C E S E D E N.

ASPECTOS CONJUNTOS DE LA GUERRA ELECTRONICA

- Por D. Pedro Luis ALDEA GRACIA,
Teniente Coronel de Aviación ETS.

Marzo 1988.

BOLETIN DE INFORMACION nº 208-V.

0. INTRODUCCION

Si se sigue la historia de la conducción de la guerra y sus métodos, se ve claramente que fue siempre la técnica la que determinó las formas, procedimientos y tácticas de combate, y la que contribuyó de forma determinante a su desarrollo. El ejemplo más característico es el combate por el fuego, que debe su existencia a la invención de la pólvora. Y el combate acorazado y la elevación de la movilidad de las tropas, que encuentran su origen, en el motor de combustión.

El combate electrónico se ha convertido, al ir aumentando la utilización satisfactoria de la electrónica en amplios sectores de la tecnología militar, en una disciplina militar propia, cuya importancia se ha subestimado, en muchas partes, durante mucho tiempo.

La evolución de la EW se sitúa en una época marcada por una verdadera revolución tecnológica debido a:

- La evolución de las técnicas básicas de la electrónica.

- La explosión de la informática.

- La importancia, cada vez mayor, adquirida por la electrónica y la informática en la mayor parte de las funciones militares.

La década de los 80 ha visto la aparición de nuevas técnicas, que han cambiado la naturaleza de las emisiones radioeléctricas y ejercido notable influencia sobre la EW, estas técnicas son:

- Paso generalizado de una información analógica a una digital.

- Aparición sistemática de nuevas técnicas de emisiones (saltos de frecuencia, espectro ensanchado, compresión de impulsos, emisiones comprimidas, etc.).

- Hermetismo cada vez mayor de las emisiones (codificación, cifrado, técnicas de modulación, etc).

- Extensión, muy importante, de las emisiones hacia las zonas altas del espectro electromágnético (ondas milimétricas, ondas ópticas, etc.).

- Utilización cada vez más extendida de técnicas de optrónica y de visiónica en los sistemas de armas.

- Utilización de las ondas electromagnéticas en el dominio, todavía nuevo y particular, que constituye el espacio.

Paralelamente la década de los 80 se ha caracterizado por una verdadera "explosión de la informática" en sus diferentes componentes ("hardware y software) que han permitido una evolución prodigiosa de los sistemas de armas, donde gran parte de las funciones militares utilizan cada vez más la electrónica. La informática permite la integración de los sistemas electrónicos en otros sistemas, así como la automatización y la gestión de los sistemas electrónicos por si mismos.

Pero esta evolución tecnológica y su impacto puede ser secundaria. La verdadera revolución de la EW es verdaderamente la que resulta del uso generalizado de la electrónica y de la informática sobre el campo de batalla, y ello se nota en los armamentos, en las funciones de transmisión o tratamiento de la información, en las funciones de observación, vigilancia y apoyo, etc., en todas ellas se puede decir que la electrónica ha tomado un lugar cada vez más preponderante.

Este trabajo trata de presentar un nuevo concepto de la EW, considerándola, como una parte importante de la estrategia miligar global, mostando una serie de técnicas y tecnologías que afectan directamente a la EW.

1. PRINCIPIOS Y GENERALIDADES DE EW

Podemos afirmar que la proliferación de armas modernas controladas, dirigidas y guiadas electrónicamente, es la -- gran causa de la expansión de la EW.

El concepto básico de la EW es "la exploración de - las emisiones electromagnéticas del enemigo en toda la gama del espectro electromagnético con la finalidad de obtener información de su Orden de Batalla, intenciones y capacidad, y utilizar las contramedidas, que degraden la efectividad de sus sistemas de comunicaciones y armas, protegiendo el uso propio del mismo espectro".

Un principio militar, generalmente aceptado, es que "en cualquier guerra futura, obtendrá la victoria quien mejor - controle el espectro electromagnético".

