LA GUERRA ELECTRONICA

UNA REALIDAD MAYOR

PRIMERA PARTE

Por

F. De QUEYLAR

Capitán de navío, Armada de Francia

Con la mutación que se aprecia, en la era de los misiles, en los medios de detección y de guía, la guerra electrónica ha tomado una nueva dimensión, revelada por la guerra de Vietnam y el reciente conflicto del Medio Oriente. No es más un fenómeno marginal, sino una realidad de todos los días y es, además, una forma de acción privilegiada en la conducción de las crisis.

L CUARTO conflicto árabe-israelí ha puesto de moda la guerra electrónica, especialmente con los SAM 6 y los SAM 7 y los esfuerzos desplegados por los israelíes para neutralizarlos.

¿Por qué este interés repentino, cuando para los especialistas, la guerra electrónica se remonta a más de medio siglo? Se sabe por ejemplo la ventaja que la escucha de las redes rusas ha dado a los alemanes durante la batalla de Tannenberg, episodio dramático del cual Soljenitsyn ha hecho el tema central de su novela "Agosto 1914".

La historia de la Segunda Guerra Mundial no es menos fértil en ejemplos variados de guerra electrónica: las maniobras de decepción efectuadas por los japoneses en sus redes de transmisiones radioeléctricas antes del ataque de Pearl Harbor, el empleo por los beligerantes de señuelos destinados a perturbar los radares y conocidos en esa época con el nombre de "windows", o también la confusión de frecuencias de guía de las bombas rasantes alemanas, etc. Más recientemente, la guerra de Vietnam ha ilustrado la importancia de la guerra electrónica en el duelo que oponen los sistemas tierra-aire a los aviones. El empleo racional y muy coordinado de los diferentes medios, tales como confusores

de barrera, confusores puntuales y señuelos variados ha permitido reducir a menos del décimo de su valor la eficacia de la defensa aérea nordvietnamita.

La guerra electrónica no es un asunto nuevo ni en su principio ni en sus diferentes aplicaciones, más cuanto no es el fruto de la imaginación de técnicos irrealistas. Si bien la guerra electrónica parecía ocupar, en Francia, un lugar muy modesto, es sin duda porque, salvo algunos asuntos de escucha, las guerras de Indochina y Argelia han sido guerras sin electrónica. Al menos uno de los adversarios tenía casi total falta de ella; sin duda porque el átomo, por su lugar eminente en el arsenal militar, eclipsó la electrónica de la cual, no obstante, es inseparable. Sin duda también porque la guerra electrónica aporta cambios importantes en la forma de pensar, de equipar las fuerzas y conducir las operaciones y que el cambio suscita recelo y reticencia. Finalmente, y por cierto, porque la guerra electrónica es cara o al menos parece cara de primera instancia. Aquí sucede, pues, como los seguros que no son deseados antes del accidente. La guerra de octubre de 1973 ha aportado la demostración.

El momento, entonces, ha sido bien escogido para abordar un asunto que los especialistas y técnicos han más o menos rodeado de un velo de esoterismo, contribuyendo a su desconocimiento. Para ello vamos:

— En primer lugar, a recordar la composición y las características esenciales de una "emisión" y precisar con este propósito el significado de algunos términos corrientes;

— Luego, a analizar, uno después de otro, los diferentes empleos que las Fuerzas Armadas hacen de la electrónica y de las ondas electromagnéticas, las vulnerabilidades que ofrecen, así como los medios de acción que están a su disposición;

— Finalmente, en una última parte, de manera sintetizada, a examinar las tres facetas más importantes de la guerra electrónica, es decir, por una parte las acciones ofensivas que son las "medidas de rebusca electrónica" (MRE), tendientes a la obtención de información del adversario y las "contramedidas electrónicas" (CME) tendientes a entorpecer (por la confusión) o a engañar (por ej. creando ecos falsos) la electrónica adversaria; por otra, 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 CME adversarias.

ACCIONES OFENSIVAS	ACCIONES DEFENSIVAS
MRE (Obtener información)	Medidas de Seguridad
CME (Entorpecer o engañar al enemigo)	Medidas de Defensa

MPE

Será posible, entonces, extraer los aspectos generales de la guerra electrónica y evidenciar los elementos esenciales de una política tendiente a integrar correctamente las acciones de guerra electrónica en el conjunto de las acciones militares.

Pero antes de emprender, de este modo, el estudio de esta materia, extremadamente vasta y compleja, es indispensable que sean fijados límites tan exactamente como sea posible.

En su acepción admitida más generalmente, la expresión "guerra electrónica" se aplica a la totalidad del espectro de frecuencia, pero no se refiere sino a las ondas electromagnéticas, es decir, las ondas que se propagan en el éter. En lo que toca a las ondas sonoras, a las ondas sísmicas, así como a las ondas que

se propagan en el medio marino, corrientemente no se consideran como formando parte, estrictamente, de lo que se denomina "guerra electrónica". En realidad las fronteras no son tan claras y es normal, tratándose de un campo en plena expansión.

Todo el mundo afirma, por ejemplo, que las ondas radio-eléctricas de gran longitud (varios kilómetros) penetran en el agua. Se afirma también que las ondas extremadamente largas pueden tener efectos ecológicos muy importantes. Además, en el medio marino se encuentran con los ultrasonidos prácticamente todos los problemas que posee la guerra electrónica por encima de la dioptra con las ondas electromagnéticas.

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

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

— El apoyo, que constituye la base de todas las emisiones.

— El mensaje, que es facultativo y no existe, en general, sino en las emisiones de transmisión, de identificación y, algunas 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 encaminamiento correcto de esta información.

El apoyo no tiene significación intrínseca. Sin embargo, su lugar en el tiempo o el valor de algunas de sus características comparado a los valores de referencia pueden constituir informaciones. Así, la dirección de propagación da la del emisor; la variación de frecuencia permite medir el efecto doppler y conocer así la componente radial de la velocidad del generador del eco; la variación de fase permite las mediciones de tiempo, de allí la distancia.

Además, algunas características de apoyo, tales como la frecuencia, la amplitud de onda, la longitud de impulsos, son susceptibles de indicar la función del emisor o su naturaleza. Se señala también la riqueza de informaciones que puede aportar una radiación electromagnética con el solo hecho de su existencia.

El mensaje representa en sí una información intrínseca que la señal-apoyo está encargada de transportar del emisor o respondedor hasta el receptor. Esta información puede representarse bajo una forma numérica o analógica y ser una imagen, un sonido, una seña, un dato que, eventualmente, habrá sido codificado o cifrado previamente.

