CESEDEN

LA GUERRA ELECTRONICA, UNA GRAN REALIDAD

- Por el Capitán de Navío F. de QUEYLAR

(Traducido de la Revista "DEFENSE NATIONALE" por el Comandante de Infantería del Servicio de Estado Mayor D. Félix Carrasco Lanzos).

Junio - Julio 1975

BOLETIN DE INFORMACION NUM. 93-II

LA GUERRA ELECTRONICA, UNA GRAN REALIDAD

Los cambios que sufren, en la era de los misiles, los medios de detección y de guiado, la guerra electrónica ha adquirido una nueva dimensión, puesta de manifiesto en la guerra del Vietnam y en el reciente conflicto de Oriente Medio. No se trata de un fenómeno marginal, sino de una realidad permanente y, además, constituye un medio de acción privilegiado en la "conducción de las crisis".

El cuarto conflicto árabe-israelí ha puesto de moda la guerra electrónica, principalmente con el empleo de los SAM 6 y 7 y los esfuerzos desplegados por los israelitas para neutralizarlos.

¿Por qué este súbito interés cuando, para los especialistas, la guerra electrónica tiene ya una antigüedad superior al medio siglo?. Por ejemplo, se conoce la ventaja que proporcionó a los alemanes la escucha de las redes rusas durante la batalla de Tannenberg, dramático episodio en el que centra Soljenitsye su novela "Catorce de agosto".

La historia de la II G.M. no es menos fértil en variados ejemplos de guerra electrónica: las maniobras de decepción realizadas por los japoneses en sus redes de transmisiones radioeléctricas antes del ataque a Pearl Harbour; el empleo de los beligerantes de engaños destinados a perturbar los radares y que fueron conocidos en su momento con el nombre de "windows", o también el "nublado" de las frecuencias de guiado de las bombas planeadoras alemanas, etc. Más recientemente, la guerra del Vietnam mostró la importancia de la guerra electrónica en el duelo que enfrenta a los sistemas de armas tierra-aire con los aviones.

El empleo juicioso y muy coordinado de diferentes medios tales como los "nubladores" de barreras, "nubladores" regulares y engaños variados, permitió reducir a menos de una décima parte de su valor la eficacia de la defensa aérea norvietnamita.

La guerra electrónica no es cosa nueva ni en su principio ni en sus diversas aplicaciones, como tampoco es fruto de la imaginación de teóricos irrealistas. Si bien la guerra electrónica parecía ocupar un puesto muy modesto en Francia, esto era debido, sin duda, en parte, a que exceptuadas algunas acciones de escucha, las guerras de Indochina y de Argelia fueron guerras sin electrónica -al menos uno de los adversarios estaba casi totalmente desprovisto de ella-; también, ciertamente, porque el atómo, debido a su eminente puesto en el arsenal militar, eclipsaba a la electrónica, de la que sin embargo es inseparable; seguramente también, porque la guerra electrónica aporta importantes cambios en la manera de pensar, de equipar a las fuerzas y de dirigir las operaciones, y el cambio suscita desconfianza y retinencia. En fín, ciertamente, porque la guerra electrónica es cara o al menos parece cara a primera vista. Porque sucede con esto lo mismo que con las pólizas de seguro, que sólamente son caras antes del accidente. La guerra de octubre de 1973 ha aportado la prueba de ello.

Es, pues, un momento oportuno para abordar un tema que los especialistas y los técnicos han más o menos rodeado de un velo de exoterismo que ayudaba a su desconocimiento. Por esto, nosotros vamos:

- en primer lugar, a recordar la composición y las características de una "emisión" y precisar para ello el significado de algunos términos corrientes;

- luego, a analizar uno tras otro los diferentes usos que los Ejércitos hacen de la electrónica y de las ondas electromagnéticas, las vulnerabilidades que aquéllos presentan por este hecho, así como los medios de parada con que cuentan;

- finalmente, en una última parte de carácter sintético, examinar los tres aspectos más importantes de la guerra electrónica; es decir, por una parte, las acciones ofensivas que son las medidas de investigación electromagnéticas (MIE),

que se dirigen a la obtención de información sobre el adversario, y las contramedidas electrónicas (CME), que tratan de entorpecer (por la interferencia) o de engañar (por ejemplo, — creando falsos ecos) a la electrónica adversaria; por otra parte, las acciones defensivas, llamadas medidas de protección electrónica (MPE) y que se traducen en medidas de seguridad y en medidas de defensa, respectivamente opuestas a las MPE y a las CME adversarias.

Acciones ofensivas	Acciones defensivas
M I E (obtener informaciones) C M E (entorpecer o engañar al enemigo)	Medidas de seguridad)) MPE Medidas de defensa)

Será posible entonces deducir las características generales de la guerra electrónica y poner de manifiesto los elementos esenciales de una política dirigida a integrar correctamente las acciones de guerra electrónica en el conjunto de las acciones militares.

Pero antes de emprender de esta manera el estudio de este tema, extremadamente vasto y complejo, es indispensable fijar sus límites tan exactamente como sea posible.

En su acepción más generalmente admitida, la expresión "guerra electrónica" se aplica a la totalidad del espectro de frecuencias, pero en realidad se refiere solamente a las ondas electromagnéticas, es decir , a las ondas que se propagan por el éter. Lo que concierne a las ondas sísmicas, así como a las ondas que se propagan en el medio marítimo, no es considerado ordinariamente como formando estrictamente parte de eso que se llama "guerra electrónica". En realidad, las fronteras no están muy claras, cosa normal tratándose de un asunto en plena expansión.

Todos sabemos, por ejemplo, que las ondas radioeléctricas de mucha longitud (varios kilómetros) penetran en el agua. Sabemos también que las ondas extremadamente largas pueden producir efectos ecológicos muy importantes. Por otra parte, en el medio marino, con los ultrasonidos, se dan prácticamente todos los problemas que plantea la guerra electrónica con las ondas electromagnéticas.

Si bien yo me limito, en este estudio, al examen de lo que constituye la guerra electrónica en el éter, estimo sin embargo necesario advertir al lector que el verdadero problema es en realidad más amplio que lo tratado aquí. En el plan técnico, es realmente fácil separar los estudios, los materiales, los procedimientos relativos a los diferentes tipos de ondas. En el plan operativo no ocurre lo mismo y es, por ejemplo, indispensable integrar, para las operaciones marítimas, la guerra electrónica y la guerra de ultrasonidos.

Una radiación electromagnética comprende, según su finalidad, una o dos partes:

- el soporte, que constituye la base de todas las emisiones;

- el mensaje, que es facultativo y sólo existe, por lo general, en las emisiones de transmisión, de identificación y, a veces, de ayuda a la navegación. El mensaje se descompone a su vez en dos elementos: el texto, que representa la información propiamente dicha a transportar, y la envoltura, que es necesaria para el correcto envío de esta información.

El soporte no tiene significación intrínseca. Sin embargo, su situación en el tiempo o el valor de algunas de sus características comparado con los valores de referencia, pueden constituir información. De esta forma, la dirección de propagación da la del emisor; la variación de frecuencia permite medir el efecto Doppler y conocer con ello la componente radial de la velocidad del generador del eco; la variación de fase permite medidas de tiempo y, en consecuencia, de distancia.

