Formación de su unidad sobre el espectro: un plan de 30 días para comandantes de compañía o batería

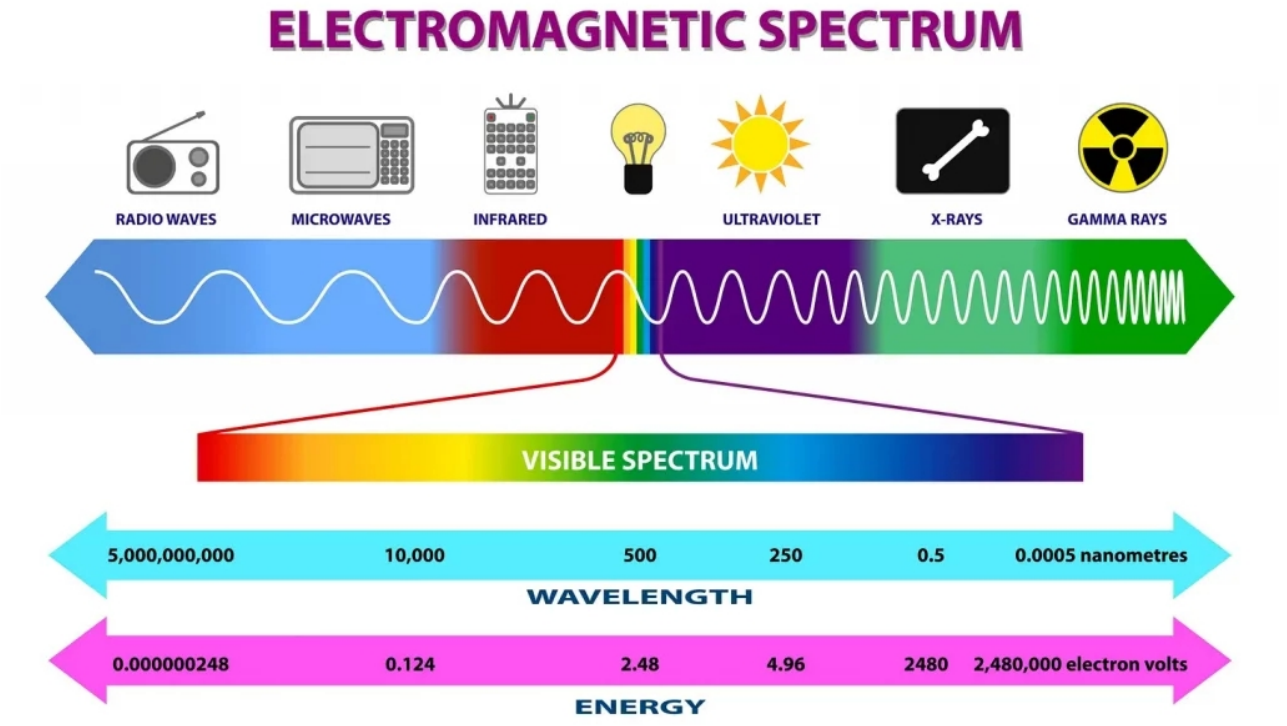
Traducido por Aitor Saiz Lasheras, con el siempre amable permiso del *Major* Geoff Ball

Una guía práctica y sin florituras para desarrollar competencias en el espectro electromagnético con el equipo del que ya dispone.

EMS 2025

24 de febrero de 2026

Nota de los editores: The CxFile se ha asociado con EMS 2025 para proporcionar a nuestros lectores una comprensión práctica del espectro electromagnético (EMS). En el campo de batalla moderno, la infantería debe comprender la gestión del espectro con la misma fluidez con la que comprendemos las zonas de peligro en superficie. Para ayudar a salvar esta brecha, EMS 2025 traduce conceptos técnicos complejos a términos accesibles para quienes se inician en este ámbito. Le recomendamos encarecidamente que se suscriba a su Substack y aproveche su excelente recopilación de artículos existentes. ¿Tiene preguntas específicas que le gustaría que EMS 2025 respondiera? ¡Escríbanos y se las haremos llegar! Por último, este artículo ha sido escrito por un oficial del Ejército, para un público del Ejército; no todo se trasladará perfectamente a la TO/E del Cuerpo de Marines.



