Manual de Operaciones de Guerra Electrónica

Primera Parte

Conceptos Básicos de Guerra Electrónica

Capítulo I

Generalidades de la Guerra Electrónica

Primera Sección

Introducción

1. El propósito de este manual, es proporcionar a las y los militares de todas las jerarquías del servicio de transmisiones y otras especialidades que tengan injerencia, los elementos necesarios, para considerar a la guerra electrónica como un factor decisivo y esencial en el cumplimiento de las misiones que se tengan encomendadas. Su aplicación no garantiza la victoria, pero sin su consideración es eminente el fracaso.

2. La importancia de la guerra electrónica ha crecido firme y constantemente desde el fin de la II guerra mundial. La utilización bélica en el campo de batalla de equipos, ingenios e implementos electrónicos se ha puesto de manifiesto en los tres niveles de la guerra, es decir, el estratégico, operativo y el táctico.

3. Las acciones de guerra electrónica se realizan en cualquier ámbito en que se lleve a cabo un conflicto, es decir aéreo, marítimo, terrestre, aeroespacial e inclusive submarino.

4. El empleo adecuado de los equipos y sistemas electrónicos, permite a las y los comandantes a cargo de las operaciones incrementar de manera sustancial y significativa algunas de sus características, principalmente la velocidad de reacción o tiempo de respuesta y la potencia de combate.

5. Aunque esto representa grandes ventajas en el campo táctico, también presenta un inconveniente, dicho en otras palabras, nos convertimos en blancos electrónicos vulnerables a los efectos destructores de la fuerza enemiga.

6. En un conflicto, las fuerzas adversarias contarán normalmente con sistemas y equipos destinados a realizar las mismas actividades que nosotros llevamos a cabo para obtener información de ellos, es allí precisamente donde la guerra electrónica entra en acción y comienza la lucha por el poder y control del espectro electromagnético.

7. Con el desarrollo de tecnologías aplicadas a fines bélicos, la guerra electrónica se ha convertido en un factor decisivo para obtener el éxito en las operaciones; este desarrollo ha ocasionado cambios en las formas de conceptuar la guerra convencional. La destrucción de los sistemas de mando y control, así como de defensa aérea, serán por lo regular una de las primeras acciones de hostilidad en un enfrentamiento.

8. Las fuerzas armadas modernas se despliegan en escenarios muy extensos, con entornos en constante evolución, donde sus necesidades de reacción rápida y adaptabilidad requieren de complejos sistemas sensores y de comunicaciones a fin de tener una visión total del lugar que ocupan y las áreas de interés.

9. Los conflictos contemporáneos han demostrado que la conquista de la superioridad aérea es un requisito indispensable para obtener la victoria, sin embargo, dicha superioridad está condicionada al hecho de obtener la superioridad electrónica. Solo de esta forma y con eficientes y confiables procedimientos de coordinación es posible obtener resultados positivos y disminuir la capacidad combativa de la fuerza adversaria.

10. Actualmente, los conflictos bélicos modernos se caracterizan por el uso intensivo de medios electrónicos, basados en el empleo de energía electromagnética para ejecutar y apoyar las operaciones militares, motivo por el cual, la guerra electrónica se ha posicionado como un arma imprescindible en el desarrollo de los conflictos armados.

11. Los sistemas electrónicos en las operaciones de combate, cumplen las siguientes funciones:

A. Enlace. Los modernos sistemas de comunicaciones permiten el control oportuno de todas las fuerzas en un teatro de operaciones y facilitan a quien ejerce el mando el intercambio y la obtención de información, necesaria para estimar la situación y emitir su decisión.

B. Detección y vigilancia. Los sistemas de radar e infrarrojo proporcionan un medio eficaz para conocer los movimientos de la fuerza adversaria, con anticipación suficiente, para emitir la alerta y evitar la sorpresa.

C. Adquisición de blancos. La artillería, la aviación y otros medios de apoyo de fuegos, emplean diversos sistemas de sensores, como el radar, térmicos y acústicos, entre otros, con el fin de ubicar sus blancos, guiar sus granadas y proyectiles.

D. Radionavegación. Las fuerzas combatientes terrestres, aéreas y navales requieren de sistemas de ayuda a la navegación, que les permitan conservar la orientación geográfica propia y de la fuerza enemiga, así como conducir sus movimientos en la dirección correcta. Ejemplo de esta aplicación es el Sistema de Posicionamiento Global y el Radiofaro Omnidireccional de muy alta frecuencia.

Segunda Sección

Antecedentes Históricos

12. El empleo de la guerra electrónica se ha utilizado desde que el italiano Guillermo Marconi inventó en el año de 1897 la denominada “telegrafía sin hilos” lo que era realmente una versión austera del radio actual.[1]

[1] Secretaría de la Defensa Nacional. Manual de Operaciones de Guerra Electrónica. México. SECRETARÍA DE LA DEFENSA NACIONAL. 2010. P.13

13. A partir de este momento las fuerzas armadas en algunos países sufrieron un cambio repentino y significativo, se produce un rápido desarrollo de la radio y las flotas de los países más avanzados incorporan de inmediato la telegrafía sin hilos a sus buques.

14. A través del tiempo, la forma de contender de los ejércitos en los conflictos armados ha evolucionado en forma sorprendente, debido principalmente a los descubrimientos y avances tecnológicos que el hombre ha desarrollado, con el objeto de emplearlos en su beneficio y obtener una ventaja significativa sobre sus enemigos.

15. Hasta finales del siglo XIX, los ámbitos tradicionales de combate se restringían a la tierra y el mar; con el nacimiento de la aviación, surgió un nuevo ambiente de combate, por lo que fue necesario desarrollar las fuerzas para operar en dicho entorno.

16. El nacimiento de la comunicación por radio, permitió a las fuerzas combatientes contar con un medio para establecer el enlace de manera instantánea, lo que coadyuvó a desarrollar nuevas tácticas, incorporándose de esta forma el espectro electromagnético en el desarrollo de las operaciones militares.

17. A principios del siglo XX, la energía electromagnética comenzó a aplicarse en el arte militar en el campo de las comunicaciones; con ello, los mandos y sus tropas dispusieron de un medio de enlace más expedito para el control de las operaciones.

18. Las observaciones de las y los operadores de los equipos de radiocomunicación, de que en determinadas ocasiones, la actividad en las frecuencias empleadas por las fuerzas adversarias se hacía más intensa de lo normal, generalmente era indicio de un inminente ataque.

19. La simple manipulación de la llave telegráfica de un transmisor, no para transmitir mensajes, sino para producir ruido, perturbaba las frecuencias de trabajo, dificultando la organización para el combate y la acción de mando enemiga.

20. Estas observaciones, intuitivas o deliberadas, dieron inicio a lo que hoy se conoce como guerra electrónica, cuya aplicación en los campos, tanto estratégico, como táctico ha ido creciendo, originando que los mandos y sus auxiliares aprendan a explotar sus ventajas.

21. Las posibilidades de la guerra electrónica se incrementaron cuando apareció el radiogoniómetro, el cual consiste básicamente en un receptor sensible a señales electromagnéticas débiles y un sistema de antenas directivas, que permiten determinar la dirección de procedencia de las señales interceptadas.

22. El análisis de tráfico de las comunicaciones empleado conjuntamente, con la posibilidad de localizar físicamente a los emisores, permitió ubicar los centros de transmisiones enemigos, generalmente yuxtapuestos a los cuarteles generales o puestos de mando.

23. La radiogoniometría permitió la deducción del orden de batalla enemigo, la organización de sus unidades, su esquema de maniobra y, siguiendo las posiciones sucesivas en el terreno de los centros de transmisiones, conocer sus posibles intenciones.

24. Otra innovación en la guerra electrónica se dio con la aparición del radar, el cual consiste en un emisor electromagnético de gran potencia asociado a receptores que miden el retraso de la energía transmitida que se refleja en un blanco y permite determinar su ubicación, distancia a la que se encuentra y velocidad, entre otros datos, por lo que es un transceptor que realiza funciones de detección y vigilancia.

25. El apoyo de fuegos y la guerra electrónica se asociaron cuando el empleo de la energía electromagnética permitió detectar y ubicar los blancos de la artillería, y demás elementos de apoyo de fuegos, así como guiar sus granadas y proyectiles, además de controlar electrónicamente sus disparos, dando origen al concepto de “sistema de armas”.

26. Una de las primeras acciones consideradas como guerra electrónica se registró en el año de 1905 con el conflicto ruso-japonés. En esta batalla el personal de operadores de los navíos rusos detectaron las emisiones de radio de los japoneses, pero no los interfirieron hasta que fue demasiado tarde, consumando la derrota de los rusos.

27. Una acción bélica en la que se vio involucrada la guerra electrónica fue la batalla naval de Tsushima, el comandante de un navío ruso, el Ural, pide permiso para interferir las comunicaciones japonesas a fin de tratar de limitar la efectividad de las comunicaciones y con ello debilitar la capacidad de mando de los japoneses, el almirante de la flota rusa no lo admitió, lo que realmente pedía su subordinado, era autorización para realizar una acción que hoy se conoce como Contramedidas Electrónicas.

28. Los tiempos en que las victorias se ganaban asaltando trincheras, hoy solo es parte de la historia; un ejército luchará de manera incesante por obtener la superioridad en el empleo y control no solo del ámbito terrestre, aéreo o marítimo, sino también del espectro electromagnético.

29. Las transmisiones no pueden considerarse como algo separado de la situación de combate, sino que forman parte de la misma y como tal, requieren de tácticas de aplicación que se adapten a las condiciones que la propia situación imponga.

30. Actualmente la guerra electrónica también contribuye al combate, mediante el empleo de armas de energía dirigida, capaces de destruir o neutralizar los blancos contra los que se aplica, por medio de un haz de radiación electromagnética, o bien, rayos de partículas atómicas o subatómicas.

31. El Pulso Electromagnético, consistente en la generación de una gran cantidad de energía electromagnética ambiental, capaz de dañar y neutralizar todos los sistemas eléctricos y electrónicos dentro de su radio de acción, generalmente como resultado de la detonación de un arma nuclear.[2]

---

[2] Department of the Army. Electronic Warfare in Operations. FM 3-36, Operations. Washington, D.C. DEPARTMENT OF THE ARMY. February 2008. P.16.

32. En la guerra moderna ha tomado un auge inusitado el concepto de “sistemas de mando y control” debido a la importancia vital que reviste su presencia y buen funcionamiento en el campo de las operaciones.

33. Un sistema de mando y control, se define como la integración de personal y sistemas de comunicaciones e información, que facilitan al o la comandante la concepción, preparación y conducción de las operaciones, mediante una completa y oportuna reunión de elementos de información, que facilitan la toma de decisiones y puesta en práctica de los planes formulados, además del control de los elementos ejecutantes.[3]

34. La evolución de las aplicaciones de la guerra electrónica al campo estratégico, quedó de manifiesto cuando se empleó en la intercepción y decodificación del tráfico transmitido y recibido en las embajadas extranjeras, con representación en los países que la practicaban.

35. Esta información de carácter estratégico, no solo permitía el conocimiento de aspectos puramente militares sino también de carácter político y económico, lo cual facilitaba la toma de decisiones de alto nivel gubernamental.

36. Estos procedimientos de espionaje electrónico, demostraron su eficiencia y bajo costo comparados con los procedimientos que se practicaban tradicionalmente.

37. Hasta hace poco, la guerra electrónica no se manifestaba como una forma de enfrentamiento físico directo contra los medios tradicionales de combate. Los actuales desarrollos en la materia, permiten a las fuerzas combatientes la destrucción o neutralización física y electrónica de los medios de acción de la fuerza adversaria sobre el campo de batalla, mediante el empleo de la energía electromagnética.

---

[3] Academia de Artillería de Segovia. Guerra Electrónica. ACART FM-55. España. ACADEMIA DE ARTILLERÍA DE SEGOVIA. 2006. P.32

38. La guerra electrónica se manifiesta como una forma de combate, cuyas acciones permiten obtener la superioridad táctica, no obstante que nuestras fuerzas sean numéricamente inferiores, esto es posible mediante la desorganización de los sistemas enemigos de mando, control, información, detección y vigilancia, de forma tal que los resultados de su aplicación consisten en la destrucción, neutralización o desorganización de las unidades enemigas, así como sus sistemas de apoyo de combate y de servicios.

Tercera Sección

Fundamentos de Guerra Electrónica

Subsección (A)

Conceptos Básicos de Energía Electromagnética

39. Aparentemente un estudio de guerra electrónica debería de iniciarse con los conocimientos específicos de la materia, sin embargo, existen conceptos básicos de otras ciencias que permiten un mejor entendimiento del tema; tal es el caso de la energía y sus aplicaciones en el arte militar.

40. Las tácticas de guerra en los actuales ejércitos, han sufrido modificaciones inimaginables debido a la integración de la energía con los sistemas de armas y su poder destructivo.

41. El requisito fundamental que debe cubrir un sistema de armas en la actualidad, es detectar la presencia de un blanco en base al tipo de energía que emita o refleje.

42. Los tipos de energía más usuales son: la eléctrica, lumínica, mecánica, acústica, térmica y química.

43. Un sensor es un dispositivo diseñado para recibir información del exterior y transformarla en otra magnitud, normalmente eléctrica, que seamos capaces de cuantificar y manipular, transmitir esta información a otro subsistema y efectuar alguna acción que permita la identificación, ubicación y si procede la destrucción del blanco (Ver figura Núm. 1).

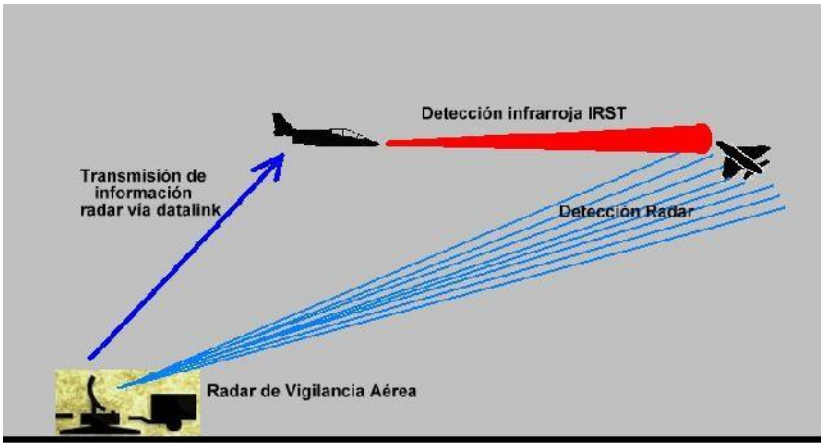

Figura Núm. 1
Detección Infrarroja

44. Los sensores pueden ser de los siguientes tipos:

A. De posición.

B. Fotoeléctricos.

C. Térmicos.

D. De ultrasonido.

E. De movimiento.

F. De velocidad.

G. De aceleración.

45. De todas las formas de energía, la electromagnética es la de mayor aplicación en los implementos bélicos de comunicación, detección, guía y control de los sistemas de armas.

46. Se aplica el término "electromagnético", a éste tipo de energía porque las ondas irradiadas tienen propiedades tanto magnéticas como eléctricas.

47. La radiación electromagnética combina los campos eléctricos y magnéticos que oscilan, esto permite que las ondas electromagnéticas se propaguen a través del espacio mientras llevan energía de un lugar a otro.

48. A pesar de que la luz visible y las ondas de radio parecen distintas, ambas son energía electromagnética, como lo son también los rayos infrarrojos, los rayos x y los rayos gamma; la distribución de la energía de cada una de estas ondas conforma el “espectro electromagnético” (Ver figura Núm. 2).

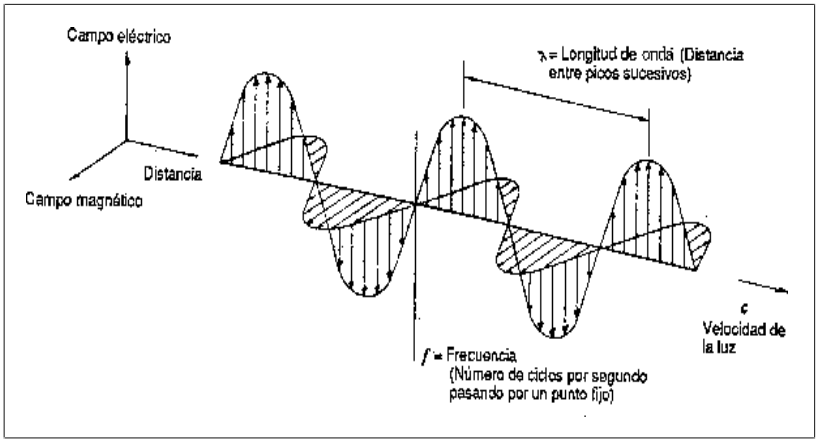

Figura Núm. 2
Componentes de una onda electromagnética.

49. La velocidad de la luz en el vacío es por definición una constante universal de valor 299 792 458 m/s (suele aproximarse a $3x10^{-8}$ m.

50. La energía electromagnética tiene una forma de propagación característica determinada por su frecuencia y su longitud de onda.

51. Todas las ondas de radio se propagan a la velocidad de la luz independientemente de su frecuencia.

Subsección (B)

Frecuencia

52. El Sistema Internacional especifica que la medida de la frecuencia es el Hertz (Hz); se define como el suceso que se repite una vez en un segundo, también conocido como ciclo por segundo (cps).

53. Debido a que los equipos electrónicos emiten frecuencias del orden de los miles y de los millones de Hertz, en la práctica el valor de la unidad básica se modifica a base de prefijos.

54. La frecuencia indica el número de ciclos que se suceden en un segundo en una onda electromagnética.

55. En un equipo de radio, la frecuencia indica la banda o segmento del espectro electromagnético en que este opera.

56. La banda de frecuencia es el intervalo de frecuencias entre dos límites establecidos que condicionan su aplicación. Cabe destacar que la frecuencia mantiene una relación inversa con la longitud de onda, es decir, a mayor frecuencia, menor longitud de onda y viceversa (Ver figura Núm. 3).

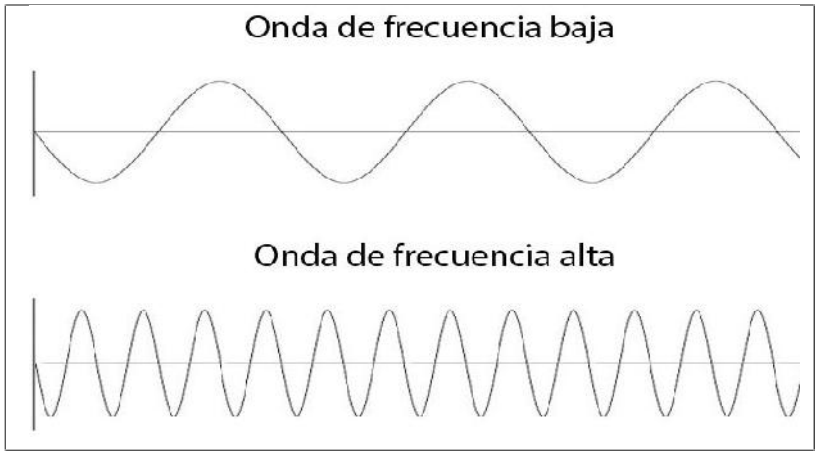

Figura Núm. 3
Comparación de una Frecuencia Alta y una Baja.

57. Los prefijos más comunes que se emplean para modificar el valor de la unidad básica de frecuencia son:

A. La letra minúscula "k" que significa "kilo" y representa un valor de mil.

B. La letra mayúscula "M" que significa "mega" y representa un valor de un millón.

C. La letra mayúscula "G" que significa “giga" y representa un valor de mil millones.

D. La letra mayúscula "T" que significa "tera" y representa un valor de un millón de millones.

58. Ejemplo: un radar que opera en la frecuencia de "dos mil quinientos millones de Hertz" (2,500,000,000 Hz) se puede expresar también como "dos millones quinientos mil kilo Hertz" (2,500,000 kHz.), "dos mil quinientos Mega Hertz" (2,500,MHz) o bien "dos punto cinco Giga Hertz" (2.5 GHz). La última expresión es la más usual por el menor número de cifras que maneja.

Subsección (C)

Longitud de Onda

59. La longitud de onda es una característica importante de las ondas electromagnéticas; se define como la distancia real que recorre una onda en un determinado intervalo de tiempo, ese tiempo es el transcurrido entre dos máximos consecutivos de alguna propiedad física de la onda (Ver figura Núm. 4).

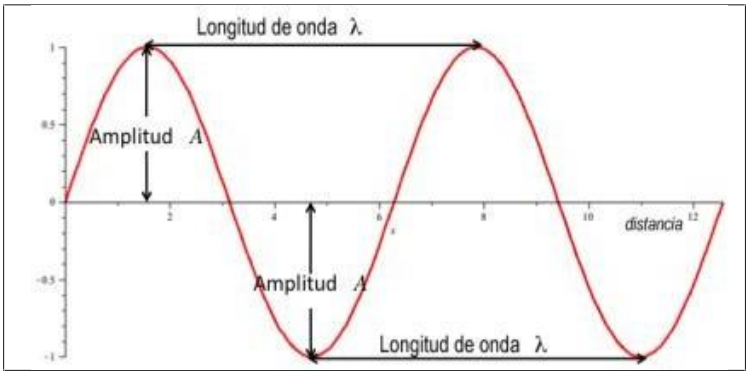

Figura Núm. 4
Longitud de Onda

60. La longitud de onda es un parámetro importante de las señales de radio porque determina el tamaño físico de la antena.

61. La longitud de onda se representa matemáticamente por la letra griega lambda (λ).

62. La frecuencia y la longitud de onda se relacionan con la velocidad de propagación de la siguiente manera:

$$\text{Longitud de Onda} = \frac{\text{Velocidad de Propagación (c)}}{\text{Frecuencia (f)}}$$

63. La interpretación de esta sencilla relación indica que la frecuencia y la longitud de onda son inversamente proporcionales, es decir, cuando una se incrementa la otra disminuye y viceversa.

64. La guerra electrónica, en una de sus misiones, tiene como objetivo la búsqueda de la información de estos parámetros de los emisores que operen en una área de interés táctico, para cuando sea necesario apoyar las operaciones que deban realizarse en esa área, nulifique, degrade o destruya según sea el caso, las funciones específicas que realicen esos emisores.

Cuarta Sección

El Espectro Electromagnético

65. La guerra electrónica es una disputa por el control y empleo del espectro electromagnético, por lo que es conveniente estudiar este recurso natural ilimitado desde los puntos de vista de su definición, división, reglamentación y aplicación en tiempo de paz.

66. Espectro electromagnético. Referido a un objeto se denomina espectro electromagnético o simplemente espectro a la radiación electromagnética que emite (espectro de emisión) o absorbe (espectro de absorción) una sustancia. Dicha radiación sirve para identificar la sustancia de manera análoga a una huella dactilar.

67. Los espectros se pueden contemplar mediante espectroscopios que, además de permitir observar el espectro, permiten realizar medidas sobre el mismo, como son la longitud de onda, la frecuencia y la intensidad de la radiación. La longitud de una onda es el período espacial de la misma, es decir, la distancia que hay de pulso a pulso.

68. El espectro electromagnético para su estudio se divide en segmentos o bandas de frecuencias principiando teóricamente en los cero Hertz para terminar indefinidamente. El ser humano ha sido capaz de generar cada día frecuencias más altas y es prácticamente impredecible fijar un límite.

69. Representa el ambiente en donde operan los equipos de radiocomunicación, los radares, la fibra óptica, el láser, los sistemas infrarrojos y satelitales, pudiendo ser considerado como una dimensión más dentro de los teatros de operaciones, es un recurso ilimitado, cuyo empleo queda restringido únicamente por la disponibilidad de equipos electrónicos que operen en las diversas bandas de frecuencia en que se divide.

70. Como ya se indicó, el espectro electromagnético abarca todo el intervalo de frecuencias existentes, sin embargo, solamente dos segmentos del mismo son utilizados en beneficio de las operaciones militares: el espectro radioeléctrico y el espectro óptico. (Ver tabla Núm. 1)

<table>
<tr><th colspan="2">Denominación</th><th>Frecuencia</th><th>Banda de Frecuencia</th><th>Aplicación</th><th></th></tr>
<tr><td>ELF</td><td>Frecuencias Extremadamente Bajas.</td><td>30-300 Hz.</td><td colspan="3" rowspan="3">Espectro de audio frecuencia</td></tr>
<tr><td>VF</td><td>Frecuencias de voz.</td><td>300 Hz.-
3 kHz.</td></tr>
<tr><td>VLF</td><td>Frecuencias muy bajas.</td><td>3-30 kHz.</td></tr>
<tr><td>LF</td><td>Frecuencias bajas.</td><td>30-300 kHz.</td><td rowspan="2">30-650 kHz.</td><td rowspan="2">Servicios de Radio navegación</td><td rowspan="8">Espectro Radioeléctrico.</td></tr>
<tr><td rowspan="3">MF</td><td rowspan="3">Frecuencias medias.</td><td rowspan="3">300 kHz.-
3 MHz.</td></tr>
<tr><td>650 kHz.-1.7 MHz.</td><td rowspan="2">Comunicación de largo alcance</td></tr>
<tr><td>HF</td><td>Frecuencias altas</td><td>3-30 MHz.</td><td>1.7-30 MHz.</td></tr>
<tr><td>VHF</td><td>Muy altas frecuencias</td><td>30-300 MHz.</td><td rowspan="2">30 MHz-1 GHz.</td><td rowspan="2">Comunicación táctica de corto alcance
(Línea de vista)</td></tr>
<tr><td rowspan="2">UHF</td><td rowspan="2">Ultra altas frecuencias.</td><td rowspan="2">300 MHz.-3 GHz.</td></tr>
<tr><td rowspan="3">1 - 300 GHz.</td><td rowspan="3">Microondas (Comunicaciones por enlace terrestre y satelitales)</td></tr>
<tr><td>SHF</td><td>Súper altas frecuencias.</td><td>3-30 GHz.</td></tr>
<tr><td>EHF</td><td>Extremadamente altas frecuencias</td><td>30-300 GHz.</td></tr>
<tr><td colspan="2">Infrarrojo</td><td colspan="2">300 GHz.-384 THz.</td><td>Visión nocturna, sensores térmicos, etc.</td><td rowspan="4">Espectro óptico.</td></tr>
<tr><td colspan="2">Espectro de luz visible</td><td colspan="2">384 - 789 THz.</td><td>Laser, Comunicaciones ópticas, etc.</td></tr>
<tr><td colspan="2">Ultravioleta</td><td colspan="2">789 Thz. - 30 PHz.</td><td>Sensores</td></tr>
<tr><td colspan="2">Rayos X</td><td colspan="4">30 PHz. - 30 EHz.</td></tr>
<tr><td colspan="2">Rayos Gamma y Cósmicos</td><td colspan="4">30 EHz.</td></tr>
</table>

Tabla Núm. 1
El Espectro Electromagnético

71. Para los fines de este manual, es suficiente identificar tres divisiones del espectro electromagnético que por sus efectos y aplicaciones resultan importantes para una mejor comprensión de la guerra electrónica. Estos segmentos son:

A. El espectro de audio-frecuencias.

B. El espectro de luz visible.

C. El espectro radioeléctrico.

72. Espectro de audio-frecuencias. Es un segmento de frecuencias que los seres humanos experimentan directamente en la banda que comprende la energía sónica o de sonido.

73. El oído humano es capaz de escuchar un rango de frecuencias comprendidas entre los veinte y los veinte mil Hertz. Los sonidos arriba de los diez mil Hertz no todos los seres humanos son capaces de escucharlos, aunque algunos animales si los perciben.

74. Con todo esto, el espectro de audio comprende las frecuencias desde uno a los veinte mil Hertz. Cualquiera que sea capaz de escuchar puede sentir las características del espectro audible desde las graves notas de una tuba, hasta los agudos sonidos producidos por un pícolo, los violines y las trompetas.

75. El sonido. Es la sensación o impresión que se produce en el oído debido a un conjunto de vibraciones que se propagan a través de un medio elástico como el aire.

76. La velocidad de propagación del sonido. En el aire el sonido tiene una velocidad de 331.5 m/s cuando la temperatura es de 0 grados centígrados y una presión de una atmosfera a nivel del mar y se presenta una humedad relativa de cero por ciento (aire seco).

77. Existen radiaciones electromagnéticas de igual frecuencia a las comprendidas en el espectro de audio, solo que sus longitudes de onda son alrededor de un millón de veces más grandes que las correspondientes a las frecuencias emitidas por la energía acústica.

78. Otra razón para considerar al espectro de audio en este estudio, se debe a que la voz humana es una de las formas de inteligencia que se emplea para modular las señales de radio.

79. Las ondas electromagnéticas se emplean como portadoras de la voz humana, para hacerla llegar más lejos, aprovechando sus propiedades de propagación.

80. El espectro de luz visible. Cuando observamos un arco iris, estamos contemplando el rango de frecuencias denominado de luz visible.

81. Para el ojo humano estas frecuencias las interpreta como colores que van desde el rojo hasta el violeta.

82. Estos dos colores, por ser los extremos del espectro de luz visible, a menudo se toman como referencia, por lo que es frecuente el empleo de términos como infrarrojo y ultravioleta para referirse a frecuencias inferiores o superiores respectivamente al espectro visible.

83. Si el ojo humano tuviera la capacidad de ver todas las frecuencias que comprende el espectro electromagnético al momento de propagarse de igual forma como se puede ver el arco iris, parte de este manual no tendría razón de ser, más sin embargo, esto no es posible.

84. El rango que el ojo humano es capaz de percibir es un pequeño segmento del extremo superior del espectro electromagnético.

85. El espectro radioeléctrico. Este segmento del espectro electromagnético se denomina de esta manera porque es la parte donde se emplean las señales radioeléctricas.

86. El espectro radioeléctrico principia en los 3 kHz. y termina en los 300 GHz., dividiéndose en ochos bandas con denominaciones en el idioma Inglés. la terminología acorde a la nomenclatura empleada por la Secretaría de Comunicaciones y Transportes se refiere a los múltiplos del metro.

87. Las bandas del espectro radioeléctrico tienen empleos específicos y formas de propagación diferentes por lo que a continuación se enlistan sus aplicaciones.

88. Bandas de VLF y LF. Estas bandas se emplearon inicialmente al ser aplicados los fenómenos electromagnéticos al campo de las comunicaciones requiriendo de sistemas de antenas gigantescas 30 kHz. Tiene una longitud de onda de 10 km, actualmente las frecuencias de estas bandas se emplean en sistemas de radio navegación marítima y aérea.

89. Banda de MF y HF. Estas bandas se emplean para radiodifusión, transmisiones intercontinentales de onda corta y radioafición; las radiaciones electromagnéticas en estas dos bandas presentan importantes propiedades al ser refractadas y reflejadas por una capa de la atmósfera terrestre llamada ionosfera.

90. Banda de VHF (30 a 300 MHz.), tiene una longitud de onda de 10 m a 1 m; esta banda se emplea en la televisión, radiodifusión en FM, servicios de banda aérea, comunicaciones navales y control de tráfico marítimo.

91. Banda de UHF (300 MHz. a 3 GHz.), tiene una longitud de onda de 1 m a 100 mm y se emplea en televisión, comunicaciones por microondas, hornos de microondas, GPS, redes inalámbricas, bluetooth, sistemas de radar y telefonía móvil.

92. Las comunicaciones en las bandas de VHF y UHF requieren que las antenas transmisora y receptora se encuentren en línea de vista, por lo que sus alcances son pequeños comparados con los obtenidos en las bandas de MF y HF.

93. El concepto de línea de vista, implica que las antenas se encuentren en línea visual una con otra, se refiere a un camino o trayectoria; debido a que los obstáculos naturales o artificiales que se interpongan entre ellas afectan la eficiencia de las comunicaciones.

94. Microondas. A las frecuencias arriba de los mil mega Hertz se les conoce comúnmente con el nombre de microondas y se emplean ampliamente en las bandas de radar, sistemas y en tipo de comunicaciones llamado de banda ancha, sistemas de control de fuego y las comunicaciones en banda ancha.

95. La característica principal de propagación de la microondas es que se pueden ser transmitidas en un haz angosto de energía electromagnética, comportándose como rayos luminosos. Esta característica las hace particularmente útiles en sistemas de comunicaciones de punto a punto.

96. La longitud de onda en el rango de 3 a 30 GHz (SHF) es del orden de los centímetros y arriba de estas frecuencias se vuelve del orden de los milímetros, lo cual representa la gran ventaja de emplear antenas muy pequeñas.

97. Una ventaja de emplear las microondas es que se puede manejar un amplio ancho de banda; también se pueden transmitir grandes cantidades de datos, los costos de construcción son relativamente bajos comparados con otras tecnologías.

98. Como resultado del concepto de línea de vista, las comunicaciones a grandes distancias en estas frecuencias requieren de sistemas de repetición.

99. Otra de las desventajas que presenta el empleo de estas frecuencias tan elevadas es la afectación de las comunicaciones a causa de líneas de transmisión eléctrica, motores eléctricos, turbinas eólicas, fenómenos meteorológicos como humedad pesada, nieve, niebla y especialmente la lluvia debido a que cada gota de agua se convierte prácticamente en una antena que refleja, absorbe o disipa la energía electromagnética impidiendo llegar eficientemente a su destino.

100. Una alternativa para eliminar los efectos perturbadores de la atmósfera consiste en enviar la energía electromagnética a través de cables blindados, llamados coaxiales, o sistemas cerrados llamados guías de onda. Otra técnica reciente es la transmisión por fibras ópticas.

101. El que un sistema de transmisiones emplee la propagación electromagnética a través del espacio, o bien lo haga a través de cables, depende del tipo de comunicación que se requiera, de igual modo, en las bandas del espectro radioeléctrico, se emplea el tipo de propagación que más alternativas de solución ofrezca y la que menos posibilidades de intercepción brinde al enemigo.

Subsección (A)

Legislación del Espectro Radioeléctrico

102. Internacionalmente el empleo del espectro radioeléctrico está regulado por el organismo denominado "Unión Internacional de Telecomunicaciones" (U.I.T.) con sede en Ginebra, Suiza.

103. La U.I.T. es un organismo especializado integrante de la Organización de las Naciones Unidas (ONU) y se encarga de regular el espectro radioeléctrico y sus orbitas satelitales, así como elaborar técnicas para garantizar la interconexión de redes y tecnologías.

104. La U.I.T. tiene como misión desarrollar estándares para facilitar la interconexión eficaz de la infraestructura de comunicaciones nacionales con las redes globales, permitiendo el intercambio de información desde cualquier parte del mundo.

105. México es miembro signatario de esta organización que agrupa a 193 países.

106. La U.I.T. en su organización comprende tres organismos que desde los puntos de vista jurídico y técnico regulan las telecomunicaciones en el mundo a través de sus reglamentos estos organismos son:

A. U.I.T.-R Sector Radiocomunicaciones (antes C.C.I.R.)

B. U.I.T.-T Sector Normalización de Telecomunicaciones (antes C.C.I.T.T.).

C. U.I.T.-D Sector Desarrollo de las Telecomunicaciones.

107. El artículo 45 del convenio internacional de telecomunicaciones suscrito por México especifica: “Los miembros asociados reconocen la conveniencia de limitar el número de frecuencias y el espacio del espectro utilizados al mínimo posible para asegurar de manera satisfactoria el funcionamiento de los servicios necesarios”.