Además, ciertas características del soporte, tales como la frecuencia, la anchura de banda, la longitud de los impulsos, pueden indicar la función del emisor o su naturaleza. Se comprende así la riqueza de informaciones que puede aportar una radiación electromagnética por el solo hecho de su existencia.

El mensaje representa una información intrínseca que la señal-soporte se encarga de transportar desde el emisor o repetidor hasta el receptor. Esta información puede presentarse bajo forma numérica o analógica y referirse a una imagen, a un sonido, a un "signo", a un dato, que habrá, probablemente, sido previamente codificado o cifrado.

Este análisis es necesario para comprender bien el interés y la vulnerabilidad que presentan las emisiones electromagnéticas, qué ventajas puede presentar al adversario su captación y que acciones pueden ser realizadas para anular, perturbar o, por el contrario, proteger tales emisiones. Por otro lado, para la buena comprensión del tema, recordaré aquí algunas definiciones elementales:

- se llama "vela" electromagnética toda acción dirigida a la captación de emisiones electromagnéticas;

- si la emisión captada es una emisión amiga, hay "recepción" si es enemiga, hay "interceptación";

- cuando el objetivo de la interceptación es la apropiación de "un mensaje" por persona distinta de su destinatario, se emplea preferentemente el término "escucha" en lugar del de "vela".

OMNIPRESENCIA DE LA ELECTRONICA EN MATERIA DE DEFENSA

Toda organización, todo sistema exige para funcionar una cadena ascendente de informaciones necesarias a la toma de decisión, y una cadena descendente de órdenes necesarias para la ejecución de la decisión y para la acción. Esto es verdad en los Ejércitos, y tanto para una organización del más elevado nivel, tal como el Mando Estratégico, como para un sistema del nivel más elemental, como el del auto-dirección de un misil.

El cuadro siguiente indica de una manera esquemática los principales medios que pueden constituir la cadena de información y la cadena de acción, que utilizan, en diferentes grados y bajo las más diversas formas, las ondas electromagnéticas. Todos, en consecuencia, pueden ser vulnerables a las acciones de guerra electrónica del adversario y necesi-

tan, por lo tanto, ser protegidos; porque además, mediante la intercepta-ción de sus emisiones, corren el peligro de proporcionar preciosas infor-maciones al adeversario. Estas vulnerabilidades, estas interrupciones y estos riesgos, es lo que nosotros vamos a examinar.

Obtención de información	- detección electromagnética, - sistema de identificación, - velas (radio, radar, infrarrojo), - sistemas de ayuda a la navegación.
Transmisión de la información	- telecomunicación por vía hertziana

Decisión

Transmisión de las órdenes	- telecomunicación por vía hertziana
Medios de acción	- sistemas de armas, - contramedidas electrónicas.

I.- LA OBTENCION DE INFORMACION.

La detección electromagnética.

Los radares constituyen el elemento esencial de la detección electromagnética, que es hoy día una de las bases de la información tácti-ca.

Los radares son vulnerables y su neutralización puede lograrse, bien por medios activos, productores de interferencias que, emitiendo en la misma frecuencia de trabajo del radar, saturan la recepción e impiden la percepción del eco; bien por medios pasivos, los engaños, utilizados como barrera y que forman un muro reflectante tras el cual escapa a la detección el objeto buscado. Estos engaños ("chaffs en inglés), se presentan ordinariamente bajo la forma de tiritas o de agujas metalizadas, cuya longitud se adapta evidentemente a la de la onda a reflectar, y que son esparcidas en nubes dispuestas de manera apropiada, para la mejor protección del objeto cuya detección debe evitarse.

Los radares son asimismo vulnerables a las acciones consistentes en producir, con interferencias o engaños de tipo especiales, ecos de diversión. Estas acciones dirigidas a engañar al enemigo forman parte de lo que se designa con el nombre de "decepción".

Así, durante la última guerra, ocurrió que los submarinos soltaban un globo del que colgaba un cilindro metálico que remolcando una guia en el agua moderaba la deriva. Los destructores, al tomar contacto con este objeto por medio del radar, si la noche era suficientemente oscura y la visibilidad nula, lo confundían con el "schnorchel" del submarino perseguido, el cual eludía así el peligro.

Frente a estas acciones adversarias el radar no queda indefenso porque puede contar con: variados medios que forman parte de lo que se denomina en guerra electrónica las "medidas de defensa", de las interferencias. Citemos entre otros: el cambio de frecuencias para huir de las interferencias, los cambios de tipo de emisión para hacerlo inoperante, la capacidad de eliminar á priori los ecos que no presenten determinadas características. Estos medios de defensa pueden ser maniobrados, bien por el hombre, el operador, que ha debido recibir para ello un gran entrenamiento, o bien por un ordenador de control que reaccionará más rápidamente y con más seguridad que el hombre, salvo si se encuentra ante una dificultad, siempre posible o probable en guerra electrónica.

El principal defecto táctico del radar consiste en su indiscreción, inherente a la potencia radiada; la distancia a la que puede ser detectado un radar es muy superior a la que él mismo es capaz de detectar. En muchos casos, y especialmente si se trata de radares fijos y bien conocidos, no tiene importancia esta indiscreción. En otros, por el contrario, la

discreción puede tener más importancia para el vector portador del radar que la capacidad de protección que éste le proporciona. La elección del régimen y de las condiciones de empleo es asunto del Mando. Es a éste último, a los operativos, y no a los técnicos a quien corresponde decidir en función de la misión y de los riesgos implicados por una u otra solución.

La identificación electrónica

A causa del crecimiento de las velocidades de los móviles, del aumento de los alcances de los radares y de las armas, del desarrollo de los medios de visión nocturna, se vigila y se lucha cada vez más lejos. La distancia o la noche no permiten la identificación por la vista; la identificación debe ser lejana y "todo tiempo". Además, en un combate que corre el peligro de tomar una forma confusa, la identificación debe ser todo lo rápida, precisa y segura que sea posible. Por ello solamente puede ser electrónica.

Es decir, que los materiales de identificación, constituídos en su mayor parte por los equipos conocidos con el nombre de IFF (Identificación Friends and Foes) son, lo mismo que los materiales de detección, vulnerables a la interferencia y a la decepción. Al igual que éstos, son indiscretos, si bien la causa de su débil potencia de emisión, comparada con la del radar al que están asociados generalmente y de la movilidad de sus antenas, esta indiscreción no tiene importancia las más de las veces.

En realidad, es la vulnerabilidad a la decepción la que es, con mucho, la más grave; por ello se hace necesario, inspirándose en procedimientos de cifra, el desarrollo de materiales de identificación cada vez más protegidos y, en consecuencia, cada vez más perfeccionados y costosos.

La investigación electromagnética.

La captación de las radiaciones electromagnéticas emitidas por el adversario, constituye otra fuente de información. Esta captación presenta la considerable ventaja de ser, salvo casos muy excepcionales, perfectamente discreta. En contrapartida, esto no es posible sino en la medida en que el adversario sea indiscreto. Su eficacia es, pues, aleatoria, y hay que procurar no deducir conclusiones definitivas, de una ineficacia aparente.

