Teorías y conceptos para entender la guerra electrónica



Teniente Primero
GABRIEL DONAYRE MONTESINOS

(Del concepto de Guerra Electrónica al de Guerra de Señales o de la Información)



1. Introducción

La guerra sufre constantemente cambios tecnológicos. Para algunos profesionales de la guerra, este cambio es sustancialmente radical y revolucionario; para otros, no son cambios tan revolucionarios sino más bien el producto de una evolución que no acaba, sino que desarrolla y refina diferentes elementos de una larga trayectoria en el arte de la guerra.

Para analizar los cambios en las formas de hacer la hoy llamada "Guerra Electrónica", se manejan diferentes teorías y numerosos conceptos doctrinarios que se entrecruzan y que pueden ser utilizados con diferentes sentidos, en diferentes momentos, por diferentes autores y actores. Los conceptos se solapan, se incluyen y modifican, de tal manera que para quien intenta introducirse en la comprensión del estado en cuestión, la imagen se vuelve bastante confusa.

Seguramente el presente ensayo no encontrará todos los conceptos finales y definitivos, pues ante la verdad absoluta todas son verdades relativas. Sin embargo, es de esperar que esta selección contribuya a situar mejor algunos de los puntos, lo cual permita dar una visión más comprensible del tema en debate y su amplitud.

Pese a las diferencias entre los conceptos, se observa una serie de direcciones a las que todas apuntan, pues la filosofía es la misma, son únicamente los medios y sus nombres los que cambian.

Pero sería bueno empezar por definir qué se entiende por Guerra Electrónica, pues en general se le está dando un sentido muy limitado a este concepto.

2. Análisis

2.1 Guerra Electrónica

Se entiende, según las diversas fuentes consultadas tanto en exposiciones como en Internet, que la Guerra Electrónica (*EW: Electronic Warfare*) tiene como finalidad "emplear el **Espectro Electromagnético** en nuestro provecho y negar su empleo al enemigo"[1]. Otros añaden que es toda acción militar que involucra el uso del espacio electromagnético para determinar, aprovechar y reducir o prevenir el uso hostil del mismo por parte del enemigo.

Si bien es cierto que muchas de las señales viajan a través del espacio electromagnético, la representación correcta debería incluir a todo medio por donde las señales viajan y se propagan, como por ejemplo el magnético, físico o eléctrico. Una señal es toda aquella emisión que nos da indicio de algo, que puede ser percibido de manera natural o artificial, y que nos da de manera directa o indirecta *información* de algo.

La información, está contenida en una señal, cualquiera sea su tipo. Por ejemplo: un sonido, calor, anomalías magnéticas, luz y ondas de radio, entre otros, pueden dar información de algo: ¿Qué es?, ¿dónde está?, ¿qué dice o significa?, etc.

La Real Academia Española define "electrónica" como: "El adjetivo que puede aplicarse a todo lo que funciona o se produce a través de dispositivos o procedimientos electrónicos".

En realidad, el nombre de "Guerra Electrónica" nació como tal a raíz de los avances de la electrónica con la invención del radar en la Segunda Guerra Mundial. Pero su filosofía no es nueva, siempre existió, fue desde siempre una "Guerra de Señales". Darle un nombre encasilla sus múltiples campos de acción a uno solo.

Se presenta un ejemplo:

Las palomas mensajeras son uno de los medios de comunicación más antiguos, pues las primeras noticias que se tiene de su uso datan de hace más de 3.500 años. En Persia, en el siglo XV a. C., alguien observó la capacidad que tenían algunas palomas de encontrar el camino de vuelta a casa, y decidió explotarlo en su provecho. Ató a la primera paloma mensajera de la historia el mensaje que deseaba transmitir, la paloma despegó y poco tiempo después alcanzó su destino con el mensaje. Al ver este medio, los enemigos de los persas trataron de obtener los mensajes que iban en las palomas, iniciando así un tipo de "Inteligencia de Señales".