Eres comandante de compañía/batería. Tu S-6 acaba de informarte de que la próxima rotación en el NTC/JRTC/JRMC incluirá una fuerte oposición de guerra electromagnética. Tu comandante de batallón quiere que todos los líderes de compañía/batería comprendan las «operaciones del espectro». Y tienes 30 días antes de tu próximo ejercicio de campo para conseguirlo.

El problema es este: no hay ningún ATP para esto. Tu pelotón de guerra electrónica (si es que tienes uno) carece de personal suficiente. Tus suboficiales de transmisiones entienden de redes, pero no necesariamente de guerra de radiofrecuencia. Y tus soldados piensan que el «espectro» es algo de la televisión por cable o algo que está muy por encima de su nivel.

Esta guía está diseñada para solucionar eso. En 30 días, utilizando únicamente el equipo de tu TOE y una gestión creativa del entrenamiento, puedes crear una compañía/batería que comprenda el entorno electromagnético, reconozca las amenazas y emplee tácticas básicas de espectro.

Lo que este plan NO es:

Un sustituto del entrenamiento formal en guerra electrónica.
Cursos técnicos de ingeniería de RF.
TTP clasificadas (todo aquí es de carácter no clasificado y divulgable).
Dependiente de equipo especializado de guerra electrónica que no tienes.

Lo que SÍ es este plan:

Una progresión de entrenamiento gradual: gatear, caminar, correr.
Basado en el equipo que ya tienes (ASIP, SINCGARS, teléfonos móviles, etc.).
Diseñado para encajar en el tiempo normal de entrenamiento de la compañía/batería.
Centrado en aplicaciones tácticas prácticas.
Exportable a los jefes de pelotón para su propio entrenamiento.

La filosofía de entrenamiento: «Obsérvalo, modifícalo, combátelo»

Este plan de 30 días se basa en tres fases:

1. Semanas 1-2: OBSÉVALO - Desarrolla la conciencia del entorno electromagnético.
2. Semana 3: MODIFÍCALO - Aprende a controlar y manipular el uso del espectro por parte de las fuerzas amigas.
3. Semana 4: COMBÁTELO - Aplica tácticas ofensivas y defensivas en el espectro.

Cada fase se basa en la anterior. No te saltes ninguna.

Preparación previa al entrenamiento (antes del día 1)

Lo que necesitas:

Radios: ASIP, SINCGARS o cualquier radio táctica que figure en tu TOE.
Teléfonos inteligentes: Los teléfonos personales de los soldados (de todos modos, los tienen encendidos todo el tiempo).
Herramientas/aplicaciones (gratuitas/de bajo coste):
    Aplicación de análisis de Wi-Fi (Android: «WiFi Analyzer» de farproc o Apple: «Fing-Network Scanner»).
    Aplicación de detección de señales de RF (Android: «Cell Tower Locator» o Apple: RF Signal Detector).
    Analizador de espectro si su S-6 dispone de uno (recomendable, pero no obligatorio).

Área de entrenamiento: Cualquier lugar donde se pueda llevar a cabo entrenamiento de radio (parque móvil, campo de tiro, área de entrenamiento)
Tiempo necesario: 2-3 horas a la semana, además de la integración en las actividades de entrenamiento habituales

Requisitos de coordinación:

S-6/SIGO: Informarles de su plan, solicitar cualquier herramienta de espectro disponible.
S-3: Integrar el entrenamiento sobre el espectro en el calendario de entrenamiento.
Batallón: Asegurarse de no infringir ninguna política local de gestión del espectro.
Seguridad: Recordar a los soldados las normas de seguridad de RF (no transmitir cerca de la cara, respetar las distancias de seguridad establecidas).