Las escuchas son evidentemente sensibles a interferencias pero, por paradógico que esto pueda parecer, las interferencias producidas por los amigos son las que más frecuentemente molestan. Un emisor amigo, perteneciente a la misma unidad o a una Unidad vecina, estará casi siempre más cerca que el emisor adversario que se trata de interceptar. A poco que este emisor amigo trabaje o emita armónicas a una frecuencia aproximada a la que se quiere interceptar, las posibilidades de interceptación serán reducidas. Las escuchas imponen, pues, severas condiciones de coordinación.

Finalmente, las escuchas son vulnerables a las acciones de decepción. Para comprender bien esta vulnerabilidad, es preciso conocer los principales objetivos de las escuchas de interceptación. Estos objetivos pueden ser clasificados en cuatro categorías:

- la información electromagnética técnica: su trabajo consiste esencialmente en el conocimiento de las características técnicas de los medios de que dispone el adversario en general (o en particular en tal sitio para dotar, por ejemplo, a tal tipo de avión). Permite, además, prever los medios de CME o tomar las medidas de protección apropiadas.

Contra este tipo de información, la mejor medida consiste en la prohibición o la limitación de las emisiones cuyas características se quiere ocultar. De este modo, los egipcios, que posiblemente tuvieron la prudencia de no servirse, con fines de entrenamiento o de ajuste, de sus SAM-6 antes del día del ataque, lograron que los israelitas ignorasen la presencia de estos SAM-6 y sus características exactas, y que no pudieran por lo tanto prever contramedidas correctas.

- la información operativa o táctica, cuyo objetivo principal es el conocimiento de la presencia y del dispositivo del adversario, la localización de sus fuerzas, su identificación . Su trabajo implica, por lo general, la goniometría de las emisiones interceptadas y su análisis, para su identificación por comparación.

Frente a la información operativa, es relativamente fácil engañar a las escuchas enemigas simulando, por ejemplo, mediante falsas redes radio, la presencia de las fuerzas allí en donde solamente existen -

emisores-trampa. Las operaciones de goniometría, por otra parte, sobre todo cuando necesitan marcaciones simultáneas por varias estaciones, exigen un mínimo de tiempo; el empleo de emisiones extremadamente cortas, de una duración del orden de unas milésimas de segundo, hace muy difíciles estas operaciones.

- la información necesaria para el empleo de sistemas de armas o de contramedidas, que puede implicar, según el caso, una localización extremadamente precisa, la prohibición de emisiones particulares (tales como las emisiones de infrarrojos de los escapes de reactor) o la determinación exacta de características cuyo conocimiento es necesario para el óptimo empleo de los emisores de interferencia. Esta información, de carácter específico, se identifica a veces bajo la denominación de "medida de apoyo de guerra electrónica" (MAGE).

Las emisiones apuntadas por este género de información son, o voluntarias (radar) o involuntarias (irradiación infrarroja). Permiten - merced a su interceptación por materiales apropiados, el guiado pasivo, hacia el objetivo emisor, de un misil o de cualquier otro móvil. Para el objetivo, la mejor defensa consiste en engañar al misil, mediante, por ejemplo, el empleo de bombas de desprendimiento de calor, lanzadas por cohetes y simuladoras de la radiación infrarroja del objetivo.

- la información general, o sea, la relativa a las acciones, las actitudes y las intenciones del adversario. Tal tipo de información será proporcionada frecuentemente por el examen de las condiciones de empleo de los medios electrónicos enemigos y sobre todo por la interpretación de mensajes (es decir, por las escuchas) y, si es necesario, su descriptación y su interpretación. Citemos, a título de ejemplo proporcionado por una variación de las condiciones de empleo, el siguiente caso, totalmente clásico: el radar enemigo que usted intercepta aumenta su velocidad de rotación de antena, reduce la longitud de los impulsos de emisión, así como su intervalo; esto significa que este radar pasa de un tipo de "vigilancia" a un tipo de "ataque" y que es inminente un tiro.

Frente a acciones dirigidas a la búsqueda de información general, se pueden emprender acciones de decepción, haciendo variar, por ejemplo, de manera artificial, la densidad del tráfico en una red de transmisiones para hacer creer en un cambio de actividad; o también haciendo interceptar falsos mensajes que nada, a la vista del interceptador, distingue de los verdaderos.

En conclusión, si las escuchas de interceptación son, cualquiera que sea su objetivo, un medio notable de información y, en muchos casos, insustituíbles, no constituyen, sin embargo, una panacea: pueden ser ineficaces si el adversario se calla; pueden hacerse autoritarias si obligan a limitar las emisiones amigas y, finalmente, engañosas si dan lugar a resultados erróneos originados por una contra-acción enemiga de decepción.

Las ayudas radioeléctricas a la navegación.

En cumplimiento de misiones de información o de acción, los móviles amigos se desplazan cada vez más de prisa por espacios cada vez más vastos. Para informar con exactitud o para actuar en condiciones óptimas deben, en todo momento, conocer su posición con seguridad y precisión. Es cierto que para ello existen sistemas de navegación por inercia, pero son onerosos y necesitan ser nivelados muy a menudo, en su lugar se utilizan sistemas radioeléctricos, cuyos principios de funcionamiento y sus longitudes de ondas variarán según el alcance y la precisión exigidos.

No es cuestión de describirlos aquí todos, porque su gama se extiende desde los sistemas de cobertura mundial, que implican ondas muy largas o el relé de satélites, a los sistemas de muy corto alcance tales como, por ejemplo, los materiales de aterrizajes sin visibilidad, las sondas altimétricas, o ciertos radares llamados de evitación de obstáculos. Sepamos solamente que estos sistemas presentan las mismas vulnerabilidades de todo sistema electrónico; son sensibles a interferencias y a la decepción; sin embargo, uno y otro no son, por lo general, fácilmente realizables si no es sobre su propio territorio o en las zonas vecinas. La mejor defensa del sistema reside en el empleo de fuertes potencias de emisión, en el cambio aleatorio de frecuencias y en la utilización de señales de código que puedan ser distinguidas de las señales falsas.

Además, deberán tomarse determinadas precauciones de camuflaje técnico, tales como el intervalo de fase o el intervalo temporal, para evitar que el adversario pueda utilizar en su propio beneficio nuestro sistema de ayuda a la navegación.

II.- LA TRANSMISION DE LAS INFORMACIONES Y DE LAS ORDENES.

Las informaciones recogidas solamente serán provechosas en la medida en que lleguen en forma explotable al centro de decisión en cuyo favor fueron captadas, bien sea este centro de decisión el Puesto de Mando del Jefe Supremo de un Teatro de Operaciones que cubra la cuarta parte del globo o el mini-calculador de un misil destinado a controlar su navegación y a actuar sobre sus mandos. Innumerables medios pueden, según el caso, permitir este envio ascendente de la información y, una vez tomada la decisión el descendente de la orden de ejecución. Nosotros sólo nos interesaremos por los medios que hacen uso de las ondas hertzianas.

Los receptores propios, encargados de recibir, bien sea en beneficio del centro de decisión en la ascensión, o en provecho del órgano de ejecución en el descenso, son sensibles a las interferencias. Teniendo en cuenta lo que se puede conocer sobre los medios de que disponga el adversario, la eventualidad de la interferencia presenta, si no una realidad, si al menos una gran probabilidad.

