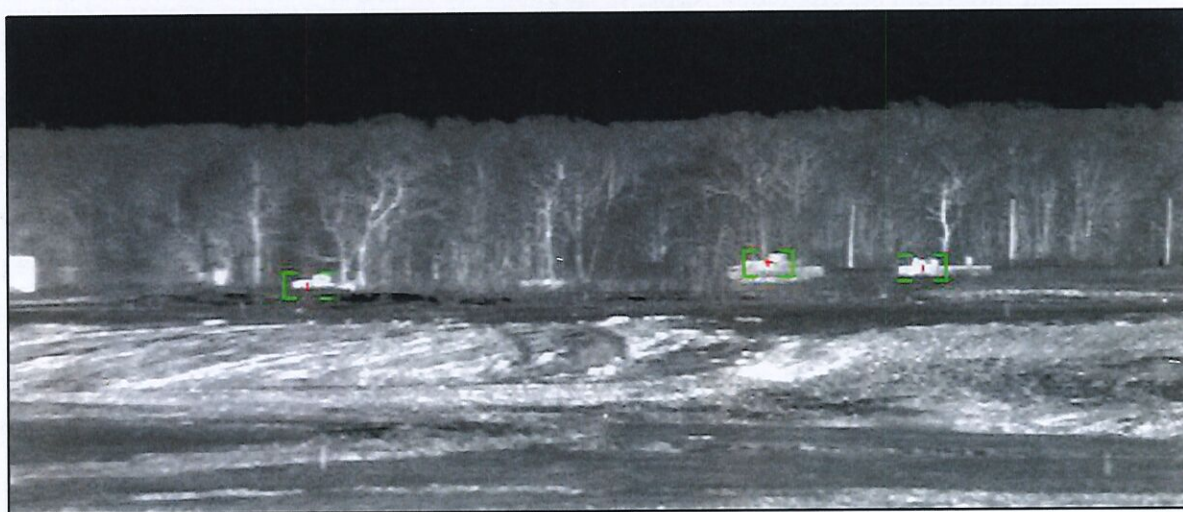
---

<sup>6</sup> *Observación y Campo de Tiro, Obstáculos, Cubiertas, Encubrimiento, Avenidas de Aproximación, Terrenos Llaves.*

## 2.4. Los Sensores en Plataformas Efectoras.

Cuando se habla de “Efectores”, se hace referencia a los sistemas de armas, Elementos o tropas en contacto directo con el enemigo, que tiene una Misión con un Objetivo que puede ser Conquistar terreno, Destruir al Enemigo, o mantener un terreno para posteriormente pasar a la ofensiva.

El uso de los sensores, además de poder ser operados desde las plataformas detectoras, en base a el grado de detalle que se necesite y el grado de oportunidad para obtener esa información, se instalarán en plataformas efectoras. Esos elementos efectores, además de poder cumplir con su tarea, capten y transmitan en tiempo real las actividades, sistemas de armas y demás información de interés que se encuentre apreciando el mismo, hacia un Centro Integrador de Inteligencia, que el mismo procesará la información y producirá inteligencia, siendo diseminada por el órgano de dirección al elemento decisor.



Ejemplo de sensor en plataforma efectora – Libro “El Sistema de la Información”

Es la imagen de un FLIR que puede estar instalado en un helicóptero o en un tanque, y que le permite a su tripulación ver y saber qué es lo que tiene a su alrededor.

El FLIR, además de permitirle al operador de la plataforma en que está instalado *saber qué es lo que está pasando* (situational awareness - tener conciencia situacional), también

facilita la detección de blancos y amenazas, los tanques dentro del bosquecillo en este caso, y permite tanto su localización como también su marcación como blancos. Es lo que están indicando los marcos verdes sobre los tanques (Sistema de la Información , 2017).