108. El artículo 50 del mismo convenio se refiere a las instalaciones radioeléctricas militares como sigue: “Los miembros asociados conservaran su entera libertad en lo relativo a las instalaciones radioeléctricas militares de sus ejércitos de tierra, mar y aire, sin embargo, estas instalaciones se ajustarán en lo posible a las disposiciones reglamentarias relativas al auxilio en casos de peligro, a las medidas para impedir las interferencias perjudiciales y a las prescripciones de los reglamentos concernientes a los tipos de emisión y a las frecuencias que deban utilizarse según la naturaleza del servicio".

109. La U.I.T. ha dividido al mundo en tres grandes regiones, a cada una le asigna rangos definidos de frecuencia para fines específicos. Estas regiones son:

A. Región 1.- Comprende Europa, África y Medio Oriente, incluye la Península Arábiga, Iraq, la antigua Unión Soviética y Mongolia.

B. Región 2.- Comprende América, incluyendo Groenlandia y algunas Islas del Pacifico.

C. Región 3.- Comprende Ucrania, Federación Rusa, Georgia, Turquía, Armenia, Azerbaiyán, Turkmenistán, Uzbekistán, Tayikistán, Kirguistán, Kazajstán y la Rusia Asiática.

110. En México la reglamentación de las emisiones se realiza por medio del Instituto Federal de Telecomunicaciones (IFT), órgano autónomo federal.

111. El funcionamiento del IFT se rige por las disposiciones del reglamento de radiocomunicaciones de la U.I.T ejerciendo su acción a través de estaciones radio monitoras instaladas en el territorio nacional que tienen como objetivos:

A. Conocer el grado de ocupación del espectro de frecuencias.

B. Detectar e identificar emisiones al margen de la ley o causantes de interferencias perjudiciales.

C. Evitar las interferencias perjudiciales entre permisionarios o concesionarios de frecuencias en el país.

112. Los usuarios del espectro radioeléctrico deben obtener una licencia de operación para hacer funcionar un emisor electromagnético de cualquier tipo y en cualquiera de las bandas de frecuencias.

113. En la república mexicana es el IFT es el organismo que decide bajo qué circunstancias y condiciones las y los ciudadanos mexicanos puede obtener una licencia de operación, aun con fines de experimentación o de radio-afición.

114. El empleo total del espectro radioeléctrico (3 kHz.-3000 GHz.) está condicionado por la generación de frecuencias; conforme los avances tecnológicos lo permitan, dicho espectro será más aprovechado y necesariamente reglamentado para evitar las interferencias perjudiciales.

115. Por ejemplo, la banda de radiodifusión de amplitud modulada (AM) que comprende el segmento de 535 a 1605 kHz. está reglamentada para que en una misma localidad trabaje un número determinado de concesionarios para evitar problemas de interferencia, con lo cual se presta un servicio eficiente.

116. Las mismas limitantes se aplican en la banda de radiodifusión de frecuencia modulada (FM), a los canales de televisión (TV) y en general a todos los servicios que empleen el espectro radioeléctrico.

Subsección B

Propagación de las Ondas Electromagnéticas

117. El término "propagación electromagnética" de algún modo se le asocia con grandes desarrollos matemáticos o conocimientos de alto nivel académico. Aunque esto es relativamente cierto, también se debe reconocer que no es posible hablar de radiocomunicación y guerra electrónica si se desconocen los conceptos básicos que rigen estos fenómenos.

118. Radiación electromagnética. Ocurre cuando se hace circular corriente eléctrica alterna con la suficiente intensidad a través de una antena que cubre el requisito de tener el mismo tamaño físico que ¼ de la longitud de onda generada o múltiplo de la misma.

119. Antena. Es un conductor eléctrico cuya función es radiar e interceptar energía electromagnética, por lo tanto, puede ser utilizada para transmitir o para recibir dicha energía.

120. Los equipos de radiocomunicación denominados "transceptores" emplean una sola antena para realizar ambas funciones.

121. Patrón de radiación. Es la forma característica de como transmite o recibe una antena. Generalmente se reconoce por su forma geométrica en un espacio de tres dimensiones.

122. Las antenas verticales ofrecen el patrón de radiación más uniforme. Este patrón se llama omnidireccional uniforme ya que su intensidad es aproximadamente la misma en todas las direcciones que rodean a la antena.

123. La gran ventaja de las antenas con patrón omnidireccional es cubrir un área tal que las estaciones receptoras puedan instalarse en cualquier punto alrededor del alcance práctico del transmisor.

124. El patrón de radiación omnidireccional resulta inapropiado cuando se requiere una comunicación punto a punto, en este caso, la energía transmitida resultaría desperdiciada, pudiéndose causar interferencias a transmisiones amigas, o bien, facilitar las misiones de intercepción del enemigo.

125. Las antenas con patrones de radiación dirigidas, tienen la gran ventaja de concentrar la energía en direcciones determinadas, generalmente, establecidas en función de la ubicación del enemigo o de la necesidad de proteger a nuestras propias estaciones de la vista electrónica de la fuerza adversaria.

126. La antena horizontal, también llamada dipolo, se caracteriza por representar un patrón de radiación bidireccional.

Subsección (C)

Normas de Propagación

127. Cuando la onda de radio despega de una antena vertical, el campo establecido tiene la apariencia de una gran dona con centro en la propia antena.

128. Parte de la onda radiada se mueve en contacto con la superficie de la tierra y otra parte se desplaza hacia arriba de la propia antena.

129. La parte de la onda electromagnética propagada cerca del suelo se le llama onda de superficie u onda de tierra y a la parte que se desplaza hacia arriba de la antena se le conoce como onda celeste, onda espacial u onda de cielo.

130. Conductividad Eléctrica. Es la medida de la capacidad de un material o sustancia para dejar pasar la corriente eléctrica a través de él.

131. Lo anterior, provoca que la onda propagada a su paso a través de la superficie terrestre se debilite rápidamente, este fenómeno se debe a la absorción de energía por el terreno.

132. La propagación por onda de superficie también está condicionada por la frecuencia de operación; en general su empleo está prácticamente limitado a los 30 MHz.

133. El agua de mar presenta una elevada conductividad eléctrica, a la que contribuyen la polaridad del agua y la abundancia de iones disueltos. Las sales en agua se disocian en iones. Un ion es un átomo cargado positiva o negativamente y que, por tanto, intercambia electrones con él.

134. La onda de superficie tiene dos componentes que son:

A. Onda Directa o de Línea de Vista. Se propaga a través del espacio directamente desde la antena transmisora a la antena receptora.

B. Onda reflejada. No sigue una trayectoria directa entre las antenas transmisora y receptora, sino que se refleja en cualquier obstáculo natural o artificial antes de llegar a la antena receptora en forma poligonal.

135. La propagación de línea de vista tiene amplias aplicaciones en el campo táctico con equipos de radiocomunicación de baja potencia que son operados por el propio personal combatiente.

136. Los equipos de radiocomunicación empleados en el Ejército e instalaciones terrestres de la Fuerza Aérea Mexicana utilizan en promedio potencias del orden de los 100 watts para establecer enlaces prácticamente a lo largo y ancho del territorio nacional en la banda de 3 a 30 MHz. (HF).

137. Se desprende por lo tanto que este tipo de propagación tiene amplias aplicaciones de tipo estratégico utilizando la ionosfera como un gran espejo electrónico.

Subsección (D)

Criterios Básicos de Propagación

138. Todas las emisiones electromagnéticas tienen en mayor o menor grado las normas de propagación celeste y de superficie, comportándose mayoritariamente de una u otra forma en función de la frecuencia de operación utilizada. Esto prácticamente se traduce en alcances mayores o menores de acuerdo a la potencia transmitida (Ver Tabla Núm. 2).

Banda	Onda de tierra	Onda celeste	Potencia de Transmisión
L F	cero a 1500 km.	800 a 12 mil km.	mayor de 50 kW.
M F	cero a 150 km.	150 a 2500 km.	de 1 a 50 kW.
H F	cero a 80 km.	150 a 12 mil km.	de 1 a 5 kW.
V H F	cero a 40 km.	80 a 200 km.	menor de 500 W.
U H F	cero a 80 km.	- - - - - - - -- - - - - -	menor de 500 W.

Tabla Núm. 2
Criterios Básicos de Propagación

139. Los criterios que pueden establecerse para la propagación electromagnética son:

A. En frecuencias menores a los 5 MHz, la forma de propagación se realiza mayoritariamente por medio de la onda de superficie; en forma general se puede afirmar que la propagación por onda de superficie es más eficiente cuanto más baja sea la frecuencia de operación.

B. En el rango comprendido de los 1.5 a los 30 MHz. la forma de propagación es mayoritariamente ionosférica empleando la onda celeste, la cual tiene grandes aplicaciones en las comunicaciones de carácter estratégico.

C. Las comunicaciones en frecuencias superiores a los 30 MHz. se requiere que las antenas se encuentren en línea de vista, debido a que arriba de estos valores de frecuencias el comportamiento de la energía electromagnética es directivo.

Quinta Sección

Definición y Estructura de la Guerra Electrónica

140. La guerra electrónica en las operaciones militares comprende las acciones para asegurar la explotación del espectro electromagnético por parte de nuestras fuerzas, e impedir o limitar su uso por parte del enemigo, así como destruir o neutralizar sus medios de acción, mediante el empleo de energía electromagnética.[4]

141. Lo anterior, nos permite obtener las siguientes consideraciones respecto a la guerra electrónica:

A. Es un conflicto por el empleo y control del espectro electromagnético.

B. Es aplicable en tiempo de paz y en tiempo de guerra.

C. Tiene aplicaciones en los campos estratégico y táctico.

D. La guerra electrónica reviste aspectos ofensivos y defensivos

E. Puede aplicarse en forma activa y pasiva.

F. Sus aplicaciones en tiempo de paz se ubican en el campo estratégico mediante la radio vigilancia que permite obtener información militar, política y económica.

G. Sus aplicaciones en el campo táctico se emplean para incrementar el poder combativo de las tropas utilizándola como arma de apoyo.

[4] Academia de Artillería de Segovia. Op. Cit. P.21-23

142. Tácticamente la guerra electrónica se divide en dos componentes principales que son:

A. Combate electrónico.

B. Guerra electrónica defensiva.

143. De acuerdo a su naturaleza, las actividades de guerra electrónica, se clasifican de la siguiente forma:

A. Medidas de apoyo electrónico.

B. Contramedidas electrónicas.

C. Medidas de protección electrónica.

144. Con fundamento en las misiones generales del Ejército y Fuerza Aérea Mexicanos, y tomando en consideración que desde el punto de vista legal la organización, equipamiento y adiestramiento de dichas fuerzas armadas deben estar orientadas al cumplimiento de las referidas misiones generales.

145. Lo anterior implica que, desde tiempo de paz, se organicen unidades de guerra electrónica que cuenten con el equipo y adiestramiento necesarios, para desarrollar las actividades inherentes a su especialidad, en beneficio de las operaciones militares que se desarrollen para la defensa de la nación.

146. Con el fin de tomar conocimiento del contexto internacional en la doctrina nacional, se asienta para cada uno de éstos componentes el acrónimo por el que es conocido en el ámbito internacional, así como su significado:

A. Medidas de apoyo electrónico.

B. Contramedidas electrónicas.

C. Medidas de protección electrónica.

147. Ninguno de estos componentes puede clasificarse categóricamente dentro de una función táctica específica, ya que todos y cada uno de ellos conllevan la ejecución de actividades ofensivas, defensivas y de apoyo dentro del conjunto. Sin embargo, de acuerdo a su principal campo de acción, dichos componentes se pueden considerar de la manera siguiente:

A. Componente ofensivo: se encuentra representado por las contramedidas electrónicas, debido a que permiten actuar ofensivamente sobre los equipos o sistemas electrónicos enemigos que emplean el espectro electromagnético, ya sea simplemente para reducir su eficacia, o bien para dañarlos físicamente, así como para confundir, distraer o engañar al enemigo. Estas actividades tienen basicamente dos objetivos:

a. Uno es romper la vigilancia y las comunicaciones, de modo que el enemigo sea incapaz de hacer el mejor uso de la recolección de información de sus sensores electrónicos y las comunicaciones, los cuales sirven a sus necesidades de comando y control.

b. El otro objetivo es reducir la letalidad de sus armas, cañones y misiles, los cuales dependen de la electrónica para apuntarlos y guiarlos al blanco, con el fin de hacer que algunos o todos los disparos dirigidos al blanco, sean fallados.

B. Componente defensivo: se encuentra representado por las medidas de protección electrónica, las que se realizan para proteger a la totalidad de las emisiones propias, a pesar de la utilización de la energía electromagnética por parte del enemigo.

C. Componente de apoyo. Se encuentra representado por las medidas de apoyo electrónico, ya que constituye una de las principales fuentes de obtención de información para el desarrollo de las operaciones, por lo que requiere estrecha coordinación y órganos específicos de enlace entre esta función y la de inteligencia.

148. El empleo de estos componentes está regido por el principio de centralización, considerando las operaciones militares como un todo.

149. No obstante lo anterior, y siempre sin vulnerar en ningún caso el principio de centralización, el apoyo particular que pueda prestar alguno de los componentes, se materializa mediante cambios en las prioridades de las medidas correspondientes o por cambios temporales en el esfuerzo sobre objetivos concretos.

150. Como consecuencia, la detección de la amenaza, su análisis e identificación, así como la respuesta en tiempo real para contrarrestarla, deben ser completamente automáticos y con supervisión manual.

151. Para satisfacer estas necesidades, y en especial poder reaccionar contra cualquier amenaza moderna, se requiere que esto lo haga una computadora, donde la operación del equipo es programada por software, de allí la importancia de la electrónica en los implementos bélicos.

Subsección Única

Misión y Objetivos

152. La guerra electrónica. Es un conjunto de acciones de carácter militar tácticas y/o técnicas, conducidas conforme a los principios de la guerra, en coordinación con el uso de las armas.

153. Tiene como misión incrementar la potencia de combate de las tropas mediante el empleo de energía electromagnética, así como coadyuvar a la obtención de la seguridad.

154. Para cumplir eficazmente con su misión, las actividades de guerra electrónica se desarrollan con los objetivos siguientes:

A. Obtener información para deducir el orden de batalla enemigo.

B. Neutralizar los sistemas enemigos de detección y vigilancia.

C. Nulificar las funciones de adquisición de blancos, guía y control de los sistemas de armas.

D. Desorganizar los sistemas de mando y control enemigos.

E. Dañar físicamente los medios de combate del enemigo mediante el empleo de la energía dirigida.

F. Asegurar el uso efectivo del espectro electromagnético y brindar protección a nuestras fuerzas contra el empleo enemigo de la guerra electrónica.

Sexta Sección

Importancia de la Guerra Electrónica

155. Las aplicaciones tecnológicas en el campo del arte militar son múltiples. Hoy en día el personal combatiente deben convertirse, a través del adiestramiento, en técnicos especializados para cumplir con eficiencia las tareas que los ingenios bélicos y sus tácticas novedosas le exigen.[5]

156. El empleo de sistemas electrónicos alcanza a todos los niveles en un conflicto bélico, en especial los equipos de comunicaciones, ya que permiten el conocimiento en tiempo real de las actividades que llevan a cabo las fuerzas desplegadas bajo su mando, facilitando a su vez la obtención de datos para una acertada evaluación de la situación que se vive.

[5] S.D.N. Manual de Operaciones de Guerra Electrónica. Edición 2010. Op. Cit. P.18-22.

157. Los ejércitos del mundo reconocen la importancia que el espectro electromagnético y la guerra electrónica tienen en el terreno de la estrategia, y de la táctica, y cómo se han interrelacionado, a tal grado que han generado la doctrina de empleo necesaria para su adecuada explotación.

158. El número de emisores electromagnéticos que operará en futuras guerras convencionales se prevé irá en aumento. Se calcula por ejemplo, que una unidad de nivel división en operaciones, podría hacer funcionar más de tres mil emisores, entre transmisores que manejen contenido de comunicaciones y transmisores de no comunicaciones, como el radar.

159. A este número de emisores empleados en la división hay que agregar los de las grandes unidades adyacentes, los de las comunicaciones civiles en el área y los de las fuerzas enemigas.

160. Esto demuestra que en toda guerra, además de los combates realizados en los ámbitos convencionales (tierra, mar y aire), se lleva a cabo una disputa por el uso y control del espectro electromagnético.

161. En la actualidad, quienes ejercen el mando en todos los niveles, dependen más que nunca de un sistema de mando y control, que opere de forma eficiente y confiable, por lo que debe contar con recursos de guerra electrónica tecnológicamente avanzados, para asegurar la protección y funcionamiento de dicho sistema.

162. De igual forma, las actividades de inteligencia han cobrado inusitada importancia recolectando y procesando información ininterrumpidamente, para reunir y difundir elementos de juicio que permitan a las y los comandantes tomar decisiones acertadas y oportunas, de manera que tengan una visión lo más completa posible de la fuerza adversaria y las actividades que lleva a cabo.

163. Sin embargo, para que un sistema de inteligencia funcione eficientemente, debe estar asociado a un sistema de comunicaciones que permita la oportuna transmisión de la información al lugar indicado.

164. Durante la concepción de las operaciones, quien ejerce el mando desarrolla actividades de análisis para emitir su decisión, confrontando sus cursos de acción con las posibilidades del adversario. En este sentido, los cursos de acción no solo deben considerarse en función de los medios de combate disponibles, sino también de la coordinación y control que de los mismos permitan los sistemas de mando y control.

165. Las o los comandantes de los teatros de operaciones y las fuerzas que en ellos operan, deben reconocer que la clave del éxito de sus actividades será un eficiente sistema de mando y control, al cual la fuerza adversaria atacará empleando la guerra electrónica para desorganizarlo, neutralizarlo o destruirlo como un objetivo de primordial importancia.

166. Por ello resulta obvio que las comunicaciones no pueden considerarse como algo separado de la situación de combate, sino que forman parte de la misma y como tal requieren de tácticas de aplicación que se adapten a las condiciones que la propia situación imponga.

167. Las actividades de guerra electrónica han ido en constante aumento, aunado a un grado de complejidad técnica y a una eficiencia operativa cada vez mayores, estando esta última en función de tres factores principales:

A. Disponibilidad de un sistema de inteligencia capaz de responder a la tecnología y actividades de enemigos potenciales (inteligencia de señales), complementado por un plan de operaciones de guerra electrónica basado en la evaluación de la tecnología por enfrentar y el grado de amenaza que represente.

B. Contar con un equipo de trabajo integrado por recursos humanos debidamente adiestrados y capacitados técnicamente en estas actividades.

C. Disponer de un sistema de mando y control que permita una óptima coordinación y armonía de esfuerzos entre las actividades de guerra electrónica.

168. De lo anterior se desprende que quien ejerce el mando debe estar preparado para explotar y asegurar el control del espectro electromagnético, de lo contrario está expuesto a la derrota en el campo de batalla.

169. Desde sus orígenes, el papel desempeñado por la guerra electrónica como elemento de apoyo a las operaciones militares, ha adquirido una importancia primordial en el combate y la batalla, llegando incluso a constituirse como uno de los factores decisivos del éxito o fracaso de las fuerzas combatientes.

170. Todas las medidas aplicadas en la guerra electrónica tienen sus tácticas defensivas, por lo cual, a las medidas de apoyo electrónico se oponen las contramedidas electrónicas y al conjunto de las anteriores, las medidas de protección electrónica.

171. Cualquier sistema electrónico será seguro mientras no sea puesto en operación. Una vez hecho esto, la guerra electrónica estudiará sus puntos débiles y buscará la manera de nulificar o degenerar su empleo. Es por esta razón, que las innovaciones en materia de guerra electrónica tienden a mantenerse en secreto.

172. Al concebir la ejecución de operaciones de guerra electrónica, se puede pensar que para su realización se requiere de grandes y costosas instalaciones y de equipo muy sofisticado; aunque esto es parcialmente cierto, es posible realizar actividades de guerra electrónica de manera elemental con equipos comunes de radiocomunicación, como por ejemplo:

A. Con un simple receptor, en las tareas de búsqueda e intercepción, análisis de señales y formación de una base de datos confiable que facilite la toma de decisiones.

B. Disponiendo de un transmisor, en las tareas de perturbación y engaño electrónicos.

C. El contar con la experiencia que proveen las tareas anteriores, permite adiestrar a nuestro personal en las técnicas orientadas a protegerse de sus efectos.

173. La guerra electrónica es una forma de combate que puede ser aplicada desde antes de las hostilidades, y es la única donde los contrincantes aplican sus principios y procedimientos, de igual manera en tiempo de paz que durante los conflictos bélicos.

174. Es también una guerra silenciosa, pero intensa y constante que no descansa las 24 horas durante los 365 días del año y que actualmente ha alcanzado una importancia preponderante, ya que su aplicación abarca desde el espionaje electrónico, hasta las mejores formas de evadir como el radar y los elementos de guía y control de los sistemas de armas de la fuerza adversaria.

175. Todo lo antes expuesto nos permite establecer las siguientes conclusiones:

A. Es indispensable que las y los militares destinados a ejercer el mando y fungir como sus auxiliares en las pequeñas y grandes unidades de combate, posean una adecuada formación respecto a la importancia, aplicaciones, posibilidades y limitaciones de la guerra electrónica.

B. Explotar en forma íntegra esta moderna forma de combate, en beneficio de las operaciones realizadas para el cumplimiento de las misiones generales de las fuerzas armadas.

C. En operaciones, este requerimiento se hace extensivo a toda o todo elemento perteneciente a dichas unidades, independientemente de su jerarquía, arma o servicio, quienes deberán estar compenetrados sobre los aspectos generales de la guerra electrónica, para contribuir a la conservación de la seguridad en la fuerza a que pertenezcan, y de este modo, coadyuvar con la supervivencia de su unidad en el campo de batalla.

Capítulo II

Las Medidas de Apoyo Electrónico

Primera Sección

Generalidades

176. Las medidas de apoyo electrónico. Son las acciones que se toman para investigar, interceptar, localizar, registrar y analizar la energía electromagnética con el fin de aprovecharla en el desarrollo de las acciones militares. Con estas acciones se espera detectar y ubicar geográficamente los equipos que emplea la fuerza adversaria para poder neutralizarlos mediante acciones pasivas (interferencia, bloqueo) y activas (empleo de la artillería).[6]

177. Coadyuvan de forma preponderante, ya que sirven de base para determinar la materialización de las contramedidas electrónicas y las contra-contramedidas electrónicas.

178. Comprenden las siguientes actividades:

A. Búsqueda e Intercepción.

B. Radiogoniometría.

C. Análisis de señales.

179. Para materializar estas funciones, las unidades de guerra electrónica despliegan sistemas electrónicos de sensores pasivos para escuchar, localizar e identificar las emisiones del enemigo.

[6] A. Yaselga Pavón Luis y Ligña Díaz Daniel; PROYECTO DE DISEÑO PARA MODERNIZAR EL SISTEMA DE INTERCEPTACIÓN DE TELECOMUNICACIONES, APLICADA AL SISTEMA COMINT DE GUERRA ELECTRÓNICA, Esc. Politécnica Ejército de Ecuador, LATACUNGA 2001.

180. El objetivo de las medidas de apoyo electrónico, es la explotación de las emisiones electromagnéticas del enemigo en beneficio de las fuerzas propias, para obtener los propósitos siguientes:

A. Información de interés respecto al enemigo y terreno dentro del área de operaciones.

B. Alarma y reconocimiento inmediato de amenazas.

C. Información de blancos para la ejecución de contramedidas electrónicas y otras acciones tácticas.

181. Las medidas de apoyo electrónico deben encontrarse interrelacionadas con otras actividades militares, a las que apoyan de la forma siguiente:

A. Inteligencia militar. Complementan el sistema de inteligencia existente (incluida la inteligencia de señales), proporcionando a los órganos superiores la información de valor militar que sea recolectada en el campo de batalla, la cual permita disponer de la más completa y oportuna información sobre el factor enemigo.

B. Operaciones de vigilancia. Los sensores en el campo de batalla, complementan la vigilancia, esto permite el conocimiento oportuno de los movimientos y acciones del enemigo, para la eficaz y pronta detección de amenazas a nuestras fuerzas.

C. Operaciones de reconocimiento. Al igual que en las operaciones de vigilancia, sus sensores permiten la ejecución del reconocimiento electrónico para apoyar las operaciones de reconocimiento y contrarreconocimiento, para obtener la mayor información posible de la ubicación, dispositivo, situación y actividades de la fuerza adversaria.

D. Coordinación de Fuegos de Apoyo (C.F.A.). Proporcionan a través de sus sensores un medio adicional al sistema de observación de la C.F.A., mediante la detección, ubicación y seguimiento de emisores, permitiendo de esta manera la asignación de blancos específicos a los diversos medios de apoyo de fuegos, incluyendo las contramedidas electrónicas.

182. Para poder apoyar de manera adecuada a las actividades antes enlistadas, la ejecución de las medidas de apoyo electrónico debe estar orientada por las necesidades de información del o la comandante respectivo, expresadas a través de sus elementos esenciales de información en el correspondiente plan de búsqueda de información.

183. Las medidas de apoyo electrónico pueden ser ejecutadas tanto por equipos terrestres, como por aquellos que operen a bordo de plataformas aerotransportadas. En este último caso extienden sus alcances de forma considerable.

184. Lo anterior, se materializa mediante el despliegue de “líneas de base”, las que consisten en establecer una cantidad variable de equipos (terrestres o aerotransportados), desplegados en las zonas avanzadas del área de operaciones, formando parte de las tropas más adelantadas y de aquellas ubicadas en los flancos del dispositivo general, con la finalidad de obtener la mayor cobertura posible sobre las emisiones dela fuerza oponente.

Segunda Sección

Búsqueda e Intercepción

185. Búsqueda e Intercepción. La ejecución de esta función proporciona las bases para llevar a cabo las demás funciones de apoyo electrónico. Implica la realización de dos actividades estrechamente relacionadas que no deben ser materializadas en forma aislada, por lo que es necesario que ambas actividades sean realizadas por un mismo organismo dotado de personal y equipo especializados.

186. La función de búsqueda e intercepción se materializa sobre redes de operación de sistemas electromagnéticos, las cuales se clasifican desde el punto de vista de protección de la información de la siguiente forma:

A. Redes protegidas. Son aquellas en las que la información que se maneja ha sido procesada por medio de algún tipo de cifrado o bien empleando equipos con diversos esquemas de seguridad, con el fin de evitar que terceros no autorizados conozcan su contenido.

B. Redes no protegidas. Son aquellas en que se maneja información en lenguaje claro (sin cifrar), por lo que además de los parámetros de las emisiones, proporcionan información detallada sobre las comunicaciones de la fuerza adversaria.

187. La Búsqueda. Consiste en el reconocimiento permanente del espectro electromagnético en busca de señales explotables.

188. El objetivo de las actividades de búsqueda es obtener información detallada sobre las porciones del espectro y sistemas electromagnéticos empleados por el enemigo. Por este motivo, las citadas actividades son indispensables durante la concepción y preparación de las operaciones de guerra electrónica, para proveer la información necesaria que sirva de base para el despliegue y empleo de los medios de intercepción, radiogoniometría y análisis de señales.

189. Para su adecuada ejecución, las actividades de búsqueda deben ajustarse a los siguientes preceptos:

A. Llevarse a cabo de forma continua, por lo que requiere la asignación permanente de recursos humanos y materiales dedicados a su ejecución.

B. Realizarse en tantas bandas del espectro electromagnético como sea posible y sobre sistemas electrónicos tanto de comunicaciones como de no comunicaciones.

C. Estar orientadas por una base de datos de los emisores existentes en el área, así como por las necesidades de información del o la comandante. Respecto a la base de datos, ésta contendrá los datos disponibles con anterioridad a las operaciones, y podrá ser proporcionada por los órganos de inteligencia del alto mando o bien, por otras dependencias gubernamentales.

D. El adiestramiento de las y los operadores de búsqueda es fundamental, debiendo considerarse entre otros los aspectos siguientes:

a. Dominio en la operación de sus equipos, para responder rápidamente a los cambios de frecuencia de los emisores de interés y darles seguimiento.

b. Poseer conocimientos del idioma o dialecto empleado en las comunicaciones del enemigo.

190. La Intercepción. Es la recepción y registro de las señales electromagnéticas que el enemigo emite a través de sus sistemas electrónicos.

191. El objetivo de la intercepción es conocer el contenido y/o naturaleza de las emisiones realizadas en aquellas frecuencias de interés obtenidas por las o los elementos de búsqueda. Esto se logra mediante el monitoreo de la información transmitida a través de redes no protegidas, así como aquellas protegidas cuyo esquema de seguridad sea vulnerable.

192. Para la óptima ejecución de las tareas de intercepción deben observarse los siguientes preceptos:

A. Llevarse a cabo sobre las frecuencias o señales de interés detectadas por los elementos de búsqueda.

B. Ser realizada indistintamente contra redes protegidas y no protegidas.

C. Toda la información obtenida por las o los elementos de intercepción debe ser remitida a los correspondientes elementos de análisis de señales.

D. Las y los operadores deben estar en condiciones de estimar la importancia relativa de una red, tomando como base los patrones de tráfico que maneja, aún tratándose de redes protegidas.

193. Es importante resaltar que el contenido de las señales interceptadas de las redes protegidas podría no ser conocido de forma inmediata, por lo que serán grabadas, registradas y actualizadas en las bases de datos, para posteriormente ser transferidas a otras o otros elementos superiores de guerra electrónica e inteligencia para su estudio y análisis.

194. Para lograr lo anterior, puede ser necesario el apoyo de otras dependencias gubernamentales que generen inteligencia, para poder explotar adecuadamente las señales a personal especialista en criptología y análisis.

Tercera Sección

Radiogoniometría

195. La Radiogoniometría es la localización de la ubicación geográfica de un emisor electromagnético sobre el terreno[7].

196. El objetivo de la radiogoniometría es proporcionar información sobre la ubicación geográfica aproximada de los emisores enemigos. Cuando esta información se integra con aquella obtenida por los elementos de búsqueda e intercepción, proporciona datos de valor sobre el orden de batalla enemigo, permitiendo así un conocimiento más amplio de la situación táctica.

197. Para localizar un emisor, la radiogoniometría generalmente utiliza el método de triangulación. Para el efecto, a lo largo de una línea de base se emplean dos o más estaciones de radiogoniometría, cada una proporcionando simultáneamente una línea de marcación hacia el emisor objetivo. A una distancia de operación de la línea de base de 15 kilómetros se puede obtener una precisión máxima de 1,000 metros.

[7] S.D.N. Manual de Operaciones de Guerra Electrónica. Edición 2010 Op. Cit. P.72.

198. En la actualidad, también es posible determinar la ubicación geográfica de un emisor que opere en la banda de HF, mediante el empleo de un solo equipo que utiliza técnicas de interferometría.

199. En la ejecución de las actividades de radiogoniometría, es necesario observar los siguientes preceptos:

A. La precisión de las líneas de marcación se ven afectadas por las características del equipo y del terreno, así como por la intensidad y reflexión de la señal.

B. Para obtener mayor precisión en la ubicación de los emisores enemigos se debe considerar:

a. El empleo del mayor número posible de estaciones de radiogoniometría, incrementando de esta forma el número de líneas de marcación.

b. Siempre que sea posible, operar las estaciones de radiogoniometría desde posiciones elevadas del terreno, o bien, en forma aerotransportada.

C. Cuanto más elevada sea la frecuencia de operación empleada por el emisor objetivo, será mayor la precisión en la obtención de su ubicación.

D. Las principales acciones de protección electrónica del enemigo que limitan la efectividad de esta función son las siguientes:

a. El empleo de antenas direccionales (se obtienen mejores resultados contra emisores que usan antenas omnidireccionales).

b. La realización de transmisiones cortas y/o en movimiento.

c. El empleo de técnicas de transmisión en espectro disperso, como el salto de frecuencia.

E. Debido a que la ubicación obtenida es aproximada, la radiogoniometría por sí sola no puede ser empleada como un sistema de adquisición de blancos para el apoyo de fuegos; sin embargo, esta información proporciona una excelente guía u orientación a otros sistemas de detección, para localizar y fijar objetivos con la precisión suficiente para actuar en su contra.

F. La localización en una misma área de un gran número de sistemas emisores puede ser indicativo de la ubicación de un importante centro de mando, tal como un cuartel general.

Cuarta Sección

Análisis de Señales

200. Análisis de señales. Es el conjunto de técnicas que se aplican para reunir, organizar e interpretar la información obtenida por nuestros sistemas sensores, para estimar y deducir el orden de batalla electrónico de la fuerza oponente, y evaluar las medidas de seguridad de señales propias.

201. Objetivo del análisis de señales. Producir información concerniente al orden de batalla, fuerza, intenciones, identificación de unidades y desarrollo de equipo electrónico de la fuerza adversaria, que proporcione como resultado inteligencia relativa a los siguientes aspectos:

A. Alerta inmediata de amenazas.

B. Obtención de blancos para las contramedidas electrónicas y medios de apoyo de fuegos.

C. Evaluación de la efectividad de las contramedidas realizadas.

D. Evaluación de los resultados de otras operaciones, tales como las psicológicas.

E. Sistemas electrónicos empleados por la fuerza adversaria.

202. Para el adecuado desarrollo del análisis de señales, se deben observar los preceptos que a continuación se indican:

A. Para deducir de la mejor manera posible el orden de batalla electrónico de la fuerza adversaria, el personal de analistas deben concentrar la totalidad de información proveniente de los sistemas sensores, de la forma siguiente:

a. El personal de la sección de intercepción proporciona toda la información relativa a frecuencias, distintivos de llamada, tipo de red, contenido de mensajes, el flujo de tráfico, los patrones de actividad y los tipos de transmisión.

b. Para señales de radio y radar, la intercepción buscara identificar sus características y parámetros técnicos.

c. Las estaciones de radiogoniometría proporcionan las posiciones y el seguimiento de los movimientos de los emisores.

B. El análisis de señales debe efectuarse en el menor tiempo posible y de la manera más precisa, esto con la finalidad de que la informacion se haga llegar oportunamente a los mandos y pueda ser aprovechada en beneficio de las operaciones o actividades que se realizan.

C. La construcción del orden de batalla electrónico de la fuerza adversaria es un proceso lento. Si éste aplica efectivas medidas de protección electrónica, dificulta el proceso de obtención de información y por lo tanto, su análisis. La información obtenida inicialmente será fragmentaria, adquiriendo coherencia conforme el proceso de obtención y análisis de la información sea desarrollado.

D. La información perecedera en tiempo y que sea susceptible de explotación inmediata deberá ser remitida de forma expedita directamente al órgano de inteligencia o nivel de mando que corresponda, a fin de que se tomen las acciones que en cada caso sean necesarias.

E. El análisis de señales se ve facilitado por el empleo de herramientas automatizadas, lo que agiliza su realización. Las principales herramientas a emplear son las bases de datos y programas de procesamiento de la información (software analítico).