La Guerra Electrónica es un campo en evolución dinámica que debe, según las necesidades, responder a unas amenazas que también están en constante desarrollo. No voy a narrar la historia de la EW, simplemente voy a tratar de ampliar el concepto de EW como elemento vital y básico de la estrategia militar, que, junto con otros medios militares, proporciona un método para neutralizar la fuerza del enemigo (efecto divisor de fuerza) incrementando a la vez el poder de la fuerza propia (efecto multiplicador de fuerza).

El concepto moderno, considera la EW como una parte importante de la estrategia militar global, concentrada en la neutralización del sistema de mando y control enemigo (C3), manteniendo simultáneamente la capacidad operativa del sistema C3 propio.

Los soviéticos han desarrollado una estrategia llamada "Combate Radioeléctrico" o REC, que definen como la "integración de la EW con la destrucción física de las armas para evitar el control electrónico del enemigo". El REC es una parte integral de su plan de batalla. Su estrategia en caso de conflicto con la OTAN es destruir por medio de la artillería y ataques - aéreos el mayor número de fuerzas de la OTAN como sea posible, antes de la batalla principal. Simultáneamente, deben estar espuestos al REC, cierto número de elementos seleccionados de sistemas de Mando y Control, dejándolos confundidos y totalmente - neutralizados. Si el plan tuviese éxito, el resto se debilitaría y serían rápidamente sometidos.

La apreciación de los soviéticos del concepto REC proviene, aparentemente, de su énfasis en el control "top-down" y la confianza en las misiones planeadas de antemano por su estrategia militar.

Esto ha generado en los soviéticos una gran fé en su estructura de mando y control,que se manifiesta en el uso excesivo y redundante de las comunicaciones y puestos de mando.

La estrategia de los EE.UU. equivalente al REC, llamada Contramedidas C3 (CC3), se ha articulado recientemente. La EW es un componente de esta estrategia cuya función es controlar el espectro electromagnético, al igual que las armas, aviones de combate, inteligencia, comunicaciones y otras disciplinas militares, tienen funciones específicas dentro de esta estrategia.

La forma de estudiar los sistemas de EW actuales depende de las necesidades de la misión. Una divisón conveniente se basa en la amenaza contra plataformas terrestres, navales o aéreas. La filosofía de EW empleada actualmente en la OTAN es - del tipo "Stand Alone". Su principal misión es la autoprotección electrónica de las plataformas y su consideración fundamental la supervivencia.

1.1. TAXONOMIA DE LA EW

Vemos que resulta difícil clasificar las subdivisiones de un campo en respuesta a las amenazas en constante evolución, como es la EW. Por ello es necesario disponer de un área de trabajo común, para todos los que están interesados en esta materia.

La EW se define como "Una acción militar que implica el uso de la energía electromagnética para determinar, explotar, reducir o prevenir la utilización hostil del espectro electromagnético y al mismo tiempo permitir la utilización del mismo por las fuerzas propias".

Se divide en tres campos ESM o medidas de apoyo de Guerra Electrónica, ECM o Contramedidas Electrónicas y ECCM o Anti/Contramedidas Electrónicas.

Las ESM pretenden interceptar , identificar, analizar y localizar las fuentes de radiación hostiles. Se utilizan con fines tácticos. Se dificultan las acciones ESM con planes -

de Control de Emisiones (EMCON), mediante los cuales se restringen las emisiones propias sometidas a vigilancia.

Las ECM o Contramedidas Electrónicas tienen como objetivo ocultar al enemigo la información que busca, o enmascarar su respuesta con datos y objetivos falsos, o bien saturando con datos falsos la capacidad del sistema víctima. Las ECM contra objetivos radar prevalecen en acciones navales o aéreas, sin embargo en combates terrestres, la principal actividad será interceptar, localizar y en su caso perturbar las comunicaciones radio - del enemigo.

Las Anti/Contramedidas electrónicas pretenden eludir las acciones ECM y ESM. Así un sistema ESM puede eludirse evitando la zona donde se encuentra o bien impidiendo el uso de las - emisiones propias.