Continuando con el ejemplo de los párrafos anteriores, el helicóptero al tener los sensores incorporados que capturan las imágenes, como así también, cuentan con sistemas transmisores, donde pueden llegar a transmitir en tiempo real directamente al elemento decisor, como así también, al Centro Integrador de Inteligencia, para que procese esa información, produzca la inteligencia pertinente y luego sea diseminada por el órgano de dirección a los elementos decisores.

## **2.5. Conclusiones Parciales del Capítulo II.**

La Zona de Retaguardia de una Brigada Mecanizada que ejecuta una Defensa de Zona, cuenta en sus Puestos Comandos con elementos en apoyo, desde Comunicaciones y GE hasta Inteligencia; elementos éstos encargados de la alerta y de la seguridad. Esos elementos cuentan con sistemas de obtención de información, como así también, elementos designados como medios de obtención. Para realizar esta actividad, todos ellos utilizan el EEM. Los elementos de obtención pueden ser captores (radares, ANT, etc) o efectores (tropas, helicópteros, tanques, etc), donde operan con sensores a través de los cuales captan y obtienen información en tiempo real enviando la misma a un centro integrador de inteligencia para luego procesarla y producir inteligencia la que será diseminada por medio del órgano de dirección.

La transmisión de información y el tiempo que tarda el proceso de la misma y la diseminación de la inteligencia resultante a través del órgano de dirección, hace que el tiempo en la toma de decisiones sea más lento, por lo cual, la misma debería ser por medio de un canal directo entre captor o efector que la transmite y el decisor, para que puede tener una dinámica más fluida en su toma de decisión.

La falta de un canal directo entre el captor/efector que tiene el sensor y el elemento decisor y la capacidad de los medios disponibles para las operaciones, permite

concluir que, para la seguridad de los puestos comandos y logísticos, se deben implementar sistemas de alerta más dinámicos, como así también, un fluido ciclo de la información más directo entre el medio que obtiene la información y el decisor, ya que, el decisor al no contar directamente con la información en oportunidad, pone los elementos mencionados anteriormente en vulnerabilidad de ser afectados por medios del enemigo, debido a una toma de decisión tardía por no contar con la información suficiente en tiempo y oportunidad.

## **CAPÍTULO III**

### **DETERMINACIÓN DE LOS MODELOS DEL ENEMIGO UTILIZANDO EL EEM**

#### **3.1 Introducción**

A través del EEM, mediante la utilización de sensores, instalados en plataformas captoras y efectoras, se puede obtener información en tiempo real, con menor o mayor grado de detalle. Esa información es importante que sea transmitida en oportunidad y lo más íntegra posible, para que una vez procesada y posteriormente el resultado de ese proceso sea diseminado al elemento decisor, se puedan crear modelos del enemigo, haciendo hincapié, en su poder de combate, capacidades y debilidades, de manera tal que, una vez desarrollados esos modelos se obtengan todas las opciones o variables probables que pueda adoptar el enemigo en sus procedimientos para afectar los propios sistemas.

En el presente capítulo se desarrollarán los diferentes modelos del enemigo que se pueden crear, resultado del proceso de los datos e información obtenida a través de los sensores instalados en las diferentes plataformas captoras y efectoras. Estos modelos, se basarán en las diferentes opciones o formas en la que el enemigo puede accionar ofensivamente sobre los elementos emplazados en la zona de retaguardia, durante una defensa de zona de una Br Mec, haciendo hincapié en los medios logísticos y puestos comandos, blancos más sensibles a afectar por el enemigo, que de ser alcanzados por el mismo pueden convertirse en una vulnerabilidad para la propia fuerza.

#### **3.2 Modelos del Enemigo**

Cuando se habla de modelos del enemigo, es responder a las preguntas “¿Qué hay?” “¿En dónde?” Haciendo referencia que elemento es la amenaza y donde se encuentra en

tiempo y espacio, haciendo hincapié en sus capacidades y debilidades, en base a lo que detectan los sensores.