Este análisis es necesario para comprender bien el interés y la vulnerabilidad que presentan las emisiones electromagnéticas, cuáles ventajas puede presentar su recolección para el adversario y cuáles acciones pueden conducirse para atacar, perturbar o, al contrario, proteger tales emisiones. Además, para una buena comprensión de la materia, recordaré aquí algunas definiciones elementales:

— Se denomina "alerta" electrónica a toda acción tendiente a la recolección de emisiones electromagnéticas.

— Si la emisión recolectada es una emisión amiga, hay "recepción", si es adversaria, "interceptación".

— Desde el momento que el objetivo de la interceptación es la apropiación de un "mensaje" por otro que no sea su destinatario, el término de "escucha" es empleado con preferencia al de "alerta".

OMNIPRESENCIA DE LA ELECTRONICA EN MATERIA DE DEFENSA

Toda organización, todo sistema, exige para su funcionamiento una cadena creciente de informaciones para la toma de decisiones y una cadena descendente de órdenes necesarias para la ejecución de la decisión y para la acción. Esto es efectivo en las FF.AA., así como para una organización del más alto nivel, tanto para el mando estratégico, como para un sistema de nivel más elemental como el auto-director de un misil.

Recolección de información	— detección electromagnética — sistema de identificación — alertas (radio, radar, infrarrojo) — sistema de ayudas a la navegación
Transmisión de la información	— telecomunicaciones por vía hertziana
Decisión	
Transmisión de las órdenes	— telecomunicaciones por vía hertziana
Medios de acción	— sistemas de armas — contramedidas electrónicas.

La tabla de arriba indica de manera más bien esquemática los principales medios que pueden constituir la cadena de información y la cadena de acción y que emplean, en diferentes grados y bajo diversas formas, todas las ondas electromagnéticas. Todas, en consecuencia, pueden ser vulnerables a las acciones de guerra electrónica del adversario y tienen, por consiguiente, necesidad de ser protegidas. Todas además, por la interceptación de sus emisiones, arriesgan dar al adversario informaciones preciosas. Estas son las vulnerabilidades, las acciones y los riesgos que vamos a estudiar.

I. LA RECOLECCION DE LA INFORMACION

La detección electromagnética

Los radares son el elemento esencial de la detección electromagnética, hoy día, una de las bases de la información táctica.

Son vulnerables y su neutralización puede ser obtenida ya sea por medios activos, los confusores, que emitiendo en la frecuencia dé trabajo del radar saturan la recepción e impiden la percepción del eco, ya sea por medios pasivos, los señuelos, utilizados en barrera y que forman un muro reflector tras el cual el objeto rebuscado escapa a la detección. Estos señuelos (en inglés: chaffs) se presentan a menudo bajo la forma de cintas o agujas metalizadas cuya longitud es (evidentemente) adaptada a la de la onda a reflejar y que son esparcidas en nubes dispuestas de manera tal de proteger en la mejor forma el objeto cuya detección debe ser evitada.

Los radares son igualmente vulnerables a las acciones consistentes en producir con los confusores y señuelos de tipos especiales, ecos de diversión. Estas acciones tendientes a engañar al enemigo forman parte de lo que se denomina la "decepción".

Así, durante la última guerra, ocurría que los submarinos soltaban un globo sosteniendo un cilindro metálico cuyo freno penetraba en el agua frenándolo a la deriva. Los escoltas tomaban contacto con este objeto en el radar y, si la noche era suficientemente opaca y la visibilidad mala, lo confundían con el snorkel del submarino perseguido, el que alejaba así el peligro.

Frente a estas acciones opuestas, el radar no queda sin defensa; la inteligencia de aquellos que lo han construido, la de los que lo sirven vienen en su auxilio. Los medios de defensa más corrientes, y que forman parte de lo que se ha dado

en llamar en guerra electrónica las "medidas de defensa" son variadas. Citemos entre otras, los cambios de frecuencia para escapar a la confusión, los cambios de tipo de emisión para hacerla inoperante, la capacidad para eliminar a priori los ecos que presentan ciertas características. Estos medios de defensa pueden ser manejados ya sea por el hombre, el operador que ha debido recibir para ello un entrenamiento extremado, ya sea por un ordenador de control que reaccionará más rápida y seguramente que el hombre, salvo si se encuentra ante una dificultad imprevista, siempre posible, si no probable, en guerra electrónica.

El principal defecto táctico del radar es su indiscreción inherente a la potencia radiada; la distancia a la cual se puede interceptar un radar es muy superior a aquélla a la que él mismo es capaz de detectar. En todo caso, y especialmente si se trata de radares fijos y bien conocidos, esta indiscreción es sin importancia. En otros casos, por el contrario, la discreción puede ser considerada más importante para el vector que lleva el radar que la capacidad de protección que procura. La elección del régimen y condiciones de empleo es en ese caso un asunto de comando. Es en este último, es decir en lo operativo y no en lo técnico, que se decide en función de la misión y de los riesgos implicados por una u otra solución.

La identificación electrónica

En razón del aumento de la velocidad de los móviles, el aumento del alcance de los radares y el de las armas, del desarrollo de los medios de visión nocturna, se vigila y se batalla cada vez más distante. La distancia o la noche impiden en lo sucesivo la identificación visual: la identificación debe ser a distancia y en "todo tiempo". Además, en un combate que se expone a tomar una forma confusa, debe ser tan rápida, precisa y segura como sea posible. No puede ser, entonces, sino electrónica.

Se dice que los elementos de identificación constituidos en gran parte por los equipos conocidos bajo el nombre de IFF (Identification Friends and Foes) son, como los materiales de detección, vulnerables a la confusión y a la decepción Como ellos, son indiscretos, pero en razón de la debilidad de su potencia de emisión comparada a la del radar al que están asociados generalmente y la directividad de sus componentes aéreas, su indiscreción es muy a menudo sin importancia. De hecho, es la vulnerabilidad a la decepción que es por mucho lo más grave; así se ha llevado, inspirándose en los procedimientos de cifrado, a desarrollar materiales de identificación cada vez más protegidos y, por consiguiente, cada vez más elaborados y costosos.

La rebusca electromagnética

La recolección de radiaciones electromagnéticas emitidas por el adversario constituye otra fuente de informaciones. Esta recolección presenta la ventaja considerable de ser, salvo casos muy excepcionales, perfectamente discreta. En cambio, no es posible sino en la medida que el adversario sea asimismo indiscreto. Su eficacia es entonces incierta y es necesario cuidarse de sacar de una ineficacia aparente conclusiones precisas.

Las alertas son evidentemente sensibles a la confusión, pero, por paradojal que ello pueda parecer, es la confusión por los amigos la que está, muy a menudo, en juicio. Un emisor amigo, perteneciente a la misma unidad o a una unidad vecina, estará casi siempre más cerca que el emisor que se busca interceptar. Por poco que este emisor amigo trabaje o emita armónicas en una frecuencia vecina de la frecuencia a interceptar, las posibilidades de interceptación serán reducidas. Las alertas imponen por consiguiente severos esfuerzos de coordinación.