1.1.1. SEAD- SUPRESION DE DEFENSAS AEREAS ENEMIGAS

La Supresión de Defensas aéreas enemigas tiene por objetivo principal la destrucción física de las mismas. Un principio secundario de esta técnica, es negar al enemigo el uso de sus sistemas electrónicos mediante la presencia en la zona de un destructor mortal de fuentes de radiación (Wild Weasel). Estos utilizan como arma más importante el misil antiradiación (ARM). Típico de la actual tecnología es el HARM o misil antirradiación de alta velocidad.

Otro medio de supresión de defensas es el PLSS o Sistemas de Localización y Ataque de Precisión, capaz de realizar la localización y ataque de precisión, cuasi en tiempo real, de sistemas emisores. El sistema localiza blancos y sistemas guiados de armas más allá de los 500 Kms. Una ventaja es su potencial efectividad contra cualquier emisor ocasional. El equipo va a bordo de aviones y cuando detecta emisiones enemigas, las sitúa, y retransmite la información a una estación de control por medio de un sistema de DATA LINK. Dicha estación de control, automáticamente, y por medio asímismo de DATA LINK, es capaz de conducir simultáneamente varios aviones o misiles para atacar los blancos localizados, siendo el error total, entre la localización y el ataque de unos 30 metros aproximadamente.

1.1.2. TECNICAS APLICADAS A LA EW

En primer lugar hablaremos sobre los

1.1.2.1. SIMULADORES DE EW

Los simuladores de EW se utilizan para entrenamiento, prueba y evaluación. Básicamente permiten ejecutar y evaluar un sistema de EW, en un entorno realista sin forzar el sistema de combate.

La simulación conlleva la presentación de los datos tal y como aparecerían en una situación operativa. El modelo de amenaza se genera normalmente a partir de un Orden de Batalla - Electrónico (EOB), enemigo simulado. El EOB se define como una relación de la localización, identificación, función y capacidad de los equipos electrónicos empleados por una fuerza militar.

1.1.2.2. MISIONES Y ESCENARIOS DE EW

Históricamente la EW se desarrolló como una serie de ECM contra unos sistemas electrónicos especiales. Las mayores - amenazas fueron los radares enemigos y en menor grado, las redes de comunicaciones.

Ya hemos nombrado la estrategia CC3 como la única viable para superar los modernos sistemas de armas y a la EW - desde el punto de vista de los requisitos de tal misión. Estos conceptos guiarán el diseño de los futuros sistemas de EW. Sin embargo, los equipos actuales tienen un diseño clásico, que incluyen las contramedidas sobre un radar específico, enlaces de comunicaciones o en algunos casos, una amenaza óptica. De ahí, que sea necesario, considerar los escenarios de amenaza radar y comunicaciones actuales como base para el diseño de los equipos de EW.

1.1.2.3. ESCENARIO DE LA AMENAZA RADAR DE EW

Los diseños de equipos de EW que desempeñan funciones contra radares se basan en la respuesta a una amenaza validada.Validación significa que los componentes del conjunto de inteligencia, responsables de determinar la amenaza, se han de-

cidido por un modelo concreto. Existen varios métodos para determinar el modelo de amenaza que vamos a comentar en relación con la amenaza radar.

Un método de determinar la amenaza es definiendo el EOB. Esto exige una tarea de inteligencia que especifique la localización, función y características de los equipos electrónicos enemigos. Este método tiende a subestimar la amenaza, puesto que es dficil obtener toda la información necesaria para su validación y el enemigo no está dispuesto a exhibir toda su capacidad, excepto en condiciones de conflicto.

Otro método de estimación de la amenaza es el "mirror-image" . Este concede al enemigo la misma capacidad de las fuerzas amigas. Una ventaja de este método es el conocimiento - bastante preciso de la capacidad actual y futura que disponen - las fuerzas amigas. Este método suele sobreestimar la capacidad del enemigo, puesto que se basa en los mejores diseños propios disponibles.