En la Segunda Guerra Mundial, a pesar de que existían ya radares algo desarrollados, el telégrafo y el teléfono funcionando en apogeo, las palomas fueron ampliamente utilizadas. La Resistencia contra los nazis, sobre todo en Francia y en Holanda, usó palomas mensajeras para sus comunicaciones. De igual forma, estas palomas fueron atacadas por los alemanes con halcones, realizando así lo que sería un "Ataque de Señales". Posteriormente, interceptaban las palomas para saber el contenido de las informaciones y luego las soltaban



La información esta contenida en una señal.

con mensajes ingleses falsos, en los que se pedía a la Resistencia los nombres de sus líderes para "coordinar" su rendición, produciéndose una nueva modalidad de "Inteligencia de Señales" y "Ataque de Señales". Al ser detectados estos ataques a sus palomas, se inicia el cifrado de los mensajes, con lo que se da la "Protección de Señales".

En esa línea de pensamiento, se puede redefinir la llamada "Guerra Electrónica", ascendiéndola nuevamente a "Guerra de Señales o de la Información", cuya sustancia y esencia no cambia y se refleja a mi criterio, en este concepto:

Comprende todas las acciones que tienen por objetivo ganar el manejo de las emisiones del espacio para nosotros y contrarrestar su empleo al enemigo.

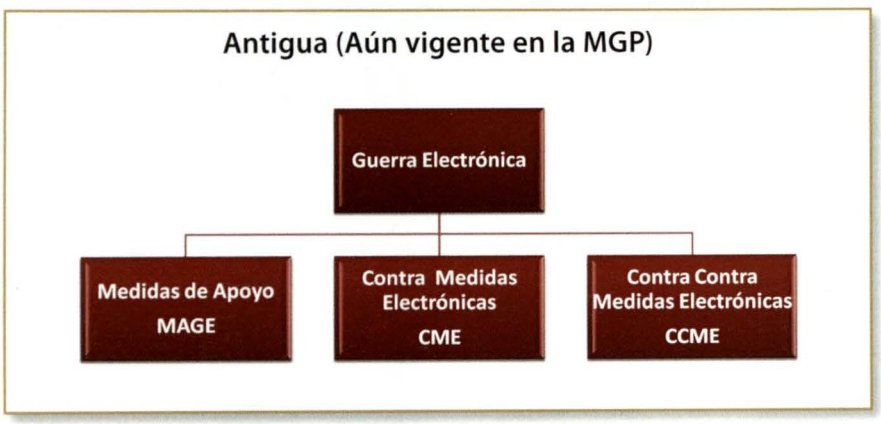
Al hablar de espacio, se refiere a todo medio de propagación donde sea posible que una señal viaje. A su vez, en el actual concepto de la llamada "Guerra Electrónica" se tienen tres componentes principales:

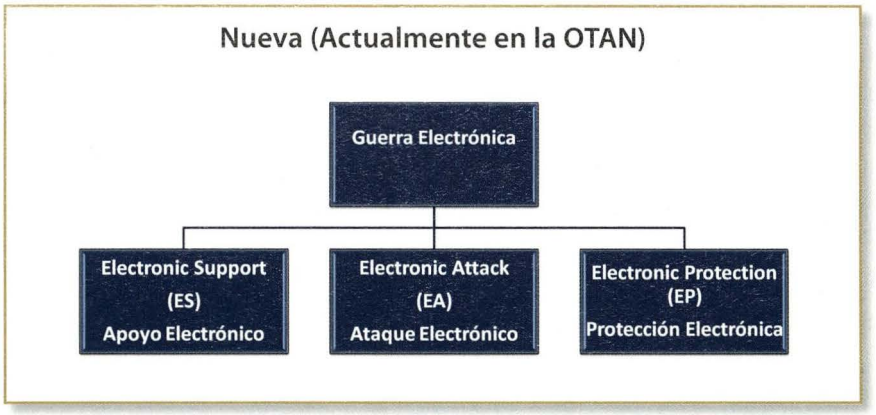
a) El Apoyo Electrónico (*ES, Electronic Support*): Equivalente a la "Inteligencia de Señales o Información".

b) El Ataque Electrónico (*EA, Electronic Attack*): Equivalente al "Ataque de Señales o Información".

c) La Protección Electrónica (*EP, Electronic Protect*): Equivalente a la "Protección de Señales o Información".