Las alertas, finalmente, son vulnerables a la acción de la decepción. Para comprender bien esta vulnerabilidad, es necesario conocer los principales objetivos de las alertas de interceptación. Estos objetivos pueden ser clasificados en 4 categorías:

—**La información electromagnética técnica:** esta rebusca tiende, esencialmente, al conocimiento de las características técnicas de los medios de que dispone el adversario en general (o en particular, por ejemplo, tal aspecto para equipar tal tipo de avión). Permite además prever los medios de CME o tomar las medidas de protección adaptadas.

Contra este tipo de información, la mejor acción es la interdicción o la limitación de las emisiones cuyas características se desea ocultar. Así los egipcios tuvieron, verosímilmente, la prudencia de no servirse, con fines de entrenamiento o ajuste, de sus SAM 6 antes del día del ataque; los israelíes desconocieron la presencia de estos SAM 6 y sus características exactas, no pudiendo por tanto, prever contramedidas correctas.

—La información operativa o técnica: cuyo objetivo principal es el conocimiento de la presencia y el dispositivo del adversario, la localización de sus fuerzas, su identificación. Esta rebusca implica generalmente la goniometría de las emisiones interceptadas y su análisis con fines de identificación por comparación.

Frente a la información operativa, es relativamente fácil engañar las vigilancias adversarias al simular, por ejemplo, por medio de red de radio ficticia, la presencia de fuerzas allí donde no hay más que emisores-trampas. Las operaciones de goniometría, además, sobre todo las que necesitan de relevos simultáneos por varias estaciones, demandan un mínimo de tiempo; el empleo de emisiones extremadamente breves, de una duración del orden de algunos milisegundos, hacen estas operaciones muy difíciles.

—La información necesaria para el empleo de sistemas de armas o de contramedidas: que puede implicar, según el caso, una localización extremadamente precisa, la interceptación de emisiones particulares (tales como las emisiones infrarrojas de los escapes libres de reactor) o la determinación precisa de características cuyo conocimiento es necesario para la utilización óptima de confusores. Esta información con carácter específico es a veces identificada bajo la denominación "medida de apoyo de guerra electrónica" (MAGE).

Las emisiones tenidas en vista por este tipo de información son voluntarias (radar) o involuntarias (radiación infrarroja). Permiten, gracias a su interceptación por los materiales apropiados, la conducción pasiva hacia el objetivo emisor de un misil o todo otro móvil. Para el objetivo, la mejor defensa consiste en engañar al misil, por ejemplo, por medio de bombas de accionamiento térmico lanzados por cohetes y simulando la radiación infrarroja del objetivo.

—La información general: es decir, aquella concerniente a las acciones y las actitudes e intenciones del adversario. Semejante tipo de información será, muy a menudo, proporcionada por el examen de las condiciones de empleo de los medios electrónicos adversarios y sobre todo por la interceptación de mensajes (es decir, por las escuchas) y si es necesario, su desciframiento e interpretación. Citemos, a título de ejemplo de información proporcionada por una variación de las condiciones de empleo, el caso siguiente, muy clásico: el radar adversario que Uds. interceptan aumenta su velocidad de rotación de antena, reduce la longitud de impulsos de emisión, así como su intervalo; ello significa que el radar pasa de un uso de "alerta" a un uso de "ataque" y que un tiro es inminente.

Frente a acciones tendientes a la rebusca de información general, se pueden emprender acciones de decepción, por ejemplo, haciendo variar, de manera artificial, la densidad del tráfico en una red de transmisiones, para hacer creer en un cambio de actividades; o aun haciendo interceptar mensajes falsos que, a los ojos del interceptor, en nada se distinguen de los verdaderos.

En conclusión, si las alertas de interceptación son, cual sea su objetivo, un medio de información notable y, en muchos casos, irreemplazable, no constituyen una panacea: pueden ser ineficaces si el adversario se silencia; pueden hacerse restrictivas si conducen a limitar las emisiones amigas y, finalmente, engañosas si dan lugar a resultados erróneos como resultado de una contraacción enemiga de decepción.

Las ayudas radio-eléctricas a la navegación

Cumpliendo misiones de información o misiones de acción, los móviles amigos se desplazan cada vez más rápido en latitudes cada vez más vastas. Para informar con exactitud o para actuar en condiciones óptimas, deben en todo momento, conocer su posición con seguridad y precisión. Cierto, existen para ello sistemas de navegación inercial, pero son onerosos y necesitan reajustes muy fre-

cuentes; en su defecto se utilizarán sistemas radio-eléctricos cuyos principios de funcionamiento y longitudes de onda variarán según el alcance y la precisión requeridas.

No es cuestión aquí de describirlos todos, su gama se extiende desde sistemas de cobertura mundial, empleando ondas muy largas o el relevo de satélites, a los sistemas de muy corto alcance como por ejemplo los materiales de aterrizaje sin visibilidad, las sondas altimétricas o algunos radares llamados de evitación de obstáculos. Digamos solamente que estos sistemas presentan las mismas vulnerabilidades que todo sistema electrónico, son sensibles tanto a la confusión como a la decepción, sin embargo, la una y la otra no son, en general, fácilmente realizables por el adversario sino en 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 incierto de frecuencias o en la utilización de señales codificadas que puedan ser distinguidas de las falsas señales.

Deberán ser tomadas, además, algunas precauciones de camuflaje técnico, tales como el desajuste de fase o desajuste temporal, para evitar que el adversario utilice en su provecho su sistema de ayuda a la navegación.

II. TRANSMISION DE LAS INFORMACIONES Y ORDENES

Las informaciones recolectadas no serán útiles sino en la medida que ellas lleguen bajo una forma explotable al centro de décisión, en beneficio del cual ellas han sido colectadas, que este centro de decisión sea el puesto de mando en jefe de un teatro de operaciones cubriendo la cuarta parte del globo o el minicalculador de un misil, destinado a controlar su navegación y a actuar en sus gobiernos. Innumerables medios pueden, según el caso, permitir este encaminamiento ascendente de la información y, una vez tomada la decisión, la descendiente de la orden de acción. No nos interesan sino aquellas que emplean las ondas hertzianas.

Los receptores amigos encargados de recibir, en beneficio del centro de decisión, en ascenso, en beneficio del órgano de ejecución, en descenso, son sensibles a la confusión. Considerado esto es que se puede saber los medios de que dispone el adversario, la eventualidad de confusión, si no una certeza, al menos una fuerte probabilidad.