Un tercer método es la aproximación al diseño genérico. Este determina las características teóricas óptimas, deduciendo, entonces, que los diseños futuros del enemigo evolucionarán lógicamente hacia este punto. Como en el "mirror-image", este método tiende a sobrestimar la capacidad enemiga.

1.1.2.4. ESCENARIO DE LA AMENAZA DE COMUNICACIONES DE EW

La segunda utilización de la energía electromagnética radiada implica la comunicación de mensajes desde un elemento de una fuerza a otro. Los equipos de comunicaciones por radio trabajan, por lo general, en zonas del espectro electromagnético de alta frecuencia HF, muy alta frecuencia (VHF), y ultra alta frecuencia (UHF). Las bandas de VHF y UHF se utilizan para comunicaciones dentro de la línea de visión, mientras que la banda de HF se usa en transmisiones más allá del horizonte mediante onda reflejada y en comunicaciones de más corta distancia, mediante ondas de superficie. También hay que considerar la baja frecuencia - (LF) y la extremadamente baja frecuencia (ELF) usadas para radiodifusión de submarinos, tanto convencionales como atómicos.

Es también importante el volumen de comunicaciones militares que se transmiten por medios telefónicos y telegráficos, bien por cable o por enlace radio, así como a través de satélites. La EW no está orientada a este tipo de sistemas de comunicaciones, puesto que los tipos por cable son difíciles de

interceptar o perturbar, mientras que las comunicaciones por satélite son altamente vulnerables y sólo se utilizan apoyadas en fuertes sistemas de seguridad.

La perturbación de las comunicaciones no se cumple indiscriminadamente, sino con objeto de conseguir un objetivo estratégico. El punto de vista actual es el de considerarla como una acción multiplicadora de fuerza. Si interrumpiendo las comunicaciones el Comandante de la fuerza, puede evitar que el enemigo dirija sus armas o las controle habrá conseguido un verdadero efecto multiplicador de fuerza.

2. APLICACIONES DE LA INTELIGENCIA ARTIFICIAL A LA EW

La inteligencia artificial es una tecnología, en evolución, que en su concepto más amplio pretende absorber, en el software del ordenador, el proceso mediante el cual los humanos resuelven los problemas.

En inteligencia artificial, a diferencia de la informática tradicional, se manejan bases de conocimientos, en lugar de bases de datos.

El ordenador de inteligencia artificial requiere una arquitectura propia, que le permita ejecutar este tipo de programas y sus necesidades, exigen generalmente, cálculos de gran intensidad, aplicados en tiempo real, y del orden de entre 10 y 100 billones de operaciones por segundo.

Se aplican técnicas de Inteligencia Artificial a la EW para: Fusión de Datos procedentes de sensores múltiples, como ayuda a la toma de decisión, en los sistemas de análisis de la amenaza, procesos de reconocimiento, vigilancia e inteligencia, en el planeamiento y ubicación de sensores y en el encaminamiento y recuperación de la información.

La metodología empleada para resolver un problema de estimación del EOB, se basa en el concepto de adquisición activa de datos.

La representación de los estados de conocimiento dentro de un programa de IA, se lleva a cabo por medio de un juego de reglas de producción. Un problema complejo puede tener hasta 20.000 reglas.

3. LAS NUEVAS TECNOLOGIAS Y LA EW

3.1. EL LASER

A principios de siglo, Nikola Tesla, físico croata emigrado a EE.UU., realizó en laboratorio un transformador con una altísima relación de transformación, tal como para proporcionar, tensiones muy altas, del orden de centenares de miles de voltios. En 1960 cuando la casa HUGUES anunció el encendido del primer laser, realizado por Macman, alguien volvió a hablar del "rayo de la muerte", nombre con el que se bautizó el invento de Tesla.

Aplicación importante del laser es la guía de sistemas de armas, como la bomba "inteligente" ("smart o laser bombs") y los misiles tipo Maverick que consiguen altísima precisión. Se trata de bombas o misiles a los que se aplican mecanismos que se autodirigen hacia las radiaciones reflejadas por un blanco "iluminado" por otro laser llamado "indicador". Otra aplicación es el LADAR (Laser Detection and Ranging) que es una simbiosis de laser y radar que se aplica en la guía de proyectiles, durante su trayectoria; para maniobrar satélites, para navegación y en todas aquellas operaciones en las que la precisión del radar ya no es suficiente.