F. Las y los analistas deberán desplegar en la ubicación donde mejor estén en capacidad de realizar su función. Los principales factores que determinan esta ubicación son:

a. Continuidad. El análisis de señales debe ser continuo para evitar que surjan vacios en el conocimiento de la situación. Por lo tanto, los analistas deben establecerse en una ubicación fija y tener capacidad para operar por escalones en caso de realizar desplazamientos.

b. Acceso a bases de datos. La función de análisis de señales requiere acceso a las bases de datos de inteligencia de señales y otras fuentes de información. Estas bases de datos proveen una referencia rápida de actividades llevadas a cabo anteriormente, agilizando el proceso de análisis.

c. Comunicaciones. Es necesario que las o los analistas reciban un gran volumen de información procedente de las funciones de intercepción y radiogoniometría; además deben enviar los resultados del análisis de señales hacia los organismos correspondientes.

d. Esto exige contar con sistemas de comunicaciones que permitan manejar la cantidad de tráfico requerida. De otra forma, será necesario que las o los analistas desplieguen junto con los sistemas sensores y así puedan procesar la información oportunamente.

G. Las o los analistas deben tener presente que el enemigo puede realizar el engaño electrónico, y por lo tanto, deben estar preparados para reaccionar en su contra. Cuando la información obtenida por los sistemas sensores denote actividad fuera de lo común, o bien, se obtenga con extrema facilidad, las o los analistas deberán corroborar o desmentir los datos recolectados en coordinación con otros órganos, agencias y fuentes de información.

Quinta Sección

La Inteligencia de Señales y las Medidas de Apoyo Electrónico

203. Inteligencia de señales. Son las actividades realizadas para la obtención de inteligencia, a partir de la intercepción de emisiones electromagnéticas en las diversas bandas de frecuencia, que permitan la identificación y localización de sistemas electrónicos de interés para el alto mando.[8]

204. De acuerdo a su campo de acción, la inteligencia de señales se divide en:

A. Inteligencia de comunicaciones. El conjunto de actividades destinadas a la obtención de material técnico e información de inteligencia de las emisiones electromagnéticas de comunicaciones de interés (código morse, telefonía, radiocomunicación, etc.).

B. Inteligencia electrónica. El conjunto de actividades destinadas a la obtención de material técnico e información de inteligencia de las emisiones electromagnéticas de no comunicaciones (radar, ayudas a la navegación, etc.). Al igual que el término anterior, este tambien es empleado para denominar la información producida por el referido conjunto de actividades.

205. Para describir en conjunto a las actividades de inteligencia de comunicaciones e inteligencia electrónica, cuando no existe la necesidad de diferenciar entre ellas se emplea como término genérico la expresión “inteligencia de señales”.

206. Al hablar de inteligencia de señales en comparación con las medidas de apoyo electrónico, se puede establecer que las diferencias entre los dos tipos de actividad se derivan principalmente del propósito y del empleo de estas funciones y del uso de la información que de ellas se deriva.

[8] Academia de Artillería de Segovia. Op. Cit. P.21-22.

207. Tanto las actividades de inteligencia de señales como las medidas de apoyo electrónico disponen de medios similares para su ejecución, consistentes en la búsqueda e intercepción, radiogoniometría y análisis de señales. Sin embargo, la inteligencia de señales tiene una finalidad estratégica y su explotación es a largo plazo, realizándose tanto en tiempo de paz como en tiempo guerra.

208. Por el contrario, las medidas de apoyo electrónico se ponen de manifiesto principalmente durante la realización de las operaciones militares, su finalidad es táctica y su explotación es inmediata. Estas medidas son también una fuente eficaz de información para la preparación del orden de batalla electrónico de la fuerza adversaria, por lo que la información que obtienen puede complementar las bases de datos producidas por la inteligencia de señales u otros órganos de la Secretaría de la Defensa Nacional.

209. Las medidas de apoyo electrónico y la inteligencia de señales, se interrelacionan ya que ambas producen información (por una parte, Inteligencia de señales para el conjunto, así como inteligencia de comunicaciones e inteligencia electrónica).

210. El alcance de las actividades de inteligencia de señales puede revestir aspectos de carácter político, económico, social y militar, tanto nacionales como internacionales; por esta razón, dichas actividades deben ser controladas y coordinadas por la Secretaría de la Defensa Nacional, tomando como base los lineamientos y objetivos trazados por el Alto Mando.

211. Debido a que la información obtenida por las actividades de inteligencia de señales es solo parte del amplio mosaico que el sistema de inteligencia militar debe procesar, los organismos de inteligencia de señales deben encontrarse subordinados en todos los aspectos a los órganos de inteligencia del Alto Mando.

212. En estas actividades, la criptografía destaca por su extensa aplicación, pues la información a nivel estratégico es protegida con complejos procedimientos y sistemas criptográficos, que requieren un alto grado de especialización de los recursos humanos por medio del adiestramiento, además de equipo y material especializado con tecnología de punta.

213. La permanente ejecución de las actividades de inteligencia de señales tiene como propósitos principales:

A. La obtención de información de interés con aplicaciones a mediano o largo plazo, que permita detectar y anticipar todas aquellas probables amenazas a la integridad, independencia y soberanía de la nación, así como a la seguridad interior.

B. La evaluación de la aplicación de las medidas de contrainteligencia, mediante el monitoreo de nuestras redes de comunicaciones para asegurar la disciplina de operación y la seguridad.

C. Proteger los sistemas emisores de carácter estratégico para la vida del país, mediante la oportuna detección de emisiones que atenten contra su óptimo funcionamiento.

214. Las instalaciones destinadas a la ejecución de actividades de inteligencia de señales deben ser de tipo permanente, dotadas de equipo especializado y personal altamente adiestrado y calificado para esta clase de actividades.

215. La amenaza latente de participar en conflictos bélicos en defensa de la nación, hacen necesario implementar las actividades de inteligencia de señales desde tiempo de paz, para que en caso de guerra, la información obtenida se explote como complemento de la inteligencia generada por otros órganos, agencias y fuentes para el apoyo de las operaciones militares.

216. El carácter concurrente del espectro electromagnético en los tres ámbitos de operaciones (tierra, mar y aire), da como resultado que las actividades de inteligencia de señales no tengan límites definidos, por lo que su ejecución en dichos ámbitos debe complementarse.

217. Para el efecto, es recomendable que desde tiempo de paz se implemente un sistema de inteligencia de señales con fines estratégicos, que sirva a las tres fuerzas armadas y que tenga como denominador común la seguridad nacional. Además, cada fuerza armada debe disponer de organismos de inteligencia de señales propias, adaptadas al ámbito en que cada una de ellas cumple sus misiones.

218. Al igual que en cualquier otro tipo de operación conjunta, cuando se realicen actividades de inteligencia de señales por parte de organismos pertenecientes a dos o más fuerzas armadas, es necesario disponer de un órgano rector conjunto que coordine y administre su funcionamiento.

Sexta Sección

Consideraciones de las Medidas de Apoyo Electrónico

219. La información obtenida de los sistemas electrónicos enemigos es un elemento indispensable para un o una comandante en la toma de decisiones. Cuando ésta se combina con la adquirida por otros medios, ayuda a resolver interrogantes como el ¿Quién?, ¿Qué?, ¿Cómo?, ¿Cuándo?, ¿Dónde?, ¿Por qué? y ¿Para qué?[9].

220. La radiogoniometría permite determinar la ubicación aproximada de los emisores de la fuerza adversaria; Esta información es útil para la determinación de sus movimientos, su dispositivo táctico y la obtención de datos acerca de blancos para perturbarlos o destruirlos, además de proporcionar a las y los comandantes indicios importantes para deducir el orden de batalla enemigo.

[9] S.D.N. Manual de Operaciones de Guerra Electrónica. Edición 2010 Op. Cit. P.74-77.

221. La integración de las funciones de búsqueda e intercepción, radiogoniometría y análisis de señales, con las demás actividades que se realizan para la obtención de información, tales como la fotografía, el interrogatorio de prisioneras o prisioneros de guerra, los datos proporcionados por las o los agentes, los reconocimientos, etc., permiten al mando visualizar un panorama completo y preciso de la situación.

222. Las y los comandantes difícilmente dispondrán del suficiente equipo y personal para interceptar y localizar todos los emisores de la fuerza adversaria, por lo que la principal prioridad serán los sistemas electrónicos de este último, que ofrezcan datos de mayor provecho para las fuerzas amigas, por ejemplo:

A. Sistemas de mando y control.

B. Sistemas de comunicaciones e información.

C. Sistemas de vigilancia aérea.

D. Sistemas de armas.

E. Otros en orden de importancia que requiera el mando de la fuerza adversaria o interfieran nuestras acciones.

223. Los demás sistemas emisores pueden ser considerados como de importancia secundaria, sin que esto signifique que dichos sistemas no deben ser interceptados y localizados.

224. Los sistemas de comunicaciones y de vigilancia del enemigo, regularmente son similares a los nuestros, por lo que los factores tales como el terreno, las condiciones meteorológicas, la distancia, la frecuencia y la seguridad son comunes y determinarán la probabilidad de localización e intercepción para ambas partes.

225. Para interceptar y localizar los equipos de radio que normalmente emplean las unidades tácticas como los de muy alta frecuencia (VHF), ultra alta frecuencia (UHF) y súper alta frecuencia (SHF), se requiere de línea de vista y que se encuentre el receptor dentro de la distancia eficaz del transmisor, por lo tanto, los equipos de búsqueda e intercepción y radiogoniometría, deben ubicarse tan a vanguardia como sea posible.

Capítulo III

Las Contramedidas Electrónicas

Primera sección

Generalidades

226. Las Contramedidas Electrónicas. Son las acciones que se toman para prevenir o reducir el uso efectivo del espectro electromagnético y medios de combate por parte del enemigo, mediante el empleo de energía electromagnética.[10]

227. Son la rama ofensiva de la guerra electrónica. A diferencia de las medidas de apoyo electrónico, que son realizadas mediante el empleo de sistemas pasivos, las contramedidas electrónicas actúan directamente contra los sistemas electrónicos y/o medios de combate de la fuerza adversaria empleando la energía electromagnética para lograr en ellos los siguientes efectos:

A. Interdicción. Mediante la restricción del empleo del espectro electromagnético para beneficio de sus operaciones, ya sea total o parcialmente, limitando a ciertos tipos los sistemas electrónicos que pueda operar.

B. Hostigamiento. Esto se logra por medio del empleo sistematico de sus sistemas electrónicos, lo cual dificulta la accion de mando por parte de la fuerza adversaria.

[10] Academia de Artillería de Segovia. Op. Cit. P.139.

C. Neutralización. Se manifiesta por los daños temporales o permanentes provocados por el empleo de armas de energía dirigida o electromagnética contra el equipamiento electrónico y determinados medios de combate de la fuerza adversaria, orientados a ponerlos fuera de servicio por un tiempo limitado.

D. Destrucción. Consistente en los daños permanentes causados por algunas armas de energía dirigida empleadas contra de la fuerza adversaria, con el fin de destruir sus medios de combate.

228. Debido a sus efectos sobre la fuerza adversaria, las contramedidas electrónicas deben ser consideradas como un medio de apoyo de fuegos a disposición de la o el comandante. Por este motivo requieren ser estrechamente coordinados con otros medios de apoyo de fuegos a través de la coordinación de fuegos de apoyo y su inclusión dentro del plan correspondiente.

229. Las medidas de apoyo electrónico se relacionan estrechamente con las contramedidas electrónicas, ya que, como se estableció en la sección anterior, las nombradas en primer término tienen como uno de sus propósitos proporcionar información de blancos para la ejecución de contramedidas electrónicas.

230. Las contramedidas electrónicas comprenden tres tipos de operaciones:[11]

A. La perturbación electrónica.

B. El engaño electrónico.

C. La neutralización electrónica.

[11] Ibid.

Segunda Sección

La Perturbación Electrónica

231. La perturbación electrónica. Es la radiación, retransmisión o reflexión deliberada de energía electromagnética, con el objeto de reducir la efectividad de los dispositivos y sistemas electrónicos empleados por la fuerza adversaria, sean estos de comunicaciones o no.

232. La perturbación electrónica aplicada en el momento oportuno sobre los blancos adecuados puede reducir de forma considerable la potencia de combate de la fuerza enemiga, negándole el empleo de sistemas electrónicos críticos.

233. La perturbación requiere una coordinación y planeación cuidadosa. En caso de que sea realizada sin la adecuada coordinación, se alertará al enemigo sobre nuestras capacidades e intenciones. De ser realizada con anticipación, proporcionará al enemigo el tiempo necesario para reaccionar y restablecer sus sistemas electrónicos y por lo tanto sus efectos serán limitados.

234. La perturbación electrónica es más eficaz en situaciones en que el enemigo depende de la energía electromagnética para el control de sus operaciones y para la obtención de información, ya que puede disminuir significativamente su aptitud para emplear su potencia de combate de manera oportuna y eficaz.

235. Las comunicaciones de la fuerza adversaria son una fuente de inteligencia, y al perturbarse, la información que proporcionan se perderá. Por lo tanto la perturbación es una actividad que debe estar estrechamente dirigida por la Sección Tercera (Operaciones) del Estado Mayor, en coordinación con la Sección Segunda (Inteligencia) del Estado Mayor.

236. Los efectos de la perturbación electrónica en el espectro electromagnético son generalizados, por lo que afecta tanto a los sistemas electrónicos propios como enemigos.

237. Las operaciones de perturbación son más exitosas cuando se les proporciona a las y los ejecutantes la mayor libertad de acción posible para atacar blancos planeados y de oportunidad. Sin embargo, deben observarse los mecanismos de control necesarios para evitar que afecten a nuestros sistemas electrónicos.

238. Para el efecto, la coordinación de estas operaciones se realiza desde el inicio de la planeación táctica, continuando durante todas las fases de la operación. Las medidas para el control de la perturbación deben estar contenidas en la orden de operaciones respectiva. Estas medidas son las siguientes:[12]

A. Control positivo. Es la impartición de órdenes específicas para perturbar a un determinado blanco o bien, alguna categoría de blancos, por ejemplo: redes de control de fuegos o radares de vigilancia. Las frecuencias y los tiempos en que se realiza no se especifican.

B. Control negativo. Es la negación de autorización para conducir operaciones de perturbación; por ejemplo: se prohíbe la perturbación antes de la hora H.

C. Control dirigido. Es el control directo de una operación de perturbación en todo momento, permitiendo o prohibiendo la perturbación de conformidad con el desarrollo de la operación. Las frecuencias a perturbar deben ser conocidas.

D. Control de frecuencias restringidas. Las listas de frecuencias restringidas son un mecanismo para evitar la perturbación de operaciones amigas que se efectúen. Se clasifican de la siguiente forma:

a. Frecuencias vedadas. Son de tal importancia que las fuerzas amigas jamás deberán perturbarlas intencionalmente; estas frecuencias son señaladas normalmente por la o el comandante de una unidad superior.

[12] National Defense. Electronic Warfare. Land Force B-GL-358-001/FP-001. Canadá. NATIONAL DEFENSE. 2004. P.74-75.

b. Frecuencias protegidas. Estas son frecuencias utilizadas por las fuerzas amigas para fines operacionales; su perturbación deberá ser restringida a menos que sea absolutamente necesaria y previa coordinación con la unidad usuaria.

c. Frecuencias de escucha. Son las empleadas por la fuerza adversaria y de las cuales se obtiene valiosa información, éstas frecuencias podrán ser perturbadas previa autorización de la o el comandante de la gran unidad, una vez que éste haya valorado lo que ganaría desde el punto de vista táctico a la luz de los datos técnicos y tácticos que dejaría de recibir al aplicar esta medida.

239. Los tipos de perturbación que pueden ser empleados para degradar o anular el funcionamiento de los emisores enemigos son los siguientes:

A. Perturbación Selectiva. Es la perturbación de una frecuencia o banda angosta de frecuencias. Provoca mínima perturbación con los sistemas amigos y permite el máximo aprovechamiento de la potencia del perturbador. Requiere de un conocimiento preciso de las frecuencias empleadas por la fuerza adversaria.

B. Perturbación de Barrera. Es la perturbación simultánea de una amplia banda de frecuencias. La potencia se distribuye en todo el ancho de banda. Permite restringir al enemigo el empleo de dicha banda de frecuencias, en lugar de una sola, por lo que para su ejecución se requiere un menor conocimiento de las frecuencias que este emplea. El empleo de este procedimiento incrementa la probabilidad de perturbar las redes amigas.

C. Perturbación de Barrido. Este tipo de perturbación combina las ventajas de las perturbaciones selectiva y de barrera. Consiste en la realización de un barrido dentro de un amplio rango de frecuencias, durante el cual se emite una señal de perturbación por un periodo de tiempo determinado en cada frecuencia o banda angosta de frecuencias del barrido. Los mejores resultados se obtienen al realizar el barrido a mayor velocidad.

D. Perturbación de Búsqueda Automática. También conocida como perturbación de respuesta, incorpora un receptor que busca actividad enemiga de forma automática en una banda determinada de frecuencias. Al detectar dicha actividad, el perturbador se sintoniza automáticamente y transmite en la frecuencia del blanco,

E. Este tipo de perturbación maximiza la efectividad del perturbador empleado a la vez que reduce su vulnerabilidad.

240. Para ser eficaz, un perturbador terrestre debe estar situado cerca de las tropas propias que se encuentren más adelantadas, para así poder tomar ventaja de su alta potencia de salida (normalmente entre uno y dos kilowatts). Esta ubicación permite que el perturbador sea eficaz contra objetivos en profundidad (como las redes de artillería), pero lo hace vulnerable en alto grado. Por este motivo los perturbadores deberán ser instalados preferentemente en vehículos blindados.

241. La instalación del perturbador en una plataforma aérea, tal como un vehículo aéreo no tripulado u otro tipo de aeronaves, puede eliminar la atenuación de la potencia de la señal causada por la intervención del terreno, permitiendo así el empleo de una emisión de menor potencia. Un perturbador aéreo de tan solo 200 watts a una distancia de 40 kilómetros puede ser tan eficaz como un perturbador terrestre de dos kilowatts a una distancia de quince kilómetros.

242. El despliegue de los perturbadores, tanto aéreos como terrestres, deberá realizarse con el fin de cubrir con sus radiaciones la mayor extensión posible del área bajo control de la fuerza adversaria, y de modo que permita la concurrencia de emisiones de dos o más perturbadores sobre un mismo blanco o categoría de blancos.

243. La eficacia de la perturbación electrónica está sujeta a los siguientes factores:

A. Potencia. Cuanta mayor sea la potencia más eficaz será la perturbación.

B. Distancia hacia el blanco. Cuanto más cerca de éste se realice, más efectiva será la perturbación.

C. Distancia del enlace. Es la distancia existente entre el transmisor y el receptor enemigos. Cuanto mayor sea esta distancia, más eficaz será la perturbación, requiriéndose menor potencia.

D. Terreno. Para perturbadores terrestres, el propio terreno proporciona cubiertas al objetivo por lo que se requiere de una mayor potencia para producir una perturbación efectiva.

E. Potencia del Transmisor Adversario. Dependiendo de la potencia de salida del transmisor enemigo, puede ser necesario destinar mayor potencia para efectuar la perturbación.

F. Las señales del perturbador deben ser compatibles con las señales por interferir.

244. En la perturbación de equipos de no comunicación, deben observarse los mismos principios que en la perturbación de las comunicaciones, existiendo tres formas de lograrlo:

A. Mediante la transmisión de una señal de mayor intensidad que la empleada para detectar o dar seguimiento a un blanco; dicha señal provoca que el sistema enemigo reciba la suficiente energía para opacar los blancos representados por las unidades amigas. Como ejemplos se pueden citar la perturbación de un radar por un transmisor de mayor potencia al eco reflejado, así como las bengalas desplegadas contra un sistema de armas guiado por infrarrojo.

B. Mediante el empleo de dispositivos pasivos que reflejan las señales transmitidas por el enemigo para dar seguimiento a blancos amigos, con el fin de opacarlos. Un ejemplo de estos dispositivos lo representa la cinta perturbadora denominada “chaffs”.

C. Mediante la retransmisión de una señal empleando dispositivos llamados “señuelos activos”, que retransmiten la señal utilizada para detectar o dar seguimiento a blancos amigos, simulando un blanco real con objeto de opacar o enmascarar a los blancos verdaderos.

245. Perturbadores desechables. Implica la colocación de un perturbador de baja potencia dentro de un radio de pocos cientos de metros del receptor a perturbar, lo que puede tener el mismo efecto degradador que un perturbador de alta potencia a 15 o 20 kilómetros de distancia. Pueden ser colocados manualmente o bien, ser lanzados desde aeronaves incluso existen modelos que pueden ser lanzados con por artillería. Son programados previamente para bloquear las señales locales de mayor intensidad o para activarse en una frecuencia específica durante un tiempo predeterminado.

246. También es posible emplear la perturbación electrónica para brindar protección a las fuerzas terrestres mediante el empleo de perturbadores que actúan contra las ojivas reguladas electrónicamente por tiempo o por proximidad, provocando su detonación prematura.

247. Otro método para proporcionar seguridad a las tropas consiste en emplear perturbadores contra artefactos explosivos de activación electrónica. Estos perturbadores generan una señal que puede provocar la activación prematura, detonación controlada, o bien, inhibir su detonación mediante la neutralización de sus circuitos de control.

Tercera Sección

El Engaño Electrónico

248. El engaño electrónico. Es la radiación, retransmisión, alteración, absorción o reflexión deliberada de energía electromagnética, de una manera destinada a confundir, distraer o engañar al adversario o sus sistemas electrónicos.[13]

[13] Ibid. Pag. 22.

249. Dentro de las operaciones de contrainformación, las acciones de engaño tienen como propósito fundamental crear en el enemigo falsos conceptos respecto a la situación, intensiones y posibilidades propias. El espectro electromagnético es un medio ideal para realizar estas acciones de engaño, ya que es común para nuestras fuerzas y las de la fuerza adversaria, lo que nos brinda la oportunidad de proporcionarle información falsa a través de sus propios sistemas electrónicos.

250. El engaño electrónico se divide en tres categorías:[14]

A. Engaño Electrónico por Imitación. Consiste en la emisión de señales electromagnéticas (con y sin contenido de comunicaciones) para infiltrarse en las redes y sistemas de la fuerza adversaria, imitando a sus emisores y hacerle creer que son parte de sus propios sistemas electrónicos, con el propósito de engañarlo, confundirlo o desorientarlo, así como obtener información. Incluye la ejecución de las siguientes técnicas:

a. La intrusión en las redes de comunicaciones de la fuerza adversaria para suplantar alguno de sus corresponsales, con objeto de obtener información, así como la impartición de órdenes o instrucciones, además de informes.

b. La retransmisión de tráfico propio de la fuerza adversaria grabada con anterioridad, destinado a crearle confusión.

c. El engaño a los radares de vigilancia de la fuerza oponente por medio de perturbadores activos o pasivos, a fin de presentarle blancos inexistentes que le indiquen una mayor composición de las fuerzas amigas.

[14] National Defense. Op. Cit. P.79.

d. La alteración o suplantación de las ayudas por radio para la navegación (Meaconing), la cual consiste en la intercepción y retransmisión de las radioseñales de dichas ayudas, en la misma frecuencia y con mayor potencia, con el fin de engañar y confundir a las o los pilotos u operadores y operadoras de aeronaves y vehículos de superficie, tanto marítimos como terrestres, a efecto de proporcionarles direcciones y ubicaciones erróneas, que los conduzcan a falsos blancos y emboscadas, o bien, perder la orientación geográfica. “Meaconing” es un término que no posee una traducción definida en nuestro idioma. Se deriva de la expresión “enmascaramiento de faro” (Masking Beacon).

B. Engaño electrónico por manipulación. Consiste en la manipulación de nuestras señales electromagnéticas (con y sin contenido de comunicaciones), modificando su contenido o características técnicas para proporcionar al enemigo información falsa sobre nuestras actividades e intenciones, degradando de esta forma la efectividad de sus actividades de guerra electrónica e inteligencia de señales.

C. Para la exitosa ejecución del engaño electronico por manipulacion, es necesario un profundo conocimiento de nuestros patrones de tráfico y características de emisión durante periodos de tiempo prolongados, así como en diversas condiciones y operaciones de combate. Entre las principales técnicas para lograrlo se encuentran:

a. Transmitir información falsa.

b. Generar o mantener niveles de tráfico falso.

c. Incurrir en Infracciones a los procedimientos de operación, de manera controlada.

d. Incrementar o reducir la actividad de emisores de no comunicación.

e. Modificar los parámetros técnicos de nuestros emisores.

D. Engaño electrónico por simulación. Son las acciones realizadas para presentar a la fuerza oponente información y/o capacidades propias, reales o ficticias, a fin de inducirlo a errar en sus apreciaciones respecto a nuestras fuerzas, empleando para ello nuestros sistemas de comunicación y no comunicación. Se divide en las siguientes categorías:

a. Simulación de unidad. Consiste en el uso de emisores para revelar que una unidad aparente se encuentra en una ubicación establecida durante un período de tiempo determinado. Por ejemplo, dotar a una unidad tipo batallón de los emisores necesarios para aparentar ser una unidad de mayor nivel.

b. Simulación de sistemas. Consiste en el empleo de sistemas que emiten señales características de un tipo de unidad en particular. Por ejemplo, un radar contra mortero o contrabatería es propio de una unidad de artillería, por lo tanto, mediante la activación de ese tipo de radar se puede indicar la aparente ubicación de una unidad de artillería.

c. Simulación de actividad. Se manifiesta mediante la operación de emisores de no comunicación para aparentar la ejecución o cambios en las actividades de una unidad. Por ejemplo, la implementación de radares de vigilancia para aparentar la adopción de una actitud defensiva, cuando la intención es atacar.

251. El engaño electrónico no debe ser practicado en forma indiscriminada, ya que normalmente es concebido dentro de un plan de operaciones de contrainformación, como parte de las medidas tácticas. Por este motivo, la responsabilidad de su planeación es responsabilidad de la Sección Segunda (Inteligencia) del Estado Mayor en coordinación con Sección Tercera (Operaciones) del Estado Mayor, por conducto del correspondiente órgano de dirección de guerra electrónica.

252. El engaño electrónico es particularmente efectivo en las circunstancias siguientes:

A. Cuando la fuerza oponente depende en gran medida del empleo del espectro electromagnético para su sistema de información y comunicaciones.

B. Cuando los sistemas oponentes emigos de inteligencia, vigilancia y reconocimiento dependen fundamentalmente de sus actividades de apoyo de guerra electrónica para la obtención de información.

C. Cuando es hábilmente conducido y plenamente integrado dentro de las acciones de engaño como parte de las operaciones de contrainformación.

D. Cuando se aplica en un momento crítico para las operaciones de la fuerza adversaria.

253. El engaño electrónico por manipulación puede ser decisión de las o los comandantes tácticos, siempre que solo emplee los sistemas electrónicos bajo su mando, debiendo establecerse la coordinación necesaria con objeto de no confundir a las unidades amigas.

254. El engaño electrónico por imitación y por simulación deben ser planeados y dirigidos por la o el jefe de la S-2 en estrecha coordinación con los demás integrantes del Estado Mayor y con el correspondiente órgano de dirección de guerra electrónica.

255. La infiltración en la red de comunicaciones de la fuerza oponente crea de inmediato una fuente productiva de información militar. Si este llegará a detectar el engaño electrónico por imitación, la fuente queda comprometida.

256. Salvo en los casos de extrema urgencia táctica a juicio de las o los comandantes subordinados, el engaño por imitación tiene que ser aprobado por el o la comandante de la gran unidad.

Cuarta Sección

La Neutralización Electrónica

257. Neutralización Electrónica. Es el uso deliberado de energía electromagnética para dañar temporal o permanentemente a los dispositivos electrónicos de la fuerza oponente.

258. Algunos ejemplos de armas de neutralización electrónica son las siguientes:

A. Armas de energía dirigida.

B. Rayos de partículas.

C. Pulsos electromagnéticos.

259. Las armas que irradian una gran cantidad de energía son empleadas para neutralizar los sistemas electrónicos de la fuerza oponente, sin embargo, esta acción representa un riesgo puesto que afecta a los sistemas propios, por lo que deberán extremarse las medidas de seguridad y cuidado en su manejo, su principal aplicación son el combate cercano y encuentros a línea de vista.

260. La doctrina de empleo de este tipo de armamento deberá estar contenida en los manuales de las fuerzas combatientes que lo empleen. Por lo tanto, las unidades de guerra electrónica no estarán involucradas directamente con la neutralización electrónica.

261. La aplicación de las contramedidas electrónicas en unidades inferiores a la brigada independiente deberá ser aprobada por el escalón superior.[15]

262. Dichas contramedidas pueden ser ejecutadas para atacar sistemas electrónicos de comunicación y de no comunicación.

263. Todas las actividades de contramedidas electrónicas deben ser ejecutadas bajo supervisión o coordinación de la Sección Tercera (Operaciones) del Estado Mayor, ya que tienen que ser reguladas para garantizar su correcta aplicación en las operaciones de combate.

264. La perturbación electrónica es la principal actividad de guerra electrónica que debe ser regulada, si no se tiene un estricto control de estas actividades podrían ocasionarse resultados catastróficos en nuestros propios medios.

[15] S.D.N. Manual de Operaciones de Guerra Electrónica. 2010 Op. Cit. P.85-89

265. Las restricciones evitan o disminuyen la perturbación a los sistemas electrónicos empleados por las unidades amigas.

Capítulo IV

Medidas de Protección Electrónica

Primera Sección

Generalidades

266. Medidas de Protección Electrónica. Es el componente de la guerra electrónica que comprende las acciones que se toman para asegurar el uso efectivo del espectro electromagnético por las fuerzas amigas, a pesar del uso de la energía electromagnética por parte de la fuerza adversaria.[16]

267. El objetivo de las medidas de protección electrónica es nulificar o reducir los efectos producidos por las medidas de apoyo electrónico y contramedidas electrónicas de la fuerza oponente, con el fin de preservar la seguridad de nuestras tropas y sistemas electrónicos.

268. Las medidas de protección electrónica constituyen la rama defensiva de la guerra electrónica que todas las unidades y personal de operadores u operadoras de los sistemas electrónicos deben practicar, su observancia es responsabilidad de todos los mandos, ya que de su correcta aplicación depende en gran medida la supervivencia en el campo de batalla.

269. Todos los comandantes son responsables de realizar una evaluación crítica de los sistemas electrónicos con que está dotada su unidad, a fin de descubrir las vulnerabilidades que pudieran ser explotadas por las actividades enemigas de guerra electrónica. Esto le permite adoptar o desarrollar las medidas de protección electrónica que mejor respondan a la situación particular.

[16] Academia de Artillería de Segovia. Op. Cit. P.22, 23, 229-249

270. Lo anterior incluye la formulación de medidas tácticas acordes con la situación táctica, las que deben ser incluidas en todos los planes de operaciones para evitar una reacción precipitada durante el combate.

271. Para desarrollar adecuadas medidas de protección electrónica, los mandos y sus auxiliares en todos los niveles deben:

A. Reconocer el alcance de la dependencia que las operaciones militares tienen con respecto a los sistemas electrónicos y la vulnerabilidad de estos sistemas a las medidas de apoyo de electrónico y a las contramedidas electrónicas de la fuerza adversaria.

B. Comprender que cualquier fuerza oponente tiene la capacidad de explotar, degradar y neutralizar todos nuestros sistemas electrónicos, ya que de aprovecharse en toda su extensión, le otorgará una ventaja táctica significativa.

C. Adoptar las medidas necesarias para asegurar que la protección de nuestros sistemas electrónicos no represente una ventaja táctica para la fuerza oponente.

272. La protección contra acciones hostiles de guerra electrónica debe realizarse tanto en tiempo de paz como en tiempo de guerra, ya que aún antes de cualquier conflagración real o potencial, la fuerza oponente aplicará las medidas de apoyo electrónico para obtener información y preparar sus operaciones futuras, reservando la aplicación de la perturbación y el engaño electrónicos para la guerra.

273. Por este motivo, la posibilidad de que nuestros sistemas electrónicos puedan afrontar y subsistir exitosamente contra acciones hostiles de guerra electrónica depende fundamentalmente del conocimiento preciso de la capacidad de los recursos de guerra electrónica adversarios, así como del equipamiento y nivel de adiestramiento de nuestras fuerzas en esta materia.

274. De acuerdo con su naturaleza, las medidas de protección electrónica permiten estructurar acciones electrónicas defensivas en dos fases: la defensa contra las medidas de apoyo electrónico en un primer tiempo y, posteriormente, la defensa frente a las contramedidas electrónicas.

275. La ejecución de contramedidas electrónicas se basa principalmente en una dirección eficaz por parte de las medidas de apoyo electrónico.

276. Lo anterior origina que algunas medidas adoptadas puedan ser empleadas en ambas fases, ya que las medidas de protección electrónica que dificulten a la fuerza oponente el empleo de sus medidas de apoyo de guerra electrónica, al mismo tiempo reducen la eficiencia de sus contramedidas electrónicas.

Segunda Sección

Clasificación de las Medidas de Protección Electrónica

277. Las medidas de protección electrónica se clasifican de acuerdo con su naturaleza, pudiendo ser de tres tipos:

A. Medidas técnicas. Aquellas que son incorporadas al diseño y funcionamiento de los equipos que emplean el espectro electromagnético como su medio de operación.

B. Medidas de procedimiento. Son realizadas por parte de las o los operadores de los sistemas electrónicos de comunicación y no comunicación.

C. Medidas tácticas. Son aquellas que las y los comandantes de todos los niveles deben adoptar con el fin de proteger a sus tropas, medios de combate y sistemas electrónicos.

278. Por los efectos provocados en la fuerza adversaria:

A. Medidas activas. Son medidas que pueden ser detectadas, tal es el caso de la alteración de los parámetros de transmisión de los emisores.

B. Medidas pasivas. Son medidas indetectables, como el caso de los procedimientos de operación y características técnicas del equipo empleado.

Tercera Sección

Medidas Técnicas

279. El desarrollo de nuevas técnicas de transmisión, cifrado y antenas buscan reducir la visibilidad electrónica del equipo, impedir la obtención de información, además de posibilitar la operación continúa de los sistemas electrónicos a pesar del uso ofensivo de la energía electromagnética.[17]

280. Ejemplo de esto son los radios tácticos que cuentan con un selector de potencia variable que puede mantenerse baja para evitar la detección o incrementarse para operar en frecuencias perturbadas. De forma similar, los radares cuentan con un control de ganancia que permite ajustar el brillo y el contraste en su pantalla para ignorar los efectos de perturbadores pasivos y revelar los blancos reales.

281. Las principales medidas técnicas de protección electrónica son las siguientes:

A. Diversidad de frecuencias. Consiste en poder operar los equipos en frecuencias de diversas bandas (HF, VHF, UHF, SHF), empleando cada banda de acuerdo a sus características para distintos tipos de aplicaciones.

[17] National Defense. Op. Cit. P.94-98.