Existen, sin embargo, acciones en la confusión: así, el cambio de frecuencia, ejecutada a priori o en reacción a la confusión. Este procedimiento es eficaz en la medida que el confusor no tenga la posibilidad de "seguir" o tiempo de hacerlo. Exige una perfecta coordinación entre el emisor y el receptor, coordinación que necesita de 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 disminuir al mínimo los efectos de la confusión. Señalemos también que el empleo de aéreos direccionales no solamente aminora la calidad de la recepción sino que puede reducir notablemente los riesgos de confusión.

Finalmente, además, existe otro peligro para los sistemas de comunicaciones, cualesquiera que sea: el de la intrusión, acción consistente en que un extraño se introduzca en una red afín y allí hacer circular informaciones erróneas u órdenes engañosas o simplemente otros mensajes cualesquiera, pero en cantidad y urgencia tales que la red en cuestión sea sobrecargada. Esto exige que el intruso conozca ciertas características técnicas de la red, a falta de las cuales la señal introducida no sería ni recibida ni demodulada por el receptor; exige también que el intruso conozca algunas reglas de explotación de la red, y en particular, aquellas relativas a las que he señalado más arriba; exige finalmente, que conozca el ciframiento o el código eventualmente empleados por la víctima. La intrusión es por tanto más o menos fácil y tiene más o menos posibilidades de éxito según el tipo de red atacada. El emisor intruso debe en alguna medida mostrar señas de identidad con el adversario, y en el caso preciso de la fonía, el sexo de la persona que habla, su acento, su pronunciación son, si se puede decir, los elementos esenciales de la identidad. Agreguemos a eso, que ningún emisor es rigurosamente idéntico a otro; tiene una personalidad que los operadores entrenados llegan a reconocer.

Todas estas dificultades no son, sin embargo, suficientes para desalentar al intruso y consagrar su acción al fracaso. Así pués, se ha llegado a desarrollar sistemas de identificación destinados a aportar al receptor la prueba que el emisor es realmente aquél que él cree y que la comunicación es por consiguiente "auténtica". No obstante, la autentificación no procura una seguridad absoluta, ya que el intruso ha podido apoderarse de la clave o reconstituirla, sobre todo si la víctima ha hecho uno inconsiderado o no ha respetado las reglas de procedimiento.

Finalmente, es necesario notar que el desarrollo de la tele-informática y las transmisiones de datos aporta a la intrusión un campo de acción nuevo y aun malamente conocido; el intruso puede no solamente dirigir una falsa información o una falsa orden, sino también perturbar el funcionamiento del ordenador.

Terminaré con la intrusión al citar, a manera de recuerdo, el caso especial que es la guerra de ondas en radiodifusión: el intruso, para tener todas las posibilidades de ser recibido por los auditores, emite en la frecuencia del vecino, pero no busca encubrir su identidad, muy por el contrario, y hay más usurpación del derecho de uso de la frecuencia que intrusión en el sentido "guerra electrónica" del término.

III. LOS MEDIOS DE ACCION

Los Sistemas de Armas

Un sistema de armas (la expresión "sistema de armas" califica corrientemente los sistemas muy complejos que pueden responder a varias finalidades y ser descompuestos en sistemas de armas "unitarios", por ejemplo un avión de interceptación que contiene un misil aire-aire autoguiado) puede ser definido como un conjunto ordenado de medios cuya finalidad es, en general, provocar a distancia útil del objetivo que se intenta destruir, la explosión de una carga, que ha sido necesario previamente conducir en buena posición. Esta operación se hace en tres fases: la "obtención" del objetivo, la "guía" eventual del portador, el "disparo" de la explosión. La intervención de la electrónica en el cumplimiento de estas tareas varía según el grado de elaboración del sistema. Examinamos por ejemplo, el caso de un sistema de armas superficie-aire o tierra-aire en el cual la electrónica es, en general, empleada bajo variadas formas.

"La fase de obtención" comprende la rebusca, exploración y localización del objetivo, generalmente mediante radares de vigilancia, que pueden ser independientes del sistema de armas propiamente dicho. Esta primera localización permite entonces apuntar al 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 su "ventana" de distancia, estos radares de tiro presentan vulnerabilidades especiales y restricciones de empleo aumentadas. Deben, para cumplir su función, permanecer apuntados al objetivo; si lo pierden, sea como consecuencia de confusión, sea a causa de movimientos de evasión del objetivo o si son engañados por falsos ecos, toda la secuencia de obtención deberá reiniciarse a partir de los elementos proporcionados por el radar de vigilancia; durante este tiempo el objetivo será sacado del campo de tiro del sistema de armas, que queda así inoperante. Los radares de tiro pueden además ser particularmente indiscretos y sus características especiales facilitan su identificación. El objetivo puede, finalmente, si es provisto de un detector de radar apropiado, descubrir a tiempo la amenaza que pesa sobre él.

"La fase de guía" puede ser conducida de diferentes maneras. Los cuatro métodos siguientes son los generalmente más usados, separada o conjuntamente:

El tirador determina en el radar las posiciones relativas del objetivo y del misil, elabora y envía a este último las órdenes de navegación. Para defenderse el objetivo debe confundir o engañar, ya sea el radar del tirador, ya sea al sistema de transmisión de orden; es un problema que hemos examinado pero presenta aquí dos particularidades:

—El objetivo no tiene sino un lapso muy breve para determinar las frecuencias a confundir y disparar la confusión.

—La emisión de confusión corre el riesgo de servir a la autoguía pasiva del misil.

La solución de decepción es, por consiguiente, en el mejor de los casos, preferida. Consiste, recordemos, en crear falsos ecos.

—El tirador destella al objetivo, el misil recibe el eco del destello reflejado por el objetivo y determina así, él mismo, sus propios elementos de navegación. Para el objetivo, la mejor defensa consiste en engañar al receptor del misil creando una confusión entre el eco verdadero y los ecos de decepción.

—El misil posee su propio radar: ésta es la autoguía activa. Para el objetivo el problema es prácticamente el mismo que el anterior; la mejor solución es el empleo de señuelos generando falsos ecos o el empleo de confusores especiales que modifican las características del eco principal.

—El misil recibe emisiones voluntarias o involuntarias del objetivo (emisión de radar - emisión infrarroja) o ve el objetivo (cámara de TV). Para el objetivo, es necesario crear emisiones parásitas a fin de engañar al misil.

"En la fase de disparo de la explosión" se trata de medir una distancia, en general muy corta, de una forma precisa. La tarea será cumplida ya sea por el misil mismo —y la variedad de métodos posibles hacen la defensa del objetivo casi imposible, en la ignorancia de cuál es el empleado— ya sea por los radares de tiro, y entonces se vuelve a llegar a los problemas precedentes.