3.2. TELEVISION DE BAJO NIVEL DE LUZ

Con las técnicas modernas de visión nocturna se ha logrado ver de noche casi con igual definición que de día. La técnica más usual es la de intensificadores de imagen que se utilizan en los sistemas de TV de bajo nivel de luz o (LLLTV) (Low Level Light Televisión). Los intensificadores de imagen mejoran la visibilidad durante los períodos de escasa luminosidad, amplificando los débiles reflejos de la luna o de las estrellas que iluminan una zona determinada.

La Televisión de bajo nivel de luz encuentra su aplicación más apropiada en los aviones (despegues, aterrizajes o navegación sin visibilidad) y en los modernos periscopios de observación de los submarinos.

3.3. LAS CONTRAMEDIDAS ELECTROOPTICAS

Según se ha extendido el empleo del láser y la TV de bajo nivel de luz, se han estudiado y realizado las contramedidas y anticontramedidas correspondientes que en este caso se denominan electroópticas.

En general para engañar a un láser se recurre a un segundo láser de características similares al primero, pero de mayor potencia, cuyo rayo se dirige sobre un punto que se encuentre a una distancia de seguridad del objetivo a proteger. Existe la posibilidad de combatirlo con contramedidas pasivas, empleando revestimiento antilaser, o atenuando su emisión mediante el uso de aerosoles, humos, aditivos químicos o de sustancias químicas que absorben o dispersan su energía.

Contra los sistemas de televisión de bajo nivel de luz y sistemas ópticos en general se usa el chaff óptico: En efecto, hoy es posible lanzar desde un avión o buque una infinidad de pequeñas lentejuelas (paillettes) con la finalidad de reflejar la luz y deslumbrar la telecámara de un sistema de búsqueda electroóptico adversario. También se utiliza la reflexión y el uso de un láser deslumbrador.

3.4. ARMAS DE MUY BAJA FRECUENCIA

Tesla, desarrolló un proyecto mediante el cual una señal que él había calculado en 8 c/s, podía atravesar la Tierra y ser recibida en la parte opuesta de nuestro hemisferio, ya que la propagación de la misma señal se hacía por ondas verticales. Según expertos americanos, con un sistema que aprovecha esta técnica, los soviéticos habrían logrado provocar algunos fenómenos sísmicos y entre ellos el terremoto de Pekín a principios de 1977. Este hecho no ha podido ser confirmado.

Algo más verosímil sin embargo, podría ser el desarrollo de un arma de ondas de baja frecuencia, que los soviéticos podrían haber extraído de las ideas de Tesla y experimentado en los últimos tiempos, probablemente en Afganistán. Esta arma funciona en frecuencia 8 c/s, que es muy cercana a la del cerebro humano, (10 c/s y amplitud 10 a 50 voltios), por lo que los científicos soviéticos podrían haber intentado interferirlo y perturbarlo de manera parecida a como se hace con las ECM de radio y radar. Parece que la emisión de impulsos en esa frecuencia puede producir en el hombre efectos que van desde la somno-

lencia a la agresividad y que dos transmisores especiales en esa frecuencia se habrían construído ya en la Unión Soviética, cerca de Riga y Gomel.

En esencia, un arma de ondas de baja frecuencia podría ejercer una influencia sobre la mente y, consiguientemente, el descontrol de todo el género humano.

Aunque admitiendo que un arma de esta clase puede ser realidad algún día, hay que comprender que, dadas las frecuencias y las potencias que se barajan, no será difícil inventar y producir una ECM adecuada, para proteger nuestro cerebro de tan sutil y peligrosa amenaza que se oculta bajo el espectro electromagnético.