La antigua y actual denominación de los componentes se presenta en los siguientes cuadros:





2.2 Apoyo Electrónico (ES)

Fue conocido anteriormente en la terminología militar como: "Medidas de Apoyo a la Guerra Electrónica" (MAGE), y comprende según la misma definición: *"Las acciones adoptadas para buscar, interceptar, identificar o ubicar fuentes de energía electromagnética irradiadas con el fin de obtener un reconocimiento inmediato de la amenaza".*

El apoyo electrónico funciona como la parte pasiva y netamente receptiva de la Guerra Electrónica. En términos generales, lo que se busca obtener de una señal es su origen, su identificación y la información que contiene.

Entonces, el término más apropiado sería "Inteligencia de Señales" (*SIGINT, Signals Intelligence*) o "Inteligencia de la Información", pues la capacidad de supervivencia de las fuerzas propias en un ambiente hostil, y la precisión y efectividad de sus armas, dependerán de la capacidad para controlar todo tipo de emisión de interés, no únicamente las que viajan en el espacio electromagnético sino las que viajan en otros medios, como las ondas acústicas, las señales eléctricas en los cableados conductores, etc.

Para dicho propósito existen dos conceptos generales dentro de la Inteligencia de Señales:

a) Inteligencia Electrónica (*ELINT, Electronic Intelligence*): Determina el origen y la identificación de toda señal de interés.

b) Inteligencia de Comunicaciones (*COMINT, Communications Intelligence*): Determina el mensaje e información que lleva o contiene la señal.

Por concepto se ve el sesgo del alcance, dado que a pesar de que se desarrollan actividades sobre señales eléctricas y acústicas, el enunciado no lo engloba, debido a que el primer enunciado ELINT se limita sólo al empleo de equipos electrónicos y del espacio electromagnético; por otro lado, el COMINT limita el concepto a los flujos bidireccionales de la información, pero este también evalúa sistemas de información que son de una sola dirección, y ambos (tanto el ELINT y el COMINT) en interacción confirman la identificación de la fuente de la señal.

Se puede entonces presentar una nueva propuesta de las partes de la Inteligencia de Señales o de la Información:

- Identificación de Señales: Identifica qué tipo de señal y a quién pertenece (¿Qué es?).
- Ubicación de Señales: Identifica de dónde proviene la señal (¿De dónde viene?).
- Contenido de Señales: Identifica el contenido o significado de la señal (¿Qué dice?).

Se presenta un ejemplo:

Los sonaristas a bordo de los submarinos son marinos entrenados en cuanto a la física de sonidos. Sus oídos reciben señales acústicas, su cerebro las procesa y las transforma en información de interés. Así es como el sonarista entrega finalmente su parte:

"Marcación al contacto 145 relativo, hélices pesadas, buque mercante, por número de batidos 15 nudos, en acercamiento".

Sin haber usado el espectro electromagnético, el sonarista descubrió el qué es, de dónde viene y la información qué dice o contiene. En efecto, la señal del sonido se propaga por un medio físico y lo que anteriormente se hizo fue una auténtica Inteligencia de Señales.

Frente a este nuevo análisis, podríamos decir lo siguiente respecto al apoyo electrónico o Inteligencia de Señales (SIGINT): Es un proceso continuo, donde se analiza todo tipo de señal de interés, con el fin de obtener su origen, identificación y el mensaje o información que contiene.