Las Contramedidas Electrónicas

Los medios de contramedidas electrónicas (CME) constituyen otro medio de acción contra el adversario; su empleo, tiende, en efecto, a reducir algunas de sus capacidades de información y de acción o bien a anularlas.

Los medios de CME se reparten en medios de confusión y medios de decepción: "los medios de confusión" se subdividen a su vez en medios activos o confusores y en medios pasivos o señuelos, tales como los "chaffs" (que propalados en nubes, constituyen un muro reflector de las ondas de radar). Los medios de "decepción" se subdividen igualmente en medios activos (esencialmente la intrusión en las redes adversarias) y medios pasivos (señuelos puntuales dando ecos falsos comparables con los del objetivo).

La principal debilidad de los confusores es su indiscreción, que deriva fatalmente del poder radiado necesario para vedar al adversario la recepción de sus propias emisiones. Además, este adversario —se trate de operadores o de ordenadores que manejan los medios de recepción— puede llegar a extraer del conjunto de ruidos la señal útil. Por consiguiente, la confusión corre el riesgo de ser poco eficaz en la medida que conserve enteramente su defecto de indiscreción.

La intrusión presenta los mismos inconvenientes para el que intenta penetrar en las redes adversarias para saturarlas o engañarlas. El intruso está obligado a emitir y por consiguiente a ser indiscreto.

Los medios activos de CME son también posibles víctimas de la guerra electrónica y las medidas de rebusca electromagnética (MRE). Este vuelco de la guerra electrónica contra ella misma es una de las razones de su extrema complejidad.

Es sobre esta reflexión que terminaré el examen del impacto de la guerra electrónica en los principales medios y sistemas que utilizan de una u otra manera las ondas electromagnéticas.

SEGUNDA PARTE

Señalemos en primer lugar las tres finalidades de la guerra electrónica:

—Se trata, en primer lugar, de utilizar las radiaciones electromagnéticas emitidas, voluntariamente o no, por el adversario para informarse o para actuar a sus expensas;

—Se trata luego de generar la electrónica opuesta con el objeto de hacer inoperante su empleo, igualmente peligrosa por engañosa;

—Y, finalmente, se trata evidentemente de procurar preservar la eficacia del empleo de nuestra electrónica, privando al adversario de las ventajas que le procuraría la interceptación de las ondas hertzianas emitidas por nosotros.

LAS MEDIDAS DE REBUSCA ELECTROMAGNETICA (MRE)

Las medidas de rebusca electromagnética tienen por finalidad la obtención de informaciones sobre el adversario. Hemos visto las cuatro categorías de informaciones rebuscadas: información técnica - información operativa o táctica —empleo de sistema de armas y contramedidas electrónicas (CME)— información general; hemos visto, igualmente, que esta rebusca se aplica a la casi totalidad de los campo de las ondas electromagnéticas.

Del análisis al cual hemos procedido, deriva la definición de las diferentes tareas de la rebusca; se comprende además la necesidad de la inserción de las MRE en el conjunto vastísimo de la información y datos sobre el adversario así como las restricciones a admitir si se tiende a evitar las interferencias que pueden provenir de medios amigos que irradian.

Las diferentes fases de una operación de rebusca son: la vigilancia del espectro, es decir, de la banda de frecuencias en las que se llevan las investigaciones —el análisis en tiempo real — el registro — el análisis diferido o tratamiento — la memorización — la identificación — la alerta y la localización.

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

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

El registro es necesario en vista de la decodificación o del desciframiento ulterior de los mensajes interceptados; es igualmente necesario para el análisis más completo que será efectuado en laboratorio.

"El análisis diferido o tratamiento" es una de las fases esenciales de la rebusca de información técnica. Necesita muy a menudo la aplicación de medios informáticos y requiere un personal muy especializado. Por estas razones, las operaciones de tratamiento son, en general, confiadas a los organismos especializados dependientes de los grados más elevados del mando.

Las características de las emisiones adversarias deben ser "memorizadas", por una parte, en beneficio de los técnicos que estudian, en particular, los materiales futuros de contramedidas electrónicas (CME) y la protección de nuestros propios materiales; por otra, en beneficio de las fuerzas operativas con el fin de facilitarles la identificación de las emisiones interceptadas en el curso de rebuscas ulteriores.

"La identificación", muy a menudo por comparación entre las características medidas por el análisis inmediato y las comunicadas por los organismos especializados que hayan practicado el análisis diferido, es una operación capital en el campo de la táctica. En efecto, la identificación de la señal permite la del emisor y por vías de la consecuencia, la del portador. Por ejemplo, habiéndose interceptado una emisión de radar de un avión adversario se conocerá el tipo de este avión incluso antes de haber obtenido la imagen en la pantalla del radar.

La interceptación de una emisión adversaria permite determinar la dirección en la que se encuentra el emisor. Permite entonces una "localización" parcial. El poder de la señal interceptada puede, si se conocen las características del emisor, dar una idea de la distancia de él. Pero una localización completa y precisa necesita que la emisión adversaria haya sido relevada por otras estaciones de interceptación, de donde la noción de cadena de goniometría comprende varias estaciones que se dan la alerta de que una emisión adversaria es interceptada.

Los detectores de "alerta" tienen una tarea bien precisa: la de advertir la proximidad de un radar adversario en funcionamiento. Se trata entonces de un equipo esencial en particular para las aeronaves que no tendrían otros medios de saber si son cogidos en el haz de un radar de defensa aérea o de un radar de armas o también de un radar autodirector de misil. Los detectores elaborados indican el tipo de radar interceptado.

Evidentemente, todas estas tareas no son siempre imperativas. Según el objetivo rebuscado, algunas podrán ser omitidas. Su enumeración permite, sin embargo, apreciar la complejidad del asunto, complejidad que se agrava por la necesaria coordinación de las medidas de rebusca electromagnética con las otras fuentes de informaciones.

En efecto, trátese de información técnica, información operativa, información general, incluso empleo de sistemas de armas y de contramedidas (CME) la información electromagnética obtenida por la interceptación de radiaciones electromagnéticas adversarias no es ella sola fuente de información.

En el campo técnico, las publicaciones extranjeras, la observación visual, entre otras, son igualmente fuentes muy importantes. Conviene por lo tanto que el empleo y los resultados de todas estas fuentes sean coordinados y correlacionados: semejante tarea necesita de la implantación en el escalón nacional de organismos especializados y exige una estrecha colaboración entre militares e ingenieros.

En el plano táctico, es en tiempo real o apenas diferido, y es a nivel de las fuerzas que debe hacerse la coordinación del empleo con los medios "clásicos" (detección de radar, vigilancia óptica, etc.). Es en las mismas mesas de ploteo o en las mismas consolas de visualización que deben ser llevadas las diferentes informaciones. La eficacia de tal coordinación ha sido demostrada repetidamente.