Preparación del líder:

Antes de comenzar a entrenar a los soldados, usted y sus jefes de pelotón necesitan una base de referencia. Dediquen juntos 2-3 horas a cubrir:

Conceptos básicos de RF (frecuencia, longitud de onda, potencia, modulación).
Cómo funcionan realmente sus radios tácticas.
Capacidades actuales de guerra electrónica (R-330Zh ruso, CS/NRJ5 chino, etc.).
Procedimientos de gestión del espectro de las fuerzas amigas (Instrucciones de Operación de Comunicaciones y Electrónica (CEOI), Instrucciones de Operación de Señales (SOI), etc.).

Lectura previa recomendada: ATP 3-12.3 *Técnicas de Guerra Electromagnética, Apéndice A (Muy recomendable; si dedica algo de tiempo a leerlo y comprenderlo, le proporcionará los conocimientos básicos que necesita)*.

FASE 1: VERLO (Días 1-14)

Objetivo: Desarrollar la conciencia electromagnética

Tus soldados se mueven cada día en un océano de energía de radiofrecuencia sin siquiera saberlo. Esta fase hace visible lo invisible.

Semana 1: Comprender nuestras propias emisiones

Día 1 - «¿Qué es el espectro?» (Aula, 90 min).

Objetivos de la formación:

Definir el espectro electromagnético.
Identificar los usos militares del espectro (comunicaciones, radar, guerra electrónica, GPS).
Comprender la diferencia entre frecuencia y longitud de onda.

Ejecución:

1. Introducción (15 min): Empezar con algo tangible
   «Cada vez que pulsas el botón de la radio, estás transmitiendo energía a través del aire. Esa energía puede ser detectada, interferida o explotada».
   Mostrar un gráfico visual del espectro (desde UV hasta radio).

Explicar por qué nos importa: *los adversarios pueden matarte a través de tus emisiones*.

2. Demostración interactiva (30 min):
   Hacer que los soldados descarguen una aplicación de análisis de Wi-Fi en sus teléfonos.
   Recorrer el área de la compañía/batería buscando redes Wi-Fi.
   Mostrar cómo cambia la intensidad de la señal con la distancia y los obstáculos.
   Debatir: «¿Qué nos dice esto sobre la detectabilidad?»
3. Conceptos básicos de radio (30 min):
   Explica las bandas de frecuencia utilizadas por el ejército (VHF, UHF, SHF).
   Muestra cómo los ASIP/SINCGARS saltan de una frecuencia a otra.
   Demuestra el silenciador y los medidores de intensidad de señal en las radios.
4. Debate sobre amenazas (15 min):
   Resumir las capacidades básicas de localización de amenazas (DF).
   Mostrar un ejemplo de Ucrania: la artillería rusa apuntando a las emisiones de radio ucranianas.
   Hacerlo personal: «Tu radio puede costarte la vida si no la usas correctamente».

Evaluación: Prueba rápida: ¿Puede cada soldado identificar tres usos militares del espectro?

Notas del comandante:

Mantén la sencillez. No te pierdas todavía en detalles técnicos.
Utiliza analogías: «La frecuencia es como el carril por el que conduces en una autopista».
Haz que sea relevante para su trabajo.

Día 3 - «Nuestra huella» (Ejercicio práctico, 2 horas)

Objetivos de la formación:

Identificar las emisiones electromagnéticas del equipo de la compañía/batería.
Comprender la disciplina de transmisión.
Reconocer los patrones de emisión.

Ejecución:

1. Preparación (15 min):
   Establecer tres estaciones separadas 200 m entre sí.
   Estación 1: Radio SINCGARS transmitiendo.
   Estación 2: Llamada con teléfono móvil.
   Estación 3: Ordenador portátil en funcionamiento.
2. Ruta de detección (45 min):
   Rotar las escuadras por las estaciones con aplicaciones de detección de RF (Android es mejor que iOS).
   Registrar la intensidad de la señal a 10 m, 50 m, 100 m y 200 m.
   Anotar los alcances de detección de cada dispositivo.
   Debate: ¿Qué te ha sorprendido? ¿Qué se detectaba a mayor distancia de lo esperado?