B. Cifrado en línea. Es el cifrado que realiza un dispositivo de comunicaciones a un mensaje que le es introducido en lenguaje claro, sin embargo, la presencia de una señal todavía puede ser detectada, lo que permite ubicar su fuente por radiogoniometría.

C. Cifrado fuera de línea. Permite realizar el cifrado de un mensaje antes de colocarlo en los dispositivos de transmisión. Puede ser realizado por medios de cifrado electrónicos, mecánicos y manuales.

D. Antenas direccionales. Consiste en emplear antenas direccionales para radiar la menor potencia posible en dirección al enemigo y reducir la visibilidad electrónica, minimizando de esta forma la posibilidad de detección.

E. Arreglo de antenas de orientación nula. Consiste en el empleo de antenas que mediante el acoplamiento con procesadores especiales permiten atenuar casi totalmente la potencia radiada en dirección al enemigo, sin afectar la potencia que se radia en las demás direcciones.

F. Transmisión en ráfaga. Consiste en el empleo de dispositivos digitales que permiten la introducción de mensajes de formato corto en una memoria para ser luego transmitidos en una sola “ráfaga” electromagnética corta, lo que reduce el tiempo de transmisión para los mensajes largos.

G. Espectro disperso. Consiste en utilizar técnicas de transmisión que emplean diversas frecuencias para establecer un canal de comunicación. El uso de estas técnicas reduce la posibilidad de ser blanco de la intercepción, radiogoniometría y perturbación enemigas, pero incrementa el riesgo de sufrir perturbación mutua entre nuestras redes. Dentro de estas técnicas se encuentra la de “salto de frecuencia”.

H. Medidas de protección electrónica técnicas en equipos de no comunicación. Además de las antes descritas, existen algunas medidas orientadas exclusivamente a proteger los equipos de no comunicación, siendo las siguientes:

a. Supresión de firma de infrarrojo. Esta técnica es empleada para impedir que los sistemas enemigos de búsqueda de infrarrojo detecten las firmas de este tipo originadas por nuestras unidades. Entre las técnicas que se emplean para suprimir la firma infrarrojo de instalaciones o posiciones amigas se encuentra el empleo de redes de camuflaje y materiales especiales que absorben la firma de infrarrojo.

b. Radar. Consiste en incorporar a los sistemas de radar técnicas de procesamiento de señales para variar sus parámetros de operación y permitir su enmascaramiento.

c. Láser. Estos sistemas se basan fundamentalmente en la aplicación del proceso de medidas de apoyo electrónico como una medida de protección electrónica, proporcionando rápidamente la información necesaria quien ejerce el mando para que tome las medidas correspondientes con el fin de no presentar un blanco facil.

d. Pulso electromagnético. Los sistemas electrónicos empleados para la ejecución de tareas esenciales para una o un comandante deben ser protegidos con blindajes electrónicos contra el pulso electromagnético. El equipo que no sea protegido deberá utilizarse en las tareas rutinarias y menos críticas.

Cuarta Sección

Medidas de Procedimiento

282. La principal defensa para impedir ser blancos de las acciones de guerra electrónica de la fuerza oponente es evitar que nuestras emisiones electromagnéticas sean detectadas.[18]

[18] Ibid. Pag. 94-110.

283. De lo anterior surge la imperiosa necesidad de proteger a nuestras redes y su grado de importancia mediante el ocultamiento de su nivel de operación, identidad, tipo de equipo empleado e información que se maneja. De esta manera, la fuerza oponente se verá forzada a empeñar mayores recursos para poder obtener información de nuestros sistemas electrónicos.

284. Antes de que la fuerza oponente ejecute acciones de perturbación y engaño electrónicos en nuestra contra, deberá efectuar el proceso de búsqueda, intercepción, radiogoniometría y análisis de señales.

285. Si el nivel, identidad, tipo de equipos empleados e información manejada en nuestras redes pueden mantenerse ocultos, es posible que la fuerza oponente considere infructuosa o innecesaria su explotación debido a la escasa o nula información obtenida.

286. Si la fuerza oponente logra identificar el nivel o identidad de una red y la considera de particular importancia al alcanzar una fase crítica del combate, dentro de sus opciones de ataque dispondrá de las acciones de perturbación y engaño electrónicos, las que solo aplicará después de una cuidadosa planeación, ya que deberá decidir si obtendrá mayores ventajas de la intercepción o de la desorganización de nuestros sistemas electrónicos.

287. Con el fin de negar cualquier ventaja al esfuerzo de guerra electrónica de la fuerza oponente, se deben adoptar procedimientos de operación unificados para nuestros sistemas electrónicos, los que tienen que ser practicados adecuadamente por el personal de operadores u/o operadoras y usuarios en cualquier situación táctica. Estos procedimientos se encuentran regidos por los siguientes principios:

A. Evitar la detección.

B. Evitar la identificación del equipo y funcion de red.

C. Mantener la seguridad.

D. Defensa contra el engaño electrónico.

E. Defensa contra la perturbación.

F. Informar sobre cualquier actividad de contramedidas electronicas.

Subsección (A)

Evitar la Detección

288. Es el principio fundamental y el objetivo primordial del personal de operadores u operadoras. Mientras más tiempo tarde la fuerza adversaria en detectar nuestros emisores, mayor será el tiempo que estos podrán permanecer activos. La aplicación de este principio implica los siguientes procedimientos:

A. Empleo de baja potencia. Consiste en emplear únicamente la potencia necesaria para asegurar el óptimo funcionamiento del sistema de que se trate, esto permite reducir la visibilidad electrónica del emisor, y se consigue principalmente por la operación de los equipos en un nivel de potencia bajo.

B. Reducir la eficiencia de las antenas. Cuando no sea técnicamente posible ajustar el nivel de potencia de los emisores, se deben emplear antenas cuya eficiencia de radiación sea baja. Si el empleo de una antena de látigo instalada sobre un vehículo permite establecer la comunicación en forma satisfactoria, se debe evitar el uso de una antena elevada con plano de tierra.

C. Minimizar el uso de emisores y realizar transmisiones de corta duración, considerando lo siguiente:

a. Todas las y los comandantes deben tener presente que una fuerza enemiga está en capacidad de detectar cualquier transmisión en cualquier banda de frecuencias, y de que las emisiones cifradas sólo protegen el contenido de los mensajes, pero en los demás aspectos son tan vulnerables como aquellas que no cuentan con esta seguridad, teniendo además la desventaja de acentuar la importancia de una red.

b. Esta vulnerabilidad puede ser minimizada mediante el uso de transmisiones cortas, en la potencia mínima y sólo cuando sea necesario. Aunque las emisiones cortas no escapan de las actividades enemigas de intercepción y radiogoniometría, hacen más difícil su adecuada ejecución. El uso de mensajes prearreglados y códigos breves también coadyuvan a reducir el tiempo de transmisión.

D. Utilizar sistemas de comunicaciones alternos.

a. La aplicación del principio de multiplicidad de medios en las comunicaciones reduce la dependencia sobre la radiocomunicación. Esto no sólo reduce el número de emisiones, sino que también proporciona medios de respaldo para el caso en que seamos blancos de la perturbación electrónica enemiga.

b. Por lo anterior, siempre que sea posible se deberán canalizar los mensajes por medios de transmisión alternos, tomando en consideración que todo medio de transmisión es susceptible a la intercepción, por lo que los mensajes cuyo contenido sea secreto deben ser cifrados.

Subsección (B)

Evitar la Identificación del Equipo y Función de la Red

289. No obstante los esfuerzos realizados por reducir la visibilidad electrónica de nuestros emisores, se debe suponer que la fuerza oponente se encuentra en posibilidad de interceptar y localizar algunas emisiones, por lo que el siguiente nivel de defensa descansa en la adopción de medidas destinadas a evitar que identifique nuestras redes y equipos de importancia que puedan representar objetivos remunerativos para posteriores ataques. Los procedimientos empleados para evitar la identificación son:

A. Implantar procedimientos de operación de radiocomunicación estandarizados.

a. Su estricta observancia, reviste una importancia fundamental dentro de las medidas de protección electrónica.

b. Cualquier infracción de los procedimientos de operación faculta al enemigo para etiquetar a un emisor y la personalidad distintiva de su operador, permitiéndole realizar la identificación y seguimiento de nuestras unidades.

c. Los procedimientos de operación consisten en la adopción de frases comunes de fácil comprensión que ayudan a ocultar el nivel de una red y la identidad de unidades, además de agilizar las comunicaciones por radio.

d. Estos procedimientos se deben observar tanto en redes protegidas como no protegidas, debido a que reducen los tiempos de transmisión y evitan las violaciones a la seguridad cometidas por las y los operadores.

e. La responsabilidad de su aplicación recae sobre las o los operadores de sistemas electrónicos, pero la supervisión es realizada por las estaciones de control y monitoreo establecidas para mantener la disciplina de operación.

B. Emplear únicamente códigos autorizados. El uso de códigos propios de una unidad que no sean autorizados por el escalón superior facilita a la fuerza oponente identificarlos. Debe tomarse en consideración que cualquier criptoanalista entrenado esta en posibilidad de interpretar los códigos no autorizados con relativa facilidad.

C. Las instrucciones operativas de transmisiones. Estas instrucciones deben ser diseñadas de manera que no sólo mantengan el orden en nuestro sistema de comunicación, sino también para confundir las medidas de apoyo electrónico de la fuerza oponente. Estas instrucciones deben incluir, entre otros aspectos, los siguientes:

a. Distintivos de llamada de estaciones.

b. Distintivos de identificación de red.

c. Grupos de direcciones.

d. Asignación de frecuencias.

D. Cuando la disponibilidad y asignación de frecuencias así lo permitan, se deben cambiar las frecuencias de operación a intervalos irregulares con el fin de dificultar las actividades de intercepción y radiogoniometría enemigas, así como entorpecer la continuidad de su esfuerzo de acopio de información para obtener mejores resultados, siempre que sea posible se debe efectuar el cambio de las y los operadores y distintivos de llamada simultáneamente con el cambio de frecuencias.

E. Cambio de firma electrónica. Al efectuar los cambios de frecuencia es recomendable utilizar antenas diferentes y cambiar el tipo de equipos empleados en la red, con objeto de dificultar al enemigo la identificación de nuestras unidades con base en el análisis de la firma electrónica emitida.

Subsección (C)

Mantener la Seguridad

290. Cualquier violación a la seguridad debe ser reportada en forma expedita, a fin de que el o la comandante evalúe la gravedad de la infracción y adopte las medidas necesarias para contrarrestar cualquier acción enemiga resultante. Dentro de las medidas de seguridad a adoptarse se debe procurar:

A. El empleo de códigos cuando se opere en lenguaje claro para evitar proporcionar información relativa a:

a. La identificación de unidades.

b. El dispositivo de nuestras tropas.

c. Personalidades.

d. Lugares geográficos.

e. Cualquier información en coordenadas, incluyendo ubicaciones confirmadas de la fuerza adversaria.

B. Evitar los malos hábitos. Los malos hábitos proporcionan un medio para la identificación y seguimiento de personal, unidades y redes específicos a través del espectro de frecuencias, ya que la forma peculiar de operar un equipo por parte de las y los operadores representa rasgos que pueden ser rastreados para su localización en el campo de batalla.

Subsección (D)

Defensa Contra el Engaño Electrónico

291. Nuestros analistas de guerra electrónica deben estar preparados para afrontar los intentos del enemigo para aplicar el engaño por manipulación y por simulación. Se debe tener presente que generalmente el engaño genera mejores resultados en fases críticas del combate en que el mando requiere más que nunca de información precisa y oportuna para la conducción de las operaciones.

292. Una vez que el adversario identifica una red importante y decide que ha dejado de tener valor como fuente de información, podrá atacar dicha red con acciones de engaño por imitación mediante la intrusión en nuestras redes. La capacidad del adversario para infiltrarse en nuestras redes se reduce considerablemente si las o los operadores permanecen alerta y se sujetan estrictamente a los procedimientos y la disciplina de operación.

293. Ante la menor sospecha de intrusión en nuestras redes por parte del enemigo se debe aplicar la autentificación, si la estación sospechosa no autentifica o demora un tiempo sospechosamente largo para hacerlo, el engaño por imitación puede ser confirmado.

294. Al detectarse el intruso, la estación directora debe indicar a las estaciones en la red que ignoren al intruso, en caso de que la acción de este interrumpa las comunicaciones, la red debe efectuar el cambio de frecuencia.

295. Es importante impedir que el adversario conozca el grado de éxito obtenido, por lo que la estación directora debe emplear códigos para advertir sobre la intrusión y ordenar el cambio de frecuencia.

Subsección (E)

Defensa Contra la Perturbación

296. El primer paso resulta en identificar este tipo de amenaza, la cual depende en gran medida de la experiencia y adiestramiento de las y los operadores. Se puede intuir la ejecución de un ataque de este tipo al detectar un aumento considerable en el nivel de ruido en la red.

297. Inicialmente la perturbación puede tener poco efecto, pero conforme la potencia del perturbador aumenta resulta progresivamente más difícil establecer la comunicación u operar el radar. La perturbación puede continuar por un período considerable antes de que sea confirmada.

298. La reacción ante un ataque de perturbación debe seguir una secuencia lógica. Tan pronto como se sospecha la presencia de perturbación en la red, las y los operadores deben:

A. Reportar la posible perturbación de inmediato.

B. Retirar la antena y/o línea de transmisión del equipo. Si la perturbación desaparece, el equipo funciona correctamente y se puede confirmar la perturbación enemiga. Por otro lado, si la perturbación no desaparece, el operador puede suponer la presencia de una falla o una fuente de perturbación local.

C. Una vez confirmada la perturbación enemiga se deben comprobar los ajustes del equipo e intentar trabajar a pesar de la perturbación.

D. Aumentar temporalmente la potencia.

E. En caso necesario y de ser posible, se deben emplear estaciones retransmisoras.

F. De persistir la perturbación, se debe reubicar la antena o el sistema, buscando interponer cubiertas entre el perturbador enemigo y nuestro dispositivo.

299. Adiestramiento de las o los operadores. Toda acción de perturbación electrónica puede ser neutralizada. Además de los deberes antes enlistados, el aspecto más importante es el adiestramiento de las y los operadores, lo que implica la incorporación de un cierto grado de perturbación en los ejercicios de militares de aplicación sobre el terreno.

Subsección (F)

Informar Cualquier Actividad de Contramedidas Electrónicas

300. Cualquier intrusión o perturbación de la fuerza adversaria en nuestras redes debe informarse de inmediato, ya que estas acciones pueden ser selectivas y otros corresponsales pueden no ser conscientes de ellas.

301. El informe deberá ser analizado para descartar que se trate de perturbación mutua con otra red amiga en cuyo caso se requieren realizar los ajustes necesarios en las frecuencias de trabajo.

302. De tratarse efectivamente de contramedidas electrónicas del enemigo los sistemas de intercepción y radiogoniometría propios se deben empeñar en la tarea de localizar la fuente para proporcionar los datos que permitan a la Sección Tercera (Operaciones) del Estado Mayor y a la Sección Segunda (Inteligencia) del Estado Mayor, fuegos de apoyo y ordenar el ataque físico a la fuerza adversaria.

303. Conductos de los informes. Todo informe debe ser transmitido por medios seguros tan rápido como sea posible a los siguientes órganos:

A. A nivel corporación, las actividades de contramedidas electrónicas enemigas que sean detectadas deben ser informadas a quien ejerce el mando de la unidad y a la o el comandante de la unidad de transmisiones respectiva, quienes canalizan el informe a la gran unidad respectiva.

B. A nivel de grandes unidades, las contramedidas electrónicas del adversario son informadas simultáneamente a la célula de guerra electrónica de la gran unidad y a la u oficial de transmisiones en turno.

a. La célula de guerra electrónica ubicada en el Estado Mayor de la gran unidad ordena la ejecución de medidas de apoyo electrónico para identificar y localizar la fuente de las contramedidas electrónicas enemigas.

b. El monitoreo de las frecuencias y los cambios que se efectuen deben ser dirigidos por la o el oficial de transmisiones.

304. Niveles de informe.

A. Informe particular. A nivel corporación se hace necesario priorizar la formulación de un informe rápido sobre uno detallado para adoptar las medidas de reacción correspondientes. A este nivel las principales actividades a ser reportadas son la perturbación y engaños electrónicos.

B. Informe general. La célula de guerra electrónica de las grandes unidades deben tomar conocimiento detallado sobre las actividades de intrusión, perturbación y suplantación de radio ayudas de navegación por parte del adversario, así como la perturbación ocasionada por sistemas amigos.

Quinta Sección

Medidas Tácticas

305. Además de las características técnicas de protección electrónica incluidas en los equipos electrónicos y los procedimientos que las y los operadores deben seguir para defenderse de las acciones de guerra electrónica del adversario, existen también diversas medidas tácticas que las y los comandantes de todos los niveles deben adoptar para proteger nuestros sistemas electrónicos. Estas medidas tácticas incluyen:

A. Política de control de emisiones.

B. Despliegue de cuarteles generales.

C. Ubicación de los emisores.

D. Cambios frecuentes de ubicación.

E. Adecuada planeación de las comunicaciones.

F. Acción ofensiva como una forma de protección electrónica.

G. Vuelo adaptado al perfil del terreno.

Subsección (A)

Política de Control de Emisiones

306. El control de emisiones comprende todas las acciones destinadas a garantizar que nuestras emisiones electromagnéticas no proporcionen información de valor al enemigo y consiste en la imposición de restricciones a nuestras fuerzas para el empleo de los sistemas electrónicos con que cuenten. Para su planeación deben tomarse en cuenta los aspectos siguientes:

A. El control de las emisiones implica la reducción de las emisiones electromagnéticas al mínimo necesario para cumplir con la misión, por lo que es el método más efectivo para contrarrestar el esfuerzo del enemigo para conducir sus medidas de apoyo de guerra electrónica en nuestra contra.

B. El control de emisiones puede ser realizado de forma selectiva o total.

a. El control selectivo consiste en la supresión de las emisiones innecesarias, manteniendo en operación de manera controlada únicamente los emisores indispensables para las operaciones de la unidad. Incluye medidas tales como la realización de transmisiones breves y la operación de los sistemas de detección y vigilancia imprescindibles.

b. A su vez, el control total puede materializarse en dos formas:

i. Silencio electrónico. Es la acción que se aplica a todos los transmisores, incluyendo radiocomunicación, radioenlaces, radar, balizas, radiofaros, sistemas activos de infrarrojo, telémetros láser y cualquier otro sistema electrónico que irradie energía electromagnética.

ii. Radiosilencio. Es la acción que se aplica únicamente a los equipos de radiocomunicación.

C. Limitaciones. El control de emisiones es el medio de defensa más eficaz contra las acciones de guerra electrónica del enemigo; sin embargo, esto no siempre es posible debido principalmente a los siguientes factores:

a. El tiempo que las y los comandantes pueden operar sin radiocomunicación, radar, u otros sistemas electrónicos, depende de la situación táctica, así como de la disponibilidad de medios alternos de comunicación para mantener el flujo de la información.

b. La duración del silencio electrónico o el radiosilencio también depende del grado de vulnerabilidad que las y los comandantes estén dispuestos a aceptar debido a la pérdida temporal de algunos sistemas electrónicos críticos, como la vigilancia del campo de batalla y la defensa aérea.

D. Administración del control de emisiones.

a. Al igual que las demás acciones de guerra electrónica, el control de emisiones se encuentra regido por el principio de centralización, lo que se debe realizar al más alto nivel de mando posible para evitar que las unidades subordinadas implementen políticas particulares incompatibles entre sí, las que permitan al adversario determinar nuestro dispositivo por el estudio de las políticas practicadas dentro de los límites de cada unidad.

b. A pesar de que existen situaciones en que el silencio electrónico o de radio debe ser obligatorio (como al encontrarse las unidades en reserva), el control de emisiones debe aplicarse cuidadosamente, ya que su imposición puede dar indicios al adversario de que se preparan cambios en la situación u operaciones importantes.

c. En estas circunstancias, el control de emisiones debe ser orientado a mantener la actividad normal en las redes de radio, radar y otros sistemas, procurando evitar tanto el aumento repentino en el tráfico como el cese o disminución de la actividad que atraiga la atención del adversario.

Subsección (B)

Despliegue de Cuarteles Generales

307. La apropiada distribución y dispersión de las instalaciones de un cuartel general proporciona por sí misma ocultación física y electrónica, por lo que en el diseño del despliegue de un cuartel general es necesario tomar en consideración los siguientes aspectos:

A. Para proporcionar una mayor seguridad al mando y sus auxiliares, se debe hacer un máximo empleo de radios de operación remota cuando así lo imponga la situación táctica, coadyuvando con esto a la ocultación y dispersión de la firma electrónica del cuartel general.

B. Aún cuando se opere con equipos de radio instalados sobre vehículos tipo puesto de mando, se deben tomar en consideración para su ubicación todos los factores para seleccionar la ubicación de un emisor y así reducir la visibilidad electrónica de un cuartel general.

C. Realizar la supresión de infrarrojos, lo que implica el empleo de redes de camuflaje de absorción de infrarrojo y materiales especiales para reducir este tipo de firma.

Subsección (C)

Ubicación de los Emisores

308. Es posible reducir la potencia que los emisores transmiten y reciben en la dirección del adversario mediante la adecuada selección de su ubicación, por lo que toda u todo comandante y radio operador u operadora deben tomar en consideración la posición del enemigo cuando se seleccione la ubicación de un emisor. Para esto es necesario tomar en cuenta lo siguiente:

A. Los sitios que brindan mayor eficiencia a las comunicaciones, como la cresta de una elevación, ofrecen poca seguridad electrónica, por lo que es preferible ubicarse en las laderas de dicha elevación y utilizar las cubiertas que proporcione el terreno hacia la dirección de la fuerza adversaria antes de poner el equipo en funcionamiento. Además de los accidentes del terreno se pueden utilizar otra forma de cubiertas, como bosques, cuerpos de agua y construcciones, los que ofrecen algún grado de protección electrónica.

B. En caso de que la misión o tarea a desarrollar exija la ocupación de una posición dominante del terreno en línea de vista hacia el adversario, es recomendable emplear equipos a control remoto para ubicar los emisores en la ladera opuesta de la elevación.

C. Recordar que de poco o nada sirve el empleo de excelentes medios de camuflaje físico si las emisiones delatan nuestra ubicación.

Subsección (D)

Cambios Frecuentes de Ubicación

309. Una acción adicional de defensa para los cuarteles generales e instalaciones de comunicaciones, es el cambio de ubicación con la mayor frecuencia posible, ya que a pesar de la buena aplicación de las medidas de protección electrónica, eventualmente el adversario será capaz de detectar, identificar y localizar nuestros elementos de mando y control. Por lo anterior, es necesario tomar en consideración los siguientes aspectos:

A. Los frecuentes cambios de ubicación no sólo obstaculizan el esfuerzo de radiogoniometría enemigo, sino también dificultan a sus analistas la labor de construir nuestro orden de batalla electrónico.

B. En todo cambio de ubicación se deben utilizar nuevos distintivos de llamada y, de ser posible, nuevas frecuencias.

C. La naturaleza de las estaciones repetidoras ocasiona que su frecuente reubicación sea particularmente compleja; por este motivo deben ponerse en operación sistemas alternos para permitir su reubicación a la vez que se mantiene una comunicación continua.

Subsección (E)

Adecuada Planeación de las Comunicaciones

310. Al momento de realizar la planeación de las actividades de radiocomunicación para apoyar una operación, se deberán considerar los aspectos siguientes:

A. Dispersión de corresponsales. Al organizar redes tácticas de radio se debe procurar no incluir en una misma red a corresponsales que se encuentren ubicados a grandes distancias, ya que una mayor dispersión de los corresponsales implica el empleo de niveles de potencia mayores, a la vez que hace a nuestros emisores más vulnerables a la perturbación enemiga. Un despliegue cercano incrementa las posibilidades de una red para evitar la detección, así como para trabajar durante ataques de perturbación.

B. Diversidad de medios y sistemas de comunicación. Este aspecto implica dos formas de acción:

a. Disponer de medios alternos de enlace. Consiste en mantener organizados y listos, en previsión de su empleo, medios alternos de enlace como los medios alámbricos, las y los mensajeros y el personal de oficiales de enlace; los últimos dos nombrados ofrecen un medio de enlace con un alto grado de confiabilidad, aunque lento. Debe tenerse presente la posibilidad de que en determinadas ocasiones (como durante la imposición del radiosilencio) lleguen a ser los únicos medios factibles de emplear.

b. Empleo de diversas bandas de frecuencia. Implica contar con equipos de radiocomunicación que puedan operar en múltiples bandas de frecuencia (HF, VHF, UHF). Al tener conocimiento que el enemigo cuenta con amplia disponibilidad de perturbadores en alguna banda de frecuencias en particular, se debe operar en otras bandas.

C. Sistemas de repetición. Al establecer sistemas repetidores para atención de una red en particular, se debe contemplar que por este hecho se destacará su importancia, lo que atraerá la atención de los elementos enemigos de intercepción. El funcionamiento particular de estos sistemas los hace extremadamente vulnerables a la intercepción, radiogoniometría y perturbación electrónica. Esta vulnerabilidad se debe minimizar mediante un adecuado planeamiento del sistema de radiocomunicación, teniendo especial cuidado al emplear y ubicar sistemas de repetición.

D. Relevadores y radioenlaces. Debido a la naturaleza direccional de sus antenas, estos sistemas se deben emplear solamente en orientación paralela a la línea del frente, para evitar radiar hacia los sistemas de intercepción adversarios.

Subsección (F)

Acción Ofensiva como una Forma de Protección Electrónica

311. Defensa por ataque físico. Una medida extrema de protección electrónica consiste en la destrucción de los elementos de guerra electrónica del enemigo por medios físicos, tales como artillería de campaña, aviación, patrullas de combate, fuerzas especiales e irregulares, entre otros. En este sentido, destacan por su forma de acción los proyectiles guiados anti-radiación. Esta medida se ve influenciada por las siguientes consideraciones:

A. Las células de contramedidas electrónicas del enemigo representan un blanco remunerativo para nuestras fuerzas, por lo que deben ser ubicados y destruidos en prioridad cuando operan en contra de nuestros sistemas electrónicos.

B. Los elementos enemigos que conducen medidas de apoyo de guerra electrónica también representan un blanco prioritario; sin embargo, generalmente son difíciles ser detectados y localizados, a pesar de lo cual deben realizarse todos los esfuerzos necesarios para establecer su ubicación y proceder a su destrucción.

312. Defensa por ataque electrónico. Consiste en el empleo de contramedidas electrónicas para nulificar los sistemas de guerra electrónica del enemigo. Un ejemplo de esta medida se manifiesta al utilizar perturbadores desechables para apoyar una operación retrograda. En este caso los perturbadores son ajustados en nuestras frecuencias de operación y se colocan más a retaguardia de las tropas en retirada, orientados hacia el enemigo.

313. Esto crea una “pantalla electrónica” de suficiente intensidad para perturbar los sistemas de intercepción del adversario y negar información relativa al movimiento retrógrado, pero se ubican lo suficientemente retirados de nuestras redes para no perturbarlas.

Subsección (G)

Vuelo Adaptado al Perfil del Terreno

314. Consiste en el vuelo de aeronaves a baja altura, principalmente helicópteros, durante el cual se adaptan en todo momento a las características del terreno, por lo que mantienen una altura casi constante. Como medida táctica de protección electrónica, es empleado por las aeronaves que practican este tipo de vuelo para evitar ser detectados por los radares enemigos.

Sexta Sección

Consideraciones

315. La guerra moderna requiere de un uso intensivo de sistemas electrónicos para ejercer la acción de mando, el control de las operaciones y la vigilancia del campo de batalla, por lo que el funcionamiento adecuado y la supervivencia de estos sistemas se ha convertido en una necesidad vital para las y los comandantes y la fuerza a sus órdenes.

316. Nuestras fuerzas deben empeñar todos los recursos a su alcance para evitar que el enemigo detecte nuestras emisiones, ya que de lograrlo estará en capacidad de identificar nuestras unidades, establecer su dispositivo y atacarlas física o electrónicamente para lograr su desorganización y destrucción.

317. Es por lo anterior que la estricta aplicación y supervisión de las medidas de protección electrónica debe de convertirse en una acción prioritaria para cada comandante y sus auxiliares, además de las y los operadores y usuarios de sistemas electrónicos.

318. La gran cantidad de emisiones presentes en el campo de batalla brinda a la fuerza adversaria oportunidades ilimitadas. Esto implica que en ocasiones le sea más productivo interceptar y ubicar a nuestros emisores que tratar de perturbarlos o destruirlos.

319. Las características de protección electrónica incluidas en el diseño de los sistemas electrónicos deben ser combinadas con medidas tácticas y de procedimientos con el fin de nulificar los esfuerzos del enemigo para aplicar sus medidas de apoyo de guerra electrónica y contramedidas electrónicas.

320. La adecuada aplicación de las medidas de protección electrónica coadyuva a alcanzar un óptimo nivel de seguridad de señales misma que debe ser tomada en consideración por toda fuerza combatiente como parte de su seguridad táctica.

321. El principal requisito para una adecuada aplicación de las medidas de protección electrónica es el adiestramiento de los mandos y sus tropas. El objetivo a alcanzar por parte de quien ejerce el mando debe ser, enseñar a su personal a "pensar” en términos de protección electrónica.

Capítulo V

La Ciberguerra

Sección Única

Generalidades

322. La ciberguerra, por analogía, es una nueva clasificación de la guerra por el medio en el que se desarrolla y se caracteriza por el empleo del ciberespacio como teatro de operaciones.

323. Se manifiesta a través de una serie ilimitada de posibilidades a través de internet, con ella cualquier país, puede librar ciberguerras contra un adversario independientemente de los recursos, ya que la mayoría de las fuerzas militares basan sus centros de mando y control en redes conectadas a internet.

324. El uso de la internet permite que desde un país a otro pueda causar daños a sus sistemas de comunicaciones, transporte, suministros de servicios indispensables, pero el uso de la guerra cibernética o ciberguerra va más allá, pues puede desestabilizar los sistemas y poner en riesgo la seguridad nacional.

325. La ciberguerra desde un punto de vista internacional, se entiende como la agresión promovida por un estado y dirigida a dañar las capacidades de otro para imponerle la aceptación de un objetivo propio o, simplemente, para sustraer información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos, es decir, lo que habitualmente hemos entendido como guerra, pero con la diferencia de que el medio empleado no sería la violencia física sino un ataque informático que va desde “la infiltración en los sistemas informáticos enemigos para obtener información hasta el control de proyectiles mediante computadores.”

326. Se considera conveniente incluir en este manual conceptos que desde un punto de vista muy general, deben ser del conocimiento del personal del servicio, ya que estos se interrelacionan con actividades de seguridad y comunicaciones.

327. Ciberespacio. Ámbito intangible, de naturaleza global, soportado por las Tecnologías de la Información y Comunicaciones (TIC´s), que es utilizado para la interacción entre individuos y entidades públicas y privadas.

328. Ciberdefensa. Conjunto de acciones, recursos y mecanismos del estado mexicano en materia de seguridad nacional para prevenir, identificar y neutralizar toda ciberamenaza o ciberataque que afecte a la infraestructura crítica nacional.

329. Ciberseguridad. Conjunto de controles, procedimientos y normas del estado mexicano para proteger y asegurar sus activos en el ciberespacio.

330. “Las tecnologías informáticas transforman nuestra manera de pensar y actuar en cualquier aspecto de nuestras vidas, introduciendo importantes cambios estructurales, al modelar objetos de todo tipo en forma de información, permitiendo de este modo su manipulación por medios electrónicos”[19]

331. Es por esta razón que el mundo es cada vez más dependiente de la tecnología, puntualmente a la internet, lo que hace a los estados más vulnerables a un ciberataque, que puede poner en jaque las estructuras criticas de un estado, ya sea en su parte militar y la no menos importante, su infraestructura que puede afectar directamente a la población civil sin necesidad de disparar una sola arma.

332. Algunos de los objetivos de la ciberguerra son:[20]

A. Dañar un sistema o entidad hasta el punto en que ya no puede funcionar ni ser restaurado a una condición útil sin que lo reconstruyan por completo.

[19] (Unión Internacional de Telecomunicaciones, ITU. 2007. P.3).

[20]Gema Sánchez Medero Profesora de Ciencias Políticas LOS ESTADOS Y LA CIBERGUERRA, Madrid, España.

B. Interrumpir o romper el flujo de la información.

C. Destruir físicamente la información del adversario.

D. Reducir la efectividad o eficiencia de los sistemas de comunicación del adversario y sus capacidades de recolección de información.

E. Impedir al enemigo acceder y utilizar los sistemas y servicios críticos.

F. Engañar al enemigo.

G. Lograr acceder a los sistemas del enemigo y robarles información.

H. Proteger sus sistemas y restaurar los sistemas atacados. Responder rápidamente a los ataques o invasiones del adversario.

Segunda Parte

Empleo Táctico de la Guerra Electrónica

Capítulo I

Organización de las Unidades de Guerra Electrónica

Primera Sección

Generalidades

333. Las unidades de guerra electrónica, son organizadas con el fin de proveer la estructura para llevar a cabo las actividades relacionadas con la aplicación de las medidas de apoyo electrónico y de las contramedidas electrónicas, así como proporcionar asesoría especializada en relación a las medidas de protección electrónica realizadas por el personal de las armas y servicios.

334. El contar con la referida estructura, permite que las unidades de guerra electrónica estén en condiciones de cumplir la misión general de incrementar la potencia de combate de las tropas suministrándoles información, protegiendo el funcionamiento de sus sistemas electrónicos, limitando el funcionamiento de los del enemigo y contribuyendo con la preservación de su seguridad e integridad, mediante la explotación del espectro y energía electromagnéticos.

Subsección (A)

Medios de Acción

335. Los medios de acción con los que se organizan las unidades de guerra electrónica para el cumplimiento de su misión general, son los siguientes:

A. Personal. Consiste en las mujeres y hombres adiestrados y capacitados para llevar a cabo acciones de guerra electrónica. Además de las cualidades que posee el personal militar en general, las características específicas con que debe contar este personal son:

a. Amplia iniciativa para poder aplicar las medidas de apoyo y contramedidas electrónicas en un amplio rango de frecuencias, inclusive en situaciones en las que se carece de órdenes específicas, pero siempre bajo la orientación de las disposiciones emitidas por el escalón superior. También se manifiesta por la capacidad de identificar y reaccionar frente a las acciones de guerra electrónica enemigas.

b. Inteligencia. Debido a las características técnicas del material puesto a su disposición, el personal debe poseer la capacidad de interactuar en forma eficiente con los equipos de guerra electrónica, a efecto de explotar sus posibilidades en forma íntegra y disminuir sus vulnerabilidades, preservando a la vez su estado de funcionamiento en forma óptima.

c. Buen adiestramiento. Debido a que las actividades de guerra electrónica demandan en muchas ocasiones de la reacción del personal en forma inmediata, lo que permite ejecutar las órdenes recibidas en forma práctica.

d. Conocimiento de otros idiomas y/o dialectos. El personal integrante de los equipos de búsqueda e intercepción y análisis de la información, deben contar con los conocimientos necesarios sobre el idioma o dialecto empleado en las comunicaciones del enemigo para poder reconocer su importancia, evaluarlo correctamente y su oportuna explotación.