3.5. EL IMPULSO ELECTROMAGNETICO (EMP)

Otro tema importante, dentro de estas nuevas tecnologías, es que una única explosión nuclear, de potencia adecuada, efectuada por encima de la atmósfera de un país, puede dañar los sistemas C3 (teléfonos, transmisores y receptores, radio y telegrafía, ordenadores, etc.) e interrumpir el suministro de energía eléctrica.

El factor desencadenante de este daño es el impulso electromagnético (EMP o Electro Magnetic Pulse), de una gran intensidad y muy corta duración que, aunque no presenta riesgo para la vida humana, puede destruir con una rapidez asombrosa -- cualquier elemento semiconductor e interrumpir las líneas eléctricas de suministro y comunicación, si no se hallan debidamente protegidas.

La OTAN ha calculado que una explosión nuclear efectuada a 300 Kms. de altura sobre el cabo LANDS END, situado al sur de Inglaterra, produciría un colapso total de las comunicaciones de todo tipo, incluídas las telefónicas, en toda Europa Occidental. El efecto calculado llegaría hasta la frontera alemana con el telón de acero y por el sur hasta el Estrecho de Gibraltar.

Hay que señalar que ya han desarrollado tecnologías contra los efectos del EMP por medio de sistemas de apantallamiento, que de momento resultan de un elevadísimo coste.

4. SISTEMAS C3

El concepto de Mando y Control, en un sentido general, se define como el "Ejercicio de la Autoridad y dirección de un comandante sobre los recursos disponibles para realizar la misión".

Los elementos básicos de cualquier sistema C3, sea estratégico, táctico o de teatro, son:

- Subsistemas de Sensores que obtienen información acerca de la localización, movimiento y actividades de los recursos amigos y enemigos.

- Subsistemas de Navegación que informan a las fuerzas amigas de su propia localización.

- Centros de Mando y Fusión que ensamblan, integran y presentan las actividades de las fuerzas amigas y enemigas a los responsables de la toma de decisiones, que deben evaluar la amenaza y determinar las respuestas adecuadas.

- Enlaces de comunicaciones entre los sensores y los centros de mando y entre éstos y las fuerzas para permitir la transmisión de información y órdenes.

Los sistemas C3 se dividen por naturaleza en dos grandes clases que dan apoyo a objetivos estratégicos o tácticos. La misión estratégica incluye principalmente la protección frente a un ataque a los recursos nacionales, mientras una misión táctica implica la utilización de fuerzas operativas durante las operaciones de combate. Los sistemas estratégicos de C3 se caracterizan por grandes instalaciones fijas cuya localización y características son bien conocidas. Los sistemas tácticos C3 son altamente móviles y dinámicos, con una mezcla de equipos apropiados para la operación manual.

La generación de las órdenes de decisión, conduce a la posibilidad de utilizar el sistema C3 como un multiplicador de fuerza. Este concepto se explica mejor mediante la ecuación de Lauchester, la cual determina que "la potencia militar efectiva de una fuerza es proporcional al producto de la efectividad de sus armas y al cuadro de su número". Por lo tanto al enfrentarse a una fuerza numéricamente superior en relación 2 a 1, es necesario contrarrestar esta con un arma que sea cuatro veces más efectiva que las armas enemigas para conseguir la igualdad. En la práctica se consigue con los sistemas C3 mediante la con-

centración de las fuerzas en enfrentamientos locales, con el fin de obtener una superioridad numérica localizada y con la asimetría en los enfrentamientos de armas, en los que, por ejemplo, se emplee un arma enviada desde el aire contra un carro de combate. Cuando se emplea un C3 como multiplicador de fuerza, se convierte en objetivo primario de los ataques enemigos puesto que, cuando se neutraliza, se consigue un efecto divisor de fuerza.