Sin embargo, existen procedimientos contra la interferencia : por ejemplo, el cambio de frecuencia realizado a priori o en reacción contra la misma. Este procedimiento es eficaz en la medida en que el emisor de interferencias no tiene posibilidad de "perseguir" o tarda tiempo en hacerlo. Exige una perfecta coordinación entre el emisor y el receptor, coordinación que necesita organización y entrenamiento. Otros procedimientos, tales como el empleo de modulaciones especiales, o el desarrollo de receptores capaces de distinguir la señal útil, permiten evitar o minimizar los efectos de la interferencia. Recordemos también que el empleo de antenas direccionales no solamente mejora la calidad de la recepción sino que puede también reducir los riesgos de ser interferidos.

Finalmente existe otro peligro para los sistemas de telecomunicaciones, cualesquiera que éstas sean: el del intruismo, acción consistente en la introducción de un extraño en una red, a fin de hacer circular -

por ella informaciones erróneas u órdenes engañosas, o simplemente mensajes cualesquiera pero en cantidad y de urgencia tales que la red en cuestión se vea sobrecargada. Esto exige del intruso el conocimiento de determinadas características técnicas de la red, sin lo cual la señal introducida no sería ni recibida ni demodulada por el receptor; exige también que el intruso conozca ciertas reglas de explotación de la red y, en especial, las relativas a eso que se ha llamado anteriormente la envoltura; exige, en fin, que conozca el cifrado o el código eventualmente empleado por la víctima. El intrusismo es pues, más o menos fácil y tiene más o menos posibilidades de éxito según el tipo de red atacada. El emisor intruso debe, en cierto modo, "mostrar la patita blanca" y, en el caso específico de la fonía, el sexo de la persona que habla, su acento, su pronunciación son, si se puede decir así, los elementos esenciales de la "patita blanca". Añadamos a esto que ningún emisor es rigurosamente idéntico a otro; existe una personalidad que los operadores entrenados llegan a reconocer.

Todas estas dificultades no son suficientes, sin embargo, para desanimar al intruso y condenarlo al fracaso. Esto ha obligado al desarrollo de sistemas de identificación destinados a aportar al receptor la prueba de que el emisor es realmente el que él cree y que la comunicación es, pues, exactamente "auténtica". No obstante, la identificación no proporciona una seguridad absoluta, porque el intruso puede apoderarse de la clave o reconstituirla, sobre todo si la víctima hace un empleo exagerado o no respeta las reglas de procedimiento.

Es preciso, en fin, resaltar que el desarrollo de la tele-informática y de las transmisiones de datos proporciona a la intrusión un campo de acción nuevo y aún mal conocido: el intruso puede no solamente enviar una falsa información o una orden falsa, sino también perturbar el funcionamiento del ordenador.

Terminaré con el intrusismo citando, como recordatorio, el caso particular de la guerra de las ondas en radiodifusión: el intruso, para tener todas las posibilidades de ser recibido por los auditores, emite en la frecuencia del vecino, pero no trata de enmascarar, antes al contrario, su identidad, y se produce entonces más bien una sustracción del derecho de uso de la frecuencia que intrusismo, en el sentido "guerra electrónica" del término.

III.- LOS MEDIOS DE ACCION.

Los sistemas de armas.

Un sistema de armas (1) puede ser definido como un conjunto ordenado de medios cuya finalidad es, por lo general, provocar a distancia útil del objetivo que se quiere destruir, la explosión de una carga que ha sido preciso colocar previamente en buena posición. Esta operación se hace en tres fases: la adquisición del objetivo; el guiado eventual del portador; la provocación de la explosión . La intervención de la electrónica en el cumplimiento de estas tareas varía según el grado de elaboración del sistema. Examinemos, por ejemplo, el caso de un sistema de armas superficie-aire o tierra-aire, en el cual se emplea generalmente la guerra electrónica de diferentes maneras.

La fase de adquisición comprende la búsqueda, el descubrimiento y la localización del objetivo, por lo general mediante radares de vigilancia, que pueden ser independientes del sistema de armas propiamente dicho. Esta primera localización permite entonces apuntar hacia el objetivo el radar de tiro o radar de armas, cuyo calculador asociado determinará los elementos de tiro del misil.

En razón de sus características y, entre otras, la estrechez de sus haces y de su "ventana" de distancia, estos radares de tiro presentan vulnerabilidades particulares y más servidumbres de empleo. Deben, para cumplir su cometido, permanecer apuntados hacia el objetivo; si lo pierden, ya sea por interferencia, ya a consecuencia de movimientos de evasión del objetivo, o bien si son engañados por falsos ecos, toda la secuencia de adquisición deberá comenzarse de nuevo a partir de los elementos proporcionados por el radar de vigilancia; durante este tiempo, el objetivo habrá salido del campo de tiro del sistema de armas, que habrá quedado inútil. Los radares de tiro, por otra parte, pueden ser especialmen-

---

(1).- La expresión "sistema de armas" califica ordinariamente sistemas de armas muy complejos que pueden responder a varios fines y descomponerse en sistemas de armas "unitarios" (por ejemplo, un avión de interceptación portador de un misil aire-aire autodirigido).

te indiscretos y sus características particulares facilitan su identificación. El objetivo puede, en fin, si está provisto de un detector de radar apropiado, descubrir a tiempo la amenaza que sobre él pesa.

La fase de guiado puede ser realizada de diferentes maneras. Los cuatro métodos siguientes son los más generalmente empleados separada o conjuntamente:

- el tirador determina por medio del radar las posiciones relativas del objetivo y del misil; elabora y envía a este último las órdenes de navegación. El objetivo, para defenderse, debe interferir o engañar, bien al radar del tirador, bien al sistema de transmisión de órdenes; éste es un problema que ya hemos examinado, pero que presenta aquí dos particularidades: -el objetivo sólo tiene un plazo muy breve para determinar la o las frecuencias a interferir y provocar la interferencia; -la emisión de interferencias tiene el riesgo de servir al autoguiado pasivo del misil. La solución de la decepción es, pues, preferida en muchos casos. Esta consiste recordémoslo, en crear falsos ecos;

- el tirador detecta el objetivo, el misil recibe el eco de esta detección reflejado por el objetivo y determina de esta forma por sí mismo sus propios elementos de navegación. La mejor defensa para el objetivo consiste en engañar al receptor del misil creando una confusión entre el eco real y los ecos de decepción;

- el misil posee su propio radar; esto es el autoguiado activo. Para el objetivo, el problema es prácticamente el mismo del caso anterior y la mejor solución es el empleo de engaños producidos por falsos ecos o el empleo de interferencias especiales modificadoras de las características del eco principal;

- el misil recibe emisiones voluntarias o involuntarias del objetivo (emisión radar - emisión infrarroja), o ve el objetivo (cámara de televisión). El objetivo necesita crear emisiones parásitas con objeto de engañar al misil.

En la fase de desencadenamiento de la explosión, se trata de medir una distancia, por lo general muy corta, de forma muy precisa. La tarea se cumplirá, bien por el propio misil -y la variedad de métodos posibles hace casi imposible la defensa del objetivo dada la ignorancia por parte de éste del procedimiento empleado-, bien por los radares de tiro, en cuyo caso volvemos a los problemas precedentes.