Corresponde al Mando, en función por un lado de las condiciones tácticas (amenazas previsibles, discreción necesaria, etc.) y por otro de las ventajas e inconvenientes de los diversos medios (por ejemplo, seguridad, precisión pero indiscreción del radar - incertidumbre, imprecisión pero discreción de los elementos de interceptación) elegir y fijar las condiciones de empleo de uno y de otros. Con un poco de oportunidad, algunos errores del adversario y una buena coordinación de los medios, la interceptación proporcionará el preaviso y la identificación del enemigo, luego el radar que se habrá empleado oportunamente dará una localización precisa.

También es necesaria una estrecha coordinación; se tiende a evitar que la interceptación no sea incomodada, hasta imposibilitada, por el empleo de medios amigos, tales como emisores próximos y poderosos trabajando en las frecuencias vecinas o confusores atacando las emisiones que se busca precisamente interceptar. Es por lo tanto imperativo que estas coordinaciones sean organizadas, tanto en el estado de preparación y de conducción de las operaciones como en el de ejecución de las tareas y del empleo de los medios.

Para terminar con las medidas de rebusca es necesario tomar en consideración una última restricción que deriva de las condiciones de propagación de las ondas. En efecto, si, más que toda fuente de información, la radiación electromagnética viene hacia Uds., no lo hace adonde Uds. están, el interceptor puede estar alejado, encontrarse en una zona de sombra o también fuera del lóbulo de emisión. Por otra parte, para ser eficaz, la interceptación exige un material apropiado.

El problema es, entonces, conducir este equipo a buen sitio y en el momento propicio. En el plano estratégico, satélites de reconocimiento electromagnético, buques y aviones especializados constituyen las soluciones; las estaciones fijas serán implantadas cerca de las fronteras, en lo posible, en las alturas o a lo largo de las costas. En el plano táctico, las soluciones eran análogas: empleo de medios aéreos, rebusca de puntos altos, y en los buques, instalación de medios aéreos en el tope del mástil.

Existen, por tanto, límites en lo que se puede esperar de la rebusca electromagnética, y a pesar de estos límites, la tarea es inmensa; la parte utilizada del espectro de frecuencia, ya muy considerable, crece sin cesar, el adversario desarrolla constantemente los medios empleando técnicas nuevas, el éter es recargado cada vez más y la discriminación de las señales es cada vez más delicada, las informaciones que se busca obtener, conciernen de ahora en adelante, a la totalidad de los territorios adversarios y de la superficie de los océanos. Sin embargo, las medidas de rebusca electromagnéticas dan y hacen esperar resultados de una calidad y una potencia tal que el interés que todas las naciones le otorgan no cesa de aumentar.

LAS CONTRAMEDIDAS ELECTRONICAS (CME)

Las contramedidas electrónicas constituyen el segundo aspecto de las acciones de guerra electrónica. De hecho, utilizadas ya sea en ataque o en defensa, constituyen un arma de la cual desearía indicar la importancia y las ventajas, en mi opinión considerables e insuficientemente reconocidas.

Si se exceptúa al hombre mismo y a los procedimientos biológicos y químicos, los medios militares de acción, tengámoslo presente, pueden repartirse en dos grupos:

—Por una parte, aquellos tendientes a reducir o eliminar una capacidad de acción del enemigo batiendo a los hombres y destruyendo los materiales que constituyen en todo o en parte esta capacidad. Estos medios son los sistemas de armas;

—Por otra, aquellos tendientes a reducir o suprimir una capacidad del adversario perjudicando, por intermedio de ondas producidas por los medios activos o pasivos, la electrónica necesaria a esta capacidad. Estos medios, cuando las ondas se propagan por el éter, toman el nombre de medios de contramedidas electrónicas, activas o pasivas.

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

Las ondas, en cambio, no atacan al hombre sino de una manera enteramente excepcional, perdonan la naturaleza en la inmensa mayoría de los casos y muy a menudo no la destruyen. No crean, salvo casos particulares (ondas sísmicas o ultrasonidos), ni lo irreversible ni lo insoportable.

Parece evidente entonces que si las armas de destrucción y sistemas de armas son los medios del estado de guerra, medios cuyo empleo arriesgan conducir a la guerra, medios cuyo empleo, de hecho, caracterizan el estado de guerra, los medios de acciones o contramedidas electrónicas, en cambio, son los medios privilegiados de las situaciones de crisis. Así, confundir en situación de crisis las telecomunicaciones del adversario para dificultar el despliegue de sus fuerzas es un acto agresivo, cierto, pero que no podrá ser considerado como "casus belli" (motivo de guerra, N. del T.).

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

—Destruirla con la ayuda de un misil o un interceptor.

—Neutralizar o engañar 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 lo mejor, por cuanto su empleo no atará a las autoridades que controlan la crisis y no reducirá su libertad de acción.

En situación de guerra, la elección se apoyará en criterios muy diferentes ya que el criterio "control de la crisis" no tendrá objeto. El medio electrónico tiene en su contra su indiscreción, la que puede ser grave, y el hecho que, más que nada para los sistemas de armas, no se puede tener la certidumbre absoluta de su eficacia. En cambio, el medio electrónico no se debilita, no se consume, en tanto que el sistema de armas dispone de un número de municiones siempre limitado, y tanto más limitado pues esta munición es costosa o difícil de almacenar.

Así resulta que cuando se determina el equipamiento de las fuerzas, los medios de contramedidas electrónicas no deben ser considerados como un simple complemento. El equilibrio a realizar entre el desarrollo de los medios de destrucción y el de los medios de contramedidas electrónicas, para una tarea dada, deberá, a falta de experimentación imposible de conducir, ser fijado en función de los resultados de los estudios de investigación operativa, tomando en cuenta el rendimiento costo-eficacia de los diferentes medios y sus características específicas.

Hemos visto en el curso de la primera fase de este estudio que las acciones de CME dependen de dos campos de ahora en adelante clásicos; la confusión y la decepción, a los que se agregan, particularmente en lo que concierne a las redes de transmisión automatizadas, la saturación resultante de una intrusión "en masa" y la perturbación del funcionamiento de los ordenadores. No reseñaré entonces, sino muy brevemente, las características esenciales de la confusión y la decepción.

La confusión puede ser activa; es el caso de los confusores de barrera o de puntuales, o pasiva, y es el caso de señuelos de los cuales los más comunes son los "chaffs"; empleadas menos frecuentemente, las nubes de aerosol son igualmente muy eficaces.