“Confeccionar un modelo no significa hacer una maqueta, sino realizar un modelo computacional.” (Sistema de la Información, 2017, pág. 70). Para esto hay que aprovechar los diferentes softwares computacionales, con capacidad de simulación, presentando las diferentes características, posibles dispositivos a adoptar, capacidades, debilidades y demás elementos que sean de utilidad para la seguridad de la fuerza.

En la confección de cada modelo, se deberá reflejar cada una de sus particularidades con el mayor grado de detalle posible, de forma tal que, los mismos los puedan utilizar desde la Grandes Unidades de Combate hasta el nivel Unidad Táctica.

En su configuración más simple estará conformado por figuras tridimensionales con forma de burbujas, semiesferas, ángulos esféricos, y otras formas, que representarán las envolventes letales en el caso de las armas, los cubrimientos en caso de los sensores, las envolventes de lanzamiento cuando los modelos son de los blancos a atacar, o envolventes de combate para las plataformas y sistemas de armas. (El Sistema de Información, 2019, págs. 70-71)

Luego, estos modelos serán posicionados en el terreno, a través de los SIG<sup>7</sup>, representando la Zona de Interés donde se ejecutarán las acciones. Estos modelos presentados hasta ahora tendrán una representación estática, en donde solo se colocan esos modelos en un determinado espacio. Posteriormente, se llevará a esos modelos a una situación más dinámica, representado de esa manera, los diferentes modelos en el terreno, con sus elementos en movimientos, demostrando de que manera pueden afectar los propios medios.

### 3.3 Los Diferentes Tipos de Modelos

Es todo aquello que podemos encontrar en la Zona de Interés, donde se podrán realizar las operaciones, confeccionándolos de manera computacional, de manera tal de poder representar todo lo que compone esa Zona de Interés junto con las capacidades y debilidades.

---

<sup>7</sup> Sistema de Información Geográfica.

Se agruparán los modelos en base a sus elementos, medios y origen, siendo los pertenecientes a:

- Potencial Enemigo.
- El ambiente.
- Terceros que compartirán el mismo espacio geográfico.

También se los podrá subdividir en:

- Terrestres.
- Espaciales.
- Aéreos.
- Navales.
- Comando y Control.

El Ambiente se lo puede subdividir en:

- Geográficos.
- De clima y Meteorológicos.
- Construcciones hechas por el humano. (El Sistema de Información, 2019,

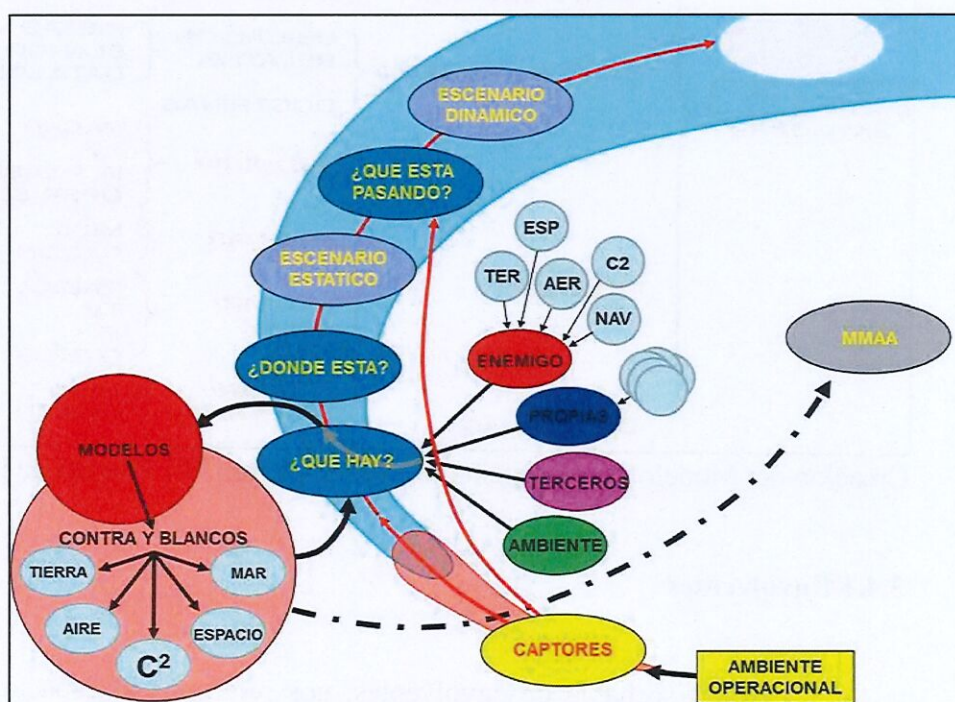
pág. 75)