2.3 Ataque Electrónico (EA)

Conocido anteriormente como "Contramedidas Electrónicas" (CME), es hoy denominado "Ataque Electrónico" y es definido como: *Las acciones adoptadas*

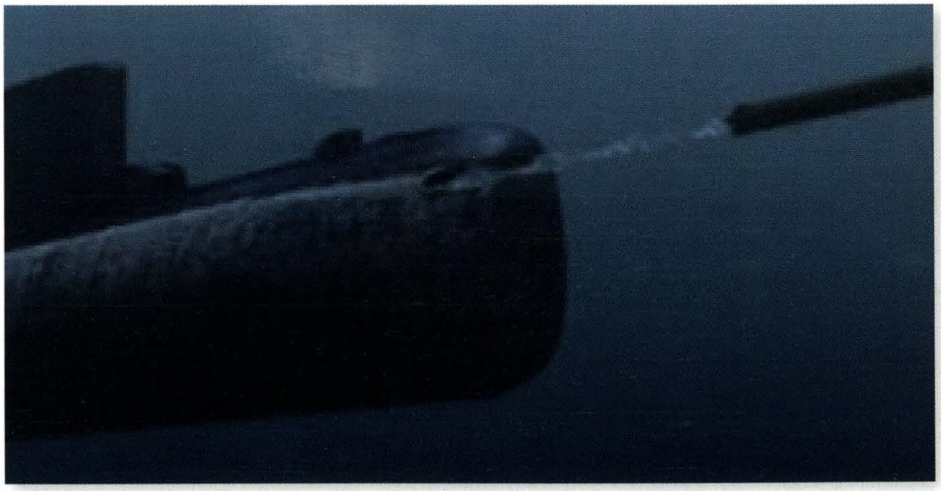
para impedir o reducir la utilización enemiga del espectro electromagnético, comprendiendo la perturbación electrónica y la decepción electrónica.

Esta acción se puede realizar tanto por medio de técnicas de engaño (llamadas *Soft Kill*) como por ataques directos o físicos (llamados *Hard Kill*). En tal sentido, la forma de hacerlo no debería ser limitada ni mucho menos reducida al espacio electromagnético; esa limitación encasilla el concepto y no permite visualizar los otros espacios donde se desarrolla.

Se presenta un ejemplo:

Los submarinos deben evitar a toda costa ser impactados por los torpedos. La unidad de guiado de un torpedo se basa en la búsqueda del sonido para alcanzar su objetivo, pues una plataforma submarina genera ruido de una u otra manera. A fin de poder garantizar la integridad de los submarinos frente a esta amenaza, se crearon los conocidos "disturbadores de torpedos". Esta clase de señuelos se caracterizan por generar un ruido adicional que fuerza el engaño por parte del torpedo hostil y lo aleja del buque. La finalidad: no permitir que el torpedo haga uso del sonido para sus fines, conduce un ataque de señales en el espacio físico (acústico) del mar.

De acuerdo con ello, y con el fin de no limitar las múltiples formas de hacer el ataque electrónico o de señales, se puede decir que se *busca impedir o reducir la utilización de las señales en todos sus medios de propagación por parte del enemigo.*



Ataque electrónico.

2.4 Protección Electrónica (EP)

Fue conocida como las "Contra Contra Medidas Electrónicas" (CCME), hoy denominada "Protección Electrónica", y consiste en el uso de estrategias para evitar el ataque electrónico del enemigo y favorecer el apoyo electrónico propio.

Dentro de este contexto, se evita que un sistema externo pueda dañar, bloquear o interceptar la comunicación propia, y en el caso de ser interceptada sea ininteligible (no entendible). El cifrado y la modulación entran en este contexto.

Se presenta un ejemplo:

Los torpedos son buscadores del sonido. Como consecuencia de ello, se inventaron los "disturbadores de torpedos", reduciendo así el uso del espacio físico (acústico) por parte del torpedo.

> "la protección electrónica o de señales comprende todo el espacio utilizable, bajo el concepto de que son todas las acciones adoptadas para favorecer y asegurar el uso propio de las señales en todos sus medios de propagación".