Las contramedidas electrónicas.

Los medios de contramedidas electrónicas (CME) constituyen otro medio de acción contra el adversario; su empleo apunta, efectivamente, a la reducción de algunas de sus capacidades de información y de acción, o incluso aniquilarlas.

Los medios CME se dividen en medios de interferencias y medios de decepción; los medios de interferencia se subdividen a su vez en medios activos o emisores de interferencia, y en medios pasivos o engaños, tales como los "chaffs" (que, extendidos en nubes, constituyen un muro reflectante de las ondas radar). Los medios de decepción se subdividen igualmente en medios activos (esencialmente el intrusismo en las redes adversarias) y medios pasivos (engaños periódicos) dando falsos ecos comparables a los del objetivo.

La principal debilidad de los emisores de interferencias es su indiscreción, que procede fatalmente de la potencia irradiada necesaria para impedir al adversario la recepción de sus propias emisiones. Además, éste adversario, lo mismo si se trata de los operadores que de los ordenadores que dirigen los medios de recepción, puede llegar a extraer del conjunto de ruídos la señal útil; la interferencia corre, pues, el peligro de ser poco eficaz al mismo tiempo que conserva íntegramente su falta de discreción.

El intrusismo presenta los mismos inconvenientes para quien intenta penetrar en las redes adversarias con el fin de saturarlas o de engañarlas. El intruso tiene absoluta obligación de emitir y, en consecuencia, se hace indiscreto.

Los medios activos de CME son, pues, también posibles víctimas de la guerra electrónica y de las medidas de investigación electromagnéticas (MIE). Este enfrentamiento de la guerra electrónica contra sí misma es una de las razones de su extrema complejidad.

Hasta aquí, el exámen del impacto de la guerra electrónica sobre los principales medios y sistemas que utilizan de una manera u otra las ondas electromagnéticas. Vamos a estudiar ahora las finalidades y las normas que hay que respetar para obtener el máximo de eficacia.

Recordemos previamente las tres finalidades de la guerra electrónica:

- Se trata, en primer lugar, de utilizar las radiaciones electromagnéticas emitidas voluntaria o involuntariamente por el adversario, para informarse o para actuar a su costa.

- Se trata, seguídamente, de entorpecer la electrónica enemiga con objeto de hacer inoperante su empleo, e incluso acaso peligroso, porque se le puede engañar.

- Finalmente, se trata, indiscutiblemente, de intentar preservar la eficacia de empleo de nuestra electrónica, privando al mismo tiempo al adversario de las ventajas que le proporcionaría la interceptación de las ondas hertzianas emitidas por nosotros.

IV.- LAS MEDIDAS DE INVESTIGACION ELECTROMAGNETICA (MIE)

Las medidas de investigación electromagnética tienen por finalidad la obtención de información sobre el adversario. Vimos anteriormente las cuatro categorías de informaciones buscadas: información-técnica-información operativa y táctica- empleo de los sistemas de armas y de las contramedidas electrónicas (CME) información general; vimos asimismo que esta investigación se aplica a la casi totalidad de los campos de ondas electromagnéticas.

Del análisis al que procedimos se desprende la definición de las diferentes tareas de investigación; conocemos además la necesidad de la inserción de las MIE en el conjunto mucho más amplio de la instrucción y de la información sobre el adversario, así como las servidumbres que hay que soportar si se quieren evitar las interferencias que puedan proceder de los medios de radiación propios.

Las distintas fases de una operación de búsqueda son: la vigilancia del espectro, es decir, de la banda de frecuencias en la que se hacen las investigaciones -el análisis en tiempo real- la grabación - el análisis diferido o tratamiento - memorización - la identificación - la alerta, y la localización.

La vigilancia del espectro necesita receptores especiales. Un tipo empleado corrientemente es el receptor panorámico; la banda a vigilar se divide en gamas y en sub-gamas que son barridas sucesivamente, y por lo general automáticamente; una pantalla de visualización permite observar la sub-gama barrida.

El análisis en tiempo real permite determinar las características esenciales de la señal interceptada y, entre otras, las necesarias para la aplicación de las CME (frecuencia, por ejemplo) o las necesarias para la identificación.

La grabación es necesaria con vistas a la interpretación o descriptación posterior de los mensajes interceptados; es igualmente necesaria para el análisis más completo que se hará en laboratorio.

El análisis diferido o tratamiento es una de las fases esenciales de la información técnica. Necesita frecuentemente la aplicación de medios informáticos y exige un personal muy especializado. Por estas razones, las operaciones de tratamiento son generalmente confiadas a organismos especializados dependientes de escalones de mando muy elevados.

Las características de las emisiones enemigas deben ser memorizadas, por un lado en beneficio de los técnicos que estudian, en particular, los futuros materiales de contramedidas electrónicas (CME) y la protección de nuestros propios materiales y, por otro, en favor de las fuerzas operativas con objeto de facilitarles la identificación de las emisiones interceptadas en investigaciones ulteriores.

La identificación, lograda muy frecuentemente por comparación entre las características medidas por el análisis inmediato y las comunicadas por los organismos especializados que hayan realizado los análisis diferidos, es una operación capital en el terreno táctico. Efectivamente, la identificación de la señal permite la del emisor y, por la vía de la

consecuencia, la del portador. Por ejemplo, interpretada la emisión radar de un avión enemigo, se conocerá el tipo de éste antes incluso de haber logrado su imagen sobre la pantalla del radar.

La interceptación de una emisión enemiga permite determinar la dirección en que se encuentra el emisor. Ella permite, pues, una localización parcial. La potencia de la señal interceptada puede, si se conocen las características del emisor, dar una idea de la distancia de éste. Pero una localización completa y precisa necesita que la emisión enemiga haya sido observada por otras estaciones de interceptación, de aquí la idea de la cadena goniométrica, que comprende varias estaciones, las cuales se dan entre sí la alerta en cuanto es interceptada una emisión enemiga.

Los detectores de alerta tienen una labor bien precisa: la de avisar de la proximidad de un radar enemigo en funcionamiento. Este es un equipo esencial, en particular para las aeronaves, que no tendrían otros medios de saber si son captadas en el haz de defensa aérea, o de un radar de armas, o incluso de un radar autodirector de misil. Los detectores combinados indican el tipo de radar interceptado.

Evidentemente, todas estas tareas no son siempre imperativas. Según el objetivo buscado, podrá evitarse alguna de ellas. Sin embargo, su enumeración permite apreciar la complejidad del asunto; complejidad agravada por la necesaria coordinación de las medidas de investigación electromagnética con las demás fuentes de información.

En efecto, lo mismo si se trata de información técnica, de información operativa, de información general, a veces incluso de la puesta en acción de los sistemas de armas o de las contramedidas electrónicas (CME), la información electromagnética obtenida por la interceptación de las radiaciones electromagnéticas adversarias no es la única fuente de información.

En el campo técnico, las publicaciones extranjeras y la observación visual, entre otras, son asimismo fuentes muy importantes. Es importante, pues, que el empleo y los resultados de todas estas fuentes sean coordinados y correlativos: una tarea de este tipo necesita la instalación a escala nacional de organismos especializados y exige una estrecha colaboración entre militares e ingenieros.