Se deberá confeccionar un modelo para cada elemento del enemigo, describiendo el ambiente donde cada uno de ellos desarrollarán las operaciones, con el mayor grado de detalle posible. Con esto se buscará representar los posibles comportamientos, tácticas y procedimientos, capacidades y debilidades, ya sea, para utilizarlo en un simulador de manera tal de confrontarlo con otros elementos y medios.

Estos modelos se deben confeccionar desde la Paz, ya que, los mismos tendrán un mayor grado de detalle debido a que el tiempo no será un condicionante, accediendo a todo este tipo de información a través de fuentes abiertas siendo de vital importancia las características de los ambientes donde se desarrollarán las operaciones.

Una vez que se hayan concretado los modelos, se deberán integrar los mismos conformando un sistema, relacionándolos entre sí en función de su posible utilización como conjunto. De esta manera, se tendrá un conocimiento más profundo de como podrían operar los diferentes elementos del enemigo, combinados entre sí, y cuales serían sus probables objetivos en lo que respecta al dispositivo propio.

“En los sistemas integrados actuales, sobre todo redes de computadoras, de comunicaciones, o de sensores, hay una enorme cantidad de puntos débiles, relativamente fáciles de acceder y degradar que pueden producir daños a veces no imaginados.” (Sistema de la Información , 2017, pág. 76)