B. Material. Consiste en todos los equipos empleados para la ejecución de actividades relacionadas con las medidas de apoyo electrónico y las contramedidas electrónicas. Entre los principales equipos se encuentran los siguientes:

a. Radio receptores de amplio rango de frecuencias.

b. Sensores de detección de radar.

c. Radiogoniómetros fijos, vehiculares, aéreos y portátiles.

d. Sistemas de búsqueda frontal de infrarrojo (FLIR) y otros sensores pasivos de infrarrojo.

e. Sistemas sensores pasivos de láser.

f. Perturbadores de diversos tipos y niveles de potencia, incluyendo los desechables denominados también no recuperables, los que pueden ser operados en forma fija, vehicular o aerotransportada.

g. Sistemas de comunicaciones que permitan el enlace e intercambio de información entre los diversos organismos de los sistemas de guerra electrónica, de apoyo de fuegos e inteligencia, incluyendo la capacidad de interactuar con los órganos de inteligencia a nivel estratégico.

h. Equipos informáticos que permitan el registro de las señales detectadas, el uso de herramientas para su análisis y el acceso a bases de datos.

i. Además de los equipos empleados por las unidades de guerra electrónica que se describen con anterioridad, las unidades de combate de las armas podrán contar con otros materiales, tales como armas de energía dirigida, proyectiles guiados antirradiación, perturbadores de protección contra granadas y proyectiles guiados con sistemas de detonación electrónica, perturbadores contra artefactos explosivos improvisados, sensores remotos del campo de batalla, entre otros.

C. Vehículos. Consisten en los medios que proporcionan la movilidad requerida por una unidad de guerra electrónica para el cumplimiento de sus misiones. La unidad puede ser dotada de vehículos ya sea para operar a bordo de ellos o solamente para transportarse, siendo lo ideal que cuenten orgánicamente con la cantidad suficiente para realizar sus actividades. Estos vehículos pueden ser:

a. Terrestres. Dependiendo del tipo de unidad apoyada, los requerimientos de movilidad, operaciones a realizar y el grado de amenaza, pueden ser consideradas dos categorías de vehículos:

i. De transporte. Son empleados solamente como medio de transporte para el personal y material de las unidades de guerra electrónica cuando no cuenten con vehículos especializados y por lo tanto su forma de operar sea fija o semifija, lo que limita en forma considerable sus capacidades de apoyo e incrementa su vulnerabilidad. Esta categoría normalmente será empleada por unidades que operen en la zona del interior, realizando funciones de inteligencia de señales.

ii. Especializados. Denominados “plataformas”, son vehículos dedicados exclusivamente para la ejecución de actividades de guerra electrónica en forma móvil o semimóvil, lo que incrementa sus capacidades de apoyo y reduce en gran medida sus vulnerabilidades. El tipo de plataformas empleadas por una unidad determina su clasificación como de guerra electrónica ligera o pesada. Las plataformas pueden ser:

D. Ligeras. Son vehículos de carácter general (camionetas o camiones ligeros), en los cuales son instalados equipos que pueden ser operados estacionados o en movimiento. Generalmente tienen reducida capacidad de carga, lo que impone limitaciones en el grado de equipamiento de la plataforma pero poseen gran movilidad. Son altamente vulnerables a los efectos del fuego enemigo, por lo que se emplean principalmente en las áreas de retaguardia o en situaciones que requieran de un elevado grado de movilidad. Conforman las unidades de guerra electrónica ligera.

E. Blindadas. Son vehículos blindados en los cuales son instalados equipos que pueden ser operados estacionados o en movimiento. Estas plataformas proporcionan mayores capacidades técnicas y tácticas debido al incremento de la capacidad de carga y la mayor protección física al personal y material, por lo que pueden operar en las áreas de combate con menores limitaciones que las plataformas ligeras. Sin embargo, su empleo incrementa los requerimientos de apoyo logístico para su conservación y mantenimiento. Conforman las unidades de guerra electrónica pesada.

F. Aéreos. Son denominados en forma general “plataformas aéreas”, y consisten en aeronaves tanto de ala fija como rotativa, que pueden pertenecer al arma de aeronáutica del ejército o a la fuerza aérea. Están equipadas para desarrollar actividades de guerra electrónica desde el aire, con lo cual extienden el alcance de los medios de guerra electrónica más allá de la línea de vista, incrementando con ello sus capacidades.

G. Sus operaciones pueden ser realizadas en forma independiente o conjuntamente con fuerzas de superficie u otros elementos aéreos y conforman las unidades de guerra electrónica aérea. Las plataformas aéreas pueden ser:

a. Tripuladas. Son aeronaves en las cuales los equipos de guerra electrónica son operados por elementos humanos en forma personal.

b. No tripuladas. Son Aeronaves No Tripuladas (A.N.T.´s) en los que la operación de los equipos de guerra electrónica es realizada en forma remota desde una estación de control. Generalmente son de dimensiones reducidas, por lo que cuentan con menores características que las plataformas aéreas tripuladas, como el equipamiento inherente a la limitada capacidad de carga, así como escasa autonomía de vuelo; no obstante lo anterior, existen A.N.T.´s de mayor tamaño que pueden superar dichas limitaciones.

H. Armamento. El armamento con que se dota a las unidades de guerra electrónica es de tipo individual, empleándolo el personal en las acciones de combate en que se vea involucrado, así como para la protección de sus medios.

Subsección (B)

Características

336. La naturaleza de las operaciones que realizan las unidades de guerra electrónica y los medios de acción de que están dotadas, permiten que estas unidades adquieran las características siguientes:

A. Movilidad. Característica proporcionada en función de los vehículos de que están dotadas sus unidades, que les permite desplazarse en el área de combate, llevando a cabo sus operaciones en movimiento.

B. Flexibilidad. Esta característica se manifiesta desde dos aspectos:

a. La flexibilidad de realizar diversas operaciones sin necesidad de cambiar de emplazamiento. Esto le permite cumplir misiones de reconocimiento electrónico, intercepción y radiogoniometría cubriendo diferentes direcciones, empeñándose contra varios blancos simultáneamente, o bien, cumplir misiones de contramedidas electrónicas concentrando su acción sobre uno o varios blancos desde ubicaciones dispersas.

b. La flexibilidad de operar tanto por unidades orgánicas como mediante la integración de agrupamientos tácticos de composición variable, de acuerdo con la disponibilidad de recursos y los requerimientos que imponga la misión, manifestada esta última por la organización para el combate.

C. Versatilidad. Se manifiesta por la capacidad de realizar diversas funciones tácticas durante el combate, por lo que una misma unidad puede llevar a cabo actividades de intercepción, radiogoniometría y perturbación de manera simultánea, además de proporcionar apoyo en la ejecución de operaciones de engaño y la aplicación de las medidas de protección electrónica.

D. Acción Técnica. Se refiere a la naturaleza eminentemente técnica de los materiales empleados en la guerra electrónica, por lo que es necesario que sus medios se mantengan actualizados tecnológicamente.

E. Vulnerabilidad. En general, el aspecto de las antenas y demás materiales empleados por las unidades de guerra electrónica, así como las emisiones electromagnéticas que generan, las hacen fácilmente localizables en el terreno de combate por las actividades de reconocimiento. Esta vulnerabilidad obliga a que en las diversas situaciones tácticas se apliquen de manera intensiva las medidas de protección electrónica, a efecto de resguardar sus medios de los efectos de ataques físicos o electrónicos del adversario.

Subsección (C)

Modos de Acción

337. Representan la forma de actuar de las unidades de guerra electrónica para el cumplimiento de sus misiones. Estos modos de acción son:

A. El Movimiento. Consiste en el desplazamiento que las unidades de guerra electrónica materializan en el campo de batalla, para estar en condiciones de cumplir sus misiones proporcionando apoyo de su especialidad a las unidades de combate.

B. El Trabajo. Consiste en las acciones realizadas para apoyar a las tropas combatientes proporcionándoles información de valor militar y coadyuvando a la preservación de su seguridad física y electrónica.

C. El Fuego. Este modo de acción no se manifiesta en el sentido tradicional del fuego “físico”, sino por la acción de los medios de perturbación electrónica, capaces de degradar o nulificar el eficaz funcionamiento de los sistemas electrónicos del enemigo. También se manifiesta por la acción de las armas de neutralización electrónica con que estén dotadas las tropas.

Subsección (D)

Funciones

338. Al actuar dentro del marco de una unidad superior, las unidades de guerra electrónica desarrollan las funciones siguientes:

A. Proporcionar alerta y reconocimiento inmediatos de amenazas mediante el empleo del material con el que están dotados.

B. Coadyuvar en la búsqueda de información como organismos de inteligencia del mando correspondiente, proporcionando datos para apoyar las operaciones en curso o el desarrollo de planes a futuro.

C. Ubicar emisores electromagnéticos enemigos asignándolos como blancos.

D. Perturbar los sistemas enemigos de mando, control, detección, armas, etc.

E. Apoyar y asesorar en la ejecución de operaciones de engaño electrónico.

F. Proveer asesoría especializada sobre la aplicación de las medidas de protección electrónica.

Subsección (E)

Posibilidades

339. Las posibilidades que pueden desarrollar las unidades de guerra electrónica son:

A. Proporcionan cobertura en toda la zona de acción de la unidad apoyada, en todo tiempo, terreno y circunstancia.

B. Conducir contramedidas electrónicas para incrementar la potencia de combate de la unidad apoyada.

C. Procesar y mantener segura la información clasificada que se les proporciona u obtienen a través de sus medios, así como los materiales con que cuente, de acuerdo con las políticas y disposiciones relativas a contrainformación y seguridad.

D. Establecen comunicaciones seguras y confiables hacia y desde los distintos organismos del sistema y escalones de mando.

E. Aseguran la continuidad de sus operaciones mediante el empleo de medios redundantes.

F. Se adaptan al grado de movilidad de la unidad apoyada así como a la situación táctica.

G. Operan sus medios a bordo de aeronaves y vehículos terrestres blindados o ligeros, sin perjuicio de operar también por medio de equipos portátiles transportados por su operador u operadora, dependiendo del grado de protección y movilidad requerida para satisfacer las necesidades de la unidad apoyada.

H. Adaptarse a entornos de guerra química, biológica y radiológica si cuentan con el material adecuado para ello.

I. Adquieren una estructura flexible mediante la organización para el combate.

Subsección (F)

Limitaciones

340. Las limitaciones de las unidades de guerra electrónica son las siguientes:

A. Complejidad para ser equipadas, debido a las características y grado de sofisticación de su material.

B. Las características técnicas del material obligan a la impartición de un adiestramiento especializado y prolongado al personal, lo que dificulta el sistema de reemplazos.

C. La evolución de la tecnología hace necesario que el material deba ser actualizado constantemente para el cumplimiento de sus misiones.

D. Reducida disponibilidad de materiales para la ejecución integral de sus actividades contra la totalidad de emisores del adversario.

E. Necesidad de protección táctica y electrónica para contrarrestar los efectos de los ataques físicos y electrónicos del adversario.

Segunda Sección

El Sistema de Guerra Electrónica

Subsección (A)

Integración Funcional

341. Para el cumplimiento de sus misiones, el material empleado por las unidades de guerra electrónica, cuenta con características técnicas que le permiten adaptarse rápidamente a los cambios de la situación electrónica del adversario.

342. Dentro de estas características se encuentra la del diseño modular, para permitir su instalación en instalaciones fijas o a bordo de plataformas terrestres o aéreas, de acuerdo con las necesidades tácticas y los medios de que dispongan las fuerzas combatientes. Esta característica del material es fundamental para determinar la estructura funcional de las unidades de guerra electrónica.

343. El diseño modular hace referencia a la disponibilidad de equipos electrónicos denominados “módulos”, cada uno de los cuales permite la ejecución de una tarea específica. De esta forma existen módulos de búsqueda e intercepción, de radiogoniometría, de análisis y de perturbación electrónica.

344. La disponibilidad de estos módulos permite la conformación de unidades orgánicas de nivel escuadra y pelotón con funciones tácticas y técnicas específicas. Por este motivo será posible organizar, entre otras, las siguientes unidades:

A. Unidades con capacidades básicas.

a. De búsqueda e intercepción.

b. De radiogoniometría.

c. De análisis.

d. De perturbación.

e. De engaño electrónico. Sobre estas unidades es necesario considerar lo siguiente:

i. Para tener éxito, las operaciones de engaño electrónico implican la participación de los diversos sistemas electrónicos de todas o la mayor parte de las unidades que integran una fuerza de combate. Por este motivo es necesario que sea realizado tanto en sistemas de comunicaciones como de no comunicaciones.

ii. Por lo anterior, cualquier unidad equipada sólo con sus medios orgánicos, únicamente tiene capacidad para conducir acciones de engaño electrónico en un grado limitado. En el caso particular de las unidades de guerra electrónica, esta capacidad se limita al engaño por imitación o manipulación realizado a través de sus propios sistemas de comunicaciones, lo que reduce significativamente la capacidad de dirección de sus propias operaciones y la obtención de información de valor militar.

iii. Debido a que los medios requeridos para realizar operaciones de engaño electrónico (en cualquiera de sus tres tipos) sobrepasan las posibilidades materiales de cualquier unidad, la integración de unidades de engaño electrónico se lleva a cabo con medios dedicados específicamente para esa actividad, ya sea que se ministren exclusivamente con ese propósito o bien, se sustraigan de otras unidades por el tiempo estrictamente necesario.

iv. Lo antes expuesto origina que estas unidades sean organizadas únicamente con el fin de cumplir misiones específicas y en apoyo de otras acciones tácticas de engaño. Tal podría ser el caso del establecimiento de redes de comunicaciones dedicadas exclusivamente al intercambio de tráfico falso para denotar la ejecución de una operación futura, para no distraer los medios de las unidades de combate de su función principal.

v. En la materialización del supuesto anterior, es necesario tener presentes los efectos del análisis de la firma electrónica de toda emisión por parte del adversario.

B. Unidades con capacidades específicas.

a. De reconocimiento electrónico. Son unidades altamente móviles que cuentan únicamente con capacidad de efectuar actividades de monitoreo pasivo para conocer la ocupación y aplicaciones del espectro electromagnético en una determinada porción del terreno.

b. De apoyo electrónico. Son unidades que integran las funciones pasivas de búsqueda, intercepción y radiogoniometría. Excepcionalmente podrá ser incorporada la capacidad de análisis.

c. De inteligencia electrónica. Son unidades que cuentan con la capacidad integral de aplicar las medidas de apoyo electrónico (incluyendo el análisis) sobre señales sin contenido de comunicaciones.

d. De contramedidas electrónicas. Son unidades que integran la capacidad de conducir operaciones activas de perturbación y engaño electrónico.

345. Las unidades antes descritas facilitan el empleo dinámico de las actividades de guerra electrónica hacia objetivos definidos, de acuerdo con las necesidades que imponga cada situación, la misión por cumplir y las posibilidades electrónicas del adversario, con el fin de evitar el dispendio de los recursos de guerra electrónica, generalmente limitados.

346. Las unidades de guerra electrónica pueden realizar operaciones con su constitución orgánica o bien, mediante la agrupación de unidades de menor nivel con capacidades básicas para integrar, mediante la organización para el combate, unidades multifuncionales de composición y estructura variables denominados:

A. Destacamentos.

B. Equipos.

C. Unidades circunstanciales básicas integradas durante el combate, con el fin de proporcionar apoyo de su especialidad a una gran unidad.

347. Con el fin de obtener mayores y mejores resultados en la ejecución de sus operaciones, la forma de operar de las unidades de guerra electrónica, orgánicas o circunstanciales, normalmente será desplegando en apoyo de las unidades de combate.

Subsección (B)

Capacidades Técnicas

348. Con base en las necesidades impuestas por la misión para la cual haya sido creado, las unidades o agrupamientos que conformen el sistema de guerra electrónica se deben integrar con los medios que les permitan adquirir todas o algunas de las capacidades siguientes:

A. Apoyo electrónico. Esta capacidad puede ser realizada por la incorporación de las siguientes acciones:

a. Búsqueda e intercepción de comunicaciones. Su propósito es reconocer el espectro electromagnético en busca de blancos que permitan obtener información suficiente en cantidad y en detalles sobre las comunicaciones del adversario.

b. Radiogoniometría de comunicaciones. Permite obtener información detallada respecto a la ubicación de los emisores adversarios, desplegando destacamentos en una línea de base.

c. Inteligencia electrónica. Realiza por sí sola la búsqueda e intercepción, la radiogoniometría y análisis de emisores de no comunicaciones. En este módulo el análisis es realizado mediante la comparación de los parámetros del emisor con una base de datos para determinar el tipo de radar o equipo, así como sus sistemas asociados.

d. Análisis de señales. Puede llevarse a cabo mediante el despliegue de analistas junto con los elementos sensores, pero es recomendable que se ubiquen en una posición tal que les permita concentrar la información proveniente de varios destacamentos. Cada nivel funcional de la estructura proporciona un nivel de refinamiento mayor al análisis, debido al mayor acceso a las bases de datos del sistema de inteligencia.

B. Contramedidas electrónicas. Se refiere a la disponibilidad de equipos que permiten atacar electrónicamente a los emisores del adversario, tanto por perturbación como por engaño electrónicos, mediante ataques planeados y contra blancos de oportunidad. Estos equipos pueden operar aisladamente o estar integrados en una misma plataforma con equipos de apoyo electrónico.

349. Además de las capacidades técnicas antes descritas, las unidades de guerra electrónica deben contar con elementos que les proporcionen los apoyos siguientes:

A. Integración al sistema de mando, control e información de guerra electrónica. Consiste en la reunión de personal, sistemas de información y comunicaciones y en su caso instalaciones, que proveen los medios para el ejercicio del mando y el control de las operaciones de guerra electrónica, además del intercambio de la información necesaria entre sus elementos, así como para la integración a los sistemas de apoyo de fuegos e inteligencia.

B. Apoyo de servicios. Las unidades de guerra electrónica, al igual que cualquier otra fuerza militar, requieren del apoyo de servicios para el adecuado desarrollo de sus funciones, destacando por su importancia el mantenimiento del material.

Subsección (C)

La Organización para el Combate

350. Debido a que la orgánica permanente de las unidades de guerra electrónica no siempre será adecuada o suficiente para el cumplimiento de sus misiones, en ocasiones será necesario recurrir a la organización para el combate, la cual consiste en colocar a las unidades dentro de agrupamientos tácticos acordes a la misión por cumplir, para proporcionar apoyo a una determinada unidad.

351. La organización para el combate se manifiesta en cada situación particular de acuerdo con el esquema de maniobra del mando y puede ser modificada en cualquier momento durante el curso de la acción, a fin de afrontar los problemas y cambios que la situación vaya presentando en su evolución. Para el efecto, una buena organización para el combate debe responder a lo siguiente:

A. Que proporcione adecuado apoyo a las unidades de maniobra, de acuerdo con su misión en el conjunto.

B. Que exista una distribución de las unidades de guerra electrónica de acuerdo con las características, capacidades y limitaciones de sus materiales, de manera de obtener de ellas el mayor provecho posible.

C. Que se faciliten las operaciones futuras.

D. Por lo que respecta a los medios de perturbación electrónica, que sea posible concentrar las emisiones de los perturbadores donde se requieran, hasta el límite del alcance de su potencia efectiva.

Tercera Sección

Las Unidades de Guerra Electrónica

Subsección (A)

Generalidades

352. El control de las operaciones de guerra electrónica, debe ser ejercido mediante la aplicación del principio de control centralizado. Esto implica que todas las unidades de guerra electrónica que actúen en un escalón determinado, sean orgánicas o en refuerzo, deben mantenerse bajo el control directo del mando táctico, a través de la o el comandante de guerra electrónica de mayor jerarquía.

353. Este control proporciona la máxima flexibilidad para dirigir las operaciones de guerra electrónica en toda la zona de acción de la unidad apoyada, evitando el dispendio de recursos y la duplicidad de esfuerzos.

354. El control centralizado a que se hace referencia debe ser aplicado en cada nivel de mando que cuente con unidades de guerra electrónica, el cual deberá regirse por las directivas, políticas y disposiciones que en materia de guerra electrónica hayan sido emitidas por el escalón superior.

355. Para efectos ilustrativos se hace referencia a la organización y funcionamiento del sistema de guerra electrónica a nivel cuerpo de ejército, definido en nuestra doctrina vigente como la unidad táctica de batalla que tiene por objetivo realizar en el terreno parte o toda la concepción estratégica de un ejército o teatro de operaciones.

356. Con el fin de describir lo anterior, sólo se establecerá que el cuerpo de ejército en función de unidad de teatro (cuerpo de ejército independiente) tiene la capacidad de dotar a las divisiones y brigadas independientes que lo integran con medios acordes al propósito de aumentar su potencia de combate; esta capacidad le permite empeñarse en diferentes direcciones y zonas de acción dentro de su esquema de maniobra.

357. Entre estos medios se encuentran los relacionados con la guerra electrónica, para lo cual el cuerpo de ejército independiente debe contar por lo menos con un batallón de guerra electrónica adscrito, sin perjuicio de que otras unidades de igual o menor nivel le sean asignadas, cuando las circunstancias así lo exijan.

358. No obstante, al hacer alusión al nivel cuerpo de ejército, los conceptos aquí asentados son aplicables a cualquier nivel de la orgánica que cuente con unidades de guerra electrónica, tanto en la realización de operaciones encuadradas en el marco de una unidad superior como de forma independiente.

Subsección (B)

Organización General

359. La estructura orgánica de las unidades de guerra electrónica comprende pequeñas unidades desde el nivel escuadra hasta nivel batallón.

360. En la organización de las unidades de guerra electrónica, la identidad, integración e intercambiabilidad son condiciones indispensables que permiten la continuidad en la acción para el cumplimiento de la misión; la orgánica flexible de estas unidades facilita la organización para el combate, la cual se realiza buscando dotar a los agrupamientos que se formen de la máxima capacidad de apoyo al combate.

361. Las unidades de nivel inferior a la compañía se organizan con medios destinados a realizar una función táctica o técnica específica en beneficio de una fuerza de combate. La denominación de estas pequeñas unidades se otorga en relación con la función que desempeña, por lo que pueden ser denominadas: de intercepción, de análisis, de apoyo electrónico, de perturbación electrónica, entre otras.

362. Es en el nivel compañía donde se manifiesta la integración orgánica y funcional de pequeñas unidades de menor nivel y distintas funciones tácticas, misma que otorga a las unidades de éste nivel y especialidad la denominación de compañía de guerra electrónica. Excepcionalmente se podrán crear de manera orgánica unidades de nivel sección que manifiesten la integración orgánica y funcional a que se hace alusión, aunque lo común será que dicho nivel se integre dentro de la organización para el combate.

363. Por lo anterior, la compañía de guerra electrónica cuenta orgánicamente con todos los recursos necesarios para cumplir su misión general proporcionando apoyo general o apoyo directo al cuerpo de Ejército Independiente y las grandes unidades elementales subordinadas.

364. Con los recursos orgánicos de que está dotada, una compañía de guerra electrónica está en condiciones de proporcionar apoyo directo de su especialidad a una gran unidad de nivel división o bien, apoyo general al cuerpo de Ejército Independiente; esto último siempre y cuando sus unidades subordinadas cuenten con apoyo directo de guerra electrónica. Para el apoyo a las brigadas independientes se deberá recurrir a la organización para el combate, segregando de una compañía orgánica los medios indispensables para el cumplimiento de la misión.

365. Con el fin de centralizar el control y coordinación de las operaciones de guerra electrónica en un teatro de operaciones, así como facilitar el apoyo administrativo inherente, las compañías de guerra electrónica se agrupan de manera orgánica en unidades de nivel batallón.

366. En la figura número 5 se muestra el esquema orgánico de un batallón de guerra electrónica “tipo” destinado a proporcionar apoyo en su especialidad a un cuerpo de ejército independiente en función de unidad de teatro, motivo por el cual cuenta con todos los recursos necesarios para desarrollar operaciones de guerra electrónica en forma integral.

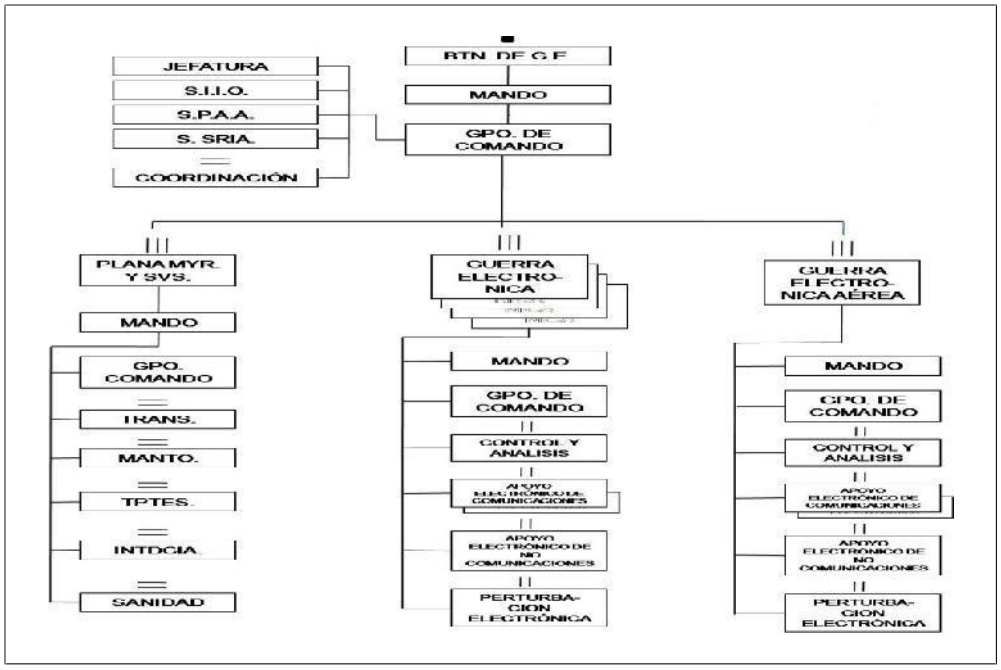

Figura Núm. 5
Organización de un Batallón de Guerra Electrónica

367. Dicha unidad cuenta con la capacidad de cumplir misiones de apoyo general y apoyo directo a la gran unidad superior y grandes unidades elementales subordinadas, a fin de incrementar su potencia de combate mediante la asignación de compañías de guerra electrónica orgánicas, o bien, de agrupamientos tácticos de guerra electrónica de composición variable y acorde a las circunstancias, pero que en todo caso contarán con las capacidades necesarias para el desarrollo de sus funciones.

368. La organización general del batallón de guerra electrónica “tipo” es la siguiente:

A. Mando.

B. Grupo de comando.

C. Una compañía de plana mayor y servicios.

D. Cuatro compañías de guerra electrónica ligeras o pesadas.

E. Una compañía de guerra electrónica aérea.

Subsección (C)

Organización Particular

369. Las unidades que integran el batallón de guerra electrónica tienen la estructura y misiones que a continuación se describen:

A. Grupo de comando. Además de la estructura clásica que conforma este organismo, en el batallón de guerra electrónica se deberá contar con un pelotón de coordinación de guerra electrónica, encargado de establecer la célula de coordinación de guerra electrónica a nivel batallón.

B. Compañía de plana mayor y servicios. Tiene como misión satisfacer las necesidades generales de vida y operación del batallón, proporcionando apoyos de alimentación, atención médica de primer escalón, transportación general, abastecimiento del equipo y material necesario para el desarrollo de sus misiones, tanto de guerra electrónica como de carácter general, así como el correspondiente mantenimiento de segundo escalón. Para el efecto, esta compañía se integrará con los servicios técnicos que sean necesarios para la evacuación de las tareas asignadas.

C. Compañías de guerra electrónica. En su conjunto, tendrán las características descritas en la subsección anterior, para lo cual se integrarán como sigue:

a. Una sección de control y análisis de guerra electrónica. Tiene como misión desarrollar todas las funciones relacionadas con el mando y control de las operaciones de guerra electrónica, en auxilio de la o del comandante de la compañía o agrupamiento correspondiente, para lo cual cuenta con los medios suficientes para establecer el sistema de mando, control, información y comunicaciones de la compañía. Se integra de la forma siguiente:

i. Pelotón de coordinación de guerra electrónica.

(A). Se organiza con el personal especialista y material necesarios para operar la célula de coordinación de guerra electrónica, yuxtapuesta al de la gran unidad a la que apoya, con el fin de auxiliar a la o el comandante de la compañía a ejercer el mando y la coordinación de las operaciones que realicen las unidades de guerra electrónica asignadas orgánicamente o en refuerzo.

(B). Debe integrar una escuadra de análisis de señales para efectuar el análisis consolidado de los datos obtenidos por las secciones de apoyo electrónico así como por todos los demás elementos del sistema, aunque no realicen actividades de búsqueda de datos, con el fin de convertirlos en información de valor militar.

(C). Cuando la compañía de guerra electrónica opera en misión de apoyo general a una gran unidad superior, este pelotón se incorpora a la C.C.G.E. establecida por el grupo de comando del batallón.

ii. Pelotón de oficiales de enlace. Se organiza con la cantidad indispensable de oficiales especialistas en guerra electrónica que desempeñan la función de las y los oficiales de enlace en aquellas unidades subordinadas a la gran unidad de que se trate y que no cuenten con el apoyo de otra unidad de guerra electrónica, para de esta forma permitirles acceder a los recursos del sistema de guerra electrónica en beneficio de sus operaciones particulares.

iii. Pelotón de operaciones de apoyo electrónico. Se organiza con el personal especialista y material necesarios para operar el centro de operaciones de apoyo electrónico (C.O.A.E.) de la línea de base, con el fin de dirigir las operaciones de búsqueda y recolección de información, ejerciendo el control táctico en tiempo real de los medios de apoyo electrónico de que dispone la unidad, de conformidad con las órdenes que reciba de la C.C.G.E. sobre el C.O.A.E. es necesario establecer lo siguiente:

(A). Controla y dirige las actividades de apoyo electrónico que realice la sección a la que pertenezca.

(B). Realiza el primer nivel de análisis de la información recolectada por las escuadras de apoyo electrónico, canalizando sus resultados a la C.C.G.E.

(C). Para desarrollar las funciones anteriores el C.O.A.E. puede ser desplegado en una posición central para atender a todas las escuadras que conformen la línea de base, o bien, operar de manera descentralizada, destacando una célula de control yuxtapuesta a cada escuadra de apoyo electrónico.

(D). Los principales factores que determinan la forma de despliegue del C.O.A.E. son las características del terreno y la disponibilidad de eficientes sistemas de comunicaciones que permitan el acceso a las bases de datos de guerra electrónica.

(E). Independientemente de que el C.O.A.E. despliegue de manera descentralizada, será necesario mantener en funcionamiento un C.O.A.E. central reducido en medios, para coordinar el funcionamiento de los Cs.O.A.E. desplegados. El C.O.A.E. central podrá ubicarse con la C.C.G.E. o bien, en la sección segunda u órgano de inteligencia del cuartel general correspondiente.

iv. Pelotón de Transmisiones. Proporciona los medios de transmisiones necesarios y suficientes para que la o el comandante de la gran unidad, su estado mayor, la C.C.G.E. y las o los oficiales de enlace ejerzan el mando y control de los medios de guerra electrónica en sus respectivos niveles de autoridad, permitiendo el intercambio de información entre todos los componentes del sistema, incluido el enlace con los sistemas estratégicos de inteligencia.

v. Dos secciones de apoyo electrónico de comunicaciones (COMINT), cada una con capacidad para desplegar una línea de base para el cumplimiento de su misión, por lo que estarán constituidas por:

(A). Dos pelotones de apoyo electrónico de comunicaciones (COMINT) constituidos por dos escuadras, cada una equipada con una plataforma (ligera o pesada) con capacidad de realizar búsqueda, intercepción y radiogoniometría de emisiones de comunicaciones.

(B). Un pelotón de reconocimiento electrónico constituido de forma similar a los de apoyo electrónico pero equipado exclusivamente con plataformas ligeras de la mayor movilidad posible para desplazarse dentro del área de operaciones en la búsqueda de emisiones con contenido de comunicaciones de interés.

vi. Una sección de apoyo electrónico de no comunicaciones (ELINT) con capacidad para desplegar una línea de base para el cumplimiento de su misión. Se compone de la manera siguiente:

(A). Dos pelotones de apoyo electrónico de no comunicaciones (ELINT), integrado cada uno por dos escuadras dotadas cada una con una plataforma (ligera o pesada) equipada para la evacuación de las tareas de búsqueda, intercepción, radiogoniometría y análisis de emisiones de no comunicaciones.

(B). Un pelotón de reconocimiento electrónico constituido de forma similar a los de apoyo electrónico pero equipado exclusivamente con plataformas ligeras de la mayor movilidad posible para desplazarse dentro del área de operaciones en la búsqueda de emisiones de interés sin contenido de comunicaciones.

(C). Una Sección de perturbación electrónica. Tiene como misión ejecutar las acciones de perturbación electrónica contra blancos planeados y de oportunidad de conformidad con las órdenes emitidas por el mando de la gran unidad apoyada.

(D). Está constituida por dos pelotones de perturbación electrónica, integrado cada uno por dos escuadras dotadas cada una con una plataforma (ligera o pesada) equipada con perturbadores capaces de degradar el funcionamiento de los sistemas electrónicos del adversario a gran distancia (su potencia típica oscila alrededor de uno a dos kilowatts). Pueden ser del tipo selectivo, de barrera, de barrido o de búsqueda automática.

D. Compañía de guerra electrónica aérea.

a. Tendrá las funciones descritas para una compañía de guerra electrónica terrestre, con la ventaja de poder desarrollarlas mediante la recolección de información y ejecución de perturbación electrónica desde el aire, conducidas por plataformas aéreas tripuladas o no tripuladas.

b. Debido a sus características, generalmente operará cumpliendo misiones de apoyo general en beneficio del cuerpo de ejército Independiente y en caso de ser asignada en apoyo de las grandes unidades subordinadas, será por periodos de tiempo breves y solamente en apoyo de operaciones específicas, para poder permanecer a disposición del mando de la gran unidad superior.

c. Su integración se llevará a cabo buscando que cuente con todas las capacidades descritas para las compañías terrestres, por lo que es recomendable que las secciones que la integren, tengan una composición similar, con las adecuaciones del caso.

d. Para ser orgánica del batallón, es necesario que se constituya con materiales del arma de aeronáutica.

e. En su defecto, puede ser constituida con medios proporcionados en refuerzo por la fuerza aérea, en cuyo caso, sus funciones serán realizadas por una unidad de nivel escuadrón, constituido por la cantidad de escuadrillas necesarias para realizar las funciones de las secciones antes mencionadas.

Capítulo II

Dirección y Coordinación de la Guerra Electrónica

Primera Sección

Niveles de Autoridad

Subsección (A)

Generalidades

370. La administración general de la guerra electrónica, como todo medio de combate, es una facultad que corresponde al mando superior que cuenta con unidades de guerra electrónica asignadas en la fuerza a sus órdenes, facultad que ejercerá normalmente por conducto del estado mayor que lo auxilie.