3. Demostración de control de emisiones (EMCON) (45 min):
    Escenario: «El equipo de localización del enemigo está en la zona».
    Practicar el paso de comunicaciones completas a una firma reducida y ver lo difícil que es detectar:
        Nivel 1: Operaciones normales.
        Nivel 2: Silencio de escucha (solo recepción).
        Nivel 3: Apagado completo.
    Mide cuánto tiempo se tarda en pasar de un nivel a otro.
    Desarrolla la memoria muscular.
4. AAR (15 min):
    ¿Qué hemos aprendido sobre nuestra propia detectabilidad?
    ¿Cómo reducirías la firma en un escenario táctico?
    ¿Cuándo podríamos necesitar EMCON en combate?

Evaluación: ¿Puede cada jefe de escuadrón ordenar y hacer cumplir los niveles de EMCON?

Día 5 - «Interpretación del entorno» (Ejercicio de campo, 3 horas)

Objetivos de formación:

Utilizar el equipo orgánico para cartografiar el entorno electromagnético local.
Identificar transmisores amigos y desconocidos.
Desarrollar la conciencia situacional.

Ejecución:

1. Resumen de la misión (15 min):
    «Tu pelotón está llevando a cabo un reconocimiento. Cartografía todas las emisiones de RF detectables en esta zona de entrenamiento».
    Asignar sectores a cada escuadrón.
    Proporcionar un formato de informe sencillo: Ubicación, banda de frecuencia, intensidad de la señal, duración.
2. Exploración de campo (2 horas):
    Los escuadrones se desplazan por los sectores con:
        ASIP configurado en modo de exploración (permite que un único ASIP, transportado por el operador, monitorice múltiples canales, redes o frecuencias simultáneamente. Recorre automáticamente los canales preprogramados, lo que permite a los usuarios escuchar el tráfico crítico en diferentes redes).
        Teléfonos personales con aplicaciones de escáner de Wi-Fi/celular.
        Portátiles para registrar los hallazgos.
    Informar de los hallazgos al TOC de la compañía/batería cada 30 minutos.
3. Análisis y debriefing (45 min):
    Consolidar los informes en un mapa.
    Identificar patrones: ¿Dónde están las torres de telefonía móvil? ¿Qué frecuencias están más saturadas?
    Discutir las implicaciones tácticas:

¿Dónde podríamos instalarnos sin interferencias?
¿Dónde colocaría el enemigo probablemente los inhibidores?
¿Qué terreno natural enmascara las RF?

Evaluación: ¿Puede cada escuadrón elaborar un mapa básico de RF de su sector?

Notas del comandante:

Se trata de reconocimiento, pero del espectro en lugar de las posiciones enemigas.
Haga hincapié en el valor de inteligencia que supone conocer el entorno de RF.

Semana 2: Comprensión de las amenazas y las interferencias

Día 8 - «Fundamentos del bloqueo» (Aula + demostración, 2 horas)

Objetivos de la formación:

Definir el bloqueo y sus tipos.
Reconocer el bloqueo cuando se produce.
Comprender las contramedidas propias.

Ejecución:

1. Aula (45 min):
   - Definir el bloqueo: transmisión deliberada de RF para interrumpir las comunicaciones.
   - Tipos de bloqueo:
     - Barrage: Ruido de fondo en toda la banda.
     - Spot: Frecuencia específica.
     - Sweep: Recorrido por las frecuencias.
   - Sistemas de amenaza: R-330Zh ruso, DZ-08 chino.
2. Demostración en vivo (1 hora):
   - Configuración: Dos radios SINCGARS en comunicación.
   - Introducir «interferencia» simulada:
     - Hacer que una tercera radio transmita. continuamente en la misma frecuencia.
     - Utilizar un walkie-talkie de alta potencia cerca de los SINCGARS.
     - Crear interferencia con la electrónica de los vehículos cercanos.
   - Hacer que los soldados intenten mantener las comunicaciones en cada condición.
   - Experimentar con contramedidas:
     - Cambiar de frecuencia.
     - Aumentar la potencia.
     - Desplazarse a un terreno más favorable.
     - Utilizar antenas direccionales.
3. Debate (15 min):
   - ¿Qué funcionó? ¿Qué no funcionó?
   - ¿Cómo sabrías si el bloqueo fue intencionado o si se trató de una interferencia accidental?
   - ¿Cuál es tu procedimiento operativo estándar (SOP) si las radios dejan de funcionar?