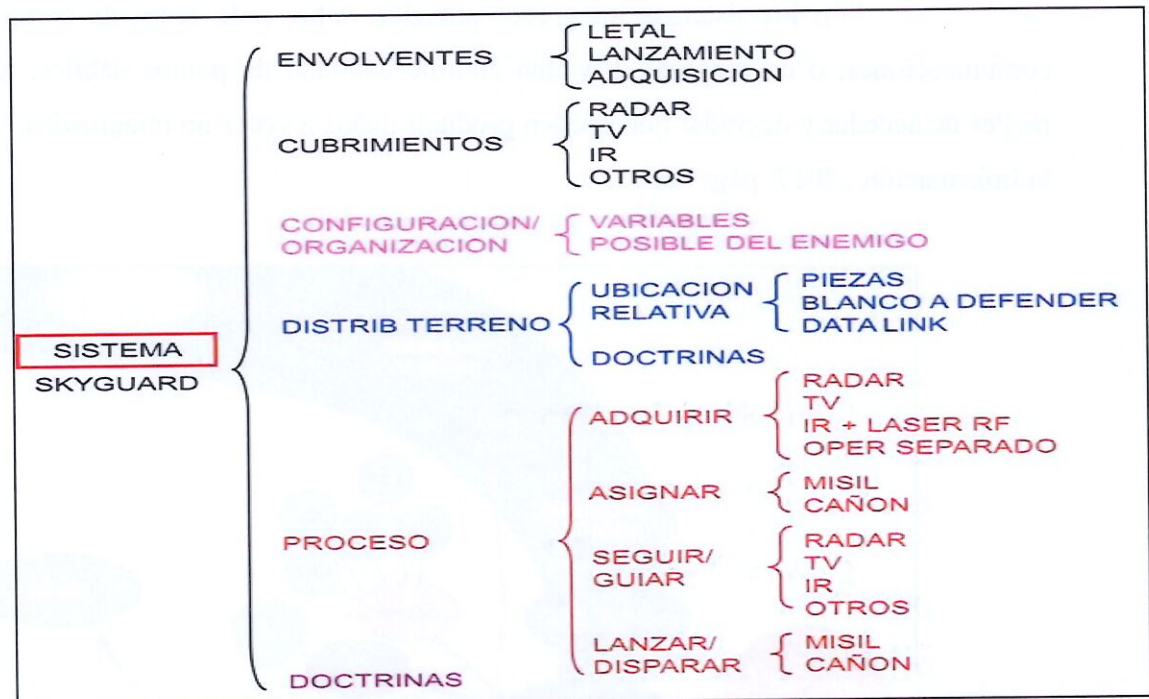


Diferentes modelos del Enemigo – Libro “El Sistema de la Información”

La integración de los modelos, permite identificar también, los puntos débiles de los sistemas de software, redes, equipos, materiales e instalaciones, siendo un conocimiento esencial para saber de que forma pueden ser afectados por ese enemigo potencial de manera tal de evitar que se interfiera, afecte y neutralice las capacidades del mismo, negando de esta manera la posibilidad que el enemigo pueda hacer uso de ellos sobre los sistemas propios.

### 3.4 Aspectos a tener en cuenta para la creación de Modelos.

A la hora de la creación de modelos del enemigo, existen una serie aspectos a tener en cuenta, que guían este proceso. Para explicar los diferentes aspectos a tener en cuenta, me basaré en el siguiente cuadro extraído del “Libro Sistema de la Información”.



Creación del Modelo de un Sistema Skyguard – Libro “El Sistema de la Información”

#### 3.4.1 Envoltentes

Cuando se habla de envoltentes, nos referimos al espacio de adquisición y ejecución que cuenta el enemigo, o sea, desde donde puede afectar los sistemas, equipos, materiales e instalaciones propias. Este aspecto es de suma importancia, ya que, brinda el punto de partida, para conocer la capacidad que tienen los sistemas captadores y efectores del enemigo.

#### 3.4.2 Cubrimientos

Este aspecto se relaciona con el anterior, ya que, se refiere al medio con el cual pueden detectar los elementos efectores propios, como así también, accionar ofensivamente

sobre los propios sistemas, equipos, materiales e instalaciones. Conocer este aspecto, proporciona la ventaja de, saber con que medios, y sistemas cuenta el enemigo, las capacidades y sus debilidades, y de esta manera poder tomar un modo de acción al respecto.

### **3.4.3 Organización**

La Organización, hace referencia a como con sus medios o sistemas, puede afectar o degradar los propios, las variables que puede llegar a adoptar y como utiliza los mismos en base a una determinada acción. Conocer este aspecto, es importante, ya que, proporciona una adecuada base para establecer un modo de acción, en base a lo que se aprecia que va a realizar el enemigo sobre la propia tropa.

### **3.4.4 Distribución en el Terreno**

La Distribución en el Terreno, hace referencia a la configuración que tienen los sistemas, medios, equipos e instalaciones del enemigo en el terreno. En este aspecto se deberá tener en cuenta, la capacidad y flexibilidad que tiene el enemigo, para ubicar sus medios y elementos en el terreno en relación a los medios propios que se quieran afectar, y la manera en que lo realizaría. Estas acciones, se van a realizar, siempre partiendo de la base de como esté conformado según su doctrina y las características propias de los materiales y sistemas. Es fundamental, hacer un exhaustivo análisis de este aspecto, ya que, va a proporcionar donde puede llegar a emplazar los medios, elementos y sistemas el enemigo y los modos de accionar a tomar por el mismo para afectar o degradar los propios sistemas, equipos, materiales e instalaciones.