En el plan táctico, es en tiempo real o apenas diferido y a nivel de las fuerzas, como debe hacerse la coordinación de empleo de los medios "clásicos" (detección radar, escucha, óptica, etc.). Las diferentes informaciones deben ser llevadas a las propias mesas de conexiones o a las propias consolas de visualización. La eficacia de esta coordinación ha sido demostrada en innumerables ocasiones.

Pertenece al Mando, en función, por una parte, de las condiciones tácticas, (amenazas previsibles, discreción necesaria, etc.) y, por otra, de las ventajas e inconvenientes de los diferentes medios (por ejemplo, seguridad, precisión pero indiscreción del radar, incertidumbre imprecisión pero discreción de los materiales de interceptación,) elegir y fijar las condiciones de empleo de unos y otros. Con un poco de suerte, algunos errores del adversario y una buena coordinación de los medios, la interceptación proporcionará el aviso previo y la identificación del enemigo; posteriormente, el radar, que se habrá puesto en servicio en tiempo oportuno, dará una localización exacta.

También se necesita una estrecha coordinación si se quiere evitar que la interceptación sea obstaculizada, o al menos imposibilitada, por el emplo de medios amigos tales como emisores próximos y potentes que trabajan en frecuencias vecinas, o productores de interferencias que ataquen a las emisiones que se trata precisamente de interceptar. Así pues, es imperativo que estas coordinaciones sean organizadas, tanto en la fase de preparación y de conducción de las operaciones como en el de la ejecución de los trabajos y en la puesta en acción de los medios.

Para terminar con las medidas de investigación, es preciso considerar una última servidumbre que proviene de las condiciones de propagación de las ondas, ya que la radiación electromagnética que llega a un equipo, puede hacerlo por un camino distinto del normal. Además el interceptador puede estár lejos, encontrarse en una zona de sombra o incluso fuera del lóbulo de emisión. Por otra parte, para ser eficaz, la interceptación exige un material apropiado.

El problema consiste, pues, en llevar este equipo al adecuado lugar y en el momento propicio. En el plan estratégico, satélites de reconocimiento electromagnético, navíos y aviones especializados constituyen soluciones; las estaciones fijas se instalarán cerca de las fronteras,

en las alturas si es posible, o a lo largo de las costas. En el plan táctico, las soluciones son análogas: empleo de medios aéreos, búsqueda de puntos altos, y, en los barcos, instalación de antenas en lo alto de los mástiles.

Existen, pues, límites a lo que se puede esperar de la investigación electromagnética y, a pesar de estos límites, la tarea es inmensa; la parte utilizada del espectro de las frecuencias, de por sí muy importante, crece sin cesar; el adversario desarrolla constantemente medios que ponen en acción nuevas técnicas; el éter está cada vez más repleto y la discriminación de señales es cada vez más delicada, porque las informaciones que se trata de obtener, afectan ya a la totalidad de los territorios adversos y de la superficie de los océanos. No obstante, las medidas de investigación electromagnéticas dan y hacen esperar resultados de calidad y potencia tales, que el interés que todas las naciones le prestan no cesa de aumentar.

V.- LAS CONTRAMEDIDAS ELECTRONICAS. (CME).

Las contramedidas electrónicas constituyen el segundo aspecto ofensivo de las acciones de guerra electrónica. De hecho, empleadas bien en ataque o bien en defensa, constituyen un arma cuya importancia y ventajas, considerables e insuficientemente reconocidas.

Si se exceptúa al propio hombre y a los procedimientos biológicos o químicos, los medios militares de acción pueden, recordémoslo, distribuirse en dos grupos:

- de una parte, los que tratan de reducir o de eliminar una capacidad de acción del adversario, atacando a los hombres y destruyendo materiales que constituyen en todo o en parte esta capacidad. Estos medios son los sistemas de armas;

- de la otra, los destinados a reducir o suprimir la capacidad del adversario atacando, con el emplo de ondas creadas por medios activos o pasivos, la electrónica necesaria para dicha capacidad. Estos medios, cuando las ondas se propagan por el éter, toman el nombre de contramedidas electrónicas activas o pasivas.

Esta somera clasificación conduce a una observación capital . Los medios biológicos o químicos atacan, casi exclusivamente, al hombre o a la naturaleza; los sistemas de armas atacan, casi ciegamente, al hombre, a lo que el hombre fabrica y a la naturaleza; unos y otros destruyen y matan, crean lo irreversible y lo insoportable.

Las ondas, por el contrario, sólo atacan al hombre de una manera excepcional, evitan la naturaleza en la mayoría de los casos y lo corriente es que no destruyan. No crean, salvo casos particulares (ondas sísmicas o ultrasonidos), ni lo irreversible ni lo insoportable.

Es, pues, evidente que si las armas de destrucción y sistemas de armas son medios del estado de guerra, medios cuyo uso puede acarrear la guerra, medios cuyo empleo, en realidad, caracteriza al estado de guerra, los medios de acción o de contramedidas electrónicas, por el contrario, son los medios privilegiados de las situaciones de crisis. Por ejemplo, interferir, en situación de crisis, las telecomunicaciones del adversario para dificultar el despliegue de sus fuerzas, es un acto agresivo, ciertamente, pero que no podría ser considerado como un "casus beli".

Tomememos, a título de ejemplo, el caso de una fuerza en la mar, o de un punto sensible, vigilado por un avión de reconocimiento. Contra esta aeronave se ofrecen dos posibilidades:

- destruirla con la ayuda de un misil o de un interceptador;

- neutralizar o engañar a uno o varios de sus medios electrónicos (radar de vigilancia, telecomunicaciones, sistemas de armas).

En situación de crisis, el medio electrónico, a condición de ser suficiente, será ciertamente el mejor, porque su empleo no compromete a las autoridades que controlan la crisis y no reducirá su capacidad de acción.

En situación de guerra, la elección se apoyará en criterios muy variados, porque el criterio "control de la crisis" quedará sin efecto. El medio electrónico tiene en su contra, su indiscreción, cosa que puede ser grave, y el hecho de que, acaso más que con el sistema de armas, no se puede tener la certeza absoluta de su eficacia. Por el contrario el medio electróni

co no se agota, no se consume, mientras que el sistema de armas dispone de una cantidad de municiones siempre limitada, y tanto más limitada cuanto que esta munición es costosa o difícil de almacenar.

Parece así que, cuando se determina el equipo de las fuerzas, los medios de contramedidas no deben ser considerados como un simple complemento. Se trata, por el contrario, en muchos casos, de una alternativa. El equilibrio a realizar entre el desarrollo de los medios de destrucción y el de los medios de contramedidas electrónicas, para una misión dada, debería, a falta de una experimentación que es imposible dirigir, ser fijada en función de los resultados de los estudios de investigación operativa, teniendo en cuenta la relación costo-eficacia de los diferentes medios y sus caracteres específicos.

Hemos visto, en el curso de la primera fase de este estudio, que las acciones de CME corresponden a dos aspectos que ya son clásicos: la interferencia y la decepción, a los cuales se añaden, particularmente en cuanto se refiere a las redes de transmisión automática, la saturación resultante de una intrusión "masiva" y la perturbación del funcionamiento de los ordenadores. Sólo recordaré, pues, muy brevemente, las principales características de la interferencia y de la decepción.