371. La administración de los medios de la especialidad es responsabilidad de la o el comandante de la respectiva unidad de guerra electrónica, quien, de conformidad con las órdenes que recibe de la o el comandante de la gran unidad, ejerce el mando de su unidad orgánica y de los elementos que haya recibido en refuerzo, por conducto de la célula de coordinación de guerra electrónica (C.C.G.E.).

372. La célula de coordinación de guerra electrónica, auxilia a la o el comandante a ejercer el mando, control y coordinación de las operaciones que realice la unidad de guerra electrónica. Se ubica yuxtapuesta al cuartel general de grandes unidades que cuenten con el apoyo de una unidad de guerra electrónica e integrada dentro del estado mayor respectivo. A esta célula se integra la o el comandante de la unidad de guerra electrónica, en su papel de asesor del mando superior en materia de guerra electrónica.

373. La célula de coordinación de guerra electrónica, es auxiliada en el control y coordinación de las operaciones de guerra electrónica por dos órganos:

A. Las y los oficiales de enlace de guerra electrónica (O.E.G.E.), quienes proporcionan enlace y coordinación entre las unidades de combate subordinadas a la gran unidad apoyada y la unidad de guerra electrónica.

B. El centro de operaciones de apoyo electrónico (C.O.A.E.) ejerce el control operativo en tiempo real de los medios de apoyo electrónico que tenga asignados, de acuerdo con las órdenes que dicte la o el comandante, ya sea que opere en forma centralizada o descentralizada.

Subsección (B)

Célula de Coordinación de Guerra Electrónica

374. Toda unidad o escalón que cuente con medios de guerra electrónica asignados orgánicamente o en refuerzo debe contar con una Célula de Coordinación de Guerra Electrónica (C.C.G.E.), conformada de acuerdo al nivel de que se trate, por elementos proporcionados por la respectiva unidad de guerra electrónica.

375. La célula de coordinación de guerra electrónica, es el centro neurálgico de todas las actividades de guerra electrónica que se desarrollan dentro de cada nivel de mando. Coordina y dirige la distribución de los medios de guerra electrónica en apoyo de unidades específicas durante las diferentes fases de las operaciones de la gran unidad.

376. Las funciones a cargo de la célula de coordinación de guerra electrónica, son las siguientes:[21]

[21] Ibid.

A. Elaborar el plan de operaciones de guerra electrónica para apoyar la operación táctica proyectada de conformidad con las órdenes emitidas por la o el comandante de la gran unidad, en coordinación con la jefa o el jefe de la sección segunda del estado mayor correspondiente, por lo que respecta a su integración con el plan de búsqueda de información y con el centro coordinador de fuegos de apoyo, por lo que respecta al plan general de fuegos de apoyo.

B. Coordinar la acción de las actividades de apoyo electrónico y las contramedidas electrónicas con otros medios de combate y de apoyo al combate, dentro del dispositivo general de la gran unidad.

C. Coordinar las actividades de apoyo electrónico y de contramedidas electrónicas de la gran unidad con las realizadas por el escalón superior y las unidades adyacentes.

D. Proveer asesoría especializada en materia de guerra electrónica a la o el comandante de la gran unidad, su estado mayor y comandantes subordinados, incluyendo lo referente a las medidas de protección electrónica a cargo de todas las armas y servicios.

E. Dirigir la ejecución de operaciones de apoyo electrónico a través de los centros de operaciones de apoyo electrónico.

F. Dirigir y supervisar la ejecución de operaciones de contramedidas electrónicas en la gran unidad. En este caso, sus responsabilidades son las siguientes:

a. En operaciones de perturbación electrónica. planear, coordinar, controlar y supervisar su ejecución por parte de la unidad de guerra electrónica.

b. En operaciones de engaño electrónico.

G. Planear todo lo relativo a las operaciones de engaño electrónico a realizarse por la gran unidad, ya sea que se trate de engaño por imitación, simulación o manipulación, bajo coordinación de las o los jefes de las Secciones Segunda y Tercera del Estado Mayor.

H. Dirigir y supervisar la ejecución de las operaciones de engaño electrónico, realizadas por la unidad de guerra electrónica (limitadas al engaño electrónico por imitación y excepcionalmente por manipulación).

I. Supervisar y orientar la ejecución de las operaciones de engaño electrónico (por imitación, simulación o manipulación), realizadas por todas las unidades subordinadas a la gran unidad, dentro del marco de operaciones tácticas de engaño.

J. Proporcionar la información recolectada por los elementos de apoyo electrónico, analizada y valuada a su nivel, a los correspondientes órganos de inteligencia.

K. Difundir a los elementos del sistema de guerra electrónica aquella información sobre la situación electrónica del adversario que se considere apropiada, o bien, la que disponga la o el comandante de la gran unidad.

L. Mantener y proporcionar enlace para la coordinación y consulta con las organizaciones estratégicas de inteligencia, tanto militares como de otras dependencias gubernamentales.

M. Proporcionar asesoría técnica a los diversos niveles de mando sobre el empleo de armas de neutralización electrónica y otros medios electrónicos empleados por las unidades de combate.

377. La adecuada coordinación de las actividades de guerra electrónica entre los diversos escalones es un aspecto de naturaleza crítica, ya que previene la duplicidad de esfuerzos y optimiza la diseminación de la información obtenida por los medios de guerra electrónica. De este hecho se deriva la importancia de la C.C.G.E.

378. La célula de coordinación de guerra electrónica de más alto nivel (generalmente del cuerpo de ejército independiente), asume el control técnico de todas las actividades de guerra electrónica en la gran unidad; es necesario recordar que, como en todos los medios de apoyo al combate y de servicios, la cadena de mando táctico (control operativo) tiene preeminencia sobre cualquier otra consideración de control o autoridad técnica.

379. En caso de que dos o más unidades de guerra electrónica de nivel batallón o inferiores, sean adscritas a un mismo cuerpo de ejército, la C.C.G.E. será establecida por la unidad que así designe la o el comandante de la gran unidad, generalmente atendiendo al nivel de la unidad y en igualdad de circunstancias, a la jerarquía de sus comandantes, buscando que la coordinación de las actividades de guerra electrónica sea ejercida por la unidad que cuente con los recursos necesarios para tal fin.

Subsección (C)

Oficiales de Enlace de Guerra Electrónica

380. Se denomina oficiales de enlace de guerra electrónica (O.E.G.E.), al personal de tal carácter que, perteneciendo orgánicamente a la unidad de guerra electrónica que presta apoyo de su especialidad a una gran unidad, es destacado en los puestos de mando de cada una de las unidades de combate (brigadas divisionarias y/o batallones), subordinadas a la gran unidad.[22]

381. La finalidad de las y los oficiales de enlace de guerra electrónica, es actuar como representantes personales de la o el comandante de la unidad de guerra electrónica, para proporcionar enlace entre los mandos de las unidades apoyada y de apoyo, resolver problemas mutuos de coordinación y cooperación y permitir que las unidades de combate puedan acceder a los recursos de guerra electrónica en beneficio de sus propias operaciones, particularmente información y en su caso, perturbación electrónica.

[22] Ibid.

382. Además de lo anterior, las y los oficiales de enlace de guerra electrónica, deben tener la capacidad de efectuar actividades limitadas de búsqueda e intercepción, por lo que se les debe dotar con un equipo portátil de tales características. La finalidad de esta capacidad es coadyuvar a la protección y seguridad de la unidad, advirtiendo a la unidad apoyada sobre las amenazas inmediatas que se presenten en su zona de acción.

383. Al igual que el personal de oficiales de enlace de otras especialidades de combate, los de guerra electrónica deben estar ampliamente familiarizados con la situación, planes y órdenes de su propia unidad, para estar en condiciones de poner dicha información en conocimiento del mando y auxiliares de la unidad apoyada.

384. Las funciones de las y los oficiales de enlace de guerra electrónica son:

A. En auxilio de la C.C.G.E.

a. Informar a la unidad apoyada respecto a las posibilidades de apoyo electrónico y perturbación de la unidad que representa.

b. Auxiliar al establecimiento y buen funcionamiento de las transmisiones entre ambas unidades.

c. Reportar a la C.C.G.E. la información respecto a la situación electrónica de la fuerza adversaria y blancos que sean obtenidos por la unidad apoyada o mediante el reconocimiento electrónico que él mismo efectúe.

d. Informar a la C.C.G.E. sobre el esquema de maniobra y planes de la unidad apoyada, así como la naturaleza de los apoyos que ésta requiera.

e. Evalúa la efectividad de las contramedidas electrónicas aplicadas en la zona de acción de la unidad apoyada.

B. En auxilio de la o el comandante apoyado:

a. Lo asesora respecto a guerra electrónica y el apoyo que pueda recibir.

b. Le advierte sobre cualquier amenaza inmediata a la seguridad de su fuerza que sea detectada mediante el reconocimiento electrónico.

c. Le proporciona toda aquella información sobre el adversario que sea obtenida por los elementos de apoyo electrónico y se autorice su difusión por la C.C.G.E.

d. Canaliza a la C.C.G.E. toda clase de peticiones de apoyo de guerra electrónica que demande la o el comandante apoyado, pudiendo tratarse de apoyos planeados con anterioridad (preplaneados) y de apoyos imprevistos (de ejecución inmediata).

e. Proporciona asesoría sobre la aplicación de las medidas de protección electrónica en beneficio de la unidad apoyada.

Subsección (D)

Centro de Operaciones de Apoyo Electrónico

385. La función principal del Centro de Operaciones de Apoyo Electrónico (C.O.A.E.) es efectuar el control directo e inmediato de las actividades de apoyo electrónico que realice la unidad de guerra electrónica, conforme a las órdenes que gire la o el comandante por conducto de la C.C.G.E.

386. Lo anterior, obliga al C.O.A.E. a mantener estrecho contacto con los elementos de apoyo electrónico desplegadas en la línea de base que establezca su unidad, para poder coordinar eficazmente su acción y orientarlas en la obtención de óptimos resultados, motivo por el cual su despliegue se efectúa en alguna de las formas establecidas en el capítulo anterior.

387. De manera general, las funciones del C.O.A.E. son las siguientes:

A. Recibe de la C.C.G.E. los blancos y las prioridades para efectuar las operaciones de apoyo electrónico.

B. Asigna misiones de búsqueda, intercepción y radiogoniometría a las unidades de apoyo electrónico desplegadas en la línea de base respectiva.

C. Reúne toda la información recolectada por las unidades de apoyo electrónico desplegadas, a fin de procesarla y convertirla en información de valor referente al orden de batalla electrónico del adversario que opera en la zona de acción de la unidad apoyada.

D. Canaliza la información del orden de batalla electrónico a la C.C.G.E., incluida la referente a los posibles blancos para la ejecución de perturbación electrónica u otras formas de ataque.

E. Evalúa la efectividad de las contramedidas electrónicas aplicadas en la zona de acción de la unidad apoyada.

388. La importancia del C.O.A.E. se fundamenta en la relevancia que adquiere la adecuada dirección de las actividades de apoyo electrónico en tareas de búsqueda de información, para determinar la continuidad del esfuerzo realizado, o bien, su reorientación.

Segunda Sección

Responsabilidades del Estado Mayor en Relación con la Guerra Electrónica

389. Para la adecuada materialización de la planeación y desarrollo de las operaciones de guerra electrónica, deberá existir un estrecho contacto entre las secciones del estado mayor y la unidad de guerra electrónica, particularmente por lo que respecta a la coordinación entre las o los jefes de las secciones de inteligencia y operaciones con la C.C.G.E.[23]

390. El estado mayor, realiza funciones de dirección, control, coordinación y apoyo de las actividades de guerra electrónica dentro de toda la zona de acción del cuerpo de ejército, mediante el desarrollo de las funciones siguientes:

A. Sección Primera (Personal). Gestiona y coordina la asignación de los reemplazos necesarios para mantener la operatividad de las unidades de guerra electrónica.

B. Sección Segunda (Inteligencia).

a. Comunica los elementos esenciales de información de la o el comandante de la gran unidad dentro del plan de búsqueda de información, en forma de tareas a las unidades de guerra electrónica.

b. Centraliza, valúa, interpreta y difunde para su explotación, la información enemiga que le es proporcionada por la C.C.G.E.

c. Recomienda a la o el comandante y demás miembros del Estado Mayor, los aspectos relacionados con información y contrainformación que involucran el empleo de las unidades de guerra electrónica.

[23] S.D.N. Manual de Operaciones de Guerra Electrónica. Op. Cit. P.104-107.

d. Realiza el planeamiento de las operaciones de engaño electrónico, en coordinación con la o el jefe de la sección tercera (Operaciones).

e. Recomienda a la o el comandante sobre los riesgos y beneficios del empleo de medidas de apoyo electrónico y contramedidas electrónicas sobre determinados blancos.

f. En lo relativo a las medidas de protección electrónica, recomienda a la o el comandante sobre los aspectos de seguridad de los emisores propios y las tropas.

g. Realiza la supervisión y evaluación de las operaciones de apoyo y engaño electrónicos, en coordinación con la o el jefe de la sección tercera.

C. Sección tercera (Operaciones).

a. Es responsable de la planeación, coordinación y evaluación de las operaciones de guerra electrónica por conducto de la C.C.G.E., con excepción de las de engaño y neutralización electrónicos.

b. Recomienda a la o el comandante la distribución de los medios de guerra electrónica y las prioridades para su empleo.

c. Coordina la instrucción y el adiestramiento en las actividades de guerra electrónica.

d. Coordina con el escalón superior, unidades subordinadas y adyacentes, las operaciones de guerra electrónica que hayan sido aprobadas.

e. Participa en la planeación de las operaciones de engaño electrónico en coordinación con la o el jefe de la Sección Segunda (Inteligencia).

f. Supervisa el desarrollo de las operaciones de guerra electrónica, en coordinación con la o el jefe de la Sección Segunda (Inteligencia).

g. Dicta los lineamientos generales para que el centro coordinador de fuegos de apoyo incluya dentro de los planes respectivos la desorganización de los sistemas electrónicos enemigos por medio de la perturbación electrónica, asi como las restricciones para perturbar determinados blancos que representen fuentes de información.

h. Por recomendación de la C.C.G.E., dicta las medidas generales para que las operaciones de guerra electrónica realizadas en contra del adversario, no limiten la eficiencia de nuestros sistemas electrónicos.

D. Sección Cuarta (Logística). Es responsable de coordinar todos los aspectos necesarios para la materialización del abastecimiento, mantenimiento y evacuación del equipo y material utilizado en las actividades de guerra electrónica.

Capítulo III

Planeación Táctica de la Guerra Electrónica

Primera Sección

Generalidades

391. Las misiones que el mando del teatro de operaciones asigna al cuerpo de ejército cuando éste opera como unidad de teatro (en forma independiente), normalmente son impartidas en forma de un plan de campaña, el cual es la base de la planeación a mediano y largo plazo de la unidad de teatro.[24]

392. El plan de operaciones del cuerpo de ejército se deriva del plan de campaña y en particular del concepto de la operación que éste contiene, el que describe, entre otros aspectos: el propósito de la operación a desarrollar y su escalonamiento, la misión, esquema de maniobra y el dispositivo para el cuerpo de ejército, el apoyo de fuegos, el empleo de la guerra electrónica y otros apoyos importantes para las fuerzas que operan en el teatro de operaciones.

393. Al contar con su misión, la o el comandante del cuerpo de ejército independiente estará en condiciones de concebir las operaciones necesarias para su cumplimiento, para lo cual desarrollará el proceso de estimación de la situación, para seleccionar el curso de acción a adoptar, lo que implica el análisis lógico y ordenado de los factores que influyen en la situación.

[24] Secretaría de la Defensa Nacional. Manual de Táctica General. Libro Tercero. México. SECRETARÍA DE LA DEFENSA NACIONAL. 2001.

394. Sin embargo, para realizar adecuadamente esta concepción, la o el comandante del cuerpo de ejército necesitará disponer de información adecuada y oportuna, la cual normalmente será establecida en su guía de planeamiento; dicha información se referirá principalmente al orden de batalla del adversario para establecer sus posibilidades de forma precisa y así poder plantear los mejores cursos de acción.

395. Esta necesidad hace imperativo a la o el comandante a empeñar todos los medios disponibles para obtener la mayor cantidad de datos relativos al orden de batalla del adversario, por lo que la gran unidad superior debe contar con suficientes órganos de búsqueda y el apoyo de agencias que obtengan información en toda su zona de acción.

396. Parte importante de estos órganos y agencias se encuentran representadas por las unidades de guerra electrónica, las que, dentro de sus posibilidades técnicas, obtendrán y proporcionarán la información deseada por la o el comandante del cuerpo de ejército, además de obtener aquella que requieran para la concepción de sus propias operaciones.

397. Al contar con la suficiente información que le permita conocer el campo de batalla, la o el comandante del cuerpo de ejército estimará la situación y emitirá su decisión, para lo cual se giran las misiones respectivas a las unidades subordinadas por medio de una orden general de operaciones.

398. Este documento incluirá, además de las referidas misiones, diversos aspectos de interés para la unidad de guerra electrónica, como son: los elementos esenciales de información (E.E.I.), los diversos apoyos (al combate y de servicios) requeridos por las unidades de maniobra, las medidas de encubrimiento y engaño, así como la política de empleo de guerra electrónica.

399. Con los datos anteriores, el batallón de guerra electrónica adscrito al cuerpo de ejército se encuentra en condiciones de efectuar su propia planeación para estar en condiciones de apoyar en forma general a la gran unidad superior y en forma particular a los elementos de maniobra representados por las divisiones y brigadas independientes subordinadas.

400. Las operaciones de guerra electrónica son destinadas a incrementar la potencia de combate de la fuerza apoyada, por lo que dentro del proceso de concepción, preparación y conducción de las mismas, se debe realizar una serie de actividades de coordinación con diversos organismos, para poder integrarlas de manera apropiada con otros medios de apoyo al combate, destacando por su importancia las actividades de inteligencia y los fuegos de apoyo.

401. Para la obtención del éxito en las operaciones de guerra electrónica, se requiere que estas sean aplicadas en forma ininterrumpida y que faciliten una pronta reacción, por lo que existen dos clases de planes de guerra electrónica:[25]

A. Los planes previamente formulados. Se pueden elaborar a través de la estimación continua de la situación, en previsión de acciones futuras, o bien, como resultado de la asignación de una misión y la aplicación de un proseso militar de toma de deciciones. Se materializan con la elaboración del plan de operaciones de guerra electrónica, el cual constituye un anexo al plan de operaciones de la gran unidad, al cual deberá estar debidamente integrado y coordinado.

B. Los planes de ejecución inmediata. Son los planes que se elaboran para responder a situaciones inesperadas que se presenten durante el desarrollo de la acción, las cuales demandan un cambio rápido en la distribución o prioridades establecidas para las unidades de guerra electrónica.

402. Para el efecto, la formulación de los planes de operaciones de guerra electrónica debe sujetarse a los siguientes principios.

A. Control centralizado.

B. Ejecución descentralizada.

C. Integración al sistema de inteligencia.

D. Integración a los fuegos de apoyo.

[25] S.D.N. Manual de Operaciones de Guerra Electrónica. Op. Cit. P.114.

E. Previsión de la acción y reacción del adversario.

Segunda Sección

Principios de la Planeación Táctica

Subsección (A)

Control Centralizado

403. Al igual que sucede con otros tipos de operaciones militares, no existe algo más desfavorable para el éxito de las operaciones de guerra electrónica, que el derrochar sus recursos en pequeñas fracciones operando cada una bajo su propio plan.

404. La aplicación del control centralizado permite la concentración de los medios de guerra electrónica en el lugar y tiempo apropiados; por el contrario, sin su aplicación, la flexibilidad pierde toda su significación. Bajo el mencionado control, el esfuerzo del apoyo y perturbación electrónicos puede ser trasladado rápidamente de un lugar a otro, de acuerdo con los cambios previstos o imprevistos que surjan en el área de operaciones.

405. Para el efecto, las políticas y directivas generales para el empleo de las operaciones de guerra electrónica dentro de un teatro de operaciones deben ser emitidas por el cuartel general de dicho teatro, las que afectarán las operaciones realizadas por las fuerzas combatientes de tierra, mar y aire presentes en el teatro.

406. A su vez, la C.C.G.E. de la unidad de guerra electrónica de máximo nivel adscrita a la unidad teatro de operaciones, con estricto apego a las directivas y políticas de referencia, materializará el control centralizado de todas las unidades de guerra electrónica del ejército, realizando el planeamiento de las operaciones de acuerdo con este principio, el cual deberá ser conservado en cada nivel de la organización de guerra electrónica, desde el principio y hasta el final de las operaciones.

407. A nivel teatro de operaciones la coordinación centralizada es realizada por la C.C.G.E. de la unidad de guerra electrónica adscrita al cuerpo de ejército, la que con base en sus resultados dicta los procedimientos para que las operaciones de guerra electrónica se mantengan estrechamente coordinadas con el empleo de los emisores electromagnéticos de las unidades de combate y de esta forma estos últimos no se vean afectados por nuestras operaciones, particularmente las de perturbación electrónica.

Subsección (B)

Ejecución Descentralizada

408. Debido a que un solo comandante no puede dirigir personalmente todas las acciones detalladas de una gran cantidad de individuos o unidades, resulta esencial el empleo de este principio fundamental, el cual establece que “el nivel superior de mando determina las misiones, para luego ordenar a los niveles inferiores la ejecución de las operaciones”.

409. Con este principio, se logra que las o los comandantes subordinados mantengan una fuerza eficaz y con capacidad de respuesta, y que la o el comandante superior tenga libertad de enfocar las operaciones de toda la fuerza a su mando para lograr el objetivo general.

410. Este arreglo no limita en forma alguna la autoridad táctica de las o los comandantes subordinados ni disminuye su responsabilidad; más bien, ubica los detalles del planeamiento de la misión al nivel de ejecución.

411. Esto implica que la unidad de guerra electrónica de máximo nivel adscrita a la unidad terrestre de teatro debe prescribir amplios planes, incluyendo los detalles necesarios para mantener la dirección general de las operaciones y para coordinar las fuerzas, de tal forma que se mantenga la iniciativa de las o los comandantes de las unidades subordinadas en apoyo a las fuerzas de maniobra.

412. Este principio demanda ceder a los subordinados los detalles de la ejecución de las misiones ordenadas, ya que durante el desarrollo de la acción pocas situaciones pueden ser previstas con precisión.

Subsección (C)

Integración con el Sistema de Inteligencia

413. Uno de los principales puntos de equilibrio de cada comandante es la información, la cual debidamente procesada produce capacidades y recursos de inteligencia militar que se convierten en un medio para neutralizar las posibilidades del adversario.[26]

414. Para lograr lo anterior, la primera tarea que debe imponerse la o el comandante es conocer el campo de batalla, de tal manera que tenga la posibilidad de concentrar oportunamente el poder de combate en el lugar y momento oportuno; a continuación debe exigir que todas las fuentes y agencias de información trabajen en forma coordinada en su beneficio.

415. Por último, conservará un ritmo constante en el desarrollo de operaciones de información y contrainformación, las cuales deben realizarse simultáneamente a las operaciones de combate, para generar inteligencia en forma continua, oportuna y acorde a la situación, funcionando como una sólida plataforma para la toma de decisiones.

416. En forma similar a la organización táctica para el combate, en la que se agrupan las unidades de las armas, la organización de inteligencia a cualquier nivel reúne diversos recursos en un sistema de información compuesto principalmente por:

[26] S.D.N. Manual de Táctica General. Op. Cit. Pag. 70-82.

A. Dispositivos electromagnéticos. Que incluyen a los medios de inteligencia de señales para la generación de información estratégica y a los medios de apoyo electrónico para la generación de información primordialmente de combate.

B. Información de combate.

C. Inteligencia proporcionada por medios aéreos del ejército o de la fuerza aérea.

D. Imágenes satelitales.

417. Es por este motivo que las operaciones de apoyo electrónico deben estar perfectamente integradas dentro del sistema de inteligencia en cada nivel de mando, y su coordinación se basa en las necesidades de información de la o el comandante de la gran unidad, expresadas en forma de E.E.I.

418. El área de interés para la obtención de información destinada a fines operativos, se prolonga de la línea de contacto hacia el terreno ocupado por el adversario, variando su extensión en profundidad de acuerdo con los diferentes niveles de mando que la requieren, creándose así lo que se denomina “zonas de inteligencia táctica”, en las que se desarrolla parte de la información estratégica y la totalidad de información de combate.

419. Los requerimientos de información de los diversos niveles de mando táctico son los siguientes:

A. La o el comandante del cuerpo de ejército establece su zona de inteligencia táctica con base en los medios de que dispone, considerando que sus necesidades básicas demandan información estratégica de carácter general en mayor proporción a la información de combate, principalmente para determinar el lugar donde debe concentrar sus fuerzas.

B. Las o los comandantes de los niveles división y brigada independiente, para la adecuada conducción de su maniobra, requieren una proporción equilibrada de información estratégica e información de combate.

C. Del nivel batallón o similar hacia escalones inferiores, los requerimientos de información se centran en información de combate.

420. Lo anterior permite establecer que los escalones subalternos requieren de menor inteligencia y más información de combate, por lo que en los informes que generan y remiten, la valuación de los datos se realiza en forma limitada; en cambio, los escalones superiores analizan desde un panorama general toda la información que obtienen de los órganos y agencias de información, coordinando la generación de inteligencia para proporcionarla a sus divisiones, brigadas, batallones e incluso compañías subordinadas.

421. La perspectiva de la inteligencia requerida en el campo de batalla conforme al nivel de mando, se explica en términos de zonas de inteligencia táctica en el cuadro siguiente (Ver figura Núm. 6).

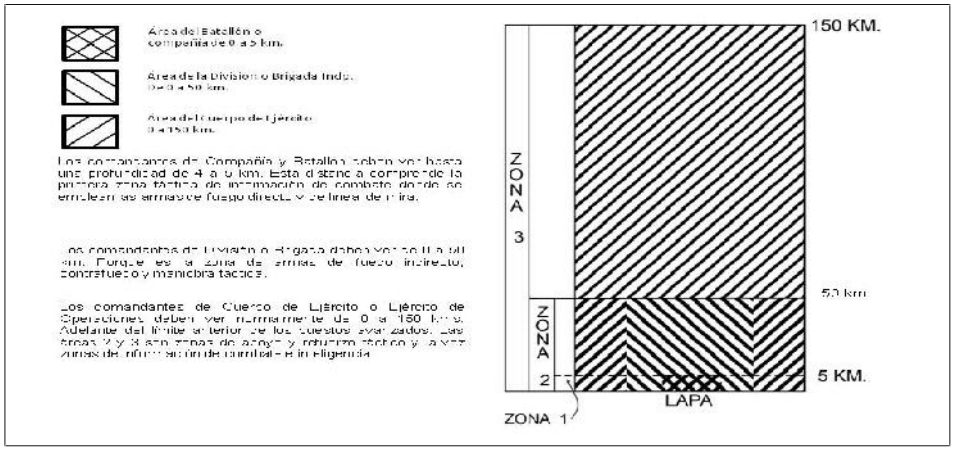

Figura Núm. 6
Zonas Tácticas de Información e Inteligencia

422. Las necesidades de información antes expresadas generan la necesidad de coordinar las operaciones de búsqueda de información de los dispositivos electromagnéticos de la manera que se indica en los subpárrafos siguientes. Cabe hacer la aclaración que al referirse en ellos a información estratégica o de combate, se hace referencia únicamente a la obtenida por los mencionados dispositivos.

A. A nivel cuerpo de ejército se deberá disponer del apoyo de los órganos de inteligencia de señales del teatro de operaciones, cuyo cometido de generar información estratégica será complementado por las actividades de unidades terrestres de guerra electrónica cumpliendo misiones de apoyo general a su dispositivo, para la obtención de información estratégica y de combate, debiendo disponer además de unidades aéreas de guerra electrónica, ya sean orgánicas del ejército o de la fuerza aérea.

B. A nivel división o brigada independiente las necesidades de información estratégica son satisfechas por los datos que difunde el cuerpo de ejército independiente; para la satisfacción de sus requerimientos de información de combate, le son asignadas unidades terrestres de guerra electrónica en cantidad suficiente para el cumplimiento de su misión.

423. De conformidad con la zona de inteligencia táctica del nivel de mando de que se trate, las operaciones de apoyo electrónico deberán ser planeadas para abarcar la extensión de dichas zonas en su totalidad, dentro de las posibilidades técnicas de los materiales con que se cuente; esta planeación queda a cargo de la C.C.G.E. que establezca la unidad correspondiente.

424. La información obtenida incluye, además de los datos sobre el orden de batalla del adversario que se generen para dar respuesta a los E.E.I. de la o el comandante, la información relacionada con los blancos electrónicos, existentes o probables, para la ejecución de contramedidas electrónicas u otras acciones tácticas.

425. El proceso que desarrolla la C.C.G.E. para satisfacer las necesidades de información de cada nivel de mando se materializa bajo el esquema que a continuación se indica:

A. Previo a la realización de una operación, la sección segunda del estado mayor de la gran unidad apoyada elabora su plan de búsqueda de información donde establece los requerimientos de información de la o el comandante (E.E.I.), para dicha operación, derivado del cual se girarán órdenes de búsqueda a sus unidades subordinadas (órganos) y peticiones a los escalones superiores y adyacentes (agencias).

B. La sección segunda del estado mayor respectivo, es responsable de coordinar las actividades de búsqueda de información de los escalones subordinados, para que respondan a lo ordenado.

C. La coordinación ejercida sobre las actividades relacionadas con guerra electrónica, se materializan por conducto de la C.C.G.E., la que auxilia a dicho organismo sobre las posibilidades de la unidad de guerra electrónica, fundamentalmente en la determinación de la cobertura del apoyo electrónico, para comprobar que se podrá disponer de la información requerida sobre la zona deseada.

D. Posteriormente, al recibirse las correspondientes órdenes de búsqueda, la o el comandante de la unidad de guerra electrónica, a través de la C.C.G.E., las convierte en misiones de apoyo electrónico, incorporándolas como anexo al plan de operaciones, impartiéndolas de ese modo a sus unidades subordinadas por conducto del C.O.A.E. dichas misiones toman la forma de actividades de búsqueda, intercepción y localización de emisores, redes o sistemas electrónicos específicos.

Subsección (D)

Integración con los Fuegos de Apoyo

426. La integración de las operaciones de guerra electrónica con los fuegos de apoyo se materializa mediante la inclusión de las operaciones de perturbación electrónica dentro del plan general de apoyo de fuegos elaborado por el centro coordinador de fuegos de apoyo (C.C.F.A.)[27] de la gran unidad, considerando dentro de un anexo a dicho plan, todos los requerimientos de acciones de perturbación en contra de los sistemas de la fuerza oponente de mando y control, de comunicaciones, de armas, de detección y vigilancia, conforme a las necesidades impuestas por el esquema de maniobra a desarrollar.

[27] Ibid.

427. Cabe hacer mención que la coordinación para el empleo de armas de neutralización electrónica es responsabilidad de las unidades de combate dotadas con este tipo de armamento, pudiendo ser asesoradas sobre el particular por la unidad de guerra electrónica.

428. A fin de lograr la correcta integración de la perturbación electrónica con los fuegos de apoyo y la maniobra, existen dos preceptos fundamentales a observar.

A. La perturbación electrónica que se ejecuta por el solo hecho de realizarla puede redundar en mayor perjuicio que beneficio.

B. La integración de todos los fuegos de apoyo ofrece el medio más eficaz para acrecentar la potencia de combate de la propia unidad.

429. Para realizar la integración de las operaciones de perturbación electrónica con los demás medios de fuegos de apoyo, es necesario conocer previamente los conceptos relacionados con la coordinación de fuegos de apoyo (C.F.A.) y el proceso de información y análisis de blancos electrónicos, por lo que estos se describirán someramente en los párrafos subsiguientes.

430. Los fuegos de apoyo son el principal recurso en manos de una o un comandante para ejercer influencia durante un combate, por lo que la efectividad con la que lo utilice dentro de su plan de acción es decisiva, para lo cual es indispensable su adecuada coordinación. La C.F.A. es una función táctica que debe realizarse en todos los niveles del mando en los que existan dos o más formas de apoyo de fuegos, tales como la artillería de campaña, el apoyo aerotáctico y la perturbación electrónica.[28]

[28] Secretaría de la Defensa Nacional. Manual de Operaciones en Campaña. Tomo I. Edición 1981. México. SECRETARÍA DE LA DEFENSA NACIONAL. 2012. P. 152.

431. La o el comandante de una gran unidad emplea todos los medios de fuegos de apoyo bajo su mando, por lo que la C.F.A. es una responsabilidad del mando en cada nivel orgánico, pero la función ejecutiva de esta coordinación siempre queda a cargo del oficial del arma de artillería con mayor autoridad que actúe en el nivel de que se trate, quien es el principal asesor de la o el comandante en estos asuntos y se encarga de todos los detalles relacionados con dicha coordinación.

432. El C.C.F.A. constituye un centro “administrador” de los fuegos de apoyo a nivel división y cuerpo de ejército; en él, se reúnen la o el comandante de la citada unidad (o su representante) y los representantes de las unidades que proporcionan el apoyo de fuegos (incluida la perturbación electrónica), con el fin de realizar el planeamiento, coordinar y controlar las actividades de apoyo de fuegos, en beneficio del mando y de las tropas de la unidad apoyada.

433. La organización y procedimientos para la C.F.A. permiten, entre otros aspectos, el adecuado control y supervisión de los fuegos de apoyo, así como su concentración, distribución y ejecución. Las operaciones de apoyo electrónico deben ser coordinadas por el C.C.F.A., para disponer de ellas en beneficio de la maniobra proyectada, con los fines siguientes:

A. Incrementar la disponibilidad de medios de apoyo de fuegos con que cuente el mando para cumplir con la multiplicidad de medios requerida.

B. Impedir que sobre un mismo blanco se efectúen ataques físicos y electrónicos, a menos que de antemano así sea concebido el ataque, evitando duplicidad de esfuerzos y dispendio de medios de apoyo al combate.

C. Permitir la economía de los medios de apoyo de fuego físico en sectores donde el ataque electrónico sea suficiente para disminuir la eficiencia de combate del enemigo, facilitando de este modo la concentración de fuerzas en aquellas áreas donde el apoyo de fuego físico sea crítico para el éxito de la maniobra.

434. El plan de fuegos de apoyo es formulado por el coordinador de fuegos de apoyo, de acuerdo con las directivas de la o el comandante de la unidad apoyada y constituye la base para la preparación de los planes de fuegos de apoyo: aéreo, naval, de artillería, de perturbación electrónica y cualquier otro. Estos últimos son apéndices del anexo “plan de fuegos de apoyo” al plan u orden de operaciones de la gran unidad.

435. La información y el análisis de blancos electrónicos. El primer paso para lograr la adecuada integración de las actividades de perturbación electrónica con los fuegos de apoyo, se desarrolla mediante el proceso denominado “información y análisis de blancos electrónicos”, similar en muchos aspectos al proceso que realiza la artillería de campaña, del cual se deriva y al cual se integra como consecuencia de la C.F.A., sirviendo de base para establecer una lista de prioridades de los posibles blancos electrónicos.