### **3.4.5 Proceso**

El proceso, es una combinación de los aspectos mencionados anteriormente, ya que, muestra la forma en como funciona el modelo del enemigo, en base a la integración de los mismos, permitiendo de esta manera, tener un concepto más detallado de su forma de proceder, en base a una situación en particular.

### **3.4.6 Doctrinas**

Este aspecto es fundamental, ya que, es como el sistema del enemigo funcionará, debido a que, además de las características propias de cada elemento y medio, su accionar se basará en las doctrinas del mismo. Se deberá conocer perfectamente este aspecto, ya que, mediante el mismo, se pueden detectar las capacidades y debilidades, que afectándolas con los modos de acción propios, se convierten en vulnerabilidades. De esta manera, se puede lograr una ventaja respecto del enemigo, al conocer el funcionamiento de sus sistemas con sus capacidades y debilidades, pudiendo contrarrestar esas amenazas, neutralizando o destruyendo su modo de acción.

### **3.5 Conclusiones Parciales del Capítulo III**

La modelos del enemigo son un aspecto fundamental en lo que respecta a la adopción de medidas de seguridad para las operaciones militares. En lo que respecta a los Elementos ubicados en la Zona de Retaguardia, durante la ejecución de una Defensa de Zona por parte de una Br Mec, su seguridad, deberá adoptar dicho sistema de creación de modelos, ya que, permite conocer con anticipación la forma en que opera el enemigo y los diferentes modos de acción que puede ejecutar sobre los elementos logísticos y puestos comandos. De esta manera se logrará una ventaja táctica sobre el enemigo. Se debe tener en cuenta que durante la paz es donde más información se obtendrá y se podrá realizar un mayor grado de detalle

La creación de los modelos del enemigo junto con el uso de los sistemas computacionales (EEM), permite concluir que, durante la adopción de medidas de seguridad para las operaciones militares, se deberán utilizar los sistemas informáticos para ubicar los modelos del enemigo creados dentro del mismo y de esta manera poder pasar de un análisis estático a uno dinámico, pudiendo de esta manera, ver los diferentes modos de acción a adoptar por el enemigo sobre nuestros sistemas, equipos, materiales e instalaciones y de esa manera, adoptar medidas de seguridad activas, buscando neutralizar o destruir ese modo de acción de manera oportuna, logrando una ventaja por sobre el enemigo, negándole su libertad de maniobra.

## CONCLUSIONES GENERALES

La gran evolución de las tecnologías, que a lo largo del tiempo fue modificando la manera de combatir y la aparición del Ambiente Electromagnético donde funcionan estas tecnologías, siendo controladas por los medios de GE, permite que, las actividades de protección electrónica y ataque electrónico deben estar destinados a apoyar y proteger los puestos comandos y elementos logísticos, siendo los blancos principales del enemigo, ya que, de destruirlos, afectarían el sostenimiento y el C3I2 de propia tropa, todo esto, encuadrado en la Zona de Seguridad de una Brigada Mecanizada, durante el desarrollo de operaciones defensivas.

La Zona de Retaguardia, durante la ejecución de una Defensa de Zona a nivel Br Mec, cuenta en sus puestos comandos, elementos en apoyo, desde Comunicaciones, GE hasta Inteligencia, encargados de la alerta y seguridad del Elemento. Esos elementos cuentan con sistemas de obtención de información, como así también, elementos designados como medios de obtención, en la cual todos ellos utilizan el EEM. Los elementos de obtención pueden ser captores (radares, ANT, etc) o efectores (tropas, helicópteros, tanques, etc), donde operan con sensores, a través de los cuales, captan y obtienen información, en tiempo real, enviando la misma a un centro integrador de inteligencia, para procesarla, producir inteligencia y ser diseminada esa inteligencia por medio del órgano de dirección.