La interferencia puede ser activa: en este caso es producida por emisores de interferencia de barrera y periódicos; o pasiva, procedente de engaños, los más comunes de los cuales son los "chaffs"; las nubes de aerosoles, corrientemente menos empleadas, son asimismo muy eficaces.

Los emisores de interferencias de barrera son, por lo general, empleados a priori. Los periódicos, por el contrario, sirven para interferir una emisión que se manifiesta y cuyas características deben haber sido previamente determinadas por interceptación. El "acoplamiento" entre el receptor de interceptación y el emisor de interferencia puede ser asegurado por un operador que regula este último en la frecuencia exacta y la lanza. También puede asegurarse automáticamente, cosa indispensable en autodefensa para la interferencia de radares de armas o de misiles, a causa de la necesidad de reaccionar casi instantáneamente.

Los "chaffs", empleados para la interferencia, se extienden en forma de nubes reflectantes, que constituyen un muro o pasillo que garanti

za la detección. Las laminillas caen muy lentamente y las nubes conservan su eficacia durante varias horas.

La máxima eficacia se obtiene combinando los diferentes medios de interferencias, muro protector y emisores activos, para lo cual es preciso una estricta coordinación por parte del mando. El dominio de esta coordinación fue una de las causas principales del bajo rendimiento de la defensa aérea norvietnamita frente a los raids de la aviación norteamericana.

Hemos visto que entre las principales acciones de decepción, es decir, las que tratan de engañar al enemigo, está la intrusión, que consiste esencialmente en inyectar falsos mensajes en las redes de transmisiones del adversario; y la simulación, que apunta más generalmente a los sistemas de detección o a los sistemas de interceptación. Los procedimientos de simulación más corrientes son los emisores de interferencias respondedores, que devuelven al radar un eco falso, y los engaños ("chaffs" o aerosoles), expandidos convenientemente a fin de crear no un muro sino solamente uno o varios ecos de diversión, que los radares de vigilancia o de guiado, o los medios de interceptación (infrarrojo, por ejemplo), confunden con el eco real.

La parte y la importancia de las contramedidas electrónicas en la defensa contramisiles aumenta constantemente. La solución de los problemas que plantea su interceptación por armas de destrucción es, en efecto, bastante ardua y aleatoria. Los CME, por la rapidez de su puesta en acción y por la instantaneidad de sus efectos de interferencia y de decepción sobre el sistema de guiado del misil, ofrecen mucho mejores perspectivas de solución.

Para alcanzar su plena eficacia, el empleo de contramedidas eldctrónicas debe respetar ciertas condiciones.

La primera de éstas es el respeto a la doble obligación de no interferencia y de discreción. En efecto, por una parte, las emisiones de CME pueden dificultar el buen funcionamiento de los materiales de interceptación amigos, los de detección, etc. Por otra, con frecuencia son muy indiscretas y el efecto obtenido corre el riesgo de ser, en fin de cuentas, el opuesto al que se busca. Además la puesta en acción, a título preventivo, de ciertos medios de CME, puede constituir un aviso favorable al adversario.

Hemos visto, por otro lado, que los medios de contramedidas electrónicas (CME) constituyen un arma, arma de privilegio si no exclusiva de las situaciones en crisis, arma cuyo empleo, en las situaciones de guerra, debe ser sopesado y en todo caso coordinado con el de las armas de destrucción.

Resulta de ello, y esta es la segunda condición, que el empleo y la ejecución de las CME no pueden constituir una operación independiente. Teniendo en cuenta la situación política, estratégica o táctica y los objetivos a alcanzar, la organización establecida debe permitir, tanto al nivel de empleo como al de ejecución, una estrecha coordinación de los medios CME con las otras armas y medios de acción.

La tercera condición resulta del hecho de que los materiales de CME están impuestos en cierto modo por la técnica del adversario y que su eficacia depende absolutamente de su adaptación rigurosa a las características de los materiales enemigos que es preciso neutralizar, engañar o frustar. Es por ello por lo que, por ejemplo, los equipos CME para una misión aérea dada, deben estar exactamente adaptados a las características electrónicas de los radares y de los sistemas de armas tierra-aire o aire-aire con los que van a encontrarse los aparatos participantes en la misión. Y este es el porqué, entre otras razones, de tantas pérdidas aéreas israelitas en los primeros días de la guerra de octubre.

Pero el gran fallo de las CME reside en la incertidumbre existente en cuanto a su eficacia. Es difícil saber, por ejemplo, si el adversario emplea una técnica nueva para escapar de la interferencia o para discriminar los buenos ecos de los producidos por los engaños; como asimismo es difícil reconocer el grado de entrenamiento de sus operadores. Y esta incertidumbre pesa igualmente sobre los sistemas de armas, porque se sufre en esto, por lo general, un desconocimiento semejante al de las posibilidades de las contramedidas electrónicas del adversario.

VI.- LAS MEDIDAS DE PROTECCION ELECTRONICA (MPE).

Veamos ahora lo esencial de lo que es preciso saber a propósito de las medidas de protección propias de la guerra electrónica. Ellas constituyen el aspecto defensivo y comprenden dos categorías de medidas muy diferentes: las medidas de seguridad que se oponen a las investigaciones adversas y cuyo objeto es evitar la interceptación, o minimizarla; y

las medidas de defensa, que se oponen a las contramedidas electrónicas -cosa que les vale, a veces, el complicado nombre de contra-contra medidas (CCME)- y cuyo fin es la defensa contra la interferencia y la decepción.

Medidas de seguridad.

Las medidas de seguridad, lo mismo que las medidas de investigación, tienen varios objetivos:

- el objetivo técnico, que debe ser perseguido incluso en tiempo de paz, trata de preservar la sorpresa técnica. Esta sorpresa técnica previene del desarrollo por el adversario de materiales de investigación y de materiales de contramedidas, adaptados a los materiales amigos. Es importante, pues, que los datos susceptibles de informarle sobre éstos, estén rigurosamente protegidos.

- el objetivo operativo, que debe ser investigado desde el tiempo de paz, pero, sobre todo, en tiempo de crisis o de guerra, y que trata de prohibir al adversario la localización, la identificación y el conocimiento del despliegue de las fuerzas amigas. Es igualmente necesario para dejar al adversario en la ignorancia de las técnicas, como asimismo de las marcas y de las condiciones de empleo de los medios.

Además, las medidas de seguridad se dirigen a prohibir al adversario la apropiación y la comprensión de las informaciones transmitidas. En fin, tienen por objeto impedir que el adversario ponga en acción con éxito, sistemas de armas dirigidas sobre las radiaciones emitidas por los materiales amigos.

- La más general y la más importante de las medidas de seguridad es el silencio. Este confiere una seguridad absoluta; pero, a veces, sus inconvenientes pueden ser desproporcionados, porque priva de todo medio de detección, de transmisión, etc. Corresponde también al mando, asesorado por especialistas, el valorar para cada situación estratégica o táctica las ventajas y los inconvenientes del silencio, los riesgos de interceptación para tal categoría de emisión, tal gama de frecuencias, tal potencia, así como los peligros que acarrearía una interceptación.