436. Este proceso normalmente será realizado dentro del C.C.F.A. y con base en sus resultados serán asignados los blancos electrónicos a la unidad de guerra electrónica. No obstante, pueden existir situaciones que impongan que el proceso de referencia sea llevado a cabo por la C.C.G.E. de la unidad de guerra electrónica respectiva.

437. Para el efecto, son considerados como blancos electrónicos los siguientes:

A. Sistemas de mando, control, información y comunicaciones. Representados por los equipos y las redes de comunicaciones empleadas por la fuerza oponente para el intercambio de órdenes, informes y comunicaciones de diversa índole (tanto de voz como de datos), destinadas a la concepción, preparación y conducción de sus operaciones tácticas y los apoyos inherentes.

B. Sistemas de detección y vigilancia. Representados por diversos sistemas sensores activos o pasivos, destinados al reconocimiento del campo de batalla para obtener información sobre nuestras fuerzas. Dentro de esta categoría se ubican los radares de diversos tipos (terrestres o aéreos), dispositivos infrarrojos o térmicos, láser, magnéticos, sísmicos o acústicos, así como los elementos enemigos de apoyo electrónico.

C. Sistemas de armas. Representados por los dispositivos electrónicos de adquisición de blancos de los sistemas de armas enemigas, particularmente aquellos radares de los sistemas de defensa aérea, de proyectiles guiados, de contra artillería, entre otros.

D. Sistemas de perturbación y neutralización electrónica. Representados por los perturbadores y armas de energía dirigida que disponga la fuerza enemiga.

438. El proceso a que se ha hecho alusión, comprende dos funciones íntimamente relacionadas, las cuales quedaron asentadas en su denominación: la información de blancos electrónicos y el análisis de blancos electrónicos.

439. La información de blancos electrónicos es el conocimiento adquirido por medio de la recolección, evaluación y difusión de todos los datos relacionados con los blancos electrónicos existentes o probables. Esta información es parte de la información de combate y comprende la identificación oportuna, la determinación exacta y la transmisión de las características de los blancos electrónicos cuyo funcionamiento deba ser desorganizado o nulificado para facilitar a la unidad apoyada el cumplimiento de su misión.

440. Requiere además, la vigilancia electrónica (intercepción) de los blancos antes y después de ser atacados electrónicamente. La adecuada y precisa información de blancos electrónicos es indispensable para su análisis. En las unidades de guerra electrónica, esta es una responsabilidad de la C.C.G.E.

441. La explotación máxima de la potencia de transmisión de los perturbadores se logra por medio del empleo efectivo de la información de blancos, por lo que deberán realizarse todos los esfuerzos posibles para obtener y explotar esta información a fin de que las tropas combatientes cuenten con este apoyo en forma adecuada y oportuna.

442. Para lo anterior, es necesario el intercambio continuo de toda la información de blancos electrónicos obtenida por las unidades de apoyo electrónico, más aquella que proporcionen los diversos órganos y agencias de información.

443. Este intercambio contribuirá no solamente a satisfacer las necesidades específicas de información sobre blancos electrónicos, sino a cumplir la finalidad de esta actividad: realizar el eficaz empleo de los medios de perturbación electrónica sobre los blancos electrónicos enemigos, para apoyar de mejor manera a nuestras tropas.

444. La recolección de la información sobre blancos electrónicos se realiza por medio de un planeamiento continuo y un esfuerzo decidido para cumplir dicha finalidad. Lo que depende de que la o el oficial de información de la unidad de guerra electrónica posea un conocimiento apropiado del orden de batalla y dispositivo del enemigo. El planeamiento de las actividades de recolección comprende los siguientes aspectos:

A. Órdenes apropiadas a los elementos de apoyo electrónico subordinados, así como peticiones oportunas a los órganos de inteligencia de señales y guerra electrónica del escalón superior, para asegurar una afluencia constante de los informes sobre blancos electrónicos.

B. Empleo y explotación de otros órganos de información, tales como observadoras u observadores, patrullas de reconocimiento o elementos clandestinos.

C. Peticiones para el apoyo de la aviación de reconocimiento (visual, fotográfico y electrónico).

445. Por su parte, el análisis de blancos electrónicos es el examen de los blancos probables para determinar su importancia militar, la prioridad por atacarlos electrónicamente y las posibilidades de los medios disponibles para desorganizar o nulificar su funcionamiento.

446. Este análisis incluye la determinación de la conveniencia de sólo interceptar a un blanco, o bien perturbarlo, de conformidad con los lineamientos y restricciones impuestas por la o el jefe de la sección tercera del estado mayor, y se realiza para efectuar ataques por perturbación tanto planeados como de ejecución inmediata.

447. El tiempo y cantidad de detalles comprendidos en el análisis de blancos electrónicos depende de la información existente, de la disponibilidad de perturbadores para batirlos, el grado de coordinación requerida y de la urgencia para atacar el blanco.

448. Este análisis puede consistir en un cálculo mental rápido o bien, en un detallado análisis escrito como es el caso de un ataque planeado con oportunidad por una gran unidad. El apropiado análisis de blancos electrónicos representa una ayuda valiosa para que una o un comandante obtenga la mayor eficiencia en el empleo de los perturbadores a sus órdenes.

449. Después de haberse realizado la recolección de información y el análisis de blancos electrónicos, el ataque electrónico por perturbación se lleva a cabo, sin embargo, el proceso continúa mediante la evaluación de los efectos del ataque sobre el blanco.

450. De forma posterior a la ejecución del ataque a cada blanco electrónico, deberá realizarse un análisis para evaluar, hasta donde sea posible, la efectividad de la perturbación electrónica. Para ello se tratarán de determinar, de la manera más precisa, los efectos causados por la perturbación electrónica (o neutralización, en su caso) sobre el funcionamiento de los sistemas electrónicos del enemigo, lo cual incide directamente sobre su eficiencia de combate.

451. Esta información es necesaria como una base para evaluar la efectividad de los diferentes tipos de perturbación, niveles de potencia y métodos de control empleados, así como de la efectividad de las medidas de protección electrónica de la fuerza enemiga y los efectos de la perturbación sobre sus sistemas electrónicos, a su vez, ésta evaluación permite incrementar la efectividad de las contramedidas electrónicas establecidas en los planes de guerra electrónica.

452. En general, la información posterior al ataque electrónico puede ser obtenida por los mismos elementos que obtuvieron la información inicial de blancos electrónicos, aunque los datos más completos y precisos se obtienen de las unidades de apoyo electrónico, mediante la vigilancia continua de los sistemas electrónicos del enemigo, evaluando el grado en que su funcionamiento se vio afectado.

Subsección (E)

La Previsión de la Acción y Reacción Enemiga

453. Este principio indica que el planeamiento debe efectuarse cuidadosamente, estableciendo las posibles ventajas y desventajas de perturbar a los sistemas electrónicos del enemigo, ya que existirán ocasiones en que, derivado del análisis del blanco, sea recomendable sólo interceptar el emisor enemigo por el tipo de datos que estemos obteniendo; de lo contrario, si dicho emisor es perturbado, se perdería esa valiosa fuente de información al alertar a la fuerza adversaria, quien lógicamente incrementará sus medidas de protección electrónica.

454. Por otra parte, la perturbación electrónica bien proyectada puede aumentar las posibilidades de nuestras fuerzas de obtener valiosos datos de información. Por ejemplo: si perturbamos a la fuerza enemiga ciertos medios de comunicación a prueba de ser interceptados, lo podemos forzar a utilizar otro tipo de medios carentes de tal protección.

455. La fuerza enemiga también puede intentar destruir a nuestros perturbadores que se encuentren degradando el funcionamiento de sus sistemas electrónicos. Por lo tanto, se deberán adoptar las medidas que garanticen que los perturbadores no serán destruidos antes de cumplir con su misión.

456. Los perturbadores deberán estar dotados de la mayor movilidad posible, con la capacidad de operar en movimiento; cuando operen en forma fija, se debe procurar el empleo del terreno que brinde la mejor protección electrónica y que sus antenas sean instaladas a distancia y ocultas a la observación enemiga; de igual forma, se deberá considerar cambios frecuentes de ubicación.

Tercera Sección

El Proceso de Planeamiento en las Unidades de Guerra Electrónica

457. El éxito de las operaciones de guerra electrónica depende de planes debidamente elaborados y coordinados con los planes de operaciones de la unidad apoyada. El proceso de planeamiento consiste en:

A. Recibir los E.E.I. de quien ejerce el mando y tomarlos como base para la impartición de órdenes de búsqueda.

B. Recolectar información precisa sobre los sistemas electrónicos empleados por la fuerza oponente (blancos electrónicos).

C. Asignación de los blancos más apropiados para ser interceptados y localizados, o bien, perturbados con los medios disponibles.

D. Estimación y determinación de los medios de guerra electrónica necesarios para apoyar a cada gran unidad, para la obtención de los resultados deseados.

E. Preparación del plan de operaciones de guerra electrónica tomando en consideración todos los aspectos anteriores, para emplear sus recursos en contra de los blancos previamente conocidos y aquellos que sean descubiertos durante el curso de la operación.

458. El formato a que se sujetará el plan de operaciones de guerra electrónica se detalla en el anexo “A”.

Capítulo IV

La Seguridad

Primera Sección

Generalidades sobre la Seguridad

459. La seguridad es una condición que busca todo ser viviente en sus múltiples actividades y toda organización o colectividad para poder existir, desarrollarse y cumplir sus propósitos. En las actividades tácticas en las que existe siempre una fuerza adversaria mediata, inmediata, lejana o potencial, es precisamente donde la seguridad juega el papel más importante.[29]

460. Toda la información relacionada con la seguridad está contenida en la doctrina vigente establecida en el manual de operaciones en campaña; sin embargo, es necesario hacer mención de algunos aspectos que sientan la base para la influencia de la guerra electrónica en el mantenimiento de la seguridad.

461. La seguridad en el ámbito de la táctica, tiene cuatro propósitos fundamentales que son:

A. Evitar la sorpresa de parte del enemigo.

B. Preparar y lograr la sorpresa en contra de la fuerza adversaria.

C. Asegurar la libertad de acción del mando y sus tropas.

D. Evitar o limitar los efectos físicos y morales del fuego y otros medios de la fuerza adversaria en las tropas propias.

[29] S.D.N. Manual de Operaciones en Campaña. Op. Cit. Pag. 125-144.

462. La seguridad se clasifica en:

A. Seguridad del mando.

B. Seguridad de las tropas.

463. La Seguridad se puede obtener por los siguientes medios:

A. El informe.

B. El secreto.

C. El dispositivo.

D. La protección.

Segunda Sección

La Seguridad en la Guerra Electrónica

Subsección (A)

Medidas de Apoyo Electrónico

464. La aplicación de las medidas de apoyo electrónico puede contribuir de forma efectiva para obtener la seguridad por el informe, proporcionando a los mandos y sus tropas todos los datos necesarios para el éxito de sus misiones.

465. Estas medidas pueden proporcionar al mando información que le permita evitar ser sorprendido por la acción enemiga y de esta forma poder concebir, preparar y conducir la maniobra de acuerdo con lo que haya proyectado.

Subsección (B)

Contramedidas electrónicas

466. La perturbación y el engaño electrónico, coadyuvan también a proporcionar la seguridad.

467. Algunas de las aplicaciones que se materializan directamente en beneficio de las tropas combatientes son:

A. Perturbadores contra dispositivos explosivos de detonación electrónica.

B. Perturbadores contra granadas y proyectiles de artillería de detonación electrónica.

Capitulo V

El Reconocimiento electrónico

Primera Sección

Generalidades sobre las Operaciones de Reconocimiento

468. En el ámbito de las armas y diversas fuerzas combatientes, el reconocimiento es una acción ofensiva que se realiza en todos los niveles del mando con el objeto de obtener información principalmente de la fuerza oponente, del terreno y recursos existentes en una zona o área de operaciones, que sirva de base para el planeamiento y conducción de operaciones militares.[30]

469. El reconocimiento se encuentra implícito en cualquier misión durante el desarrollo de operaciones y es llevado a cabo por todos los escalones, desde la más pequeña unidad, hasta las grandes unidades.

470. Así tenemos que en cualquier situación táctica que se viva, será indispensable el reconocimiento para obtener información de los factores de dicha situación táctica, que para nosotros son desconocidos o parcialmente conocidos.

471. El reconocimiento y el contrarreconocimiento son complementos uno del otro y no pueden ser considerados en forma separada, un buen reconocimiento asegura al mismo tiempo cierto nivel de seguridad (contrarreconocimiento), bajo las siguientes consideraciones:

[30] Ibid.

A. La diferencia principal es que en las fuerzas de reconocimiento tienen una misión esencialmente móvil y por lo tanto amplia libertad de acción, mientras que en las fuerzas de contrarreconocimiento se encuentran relativamente fijas en una zona determinada y definida.

B. Cuando a una unidad se le designa al mismo tiempo misiones de reconocimiento y contrarreconocimiento, se le especificará cuál de ellas tiene mayor prioridad.

472. Es fundamental que la información durante las misiones de reconocimiento o contrarreconocimiento, llegue de manera oportuna al mando.

473. Para esta función todo el personal del servicio de las diversas unidades deberá estar perfectamente adiestrado para la transmisión rápida de todos los informes que se obtengan y como consecuencia, se establecerá una conducta a seguir para simplificar la transmisión y establecer sus prioridades.

474. El reconocimiento y contrarreconocimiento ayudan a obtener información, aplicar las medidas de contrainformación y conservar la seguridad, actividades indispensables para asegurar el éxito de las operaciones militares.

Segunda Sección

El Reconocimiento Electrónico

Subsección (A)

Generalidades

475. Se denomina reconocimiento electrónico al conjunto de actividades que son realizadas por las diversas plataformas terrestres o aéreas, de la mayor movilidad posible, dedicadas a la obtención y recolección de información sobre la presencia, funcionamiento, ubicación e importancia relativa de los sistemas electrónicos de la fuerza oponente en una determinada porción del terreno, durante la ejecución de diversas operaciones, fundamentalmente en la búsqueda.

476. El propósito del reconocimiento electrónico es adquirir el máximo conocimiento respecto a los sistemas electrónicos de la fuerza oponente, a fin de:

A. Obtener información relativa a su orden de batalla, tales como ubicación, despliegue y dispositivo que emplea.

B. Determinar su potencial tecnológico, mediante el estudio de sus capacidades técnicas.

C. Obtener datos que sirvan de base para asegurar que las contramedidas electrónicas que se adopten sean acordes a la situación y capaces de responder en forma adecuada a las posibilidades electrónicas de la fuerza oponente.

477. El reconocimiento electrónico proporciona información fundamentalmente técnica, respecto a los emisores electromagnéticos existentes en áreas de interés táctico y a las acciones necesarias para nulificar o degradar su funcionamiento en beneficio de nuestras operaciones; para lo cual se realizan una serie de acciones destinadas a la búsqueda de los emisores enemigos y sus parámetros técnicos, para determinar las acciones de guerra electrónica u otras acciones tácticas que deban ser aplicadas en una situación dada.

478. Es necesario dar prioridad al análisis técnico de las señales. Esto implica someter las emisiones registradas durante el reconocimiento electrónico, a un análisis especializado y así poder establecer de forma precisa sus posibles aplicaciones por parte de la fuerza oponente.

479. La información relativa a los sistemas electrónicos del enemigo, susceptible de ser obtenida por este reconocimiento, entre otros aspectos son:

A. Ubicación geográfica aproximada.

B. Función o empleo.

C. Potencia de transmisión.

D. Lóbulo de antena (anchura del haz).

E. Frecuencia de operación.

F. Tipos de modulación.

480. Para obtener resultados satisfactorios en la ejecución del reconocimiento electrónico, es necesario contar con una sólida base táctica y técnica desarrollada por medio del adiestramiento especializado del personal integrante de las unidades de guerra electrónica.

481. En la ejecución de las operaciones de reconocimiento electrónico se debe considerar lo siguiente:

A. Los objetivos del reconocimiento electrónico son los sistemas electrónicos en conjunto; los datos que no es posible asociar a un sistema en concreto tienen muy poco valor, ya que sólo proporcionan indicios aislados sobre las capacidades tecnológicas del enemigo.

B. En el espectro electromagnético se encuentran presentes señales de origen natural y señales emitidas por sistemas electrónicos construidos por el hombre o la mujer; los fenómenos naturales son aleatorios, mientras que las señales que emiten los sistemas electrónicos son repetitivas.

C. El sistema objetivo debe ser estudiado como un todo, ya que cualquiera de sus componentes constituye una posible fuente de información. Incluso pueden existir elementos de un sistema capaces de proporcionar información que no hayan sido considerados para su explotación (como las emisiones comprometedoras).

D. Los sistemas electrónicos “objetivo” generalmente son muy complejos, es decir, se encuentran integrados por componentes que permiten disponer de una gran diversidad de datos; por lo tanto, dichos datos deben ser interrelacionados de forma compleja y no solo de una manera simple o lineal.

E. Los sistemas electrónicos regularmente son de funcionamiento semiautomático. Por lo tanto, en el análisis de los datos obtenidos es necesario diferenciar la respuesta del sistema (previsible) de las acciones de los operadores (imprevisibles hasta cierto punto), a fin de estimar en su justa dimensión el potencial tecnológico del enemigo.

F. Determinar las capacidades reales del sistema enemigo.

G. El reconocimiento electrónico debe desarrollarse en forma persistente en el tiempo, sobre todo a nivel de inteligencia estratégica.

H. Aún cuando no se almacenen los datos técnicos obtenidos, la información táctica debe ser consolidada, registrada y archivada por la sección segunda (Inteligencia), con la demás información de combate, conforme a los procedimientos de doctrina vigentes.

Subsección (B)

Principios Generales del Reconocimiento Electrónico

482. Las operaciones de reconocimiento electrónico deben sujetarse a los siguientes principios generales:

A. El ambiente electrónico debe ser estimulado para que el enemigo transmita las señales deseadas.[31] Esto puede ser realizado mediante la presentación de alguna amenaza a sus fuerzas, bajo las consideraciones siguientes:

a. La amenaza sobre el enemigo debe ser real y factible, de modo que se vea obligado a encender los sistemas electrónicos objeto del reconocimiento (como sus radares de defensa aérea).

b. Al presentar la amenaza, los sistemas sensores deben encontrarse preparados para obtener todos los datos relativos al equipamiento enemigo.

B. La provocación o amenaza debe ser acorde con el objetivo que se desea alcanzar. Una provocación realizada en época de tensiones con otros estados, puede ocasionar un conflicto armado.

C. Los alcances del reconocimiento deben establecerse de forma que se considere tanto la búsqueda de nuevos conocimientos como la confirmación de aquellos adquiridos con anterioridad. Esto incluye no sólo confirmar la información disponible, sino también su posible ampliación.

[31] Academia de Artillería de Segovia. Op. Cit. P.78-80.

D. Durante su ejecución, el reconocimiento electrónico debe permitir la realización del análisis en tiempo real de los datos recolectados, para poder utilizar la información obtenida técnica y tácticamente cuando sea necesario responder en forma inmediata a cualquier amenaza que surja.

Subsección (C)

Misiones de Reconocimiento Electrónico

483. Por la amplitud con que se realizan y el propósito buscado, las misiones de reconocimiento electrónico pueden ser:

A. Reconocimiento de zona. Consiste en el reconocimiento del espectro electromagnético en una zona del terreno fijada por los límites asignados.

B. Reconocimiento de ruta. Es el esfuerzo dirigido para obtener información sobre los emisores enemigos a lo largo de una ruta específica y el terreno circundante.

C. Reconocimiento de área. Es el esfuerzo dirigido para obtener información sobre los emisores enemigos en un área específica y es de menor amplitud que el de zona. El área puede ser un pueblo o una ciudad, un bosque, una serie de cruces de caminos o ríos, o cualquier otra característica física del terreno cuyos límites son fácilmente identificados.

484. Las misiones de reconocimiento electrónico se caracterizan por su movilidad; de igual forma, la naturaleza de las emisiones electromagnéticas, así como de la información a recolectar, implica que sean realizadas en estrecha cercanía o contacto con la fuerza enemiga, inclusive en o sobre el terreno bajo su control.

485. Por lo anterior, las misiones de reconocimiento electrónico generalmente toman la forma de reconocimiento de ruta y preferentemente, son efectuados por las diversas plataformas aéreas, bajo las siguientes modalidades:

A. Reconocimiento de ruta periférica. Es el que se realiza totalmente en o sobre terreno bajo control propio, por lo que la exposición de la plataforma a ser destruida es mínima. Sin embargo, reduce la posibilidad de obtener información de los emisores enemigos ubicados en profundidad, como los radares de defensa aérea y las redes de mando y artillería.

B. Reconocimiento de ruta penetrante. Es aquel que, partiendo de nuestro propio dispositivo, se adentra en terreno bajo control de la fuerza oponente con el fin de obtener datos confiables sobre sus emisores ubicados en profundidad. Por su naturaleza y riesgo implícitos, es recomendable que sea realizado por plataformas aéreas dotadas con capacidades defensivas (incluidas contramedidas electrónicas), o de tal ligereza que les permita sustraerse con facilidad de las amenazas enemigas; en su defecto, emplear aeronaves no tripuladas.

Subsección (D)

Aplicaciones en Tiempo de Paz

486. La ejecución de operaciones de reconocimiento electrónico es indispensable en tiempo de paz, a efecto de determinar con precisión el grado de avance tecnológico de naciones potencialmente hostiles.

487. Este conocimiento sirve de base para la realización de estudios e investigaciones en materia de guerra electrónica, que permitan establecer de forma real las necesidades de equipamiento electrónico para hacer frente a la amenaza, con el fin de proceder a su desarrollo y fabricación, o bien su adquisición.

488. En este contexto, dichas operaciones deben ser planeadas, ejecutadas y dirigidas por los órganos de inteligencia a nivel alto mando, por lo que se integran dentro del sistema de inteligencia de señales, específicamente dentro de la rama de inteligencia electrónica.

489. También sirven de fundamento para la ejecución de estas operaciones en tiempo de paz, las consideraciones siguientes:

A. Ningún sistema electrónico empleado en las operaciones militares asegura el secreto de las mismas, ya que una vez puesto en operación, se buscará desarrollar las técnicas o dispositivos que nulifiquen su funcionamiento.

B. La mayor parte de innovaciones desarrolladas en materia de guerra electrónica son clasificadas como secretas y mantenidas con ese carácter por largos periodos, por lo que raramente se hacen públicos sus resultados de aplicación.

C. El equipo de guerra electrónica disponible en la comunidad internacional está universalmente reconocido y no representa una amenaza considerable para los países que lo producen.

D. El camino a seguir por los países con menores recursos tecnológicos es el de la investigación y el desarrollo, mediante la capacitación especializada de personal dedicado exclusivamente a estas actividades para lograr diseñar y construir equipos propios que rompan la dependencia tecnológica en la materia.

Capítulo VI

Generalidades del empleo de la Guerra Electrónica en las Operaciones Tácticas

Sección Única

Generalidades

490. Al conocer la misión y el concepto de la operación de la o el comandante, la sección segunda (Inteligencia) y la sección tercera (Operaciones) del estado mayor correspondiente, el centro coordinador de fuegos de apoyo y la célula de coordinación de guerra electrónica, establecen las prioridades que serán asignadas a las unidades de apoyo electrónico y contramedidas electrónicas durante cada fase del combate, tomando en consideración la aplicación de todos y cada uno de los principios del tipo operación de que se trate.

491. Durante la organización táctica de la gran unidad, se lleva a cabo la distribución de los medios de guerra electrónica, la que puede realizarse por unidades orgánicas o mediante la organización para el combate, de acuerdo con la misión por cumplir, la cantidad de grandes unidades por apoyar y unidades de guerra electrónica disponibles, así como la importancia del esfuerzo a realizar por las unidades de maniobra.

492. A manera de ejemplo, se establece la distribución que podría ser realizada en un cuerpo de ejército, el cual está integrado por tres divisiones de infantería y es apoyado por un batallón de guerra electrónica pesada “tipo”, de la manera siguiente:

A. En apoyo general al cuerpo de ejército.

a. Una compañía de guerra electrónica pesada.

b. La compañía (o escuadrón) de guerra electrónica aérea.

B. En apoyo directo a cada división una compañía de guerra electrónica pesada.

493. Como parte de las acciones previas a la ejecución de cualquier operación táctica, es necesario efectuar los reconocimientos electrónicos que sean necesarios para poder determinar con precisión las características y tipo de sistemas electrónicos empleados por el enemigo, así como para obtener toda aquella información relacionada con el orden de batalla del enemigo, proporcionando posteriormente, dicha información al sistema de inteligencia.

494. Lo anterior implica que la o el comandante de la unidad de guerra electrónica mantenga una coordinación estrecha con los demás integrantes del estado mayor, a fin de conocer el área de responsabilidad de la o el comandante de la unidad táctica y sus E.E.I., con objeto de organizar el despliegue adecuado de los medios de guerra electrónica.

495. También es imprescindible establecer de antemano los detalles de coordinación necesarios para evitar que las operaciones de perturbación se ejecuten en frecuencias empleadas por nuestras tropas, motivo por el cual se hará un uso extensivo de los métodos de control de la perturbación dentro de la planeación de dichas operaciones.

Capítulo VII

La Guerra Electrónica en las Operaciones Ofensivas

Primera Sección

Generalidades sobre las Operaciones Ofensivas

496. Las operaciones militares dentro de un teatro de operaciones[32] se manifiestan plenamente en la maniobra ofensiva, la cual tiene como objeto destruir al enemigo y se caracteriza porque busca la iniciativa, impone la propia voluntad, hora y lugar para librar el combate, con el propósito de:

A. Destruir las fuerzas oponentes.

B. Tomar terreno clave.

C. Engañar y destruir a la fuerza oponente.

D. Obtener información.

E. Destruir los recursos del enemigo, así como su moral y voluntad para seguir combatiendo.

497. Aun cuando las operaciones ofensivas tradicionalmente están relacionadas con una proporción favorable de poder de combate y una desventaja enemiga, éstas no son necesariamente condiciones previas para una acción ofensiva, sino la movilidad, la sorpresa y la ejecución agresiva que son los medios más eficaces para lograr el éxito.

[32] S.D.N. Manual de Tactica General. Op. Cit. Pag. 58-66

498. La superioridad numérica no es necesariamente una condición previa para las operaciones ofensivas, más bien, son las y los comandantes quienes deben buscar continuamente la oportunidad de tomar la iniciativa por medio de una acción ofensiva aun cuando se encuentren a la defensiva.

499. De tal manera que la o el comandante debe buscar el “cuándo atacar", estimando cuidadosamente la capacidad de sus fuerzas para conquistar las defensas enemigas y para soportar los contraataques de la fuerza oponente, atacando cuando esté seguro que su maniobra y sus fuegos infligirán pérdidas irreparables en sus medios, neutralizará núcleos importantes o logrará algún efecto menor para un propósito específico.

500. Es por tal motivo que la o el comandante obtendrá información, determinará su propio ritmo de batalla sin perder de vista las ventajas que normalmente favorecen al defensor y evaluará cuantitativamente el costo del éxito.

501. Por lo tanto, las operaciones ofensivas deben ser planeadas con el fin de cumplir con los seis principios de la ofensiva, los cuales son:

A. Conocer el campo de batalla.

B. Concentrar una potencia de combate arrolladora.

C. Suprimir los fuegos defensivos de la fuerza oponente.

D. Causar conmoción, sorpresa y destrucción de la fuerza oponente.

E. Atacar profundamente la retaguardia enemiga para destruir su sistema de defensa.

F. Apoyar el movimiento continuo.

Segunda Sección

Los Principios de la Ofensiva y la Guerra Electrónica

502. Quien ejerce el mando de una fuerza militar debe tener presente, en todo momento, que el empleo adecuado de la guerra electrónica puede tener efectos importantes sobre la fuerza a su mando, incrementando su capacidad combativa de forma considerable.

503. Como uno de los principales elementos de apoyo al combate a disposición del mando de que se trate, la guerra electrónica tiene una aplicación fundamental en la ejecución de las operaciones ofensivas. Dicha aplicación deberá ser plasmada en el plan de operaciones de guerra electrónica respectivo, previendo cumplir con cada uno de los principios de las operaciones ofensivas antes mencionados, de la manera en que se describe en las subsecciones siguientes.

Subsección (A)

Conocer el Campo de Batalla

504. La o el comandante que planea una maniobra ofensiva debe disponer, tanto como sea posible, de información relacionada con el factor enemigo, incluyendo, entre otros aspectos: forma de defensa; efectivos en el área; capacidades y vulnerabilidades del armamento con que cuenta y su empleo táctico; moral y condición física de la fuerza; puntos débiles del sistema defensivo, entre otros.

505. Mediante el despliegue de todas las unidades de apoyo electrónico de que se disponga, es posible obtener datos de interés respecto a los aspectos antes indicados, a fin de obtener la máxima cobertura del área de operaciones, así como sobre los sistemas electrónicos que emplea en su posición defensiva, tales como los de comunicaciones, vigilancia electrónica y de armas.

506. La información así obtenida, cuando se integra al sistema de inteligencia con aquella procedente de otras fuentes, permite que la o el comandante disponga de un conocimiento más amplio y preciso del campo de batalla.

507. Además, el plan de operaciones de guerra electrónica debe contemplar el empleo de las unidades de apoyo electrónico para la obtención de información relacionada con la densidad de emisores existentes en algún sector específico, aparte de otros indicios que permitan ubicar con precisión la principal área defensiva de la fuerza enemiga, las brechas o puntos débiles en su dispositivo, obstáculos, reservas, unidades de apoyo de fuegos, principales centros de mando, entre otros.

508. Una consideración primordial para satisfacer las necesidades de información del mando, es la explotación, hasta donde sea posible, de las posibilidades que ofrecen las plataformas aéreas, las cuales facilitan la obtención de información y datos generados en las áreas de retaguardia de la fuerza enemiga.

Subsección (B)

Concentrar una Potencia de Combate Arrolladora

509. Este principio implica prever todo lo necesario para que la o el comandante de una fuerza pueda llevar a cabo la organización de una fuerza con la suficiente potencia de combate para ejecutar su maniobra; esto significa que debe mover tropas, engañar al enemigo referente a su posición, hora, dirección y magnitud ofensiva; así como frustrar toda capacidad para que obtenga información, mediante el empleo cuidadoso del terreno, del camuflaje, del movimiento en períodos de poca visibilidad, de la protección electrónica y demás recursos para contrarrestar o engañar la vigilancia enemiga.

510. Es necesario que los planes de operaciones de guerra electrónica contemplen el desarrollo de acciones tendientes a facilitar la concentración de fuerzas, como son:

A. Coadyuvar a ocultar la concentración. Encontrándose a la defensiva, el adversario recolecta información valiéndose de todos los medios a su alcance, incluyendo la guerra electrónica. Por tal motivo, tanto en el plan de operaciones de la gran unidad, como en el de la unidad de guerra electrónica, deben ser establecidas las medidas de protección electrónica necesarias, para negar al enemigo el conocimiento de las acciones relativas a la concentración y evitar que pueda reaccionar de forma tal que impida su materialización.

B. Cooperar con las acciones destinadas a engañar al enemigo sobre el área donde será concentrada la potencia de combate. El mando de la gran unidad normalmente considerará la ejecución de operaciones tácticas de contrainformación (engaño, fintas y demostraciones), tendientes a engañar o confundir al enemigo sobre el lugar, forma o momento de la concentración.

C. Estas operaciones deben ser debidamente respaldadas mediante la inclusión de operaciones de engaño electrónico dentro de los planes de operaciones de la gran unidad en forma general y de la unidad de guerra electrónica en forma particular.

D. Incluir dentro de la fuerza a ser concentrada, unidades de guerra electrónica en número y características necesarias para apoyar la ejecución de la maniobra proyectada. La concentración es el paso previo a la maniobra, por lo que durante ella se deberá prever la asignación de las unidades necesarias para apoyar la operación.

E. Las unidades que se asignen deberán ser tan móviles como la fuerza a la que apoyarán, previéndose el empleo prioritario de unidades de guerra electrónica pesada, con el fin de que se encuentren debidamente protegidas contra los efectos del fuego enemigo.

Subsección (C)

Suprimir los Fuegos Defensivos del Enemigo

511. La o el comandante de toda fuerza ofensiva debe tener presente que la concentración de fuerzas crea una situación de vulnerabilidad, que puede ser aprovechada por el enemigo para neutralizar a sus tropas aún antes de ser empleadas en el combate.

512. Por lo anterior, el plan de fuegos de apoyo debe estar en perfecta concordancia con la maniobra proyectada, considerando la supresión de los fuegos de apoyo enemigos, que ejerzan influencia en las áreas de la concentración y del empleo posterior de la fuerza concentrada.

513. En este sentido, adquiere una importancia fundamental la integración de los planes de guerra electrónica con el plan general de fuegos de apoyo de la gran unidad, a efecto de:

A. Obtener información sobre blancos electrónicos que constituyan una prioridad para lograr suprimir los fuegos enemigos, tales como: radares de adquisición de blancos y de defensa aérea, centrales de tiro, observatorios y baterías de artillería, a fin de evaluar su ataque por fuegos físicos o bien, por perturbación.

B. Perturbar las redes de comunicaciones de los medios de fuegos de apoyo enemigos para impedir la coordinación entre sus diversos elementos, dificultando de este modo su acción.

C. Perturbar los sistemas electrónicos de vigilancia y adquisición de blancos de la fuerza adversaria, impidiéndoles obtener información sobre los blancos que representan nuestros elementos de fuegos de apoyo.

514. Para lo anterior, puede ser conveniente o incluso indispensable, el empleo de plataformas aéreas para obtener información de los blancos ubicados en profundidad, así como para ejecutar acciones de perturbación a mayores distancias.

Subsección (D)

Causar Conmoción, Sorpresa y Destrucción del Enemigo

515. Una vez lanzada la ofensiva, la o el comandante deberá coordinar las acciones subsecuentes para maximizar la rapidez, la sorpresa y la violencia del ataque. Las unidades de maniobra combinan su avance con los elementos de apoyo al combate, tales como fuegos de apoyo, guerra electrónica y defensa aérea. Independientemente de la maniobra que adopten las unidades, el ataque se realiza de frente, concentrado y en profundidad.

516. Los agrupamientos propios que sean desorganizados o queden rezagados, deben ser rebasados por formaciones de segundo escalón, a fin de ejercer presión contra objetivos más profundos, dislocar las posiciones defensivas, evitar la reorganización de la fuerza oponente y destruir su sistema defensivo.

517. Para apoyar la maniobra, los planes de guerra electrónica deben contribuir a su adecuada ejecución, facilitando el avance de las tropas y la continuidad de la acción. Esto implica que las operaciones de guerra electrónica se centren en la ejecución de contramedidas electrónicas, pasando las de apoyo electrónico a un segundo término, siempre y cuando esto no se contraponga con el apoyo requerido por las tropas.

518. Es necesario contemplar la desorganización de las redes de transmisiones enemigas, privando a las tropas ejecutantes de la dirección que le proporcionan sus mandos, de tal modo que las unidades enemigas carezcan de órdenes y con ello, de capacidad de reacción. Esto contribuye de forma notable a evitar la reorganización de las fuerzas enemigas, facilitando el colapso del sistema defensivo del enemigo.