La creación de los modelos, es un proceso fundamental para el análisis del enemigo potencial que pueda afectar los medios logísticos y puestos comandos propios, debido a que, mediante el mismo, se pueden establecer sus capacidades, limitaciones y debilidades, como así también, los posibles modos de acción que podrían ejecutar para afectar a los propios medios.

Las operaciones de Guerra Electrónica juntos con la creación de los modelos del enemigo por medio de la operación de sensores a través de plataformas captoras y efectoras, permite concluir que, el uso del EEM en la Zona de Retaguardia, durante la ejecución de una

Defensa de Zona por parte de una Br Mec, es fundamental para la seguridad de los medios logísticos y puestos comandos, ya que, mediante los sistemas informáticos le dan la dinámica necesaria para poder identificar las capacidades y debilidades de los medios del enemigo, pudiendo explotar esas debilidades a través de la guerra electrónica, que por medio del uso del EEM de manera activa, a través del ataque electrónico, puede degradar o neutralizar las acciones del enemigo, como así también proteger los elementos propios por medio de la protección electrónica.

## Bibliografía

- Barbosa Larronde, J. M. (2012). *Dificultades para la obtención de la sorpresa en el nivel operacional ante el avance de las nuevas tecnologías de la información*. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas. Obtenido de <http://cefadigital.edu.ar/handle/1847939/283>
- EMCOFFAA. (2012). *PC13-50 "GUERRA ELECTRÓNICA PARA LA ACCIÓN MILITAR CONJUNTA"*. Buenos Aires: Público Militar.
- Moyano, E. R. (2016). *Seguridad en las operaciones logísticas de nivel operacional en el Teatro de Operaciones Irak 2003. (Trabajo Final Integrador)*. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas. Obtenido de <http://cefadigital.edu.ar/handle/1847939/884>
- Velasco, S. A. (2014). *El elemento de comunicaciones para la protección de la información de las operaciones militares en el Teatro de Operaciones*. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas. Obtenido de <http://cefadigital.edu.ar/handle/1847939/140>
- EMGE. (2017). ROD – 05 – 01 “CONCEPTOS BÁSICOS SOBRE SISTEMAS DE COMUNICACIONES, INFORMÁTICA Y GUERRA ELECTRÓNICA DE LA FUERZA”. Buenos Aires: Público Militar.
- Miguel Angel Silva. (2019). “EL SISTEMA DE LA INFORMACIÓN.” Buenos Aires.

**Anexo I: Encuesta realizada al Comodoro (R) Miguel Angel SILVA**

1. ¿Cuáles son las actividades que debe desarrollar una Br I Mec durante la ejecución de una defensa de zona, cuando incorpora el uso del Espectro Electromagnético dentro de las medidas de seguridad sobre su zona de retaguardia?

1. La Br I Mec deberá explotar al máximo las posibilidades que el brinda el EEM para protegerse en forma "activa", realizando operaciones de defensa OFENSIVAS, aunque se horroricen algunos doctrinarios, negándole al enemigo cualquier intento de degradación de nuestros medios en la retaguardia.

2. Los medios de detección deben estar integrados a nivel ESTRATÉGICO, para asegurar que cualquiera sea el captor, su información llegará a todos los niveles decisores de la Br I Mec, y lo hará a tiempo.

3. El uso del EEM desde ya incluye todas las actividades de índole informática, y por supuesto su degradación y protección (ver el libro El Sistema de Información).

4. Actualmente se sigue pensando que la retaguardia es un lugar seguro, porque está lejos del frente de combate. Se sigue pensando en el alcance del fusil y el mortero; y cuando se piensa en tecnología informática, sólo se piensa en el Hacker. La forma de guerrear actual va más allá de los reglamentos y doctrinas.

5. En la guerra actual no hay diferencia entre la zona de retaguardia y la zona defensiva de primera línea. Todos los blancos son alcanzables, sea por armas hard (duras) o soft (blandas).

2. ¿Existe algún tipo de Medida de Seguridad implementada para buscar amenazas de variadas índoles informáticas, que puedan causar algún tipo de degradación en los sistemas propios?