Evaluación: ¿Pueden los soldados identificar 3 tipos de bloqueo y 3 contramedidas?

Empieza alrededor de las 8:45, te ayudará a visualizar cómo funciona el bloqueo:

https://youtu.be/bm01h6NC_Ho

Día 10 - «Localización de la dirección y suplantación» (Aula, 90 min)

Objetivos de la formación:

Comprender cómo los adversarios localizan nuestras transmisiones.
Reconocer la suplantación de GPS.
Aprender técnicas básicas de contramedidas de DF.

Ejecución:

1. Resumen de la localización de la dirección (DF) (30 min):
   Explicar la triangulación: múltiples sensores fijan su ubicación mediante la señal.
   Mostrar sistemas DF de amenaza (ejemplos de Siria, Ucrania).
   Analizar los plazos de detección: ¿Cuánto tiempo tarda el enemigo en localizarle?
   Regla general: 3 transmisiones = ubicación fijada.
2. Tácticas de contramedidas DF (30 min):
   Tiempo: Mantener las transmisiones por debajo de los 30 segundos.
   Terreno: Utilizar la pendiente inversa y los edificios para camuflarse.
   Distancia: Colocación de antenas remotas.
   Engaño: Transmisiones falsas, señuelos.
   Movimiento: Disparar y retirarse rápidamente de los puntos de retransmisión.
3. Amenaza de suplantación de GPS (30 min):
   Explicar cómo se puede interferir o suplantar el GPS.
   Mostrar ejemplos: suplantación de GPS rusa en Ucrania, Mar Negro.
   Reconocimiento: saltos repentinos de posición, errores de tiempo, fijaciones de satélite inconsistentes.
   Contramedidas: navegación por estima, asociación con el terreno, navegación de respaldo.

Evaluación: ¿Puede cada líder impartir una clase rápida de 2 minutos sobre contramedidas de detección de frecuencias?

Día 12 - «Planificación PACE para las comunicaciones» (Ejercicio práctico, 2 horas)

Objetivos de formación:

Elaborar planes PACE (Primario, Alternativo, de Contingencia, de Emergencia) para comunicaciones degradadas.
Practicar la transición entre métodos de comunicación.
Desarrollar procedimientos operativos estándar (SOP) a nivel de pelotón.

Ejecución:

1. Planificación (30 min):
   Cada pelotón elabora un plan PACE:

Primario: ASIP/SINCGARS.
Alternativo: Frecuencia/red diferente.
Contingencia: Señales visuales, mensajeros.
Emergencia: Pirotécnicos, acciones predeterminadas.

Anotarlo, dar una sesión informativa.

2. Prueba de campo (1 hora):

   Llevar a cabo un movimiento hacia el contacto con degradación progresiva de las comunicaciones:

   Fase 1: Todas las radios funcionan (Primario).
   Fase 2: Red de la compañía/batería saturada, utilizar la red interna del pelotón (Alternativo).
   Fase 3: Todas las radios fuera de servicio (Contingencia/Emergencia).

   Obligar a los pelotones a actuar utilizando cada método

3. AAR (30 min):

   ¿Qué funcionó bien? ¿Qué falló?
   ¿Cuánto tiempo duraron las transiciones?
   ¿Qué debe incluirse en el procedimiento operativo estándar (SOP) del pelotón?

Evaluación: ¿Tiene cada pelotón un plan PACE escrito y ensayado? El hecho de que tu batallón o brigada tenga un plan PACE no significa que ese sea tu plan PACE; utiliza lo que funcione a tu nivel.

Día 14 - Evaluación de la Fase 1 (Ejercicio calificado, 3 horas)

Escenario: Patrulla de reconocimiento a nivel de pelotón en un entorno con interferencias electromagnéticas.

Tareas:

1. Cartografiar el entorno electromagnético en el sector asignado (30 min).
2. Mantener las comunicaciones bajo interferencias simuladas (20 min).
3. Transicionar según el plan PACE cuando fallen los sistemas primarios/alternativos (20 min).
4. Recomendar el nivel de EMCON en función de la situación táctica (10 min).
5. Identificar las posiciones óptimas para los emplazamientos de retransmisión (10 min).