Frente a esta situación, y como una forma de protección electrónica o de señales, se dotó al torpedo de capacidades adicionales, como la de generar un cambio en el tipo de búsqueda de pasiva a activa, o el empleo de espoletas magnéticas (otro espacio de propagación de las señales). En tal sentido, el torpedo optará por usar el medio de propagación más adecuado con la consigna de proteger las señales que le darán la información necesaria para alcanzar su objetivo.

Conforme a ello, la protección electrónica o de señales comprende todo el espacio utilizable, bajo el concepto de que *son todas las acciones adoptadas para favorecer y asegurar el uso propio de las señales en todos sus medios de propagación.*

---

3. División de la Guerra Electrónica

Según las diversas fuentes consultadas, la división de la Guerra Electrónica sería:



Pero según el análisis efectuado, la llamada Guerra Electrónica, ahora bajo la perspectiva de la Guerra de Señales o de la Información, debe presentarse bajo la siguiente división:



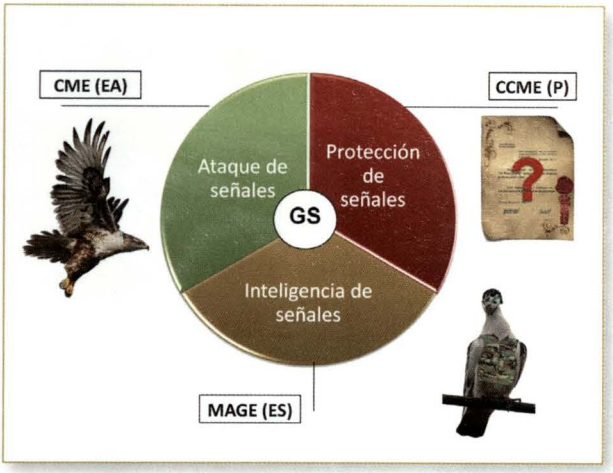
* No se da en realidades como la de Perú, pero sí la aplican países como los Estados Unidos de Norteamérica (EE. UU.).

4. Conclusiones:

Más allá de todas las características antes citadas, lo que se busca finalmente con la llamada Guerra Electrónica es controlar la información que contienen todas las señales de interés que viajan en los múltiples medios y negar su acceso al enemigo. De este modo, no se debe analizar en forma aislada el espacio electromagnético, sino que tiene que valorarse conjuntamente con todos los demás medios de propagación de señales que se disponen.

El término "electrónica" encasilla el concepto, el cual debería de nombrarse por el de la "Guerra de Señales o de la Información".

Por avanzar la tecnología no debe cambiar la filosofía de guerra, pues lo único que cambian son sus medios, debiéndose tener conceptos y denominaciones que perduren al cambio tecnológico.



Una propuesta es emplear el concepto de Guerra de Señales o de la Información, presentándose un gráfico de sus componentes, el cual está desarrollado y ha sido explicado durante todo el desarrollo del presente ensayo:

Bibliografía

1 Según la definición del Dr. Curtis Schleher en sus libros Introduction to Electronic Warfare y Electronic Warfare in the Information Age.

Referencias

- C de F. ESP Arriarán Schäffer, Arturo. Curso "Inteligencia de Señales", BAEM 2011.
- Profesor Schleher, Curtis. "Introduction to Electronic Warfare" (1986) & "Electronic Warfare in the Information Age" (1999).
- Nachrichtengewinnung &Aufklärung. Magazin alemán, CPM Forum 2005.
- Führungsfähigkeit. Magazin alemán, CPM Forum 2010.
- Air Force Doctrine Document 2-5.1(2002). Electronic Warfare (pdf).
- Cambridge University. Electronic and Information Warfare (pdf).

Web:

- Global Security. Military. *Introduction to Electronic Warfare (descargado 05-08-11) en* http://www.globalsecurity.org/military/library/policy/army/accp/ss0134/lsn1.htm
- USRadar tutorial. Types of Electronic Warfare (descargado 03-08-11)en http://www.radartutorial.eu/16.eccm/ja05.en.html
- Wikipedia. Electronic Warfare (descargado 03-08-11) en http://en.wikipedia.org/wiki/Electronic_warfare