519. La desorganización de referencia deberá materializarse de manera escalonada, actuando los perturbadores en un primer tiempo contra las unidades enemigas establecidas en primer escalón, adelantando su acción a medida que el avance de las tropas progrese.

Subsección (E)

Atacar Profundamente la Retaguardia Enemiga para Destruir su Sistema de Defensa

520. Una vez que nuestras unidades penetran las posiciones enemigas, se esforzarán por alcanzar su retaguardia, en donde normalmente se localizan los puestos de mando, los centros de transmisiones y los apoyos de combate y servicios, quienes a menudo cuentan con menor capacidad para defenderse de cualquier ataque.

521. Alcanzar la retaguardia enemiga, nuestras fuerzas buscarán la destrucción y/o desorganización de los sistemas de mando y control enemigos así como de todos los elementos de apoyo que encuentren; ya que el éxito obtenido en la retaguardia de la fuerza enemiga regularmente obligará al enemigo a abandonar las ventajas que le otorgan sus posiciones defensivas, así como a emplear desorganizadamente a sus reservas.

522. El planeamiento de guerra electrónica deberá considerar el apoyo a las fuerzas de maniobra mediante las siguientes acciones:

A. La obtención aproximada de las ubicaciones de las instalaciones enemigas establecidas en su retaguardia.

B. Asignación de los medios que faciliten la desorganización de las redes de transmisiones ubicadas en profundidad, a fin de evitar:

a. Que las unidades enemigas articulen sus esfuerzos para contrarrestar las acciones de nuestras tropas,

b. El empeño de sus reservas.

c. El envío de refuerzos a los puntos críticos de la acción.

523. Para la realización oportuna y eficiente de las acciones anteriores, es indispensable el empleo de plataformas aéreas, las que deberán ser orgánicas o asignadas en refuerzo.

Subsección (F)

Apoyar el Movimiento Continuo

524. Una ofensiva que se desarrolla exitosamente, precisará constantemente de apoyos al combate y de servicio, con el fin de mantener el ímpetu del ataque y facilitar la continuidad de la acción.

525. Todos los apoyos deben planear detalladamente sus desplazamientos, a fin de conservar el ritmo de la maniobra y facilitar su propia acción. Entre más profunda sea la penetración, más difícil será mantener abiertas las rutas de abastecimiento y evacuación, pero sobre todo, hacer que las mujeres y los hombres conserven el ánimo y resistan la acción; esto exige un planeamiento imaginativo, ejecución vigorosa, y una reacción flexible ante cualquier contingencia.

526. Lo anterior implica que en los planes de guerra electrónica, se prevean las acciones a desarrollar durante las fases de explotación y persecución, principalmente, de modo tal que se proporcione un apoyo permanente y continuo a las fuerzas de maniobra; para este fin, es necesario realizar la distribución de los medios de guerra electrónica de forma tal, que se asegure su acción en todos los sectores de la ofensiva, en estrecho contacto con las unidades que la materializan.

Tercera Sección

Apoyo de Guerra Electrónica en el Combate Ofensivo

527. El combate ofensivo puede comprender una o más de las siguientes fases.

A. Marcha de aproximación.

B. Toma de contacto.

C. Empeño.

D. Ataque.

E. Asalto.

F. Explotación del éxito.

G. Persecución.

528. En virtud de que las anteriores fases pueden o no llevarse a cabo, así como por la similitud de acciones a realizar en algunas de ellas, para efectos de ejecución de las operaciones de guerra electrónica, se consideran únicamente las fases siguientes:

A. Acciones previas al ataque.

B. Ataque y asalto.

C. Explotación y persecución.

Subsección (A)

Acciones Previas al Ataque

529. Desde la etapa de concepción de la operación ofensiva, algunas unidades de apoyo electrónico deben ser desplegadas tan a vanguardia como sea posible, con el fin de obtener información que amplíe o confirme aquella de que se disponga en relación con la unidad enemiga y así apoyar la preparación y posterior conducción de la operación.

530. Una vez que comience la ejecución de la operación ofensiva, es necesario destacar los efectivos necesarios para establecer una línea de base acompañando a la fuerza de contacto, la cual proporcionará informes de último momento respecto a las actividades y movimientos de las fuerzas enemigas, así como sobre aquellas amenazas que surjan durante el cumplimiento de su misión.

531. De igual forma, se deben asignar a la fuerza de contacto, perturbadores de tipo y cantidad necesarios para cubrir la totalidad de su sector de responsabilidad, los que apoyarán la ejecución de las acciones ofensivas de alcance limitado que realice dicha fuerza, durante la toma de contacto y el empeño.

532. Dentro de las acciones previas al ataque, será durante las fases de referencia en las cuales se manifieste plenamente la acción de la guerra electrónica, debido a que dichas fases en sí, tienen entre sus fines cubrir el despliegue del grueso y la obtención de información complementaria respecto al dispositivo, ubicación, puntos débiles y demás datos de interés sobre el enemigo.

533. La unidad de guerra electrónica también coordinará la ejecución de operaciones de engaño electrónico que sean realizadas por unidades de las diversas armas y servicios; dichas operaciones generalmente estarán orientadas a respaldar otras acciones de engaño que se ejecuten en el marco del dispositivo general, con el fin de desorientar al enemigo sobre la composición, magnitud y tipo de la fuerza atacante, así como sobre la orientación del ataque, entre otros aspectos.

Subsección (B)

Ataque y Asalto

534. De conformidad con lo establecido en los planes de operaciones de guerra electrónica que para el efecto se hayan formulado, durante estas fases la guerra electrónica deberá realizar un conjunto de acciones orientadas a disminuir significativamente la capacidad combativa de la unidad oponente.

535. Las unidades de apoyo electrónico que operen en apoyo directo de las fuerzas de maniobra, deberán ubicarse a inmediata retaguardia de las unidades que materializan el ataque, buscando con ello incrementar la cobertura de sus sensores y así obtener la mayor cantidad de datos que permitan apoyar el ataque, principalmente por la anticipación oportuna de la reacción enemiga.

536. Sin embargo, durante estas fases las operaciones de mayor importancia serán las de perturbación electrónica. Para el efecto, las plataformas de perturbación (perturbadores) deberán ubicarse en posiciones preferentemente elevadas, que les permitan emitir sus radiaciones de alta potencia en el momento oportuno y con el mayor alcance posible, procurando que al mismo tiempo les proporcionen encubrimientos contra la observación enemiga, así como el mayor grado de protección electrónica posible.

537. Los blancos de las operaciones de perturbación deberán ser asignados desde la preparación de la operación. Para tal fin, el C.C.F.A. indicará a la unidad de guerra electrónica aquellos blancos electrónicos que son susceptibles de ser perturbados durante el ataque o el asalto.

538. Los blancos de referencia generalmente estarán constituidos por los sistemas de mando y control y de armas que sean de importancia crítica para el enemigo, con cuya degradación, se disminuyan sus capacidades de coordinación y reacción ante la ofensiva de nuestras fuerzas.

539. Cuando existan blancos electrónicos que estén siendo sujetos a intercepción y se proceda a su perturbación, se deberán girar las órdenes correspondientes a fin de que por lo menos una plataforma de apoyo electrónico permanezca a la escucha en la frecuencia perturbada y proporcione informes sobre la efectividad de la perturbación, a fin de reorientarla en caso necesario.

540. Es de vital importancia mantener en reserva la cantidad de perturbadores indispensable para poder influir en el combate en situaciones imprevistas que hagan necesario el empleo de una mayor potencia de combate en el punto decisivo de la acción, como sería el caso de impedir u obstaculizar la acción de las reservas enemigas.

Subsección (C)

Explotación y Persecución

541. Durante estas fases se busca destruir toda capacidad de la unidad enemiga para reorganizar su defensa y realizar acciones retrógradas con algún grado de organización, así como procurar la destrucción de los restos de la fuerza enemiga, evitando su retirada.

542. Por tal motivo, el objetivo principal de las operaciones de guerra electrónica durante estas fases es la desorganización de los sistemas de mando y control de la fuerza oponente, principalmente los empleados por sus principales niveles de mando, a fin de evitar que coordinen acciones de cualquier tipo que tiendan a la reorganización de su defensa.

543. Lo anterior origina que las principales operaciones a ejecutar continúen siendo las de perturbación electrónica; sin embargo, como resultado de la perturbación de las principales redes de mando y control enemigas durante el ataque y asalto, los blancos electrónicos a degradar durante estas fases normalmente serán blancos de oportunidad.

544. Dichos blancos normalmente serán obtenidos por las unidades de apoyo electrónico y por las o los oficiales de enlace de guerra electrónica destacados en las pequeñas unidades de maniobra; para su perturbación, primero será necesario que sean analizados por la célula de coordinación de guerra electrónica (C.C.G.E.) y concentrados al centro coordinador de fuegos de apoyo (C.C.F.A.), a fin de que éste determine el mejor procedimiento para su destrucción o degradación. Si el C.C.F.A. haya confirmado las órdenes de perturbación, estas podrán materializarse.

545. Sin embargo, en cualquier fase de las operaciones podrán existir situaciones en las que sea necesario reaccionar de manera inmediata contra algún tipo de amenaza que el enemigo lance contra nuestras fuerzas. En tales situaciones, los perturbadores ejecutarán la perturbación sin necesidad de órdenes, informando de sus acciones a la C.C.G.E.

Capítulo VIII

La Guerra Electrónica en las Operaciones Defensivas

Primera Sección

Generalidades sobre las Operaciones Defensivas

546. Operaciones defensivas son las acciones que desarrollan las tropas, en las que emplean todos los medios a su disposición y formas de combate para las cuales han sido adiestradas, a fin de impedir, resistir o destruir un ataque enemigo.[33]

547. La defensiva tiene como finalidad:

A. Ganar tiempo hasta que se presenten condiciones favorables para emprender la ofensiva.

B. Economizar fuerzas en un área, a fin de concentrar fuerzas superiores para emprender una acción ofensiva decisiva en otra parte.

548. Consideraciones de tipo político o estratégico, pueden obligar a adoptar una actitud defensiva.

549. Estas operaciones pueden ser impuestas por la situación, ordenadas por el escalón superior, o adoptadas voluntariamente.

[33] Ibid.

550. La defensiva debe evitarse, y solamente adoptarse cuando existe una situación desventajosa o de inferioridad respecto a la fuerza oponente; cuando se asuma debe ser solamente como un medio temporal de cumplir la misión, en espera de una oportunidad de pasar a la ofensiva o para economizar fuerzas. Además, se debe aprovechar cualquier oportunidad para actuar ofensivamente mediante contraataques, fintas y ataques de desarticulación.

551. Generalmente, el resultado positivo de la batalla se deriva de las operaciones ofensivas; frecuentemente existe la necesidad de defender una posición geográfica aprovechando las ventajas que se obtienen al conocer el terreno, reconocer y preparar el área defensiva en profundidad, de colocar cuidadosamente en posición a las unidades y sus armas para disminuir sus vulnerabilidades y aprovechar al máximo sus capacidades.

552. Se puede concluir que el defensor goza de casi todas las ventajas, excepto una: la iniciativa. Para obtenerla, cada comandante debe realizar la acción que es vital en todas las operaciones defensivas: atacar; además, debe observar las siguientes reglas o principios de la defensiva en la planeación de sus operaciones:

A. Conocer a la fuerza oponente.

B. Analizar tácticamente el terreno para seleccionar el campo de batalla.

C. Concentrarse en el lugar adecuado para desplegar a la hora decisiva.

D. Combatir con una organización para el combate flexible (agrupamientos de armas combinadas).

E. Explotar las ventajas del defensor.

Segunda Sección

Los Principios de la Defensiva y la Guerra Electrónica

553. Al igual que durante la preparación de operaciones ofensivas, las formas de empleo de las operaciones de guerra electrónica deberán ser consideradas desde la elaboración del plan de operaciones de guerra electrónica respectivo, atendiendo los principios de las operaciones defensivas antes mencionados, de la manera en que se describe en las subsecciones siguientes.

Subsección (A)

Conocer a la Fuerza Oponente

554. Toda fuerza oponente que invada el territorio nacional podrá emplear doctrinas tácticas, materiales, armamentos y formas de empleo táctico diferentes a las nuestras; esta circunstancia implica para toda o todo comandante la exigencia de tener un conocimiento profundo de dichos aspectos para poder estimar en la justa medida las capacidades y limitaciones de toda fuerza oponente, y sobre esa base sólida, desarrollar los cursos de acción necesarios para cumplir una misión.

555. Algunos de los aspectos antes citados podrán ser conocidos con anterioridad a las hostilidades, para lo cual serán de importancia primordial los órganos de inteligencia del alto mando (incluidos los de inteligencia de señales) mediante el desarrollo, desde tiempo de paz, de la información del orden de batalla.

556. Otros aspectos, sólo podrán ser conocidos durante el desarrollo mismo de las operaciones, lo que implica para el sistema de inteligencia de la gran unidad, la recolección de la mayor cantidad de informes que proporcionen datos precisos sobre aquellos aspectos que de la fuerza adversaria se desconozcan o sólo se disponga un conocimiento limitado.

557. Las unidades de guerra electrónica pueden coadyuvar en la búsqueda de tales informes, por lo que es indispensable que el sistema de inteligencia les asigne de forma precisa los aspectos de interés, para orientar la búsqueda y evitar dispendio de esfuerzos.

558. Además de dichos aspectos, las unidades de guerra electrónica deberán recolectar la mayor cantidad de información sobre los sistemas electrónicos empleados por el enemigo: sus características físicas, firmas electrónicas, procedimientos de operación, táctica de empleo, entre otros, para lo cual es de vital importancia la ejecución de reconocimientos electrónicos.

Subsección (B)

Analizar Tácticamente el Terreno para Seleccionar el Campo de Batalla

559. A la defensiva, será común que nuestras fuerzas se encuentren en desventaja numérica, lo que exige saber dónde concentrar la fuerza para no ser sorprendida y aniquilada. Esto implica para la o el comandante el análisis en forma constante y minuciosa de los posibles campos de batalla, a fin de concentrar la fuerza en el momento oportuno.

560. Las y los comandantes deben tomar decisiones difíciles basándose en información incompleta, por lo que deben implementar un amplio plan de búsqueda de información, que en muchas situaciones no podrá materializarse por las medidas de contrainformación enemigas y la insuficiencia de recursos para su obtención. Dicho plan debe incluir tareas para las unidades de apoyo electrónico.

561. Las misiones que se asignen a las unidades de apoyo electrónico deberán estar orientadas a apoyar el esfuerzo de búsqueda de la información requerida por la o el comandante para satisfacer sus E.E.I.

562. Por lo regular, estas misiones consistirán en la obtención de datos para determinar con precisión, las características, magnitud, composición y equipamiento de la fuerza atacante, aspectos que son fundamentales para que la o el comandante determine, en un primer tiempo, la forma en que realizará la defensa, y posteriormente, las áreas que cuenten con las características del terreno necesarias para materializar con las mayores probabilidades de éxito la forma de defensa seleccionada.

Subsección (C)

Concentrarse en el Lugar Adecuado para Desplegar a la Hora Decisiva

563. Las y los comandantes tienen que decidir exactamente dónde y cuándo han de concentrar sus fuerzas, basándose en la información producida por su sistema de inteligencia. Para determinar el poder de combate necesario para defender la posición y conservar la operatividad de la unidad. Considerando que al contar con terreno favorable, preponderancia de artillería de campaña, de apoyo aéreo y de guerra electrónica puede ser posible la defensa contra efectivos numéricamente superiores (hasta en proporción de 5 a 1), pero por corto tiempo.

564. Quien funja como comandante a la defensiva, debe contar con suficientes unidades de guerra electrónica que le permitan ejercer el control del espectro electromagnético en la mayor medida posible, evitando de esta forma que el enemigo pueda hacer uso eficaz del mismo, lo que resulta en una disminución efectiva de su potencia de combate, al privarlo o negarle el uso de sus sistemas de mando y control, detección y de armas.

565. Para el efecto, los planes de guerra electrónica deben considerar la adecuada distribución de los medios de guerra electrónica, buscando el apoyo a todas las unidades de maniobra. En los casos en que esto no sea posible, se deberán establecer las prioridades de apoyo durante la defensiva, que normalmente corresponderán a las unidades que participen en las fases críticas de la operación, como es el caso del contraataque.

Subsección (D)

Combatir con una Organización Táctica Flexible (Agrupamientos de Armas Combinadas)

566. Las y los comandantes de grandes unidades deben organizar sus fuerzas para el combate de acuerdo con: los diferentes tipos de unidades y recursos con que cuenten, la posibilidad más factible que se le finque a la fuerza oponente y las características del terreno que debe defenderse. La organización dependerá de la manera como se decida librar el combate, que desde luego, será consecuencia del estudio del terreno, así como de los elementos de combate y apoyo al combate con que cuente.

567. Dentro de las consideraciones anteriores, la o el comandante debe establecer en su esquema de maniobra la forma en que desea que la guerra electrónica contribuya a la acción de las unidades de maniobra, superponiendo sus esfuerzos con los de las armas para el logro de la misión.

568. Este principio se encuentra estrechamente relacionado con el establecido en la subsección anterior, puesto que de una distribución adecuada de las unidades de guerra electrónica se deriva una organización flexible de las mismas, condición indispensable para proporcionar un apoyo cercano y continuo a las unidades de maniobra.

569. Debido a las propiedades de las señales electromagnéticas, en ocasiones no será necesario cambiar la ubicación de los medios de guerra electrónica para brindar apoyo a otras unidades, lo que facilita organizar a las unidades para el combate en forma flexible y por fases, de conformidad con los cambios que se vayan presentando durante la operación.

Subsección (E)

Explotar las Ventajas del Defensor

570. El éxito de la defensa dependerá, básicamente, de los siguientes aspectos:

A. la forma en la que las unidades subordinadas exploten todas las ventajas, por lo que el sistema defensivo descansa en las o los comandantes subalternos, quienes vigilan y aseguran que cada ingenio de combate está emplazado de forma de aprovechar sus características al máximo, minimizando su vulnerabilidad.

B. Aprovechamiento del terreno, reforzándolo con minas y obstáculos para retardar a la fuerza adversaria.

C. Aumentar la eficacia de las armas defensivas; de tal manera que cada centro de resistencia, punto de apoyo o puesto de combate, reúna las condiciones necesarias para la defensa.

571. Será en estas condiciones en las que resulta más crítico que en otras situaciones, el establecimiento de efectivas medidas de protección electrónica destinadas a complementar todas las medidas de seguridad prescritas por el mando táctico. Dichas medidas deberán ser establecidas por la o el comandante mediante su inclusión en los planes respectivos, para ser observadas por toda la gran unidad en conjunto, por lo que a la unidad de guerra electrónica únicamente le corresponderá coadyuvar en su supervisión.

572. La unidad de guerra electrónica contempla dentro de sus propios planes, las medidas de protección electrónica particulares para sus propios medios, destinadas a evitar que sean fácilmente localizados, neutralizados o destruidos por el enemigo, a modo de evitar su eficiente empleo durante el combate.

573. El mando táctico también dictará aquellas medidas de contrainformación que estime convenientes para engañar o confundir a la unidad adversaria, por lo que normalmente se efectuarán operaciones de engaño electrónico que las complementen. Dichas operaciones deberán ser coordinadas y supervisadas por la unidad de guerra electrónica, por lo que también serán incluidas dentro de su plan de operaciones respectivo.

Tercera Sección

Apoyo de la Guerra Electrónica a las Operaciones Defensivas

Subsección (A)

Generalidades

574. La maniobra defensiva se aplica fundamentalmente de dos formas: defensa móvil y defensa en posición organizada. Estos tipos de defensa tienen poca probabilidad de ser precisamente adaptables a una situación específica de combate; por el contrario, es probable que sea necesaria la combinación de las dos acciones considerando:

A. Las intenciones de la o el comandante.

B. La misión.

C. La fuerza disponible.

D. Caracteristicas del terreno.

E. El poder de combate relativo.

F. La movilidad.

G. Situación aérea.

H. La situacion de guerra electrónica.

575. Independientemente de la forma en que se conciba la defensa, el terreno donde se materialice la maniobra defensiva, debe proporcionar la suficiente amplitud y profundidad que permita dividir el área general de defensa en: zona de seguridad, zona de resistencia y zona de reserva, en donde operarán los respectivos escalones de: seguridad, avanzado de defensa y reserva.

576. Las operaciones de guerra electrónica tendrán diferentes funciones, responsabilidades y prioridades, dependiendo de la zona táctica de que se trate, de acuerdo con lo que se expone en las subsecciones siguientes.

Subsección (B)

La Zona de Seguridad

577. El escalón de seguridad ocupa el área ubicada más allá de la línea anterior de los puestos avanzados (LAPA) y establece contacto con el enemigo con el propósito de efectuar reconocimientos agresivos y aprovechar toda oportunidad para efectuar acciones ofensivas limitadas, a fin de retardar y desgastar al enemigo, así como obtener información.

578. De todas las fuerzas de seguridad que integran el escalón de seguridad, destaca por su importancia la fuerza de cobertura, la cual debe contar con una gran movilidad y ser representativa de todas las fuerzas de que dispone la gran unidad, incluyendo apoyos al combate y de servicios.

579. La misión de la fuerza de cobertura es lograda por la acción retardatriz, que sostiene mediante una acción ofensiva agresiva, hábiles operaciones retrógradas y el uso ingenioso de obstáculos naturales y artificiales.

580. Las operaciones de guerra electrónica que se desarrollan en esta zona son principalmente las de apoyo electrónico. Para el efecto, es necesario asignar los efectivos necesarios para que la fuerza de cobertura esté en capacidad de desplegar una línea de base que recolecte información sobre el enemigo en todo su sector de responsabilidad.

581. También se deberá considerar la asignación de los perturbadores indispensables para que, solamente en caso necesario, coadyuven en las operaciones que realice la fuerza de cobertura, principalmente durante las ofensivas limitadas y el rompimiento del combate para el empleo de los perturbadores se debe valorar el hecho de que al ponerlos en funcionamiento, el enemigo quedara en la posibilidad de estudiar sus emisiones y determinar sus características, lo que anulará cualquier sorpresa que mediante su empleo se intente lograr.

582. También se deberá prever la realización de operaciones de engaño electrónico destinadas a apoyar las fintas y demostraciones que realice la fuerza de cobertura o cualquier otra fuerza presente en la zona de seguridad, con el fin de hacer más “creíbles” las acciones tácticas realizadas por las tropas.

Subsección (C)

La Zona de Resistencia

583. La zona de resistencia es aquella en que se han de librar los combates principales, que en su conjunto hacen la batalla; se extiende desde la L.A.P.A. hacia la retaguardia, abarcando inclusive el área ocupada por las reservas de las unidades subordinadas. En otras palabras, es aquí donde se desarrollará la acción principal por parte del escalón avanzado de defensa, integrado por el grueso de las unidades de combate y apoyo al combate. La o el comandante organizará la zona de resistencia estableciendo límites entre unidades y de retaguardia que delimiten los sectores defensivos de las unidades subordinadas

584. Será en esta zona donde se contempla el principal empleo de la guerra electrónica en apoyo de las fuerzas combatientes, debido a que la defensa normalmente será realizada a toda costa, buscando impedir que el adversario desorganice el área defensiva.

585. Para lograr lo anterior, resulta de vital importancia procurar la desorganización de los sistemas de mando y control del enemigo, así como degradar las capacidades de adquisición de blancos de sus sistemas de detección y de armas, de conformidad con la asignación de blancos que emita el C.C.F.A. entre otros, dichos blancos podrán ser los siguientes:

A. Redes de transmisiones de:

   a. Unidades blindadas y de tanques.

   b. Coordinación del apoyo aerotáctico.

   c. Artillería.

B. Radares de defensa aérea y contrabatería.

586. Por lo anterior, las operaciones de guerra electrónica a desarrollarse en esta zona son principalmente las de perturbación electrónica. Es conveniente que los perturbadores dispongan de emplazamientos que les proporcionen la mayor protección electrónica posible, ya que debido a la naturaleza de sus emisiones, son susceptibles de ser localizados y neutralizados con facilidad.

587. Las operaciones de apoyo electrónico también deberán manifestarse en esta zona, mediante el despliegue de líneas de base que permitan adquirir cualquier información relativa al enemigo, que sea de interés para la conducción de la maniobra, y que permita reaccionar con oportunidad y anticipación a los cambios que se presenten en la situación como resultado de la acción enemiga.

588. Entre los principales informes que son susceptibles de obtenerse se encuentran:

A. Dirección del principal esfuerzo de la unidad oponente.

B. Ubicación de debilidades en el ataque de la fuerza adversaria, que permitan la ejecución del contraataque.

C. Identificar la ubicación y avenidas de aproximación de las fuerzas de segundo escalón.

D. Detección de amenazas en los flancos y áreas de retaguardia.

Subsección (D)

La Zona de Reserva

589. Se ubica a inmediata retaguardia de la zona de resistencia, y es en donde se sitúan las reservas de la gran unidad, así como la respectiva área de servicios, aunque en ocasiones puede ocupar también parte de las áreas de retaguardia de las divisiones. De esta zona sale hacia la vanguardia todo el apoyo logístico necesario y en ella también se localizan los principales centros de transmisiones, que son el nervio operativo de la batalla.

590. El escalón de reserva se compone por fuerzas no empeñadas en combate, que se encuentran bajo el control directo de la o el comandante de la gran unidad, para influir en el combate en el momento y lugar en que se haga necesaria su acción, con el fin de evitar el colapso del sistema defensivo. Una manera común de materializar esta acción es por medio del contraataque.

591. Las operaciones de guerra electrónica que se llevan a cabo básicamente en esta zona, son las de perturbación electrónica, destinadas a romper la cohesión del esfuerzo enemigo, para facilitar la acción de las unidades de maniobra y que éstas cumplan con su misión, ya sea el restablecimiento del sistema defensivo o bien la desarticulación del ataque enemigo, entre otros.

592. Por lo tanto, es necesario mantener como parte del escalón de reserva, las unidades de guerra electrónica necesarias para actuar en beneficio de dicho escalón, sin distraer efectivos que apoyen a otras unidades, las que generalmente se encontrarán empeñadas con el componente adversario.

593. De forma complementaria, las unidades de apoyo electrónico, tratarán de obtener datos relativos a cualquier intento de la fuerza oponente de realizar acciones de penetración o explotación hacia nuestra retaguardia, que puedan poner en riesgo la integridad del área de defensa.

Capítulo IX

La Guerra Electrónica en las Operaciones Retrógradas

Primera Sección

Generalidades sobre las Operaciones Retrógradas

594. Una operación retrógrada es la que efectúa una unidad hacia su retaguardia o hacia cualquier otra dirección que lo aleje del enemigo, partiendo de un contacto.[34]

595. Estas operaciones pueden ser forzadas o impuestas por el enemigo, llevadas a cabo voluntariamente o bien ordenadas por el escalón superior, como parte del esquema general de maniobra. En todo caso, su ejecución debe ser aprobada por el escalón superior.

596. Es preferible, aunque no siempre posible, que las fuerzas empleadas en las operaciones retrógradas, posean igual o mayor movilidad que la de la fuerza adversaria, siendo indispensable esta condición en las fuerzas de seguridad.

597. Las operaciones retrógradas pueden ser de tres tipos, a saber:

A. Maniobra en retirada.

B. Acción retardatriz.

C. Retirada.

598. La ruptura del combate es una fase de las operaciones retrógradas en la que el grueso de una unidad se despega del contacto, protegido por la acción de un escalón de seguridad.

---

[34] Ibid.

599. Un repliegue es la acción táctica consistente en retroceder. El término se emplea en dos acepciones generales que son:

A. Repliegue manteniendo el combate, en que la fuerza considerada retrocede conservando el despliegue hasta una nueva posición situada a corta distancia; puede ser realizado como parte de una operación ofensiva o defensiva de cualquier tipo.

B. Repliegue rompiendo el combate, para la realización de una operación retrógrada, en que las unidades de la fuerza considerada se concentran sucesivamente en escalones mayores, efectuando marchas retrógradas hacia nuevas posiciones o áreas de reunión.

Segunda Sección

Apoyo de Guerra Electrónica en las Operaciones Retrógradas

600. El papel de la guerra electrónica en las operaciones retrógradas varía dependiendo fundamentalmente del tipo de operación a ejecutar, ya que cada una de ellas es concebida con diferentes propósitos y bajo diferentes circunstancias. Por tal motivo, es necesario establecer los principios generales de apoyo de guerra electrónica en forma separada para cada tipo de operación retrógrada.

601. Sin embargo, existen algunas acciones comunes a realizar en los tres tipos de operación retrógrada. En relación con la ruptura del combate, que generalmente es realizada en todas las operaciones retrógradas, las unidades de guerra electrónica que apoyen la ejecución de operaciones retrógradas tendrán a su cargo las misiones principales siguientes:

A. Obtener información sobre las actividades del enemigo en contacto, particularmente cualquier indicio que permita deducir que tienen conocimiento de que se intenta realizar la ruptura y pretenden obstaculizarla, como es el caso del movimiento de refuerzos.

B. Coordinar y evaluar la eficacia de las operaciones de engaño electrónico que se efectúen para ocultar al enemigo la intención de llevar a cabo la ruptura del combate, ya sea que dichas operaciones se ejecuten coordinamente con otras acciones tácticas de engaño o no.

C. En caso necesario, facilitar la ruptura del combate mediante la desorganización del sistema de mando y control de las unidades enemigas en contacto, evitando de este modo que coordinen sus acciones, así como que puedan reportar nuestra operación para obtener apoyo de fuegos o refuerzos.

D. Degradar el funcionamiento de los radares de vigilancia terrestre y aérea, para ocultar la ejecución de la ruptura del combate tanto como sea posible.

E. Perturbar las redes de control aerotáctico enemigas, para evitar que sus aeronaves proporcionen informes sobre la ruptura del combate en forma oportuna.

602. De igual forma, en estas operaciones tendrá una importancia fundamental la aplicación de las medidas de protección electrónica por parte de las tropas, con el fin de evitar proporcionar al enemigo cualquier indicio sobre la ejecución de la operación retrógrada.

Subsección (A)

Maniobra en Retirada

603. La maniobra en retirada es una operación retrógrada conducida por grandes unidades, previamente planeada y emprendida con la intención expresa de que el grueso de la unidad se aleje de la fuerza oponente, sin que éste ejerza presión directa sobre él, o bien, con el fin de eludir el combate en la situación existente, para realizar posteriores operaciones ofensivas o defensivas en condiciones más favorables.

604. De la anterior definición se puede establecer que uno de los principales requisitos para la ejecución de la maniobra en retirada es la ruptura del combate, condición que puede ser obtenida por una gran variedad de procedimientos y medios, debiendo considerarse dentro de ellos las operaciones de guerra electrónica según lo establecido previamente.

605. Durante el desarrollo de la maniobra en retirada, las formaciones de tropas serán vulnerables a la acción aérea enemiga, por lo que es necesario que las unidades de guerra electrónica colaboren al esfuerzo de la defensa aérea, perturbando los sistemas de armas, detección y navegación de las aeronaves enemigas. Esta acción coadyuvará a evitar la supresión de nuestro sistema de defensa aérea, así como a la preservación de la seguridad de las tropas.

Subsección (B)

Acción Retardatriz

606. La acción retardatriz es una operación retrógrada ejecutada generalmente por tropas móviles, en beneficio de otra unidad superior, en la que se cambia espacio por tiempo, causando el mayor daño posible al enemigo sin empeñarse decisivamente.

607. Normalmente esta operación es concebida como parte de otra operación mayor, como es el caso de una defensiva, en la cual la fuerza de cobertura retarda y desgasta a la fuerza oponente mediante la ejecución de acciones defensivas y ofensivas de alcance limitado.

608. El apoyo de guerra electrónica en la acción retardatriz , se manifiesta primordialmente mediante operaciones de apoyo electrónico, las cuales pueden mantener informado al mando de la fuerza de retardo sobre cualquier cambio en las intenciones del enemigo al que se aplica el retardo, que represente una amenaza a la seguridad e integridad de la fuerza de retardo. Tal es el caso de un envolvimiento en sus diferentes variantes.

609. También se debe contar con el apoyo de perturbadores para facilitar la ruptura del combate, cuyo empleo estará sujeto a las limitaciones impuestas por el mando, en relación con la posterior aplicación de la sorpresa que con su empleo se pretenda lograr. Es decir, si la o el comandante considera oportuno mantener en secreto la disponibilidad de perturbadores de determinado tipo o características entre sus fuerzas, podrá ordenar que no sean empleados hasta que se desarrolle la acción del combate principal.

610. Es necesario que el mando considere la ejecución de operaciones de engaño electrónico para facilitar la acción de la fuerza retrógrada, ya sea que complementen otras acciones tácticas de engaño o no, con la finalidad de confundir a la fuerza oponente sobre la ubicación de las posiciones de retardo, proporcionar informes falsos sobre refuerzos o simular la existencia de unidades falsas.

Subsección (C)

Retirada

611. La retirada es una operación retrógrada realizada con tiempo mínimo de planeamiento y bajo presión del enemigo, para evitar la derrota o el aniquilamiento de las fuerzas que la ejecutan. Cuando se realiza, implica para los mandos y las tropas condiciones críticas debido a la presión de la fuerza adversaria, a los pocos o malos preparativos hechos con anterioridad para enfrentarla y a la necesidad de poner a salvo los efectivos.

612. En estas circunstancias, se hará lo posible por manejar a las unidades conforme a las normas y procedimientos de actuación establecidos para la ruptura del combate, los repliegues y las acciones retardatrices con la finalidad de conducir la operación en las mejores condiciones y tratando de convertirla en una maniobra en retirada.

613. Existen diversas situaciones que pueden dar origen a una retirada; para ejemplificar su acción, se expone una retirada como consecuencia de la desorganización de la posición defendida por nuestras tropas.

614. Como resultado de la desorganización de la posición defensiva, se busca poner a salvo a la mayor cantidad de fuerza posible, por lo que se ejecuta la retirada. Sin embargo, nuestras fuerzas en retirada normalmente serán hostigadas por las fuerzas de persecución enemigas, las que procurarán, por todos los medios a su alcance, evitar la retirada mediante la destrucción de nuestras fuerzas.

615. Las medidas de protección electrónica revestirán una importancia crítica en esta operación, ya que debido a los escasos preparativos, la conservación de nuestro sistema de mando y control es indispensable para asegurar la conducción de la operación. Al igual que en cualquier otra circunstancia, dichas medidas deberán ser impuestas por el mando táctico para su acatamiento por parte de todas las tropas.

616. Por su parte, las unidades de guerra electrónica deben ser empleadas proporcionando apoyo a la fuerza de seguridad, obteniendo información de los movimientos de la fuerza adversaria perturbando los sistemas de mando y control y de armas de la fuerza de persecución, de apoyo de fuegos y de control aerotáctico.

617. En el caso de que el mando determine ejecutar operaciones de engaño electrónico durante el transcurso de la retirada, la unidad de guerra electrónica también se encargará de coordinarlas.