Los confusores de barrera son usados generalmente a priori. Los confusores puntuales, al contrario, sirven para confundir una emisión que se manifiesta y cuyas características deben haber sido determinadas con anterioridad por interceptación. La "conexión" entre el receptor de interceptación y el emisor de confusión puede ser asegurada por un operador que regule este último en la frecuencia exacta y lo ponga en funcionamiento. También puede ser asegurado de manera automática, la que es indispensable en autodefensa para la confusión de radares de armas o de misiles, en razón de la necesidad imperativa de reaccionar casi instantáneamente.

Empleados para la confusión, los "chaffs" son esparcidos en forma de nubes reflectoras, que constituyen un muro o un pasillo protector de la detección. Estas agujas caen muy lentamente y las nubes permanecen eficaces durante varias horas.

El máximo de eficacia se obtiene al combinar los diferentes medios de confusión, muro protector y confusores activos, lo que necesita de parte del Mando una estricta coordinación. La dirección de esta coordinación fue una causa esencial del rendimiento bastante débil de la defensa antiaérea nordvietnamita contra los raids de la aviación americana.

Hemos visto que las principales acciones de decepción, es decir, tendientes a engañar al enemigo, son la intrusión, que consiste esencialmente en inyectar falsos mensajes en las redes de transmisión del adversario y la simulación, que se dirige generalmente a los sistemas de detección o a los de interceptación. Los procedimientos de simulación más corrientes son los confusores respondedores que reenvían al radar un falso eco y los señuelos (chaffs y aerosoles) desplegados de manera de crear no un muro sino solamente uno o varios ecos de diversión que los radares de vigilancia o de guía o los medios de interceptación (infrarrojo por ejemplo) confunden con el verdadero eco.

La parte y la importancia de las CME en la defensa contra misiles no cesa de crecer. La solución de los problemas que plantea su interceptación por las armas de destrucción es en efecto muy ardua e incierta. Por la rapidez de su empleo y por la instantaneidad de sus efectos de confusión y de decepción en el sistema de guía del misil, las CME ofrecen mejores perspectivas de solución.

Para obtener su plena eficacia, el empleo de las contramedidas electrónicas debe respetar ciertas condiciones.

La primera de éstas es el respeto de una doble restricción de no interferencia y discreción. En efecto, por una parte, las emisiones de CME pueden dificultar el buen funcionamiento de los elementos amigos de interceptación, decepción, etc. Por otra, son muy a menudo muy indiscretas, el efecto obtenido corre el riesgo de ser, a fin de cuentas, el opuesto al que se busca. Además, el empleo a título preventivo de ciertos medios de CME puede constituir una advertencia para el adversario.

Hemos visto además que los medios de contramedidas electrónicas (CME) son un arma, arma privilegiada si no exclusiva de las situaciones de crisis, arma cuyo empleo en las situaciones de guerra debe ser balanceado y en todo caso coordinado con el de las armas de destrucción.

Resulta, y es la segunda condición, que el empleo y utilización de las CME no pueden constituir una operación independiente. Teniendo en cuenta la situación política, estratégica o técnica y los objetivos a obtener, la organización establecida debe permitir, tanto a nivel del empleo como al de utilización, una es-

trecha coordinación de los medios de CME con las otras armas y medios de acción.

La tercera condición deriva del hecho que los elementos de CME son en alguna forma impuestos por la técnica del adversario y que su eficacia depende absolutamente de su adaptación rigurosa a las características de los elementos adversarios que se necesita neutralizar, engañar o decepcionar. Es por qué, por ejemplo, los equipos de CME para una misión aérea dada deben ser exactamente adaptados a las características electrónicas de los radares y sistemas de armas tierra-aire o aire-aire que los aparatos participantes en la misión van a encontrar. Y es, entre otras razones, por qué los israelíes han tenido tantas pérdidas aéreas los primeros días de la guerra de octubre.

Pero la gran debilidad de las CME reside en la incertidumbre en la cual se encuentra en cuanto a su eficacia. Es difícil saber, por ejemplo, si el adversario no utiliza una técnica nueva para escapar a la confusión o discriminar los ecos buenos de aquellos producidos por los señuelos; es difícil también conocer el grado de entrenamiento de sus operadores. Pero esta incertidumbre pesa otro tanto en los sistemas de armas ya que, generalmente, se sufre un desconocimiento semejante en cuanto a las posibilidades de las contramedidas electrónicas del adversario.

LAS MEDIDAS DE PROTECCION ELECTRONICA (MPE)

Veamos ahora lo esencial de lo que es necesario saber a propósito de las medidas de protección propias de la guerra electrónica. Ellas constituyen el aspecto defensivo y comprenden dos categorías de medidas bien distintas: por una parte, "las medidas de seguridad" que se oponen a las rebuscas adversarias, siendo su objeto evitar la interceptación o disminuirlas al mínimo; por otra, "las medidas de defensa" que se oponen a las contramedidas electrónicas —las que algunas veces merecen el término complicado de contra-contramedidas electrónicas (CCME)— y cuyo objeto es la defensa contra la confusión y contra la decepción.

Medidas de Seguridad

Las medidas de seguridad tienen, como las medidas de rebusca, varios objetivos:

—**El objetivo técnico,** que debe ser perseguido desde tiempo de paz, tiende a preservar la sorpresa técnica. Esta sorpresa técnica previene el desarrollo por el adversario de materiales de rebusca y materiales de contramedidas adaptados a los materiales amigos. Importa luego que los datos susceptibles de informarle sobre éstos sean rigurosamente protegidos.

—**El objetivo operativo** que debe ser rebuscado en tiempo de paz, pero sobre todo en tiempo de crisis o de guerra, y que tiende a impedir al adversario la localización, la identificación y el conocimiento del despliegue de las fuerzas amigas. Es igualmente necesario dejar al adversario en la ignorancia de las tácticas, así como de los rendimientos y las condiciones de empleo de los medios.

Además, las medidas de seguridad tienden a impedir al adversario la apropiación y la comprensión de las informaciones transmitidas. Finalmente, tienen por objeto impedir al adversario utilizar con éxito sus sistemas de armas guiadas en las radiaciones emitidas por los elementos amigos.

—La más general y la más importante de las medidas de seguridad es "el silencio". Confiere una seguridad absoluta, pero sus inconvenientes pueden ser a veces desproporcionados, ya que priva de todo medio de detección, de transmisión, etc. Es allí, entonces, tarea del Mando, prevenido por los especialistas, pesar para cada situación estratégica o táctica las ventajas e inconvenientes del silencio, los riesgos de interceptación para tal categoría de emisiones, tal gama de frecuencia, tal potencia, así como los peligros que acarrea una interceptación.

Es desde tiempo de paz que el silencio se impone de manera de dejar al adversario potencial en la ignorancia de las características técnicas, rendimientos, incluso de la existencia de un material dado. Esta "discreción técnica" se inscribe en el marco general del secreto industrial; en este aspecto las exportaciones deben

ser controladas ya que, aun si se imponen disposiciones de quitar marcas, modificaciones o limitaciones a los materiales exportados, estos últimos no constituyen menos que una fuente irreemplazable de información sobre el equipamiento de nuestras propias fuerzas.