El concepto actual al guerrear es el de paralizar al enemigo, el de atacar a las "fuerzas que siguen" (o vienen, desde la profundidad) lo más lejos posible, ergo, en la retaguardia.

Para ello el enemigo buscará tener medios y armas, montados en plataformas portadoras que puedan llegar a la profundidad de nuestro territorio.

Por lo tanto, al plantear el problema a resolver en la operación "defensiva" de la retaguardia, o más correctamente "en la profundidad" del propio dispositivo, debemos:

1. Determinar todo aquello nuestro que pueda ser considerado por nuestro enemigo como posible blanco a degradar o atacar; y cómo influye su degradación en el todo de nuestra operación.

2. Buscar respuesta a: ¿Con qué me va a detectar?... ¿Con qué me va a localizar?... ¿Con qué me va a (pegar) degradar o tratar de destruir?... en la profundidad (retaguardia) de mi territorio.

Las respuestas a estas preguntas conformarán las amenazas a que estaremos expuestos; y para cada una deberemos buscar la forma de protegernos y anular sus efectos, sea que nos detecten, localicen, y degraden o intenten destruirnos.

De aquí van a surgir los modelos de lo que tiene el enemigo como captorees (sensores) y efectores (armas) para hacernos daño.

A todos ellos debemos confrontarlos con nuestros propios medios captorees y efectores, para asegurarnos que tenemos cubiertas todas las posibilidades de protección que evitarán que nuestro enemigo nos produzca algún daño, o que éste será mínimo.

3. ¿Las Medidas de Seguridad que actualmente se desarrollan en la zona de retaguardia de una Br I Mec que ejecuta una Defensa de Zona, usando el EEM, son suficientes en lo referido al desarrollo actual de la tecnología informática y al consecuente cambio de paradigma sobre la forma de combatir?

**Interviene el EEM, porque nuestro enemigo:**

1. Para detectarnos y localizarnos en la profundidad (retaguardia) necesita sensores de todo tipo e información de posicionamiento geográfico (GPS u otro).

2. Para (pegarnos) degradarnos o tratar de destruirnos, también recurrirá a sensores, sistemas de apuntado y guiado, y sistemas de navegación de sus plataformas, que harán un uso intensivo del EEM para poder funcionar.

**3. Deberá coordinar sus acciones, haciendo un uso intensivo de computadoras y comunicaciones, que también son EEM.**

**Nosotros podemos intervenir en estos 3 aspectos para protegernos, no sólo en forma pasiva, sino con una protección "activa", degradando sus medios mediante el EEM, para que no pueda usarlos.**

**Al iniciar el proceso, analizaremos a todos nuestros medios como posibles blancos a atacar por el enemigo, determinando su efecto rebote en todos nuestros sistemas, para establecer sus prioridades en cuanto a su defensa y protección, y si es necesario, su redundancia para asegurar la resiliencia.**

**De aquí surgirá que nuestros medios de C2 son esenciales y prioritarios como blancos a defender, así como otros blancos de todo tipo, entre los que habrá muchos logísticos, que se constituirán en puntos esenciales a atacar por nuestro enemigo.**

- 4. ¿ Se puede diferenciar el uso del EEM de manera activa en la Zona de Retaguardia, más precisamente, para la protección de los elementos logísticos y puestos comandos, con respecto a la Zona Defensiva de 1ra Línea?**

**Los medios de retaguardia deben tener medios defensivos, ya que algunos son tanto o más importantes que los de primera línea.**

**En las guerras actuales el concepto de retaguardia se diluye al iniciarse las acciones, porque todos nuestros medios, no importa donde estén, van a ser blanco del enemigo, el que buscará atacar los "puntos esenciales" y los "centros de gravedad" para paralizarnos, como los puestos comando y los medios logísticos, no importa cuán profundo se encuentren.**