Los sistemas de EW se integrán en los C3 a traves del Centro de Mando y Fusión de EW, que es un módulo del C3, que informa del estado de los sistemas de EW y mantiene contacto con la dirección de los mismos, es decir, enlaza los recursos con el mando operativo. La finalidad del Centro de Fusión de información es la creación de un modelo de situación detallado y exacto que facilite las decisiones del Mando. Este módulo debe contener la doctrina de EW, las reglas de enfrentamiento o de combate y el orden de Batalla propio y del enemigo o amenaza y además herramientas de simulación y análisis. Debe, asímismo, ser capaz de suministrar generación de informes, presentación de gráficos posibilidad de manejo de datos, estado de las fuerzas y comunicación con otros módulos del C3 y con el Jefe del Mando Operativo, para coordinación y toma de decisiones sobre seguimiento.

De los recursos de EW se obtendrá la máxima eficacia, sólo si están integrados con el resto de los recursos del Mando Operativo.

5. CONTRA-MEDIDAS DE MANDO, CONTROL Y COMUNICACIONES (CC3)

Se puede defininir el CC3 como "utilización conjunta de seguridad de operaciones, decepción militar, perturbación y destrucción física, apoyada por la inteligencia, para negar información con el fin de influenciar, degradar o destruir la capacidad C3 del adversario y proteger la capacidad aliada ó propia contra tales acciones".

Los principios CC3 pueden resumirse de la siguiente forma:

- Para ser efectiva la acción CC3 debe estar acompañada de otras acciones militares.
- Las acciones CC3 deben ser redundantes contra un elemento específico, debido a las incertidumbres,

tanto de la estructura C3, como de la efectividad de la contra acción.

- La efectividad de las acciones CC3 están directamente relacionadas con el conocimiento detallado y la comprensión de los sistemas C3 enemigos.

Los objetivos de las acciones CC3, incluyen los puestos de mando de alto y bajo escalón, centros de correlación sensor/inteligencia, y puesto de mando de defensa y ataque aéreos. Los ataques y perturbaciones no deben ser indiscriminados sino selectivos en tiempo y lugar.

La protección de los C3 propios se extiende más allá del uso de ECCM empleadas con los sensores radar y comunicaciones. Las vulnerabilidades de los sistemas C3 pueden diferenciarse en cuatro categorías: destrucción física, perturbación, explotación y decepción.

La protección contra la destrucción física conlleva conceptos tales como movilidad, redundancia, robustez, arquitectura distribuída y cobertura. La protección contra la perturbación incluye operaciones biestáticas, señuelos, redes, ECCM, movilidad y operaciones pasivas. La protección contra explotaciones incluye COMSEC, señuelos, cobertura, movilidad y procedimientos operativos. La protección contra la decpeción incluye el - COMSEC, redundancia y procedimientos operativos. Además, el desarrollo de misiles antirradiación, orientados por las radiaciones del perturbador, pueden ser un obstáculo significativo contra las ECM C3 activas.

6. CONSIDERACIONES FINALES

Hay que recordar ahora que la EW no sirve de nada, cito como ejemplos el SHEFFIELD y el más reciente del STARK, y no sirve para nada, si no va acompañada de una buena y actualizada base de datos, una continua vigilancia y actualización de información y una firme voluntad de utilizarla.

Se debe de señalar que el verdadero desafío lanzado a la EW no es solo su evolución técnica, sino la transformación radical de sus conceptos de empleo, que deberán, lógicamente, conducir a una integración total de las funciones de EW en un conjunto de funciones militares y de sistemas de armas.

Finalmente, reseñar que lo que se llama EW era, hasta hace poco tiempo, un conjunto de técnicas radioléctricas, a menudo confiado a especialistas y también a menudo, mal integrada en la idea de maniobra de los jefes: ahora, es más real, hablar de una "confrontación electrónica" que caracterizará en el futuro el conjunto de las actividades militares.

Como la electrónica ha invadido, como hemos visto, casi todos los componentes de los Ejércitos de Tierra, mar o aire podíamos acabar diciendo como Sir John Hackett, antiguo Comandante del Ejército Británico del Rhin y de NORTHAG, que en su libro titulado "La tercera Guerra Mundial" publicado al final de la década de los 70 afirmaba que:

"En un conflicto futuro la EW no existirá la guerra será electrónica".