Estándares:

El 80 % de los soldados puede describir las amenazas del espectro.
El 100 % de los líderes puede hacer cumplir el EMCON.
El 100 % de los pelotones cuenta con planes PACE viables.
Cada escuadrón elabora un mapa básico de RF.

Enfoque del AAR del comandante:

¿Consideran los soldados el espectro como parte de la planificación táctica?
¿Entienden que la amenaza es real, no teórica?
¿Qué lagunas existen para la Fase 2?

FASE 2: CONFIGURARLO (Días 15-21)

Objetivo: Controlar el entorno electromagnético

Ahora que los soldados comprenden el espectro, enséñeles a gestionarlo activamente.

Semana 3: Gestión del espectro y engaño

Día 15 - «Gestión de frecuencias 101» (Aula, 90 min)

Objetivos de formación:

Comprender la elaboración de las Instrucciones de Operación de Comunicaciones y Electrónica (CEOI) y las Instrucciones de Operación de Señales (SOI).
Aprender a resolver conflictos entre frecuencias amigas.
Practicar la elaboración de un plan de frecuencias para una compañía o batería.

Ejecución:

1. Conceptos básicos de CEOI/SOI (30 min):
    Explicar el propósito: resolver conflictos de frecuencias, mantener la seguridad de las comunicaciones (COMSEC).
    Repasar un ejemplo de CEOI:
        Redes de mando.
        Redes de administración/logística.
        Frecuencias de MEDEVAC/CASEVAC.
        Redes de apoyo de fuego.
    Debatir por qué no podemos simplemente «elegir cualquier frecuencia».
2. Problema de interferencias (30 min):
    Caso práctico: Su red de fuego interfiere con el CAB o con la organización de aviación local.
    Repasar el proceso de resolución de conflictos.
    Practicar el uso de las reglas de separación de frecuencias (mantener una separación de 25 KHz para VHF).
    Mostrar cómo el terreno afecta a la reutilización de frecuencias.
3. Elaboración de un CEOI de compañía/batería (30 min):
    Dividirse en pelotones.
    Cada pelotón diseña un plan de frecuencias para una operación a nivel de compañía/batería.
    Debe evitar conflictos con las unidades adyacentes (proporcionar sus frecuencias).
    Explicar las soluciones, identificar los conflictos.

Evaluación: ¿Puede cada jefe de pelotón elaborar un plan básico de frecuencias?

Día 17 - «Retransmisiones y ampliación del alcance» (Ejercicio de campo, 3 horas)

Objetivos formativos:

Utilizar estaciones de retransmisión para ampliar el alcance.
Comprender los efectos del terreno en la propagación de radiofrecuencia.

Practicar el emplazamiento y la seguridad de los sitios de retransmisión.

Ejecución:

1. Preparación en el aula (30 min):
   Cómo funciona la retransmisión: la estación de retransmisión amplifica y retransmite (puede pedir ayuda a su S6/SIGO).
   Consideraciones de emplazamiento:
      Terreno elevado con línea de visión (LOS) despejada.
      Cobertura de 360° frente a direccional.
      ¿Defendido o indefendido?
   Amenaza: los emplazamientos de retransmisión son objetivos lucrativos.
2. Empleo sobre el terreno (2 horas):
   Misión: Establecer comunicaciones de compañía/batería a lo largo de 5 km de terreno accidentado.
   Cada pelotón establece un emplazamiento de retransmisión.
   Probar el alcance, ajustar posiciones.
   Practicar el desplazamiento rápido cuando se está «bajo fuego»
3. AAR (30 min):
   ¿Qué ubicaciones funcionaron mejor?
   ¿A qué velocidad se puede emplazar/desplazar?
   ¿Cuáles son los requisitos de seguridad?

Evaluación: ¿Pueden los pelotones mantener las comunicaciones a través de terreno denegado utilizando retransmisores? ¿Es necesario depender de los cuarteles generales de alta mando (HHQ) para la retransmisión?