El silencio se impone ya desde el tiempo de paz, de manera que deje al adversario en la ignorancia de las características técnicas, de las posibilidades, quizás incluso de la existencia de un material dado. Esta "discreción técnica" se inserta en el marco general del secreto industrial; a este respecto, las exportaciones deben ser controladas porque, aunque se imponen a los materiales exportados obligaciones de desmarcado, modificaciones o limitaciones, pueden constituir una fuente de información insustituible sobre el equipo de nuestras fuerzas.

Observemos además que las medidas de silencio electrónico deben ser equilibradas y generales; sería una aberración, en el plan operativo, privarse del empleo de un medio mientras que otro, igualmente indiscreto, permanece en servicio. Así, por ejemplo, las medidas de silencio radio deben estar rigurosamente coordinadas con las medidas de silencio sonar, etc. La estricta disciplina que se impone en esta materia solamente puede ser fruto del entrenamiento, y también del hábito.

Existen otras medidas de seguridad que si bien su eficacia es menos segura, en contrapartida no obligan tanto como el silencio; entre estas medidas hay tres que son de uso corriente:

- utilización de antenas direccionales,

- la limitación de la potencia radiada,

- las emisiones breves.

Las dos primeras de estas medidas limitan geográficamente la zona a partir de la cual es posible la interceptación . La tercera hace difíciles la interceptación, la goniometría, el análisis, así como la reconstitución de la información transportada. El empleo de emisiones breves es la medida que menos obliga en el plan operativo, pero también es la más delicada en el plan técnico y la más pesada en el orden financiero.

Al no poderse aplicar constantemente el silencio electrónico, y no aportar ninguna garantía absoluta las otras medidas de seguridad, deben tomarse determinadas disposiciones para limitar los efectos de la interceptación. La más eficaz y la más corriente de estas medidas es el cifrado. Bajo sus formas más modernas y más elaboradas, tales como el cifrado en línea o el cifrado de vía, este procedimiento puede ser considera

do, en cuanto se aplique a una transmisión por medios radiados, como una medida complementaria de seguridad electrónica.

Las medidas de defensa electrónica.

Las medidas de defensa electrónica tienen por objeto permitir el eficaz funcionamiento de los medios de radiación a pesar de las tentativas enemigas de interferencias o de decepción.

Para luchar contra las tentativas de interferencias se recurre a toda una serie de medidas que pueden ir desde el aumento de la potencia de los emisores propios, al empleo de antenas direccionales, de técnicas de modulación que hagan ineficaz el ruido, mejoramiento de la selectividad de los receptores, entrenamiento de los operadores para la regulación conveniente de su material y para distinguir la señal útil. Dichas medidas pueden, no obstante, ser insuficientes o de difícil aplicación. Entonces no queda otra solución que el cambio de frecuencia, medida de evasión eficaz pero a condición de haberla hecho posible en la concepción de los equipos y preparada por disposiciones reglamentarias, y el entrenamiento de los operadores.

Contra la decepción se actúa de suerte que la toma de contacto, por los sistemas de recepción, por los sistemas de tratamiento o por los explotadores, con las señales de decepción emitidas por el adversario, sea rechazada.

El medio más corriente para esto es la identificación, que consiste en comparar las características de la señal recibida con la señal deseada. La comparación puede realizarse electrónicamente y se refiere a las características técnicas de la señal (frecuencia exacta, longitud de impulsión, etc.); puede ser efectuada también por operadores y en este caso es la información transportada (el mensaje) lo que se confronta con lo que debería realmente ser, por ejemplo, mediante un código de preguntas y respuestas. La eficacia de la identificación depende estrechamente de la calidad del material y de la disciplina del personal. Así, un autodirector pasivo correctamente reglado y selectivo no se dejará confundir por un engaño infrarrojo simulador del escape de un reactor.

Digamos para terminar que las medidas de protección electrónica, como casi todas las acciones de guerra electrónica, exigen un conocimiento lo más elevado posible de los medios de todo orden de que disponga el adversario.

VII.- CONCLUSION.

El doble análisis que acabamos de efectuar, al examinar las acciones de guerra electrónica primero por campos de aplicación y luego por finalidades, ha producido, inevitablemente, algunas repeticiones. Pero al mismo tiempo ha permitido situar exactamente el impacto y la importancia de esta disciplina. Permite asimismo sacar a la luz ciertas características de la guerra electrónica:

La omnipresencia, ante todo, o la universalidad, porque la G.E. está presente en todas partes, en el tiempo de paz, crisis o guerra, en el espectro, desde las frecuencias más bajas a las más elevadas, y sobre todo en casi todas las formas de información, de transmisión o de acción.

La competitividad: los medios de G.E., efectivamente, no deben ser considerados como medios complementarios facultativos. Por el contrario, se trata de medios cuyo empleo debe ser sopesado con el de los medios clásicos, a los que puedan sustituir o complementar.

El tecnicismo: la eficacia de los medios de G.E. depende estrechamente de la valía del personal y de la calidad de los materiales de una tecnología de vanguardia.

La dependencia del adversario y sobre todo de su electrónica: no pueden existir MIE si el adversario no emite, ni CME posibles si aquél no emplea la electrónica.

Finalmente, el evolucionismo, porque en G.E. el éxito depende íntimamente de la aptitud para evolucionar constante y rápidamente, para adaptarse al adversario, para atacarle mejor y aprovechar los progresos técnicos para escaparse de él con más facilidad.

Costosos, difíciles, importantes por sus efectos, sus riesgos y sus implicaciones, los asuntos de G.E. deben ser dirigidos siguiendo -

una política rigurosa. Yo querría, a modo de conclusión, llamar una vez más la atención sobre dos principios fundamentales que, a mi entender, deben constituir la base de tal política: la integración y la coordinación.

La integración: esto quiere decir que la guerra electrónica debe integrarse en todas las formas de pensar y en la enseñanza, que debe estar en las misiones de los Ejércitos, que debe estar en la planificación de los sistemas de fuerzas, que debe integrarse en las estructuras orgánicas para que éstas permitan y faciliten la coordinación . Y esta coordinación debe aplicarse a las relaciones entre operadores, especialistas e ingenieros, al empleo de las MIE y de las otras fuentes de instrucción o de información, al empleo de las CME y de los sistemas de armas, al empleo de las medidas electrónicas de seguridad y de las demás medidas de seguridad y, en fin, deben aplicarse a la puesta en acción de los distintos medios de G.E. y de los restantes medios electrónicos. Tal es, a mi juicio, el Decálogo de la Guerra Electrónica. Ignorarlo conduciría inevitablemente a un Ejército a conocer el Infierno y la Derrota.

Que no se eche en cara al autor el no haber satisfecho el actual gusto por lo sensacional. En guerra electrónica no existe ni lo sensacional ni el milagro; además quienes saben no dicen nunca cuanto saben . Pero llegamos al término de este estudio, el lector debe tener, yo así lo espero, una idea suficiente clara de un asunto que es verdaderamente uno de los más vastos, de los más complejos y, sobre todo, uno de los más importantes, con los que los Ejércitos se han encontrado.