Señalemos además que las medidas de silencio electrónico deben ser equilibradas y generales; sería aberrante, en el plano operativo, privarse del empleo de un medio cuando otro también indiscreto permanece en servicio. Así, por ejemplo, las medidas de silencio de radio deben ser rigurosamente coordinadas con las medidas de silencio de radar, las cuales a su vez deben eventualmente ser coordinadas con las medidas de silencio de sonar, etc. La estricta disciplina que se impone en la materia no puede ser sino el fruto del entrenamiento, incluso del hábito.

Existen otras medidas de seguridad que, si son de una eficacia menos cierta, son en contrapartida menos restringentes que el silencio; entre estas medidas hay tres que son de práctica corriente:

—La 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 dificulta la interceptación, la goniometría, el análisis, así como la restitución de la información transportada. El empleo de emisiones breves es la medida menos restringente en el plano operativo pero la más delicada en el plano técnico y la más pesada en el plano financiero.

Al no poder ser aplicado constantemente el silencio electrónico y al no aportar ninguna garantía absoluta las otras medidas de seguridad, deben tomarse disposiciones para limitar los efectos de la interceptación. La más eficaz y más general de estas medidas es el ciframiento. Bajo sus formas más modernas y más elaboradas, tales como el ciframiento en línea o el ciframiento de vía, él puede, desde el momento que se aplica a una transmisión por medios radiantes, ser considerado como una medida complementaria de seguridad electrónica.

Las Medidas de Defensa Electrónica

Las medidas de defensa electrónica tienen por objeto permitir el funcionamiento de los medios que radian a pesar de las tentativas adversarias de confusión o de decepción.

Para luchar contra las tentativas de confusión, se ha recurrido a toda una serie de medidas que pueden ir desde el aumento de la potencia de los emisores amigos al empleo de elementos aéreos direccionales, el empleo de técnicas de modulación que hagan ineficaz la confusión, la disminución de la selectividad de los receptores, el entrenamiento de los operadores para regular su material y para distinguir la señal útil. Sin embargo, pueden resultar insuficientes o de aplicación difícil. No queda ahora sino cambiar de frecuencia, medida de evasión eficaz pero con la condición de haber sido posibilitada por la concepción de los equipos y preparada por las disposiciones reglamentarias y el entrenamiento de los operadores.

Contra la decepción, se procura el tomar en cuenta, por los sistemas de recepción, por los sistemas de tratamiento o por los explotadores, que las señales de decepción emitidas por el adversario sean rechazadas.

El medio más corriente es "la autentificación". Consiste en comparar las características de la señal recibida con aquéllas de la señal deseada. La comparación puede ser efectuada electrónicamente y se apoya en las características técnicas de la señal (frecuencia precisa, largo de impulsión, etc.); puede ser efectuada por los operadores, y en este caso está la información transportada (el mensaje) que es confrontada a la que debería ser, por ejemplo, por medio de un código preguntas-respuestas. La eficacia de la autentificación depende estrechamente de la calidad del material y de la disciplina del personal. Así, un autodirector pasivo correctamente regulado y selectivo no se dejará engañar por un señuelo infrarrojo simulando el escape de un reactor.

Digamos para terminar que las medidas de protección electrónica, reclaman como casi todas las acciones de guerra electrónica, un conocimiento tan exten-

so como sea posible de los medios de todo orden de que dispone el adversario.

CONCLUSION

El doble análisis que efectuamos, al examinar las acciones de Guerra Electrónica, primero por campos de aplicación, luego por finalidades, ha traído inevitablemente algunas repeticiones. Pero ha permitido situar exactamente el impacto y la importancia de esta disciplina. Permite igualmente poner en evidencia algunos caracteres esenciales de la guerra electrónica.

"La omnipresencia", en primer lugar, o "la universalidad", ya que la Guerra Electrónica está presente en todas partes, en tiempos de paz, crisis o guerra, en el espectro, desde las frecuencias más bajas hasta las más elevadas y sobre todo en casi todos los modos de información, de transmisión o de acción.

"La competitividad"; los medios de Guerra Electrónica, en efecto, no deben ser considerados como suplementarios facultativos. Se trata, por el contrario, de medios cuyo empleo debe ser balanceado con los medios clásicos que pueden reemplazar o completar.

"El tecnicismo"; la eficacia de los medios de Guerra Electrónica depende estrechamente del valor de los personales y de la calidad de materiales de una tecnología adecuada.

"La dependencia del adversario" y, sobre todo de su electrónica: no hay MRE posibles si el adversario no emite; ni CME posibles si no utiliza la electrónica.

Y, finalmente, "la evolutividad", ya que en Guera Electrónica el éxito depende estrechamente de la aptitud para evolucionar constante y rápidamente para adaptarse al adversario con el fin de atacar mejor y para beneficiarse del progreso técnico a fin de evadirlo mejor.

Costosos, difíciles, importantes por sus efectos, sus riesgos y sus implicaciones, los asuntos de Guerra Electrónica deben ser conducidos de acuerdo a una política rigurosa. Querría, en materia de conclusión, llamar una última vez la atención sobre los principios fundamentales que me parecen deben constituir la base de tal política: la integración y la coordinación.

La integración, quiere decir que la Guerra Electrónica debe estar integrada en las formas de pensamiento y en la enseñanza, debe estar en las misiones de las FF.AA., en la planificación de los sistemas de fuerzas, en las estructuras orgánicas, a fin de que ellas permitan y faciliten la coordinación. Y esta coordinación debe aplicarse en las relaciones entre elementos operativos, especialistas e ingenieros, en el empleo de las MRE y otras fuentes de datos o de información, en el empleo de las CME y los sistemas de armas, en el empleo de medidas de seguridad electrónicas, y otras medidas de seguridad y, finalmente, debe aplicarse al empleo de medios diferentes a la Guerra Electrónica y otros medios electrónicos. Tal es, a mi juicio, el decálogo de la Guerra Electrónica. Ignorarlo conducirá inevitablemente a una Fuerza Armada a conocer el "Infierno de la Derrota".

Que no se sea inflexible con el autor por no haberse ceñido al gusto actual por lo sensacional. En Guerra Electrónica, no hay ni sensacionalismo ni milagro; además, aquellos que saben, jamás dicen todo lo que saben. Pero, llegados al término de este estudio, el lector debe tener, lo espero, una idea suficientemente clara de un asunto que es, ciertamente, uno de los más vastos, más complejos y sobre todo uno de los más importantes entre aquellos a los que las FF.AA. se enfrentan.

De "Defense Nationale".