Día 19 - «Engaño electromagnético» (Ejercicio práctico, 2 horas)

Objetivos de entrenamiento:

Emplear emisiones engañosas para confundir al enemigo.
Comprender cuándo y cómo utilizar señuelos.
Practicar la planificación del engaño.

Ejecución:

**NOTA: He probado esto varias veces con diferentes organizaciones y es muy difícil de llevar a cabo sin equipo de DF real. Si quieres adentrarte en el laberinto de construir tu propio equipo de DF, este es el tipo al que debes seguir:

https://youtu.be/zsQB3cnNZ48

1. Introducción (15 min):
   Explicar el engaño electromagnético: manipular el DF/SIGINT enemigo.
   Ejemplos históricos: engaño radiofónico de la Segunda Guerra Mundial antes del Día D.
   Aplicación moderna: hacer creer al enemigo que estás en un lugar en el que no estás.
2. Técnicas de señuelos (45 min):

Transmisiones falsas: mensajes pregrabados, tráfico ficticio.
Emisores señuelo: radios no tripuladas que transmiten desde posiciones falsas.
Alteración de patrones: cambiar los patrones de emisión normales para confundir el análisis enemigo.
Practicar cada técnica sobre el terreno.

3. Ejercicio de escenario (1 hora):
   El equipo rojo, con equipo de DF, intenta localizar al pelotón azul.
   El equipo azul utiliza señuelos y transmisiones falsas.
   Rotar los roles.
   Evaluar la eficacia.

Evaluación: ¿Pueden los pelotones emplear al menos 2 técnicas de engaño de forma eficaz?

Día 21 - Evaluación de la Fase 2 (Ejercicio calificado, 3 horas)

Escenario: Ataque de la compañía que requiere gestión del espectro

Tareas:

1. Elaborar y presentar el CEOI para la operación (30 min).
2. Establecer una red de retransmisión para mantener el C2 (45 min).
3. Emplear EMCON al entrar en la zona de combate enemiga (15 min).
4. Utilizar el engaño para ocultar la posición de asalto real (30 min).
5. Cambiar a PACE cuando el sitio de retransmisión sea «destruido» (20 min).

Estándares:

El CEOI no presenta ningún conflicto de frecuencias.
La red de retransmisión proporciona una cobertura del 100 %
EMCON aplicado en menos de 2 minutos.
El engaño hace que el DF del equipo Rojo apunte a una ubicación errónea.

FASE 3: COMBATE (Días 22-30)

Objetivo: Aplicar habilidades de espectro en escenarios tácticos realistas

La fase final integra todo sin requerir equipo de guerra electrónica especializado del que no dispones.

Semana 4: Integración táctica

Día 22 - «Guerra electrónica del enemigo: cómo se ve cuando te atacan» (Aula + Ejercicio, 3 horas)

Objetivos de la formación:

Reconocer los indicadores de actividad de guerra electrónica enemiga.
Comprender las capacidades de la amenaza (lo que los enemigos PUEDEN hacer).
Practicar simulacros de respuesta sin necesidad de inhibidores reales.

Ejecución:

1. Resumen de la amenaza (45 min):

Sistemas de guerra electrónica rusos (R-330Zh, Pole-21, Zhitel): qué pueden inhibir y a qué distancias.
Capacidades chinas (DZ-08, 910A): suplantación de GPS, interferencia de banda ancha.
Lecciones de Ucrania: qué funcionó y qué no funcionó contra la guerra electrónica rusa.
Punto clave: No tendrás aviso previo. Simplemente perderás las comunicaciones.

2. Entrenamiento de reconocimiento (45 min):
    Indicadores de interferencia:
        Ruptura repentina del silenciador con ruido.
        Se puede recibir pero no transmitir.
        Conectividad intermitente que aparece y desaparece.
    Indicadores de DF:
        El enemigo conoce tu posición sin contacto visual.
        Disparos contra emplazamientos de retransmisión o puestos de mando.
        Patrón: el enemigo reacciona a tus transmisiones.
    Indicadores de suplantación de GPS:
        La posición cambia repentinamente.
        Varios sistemas muestran ubicaciones diferentes.
        Errores de fecha y hora en los equipos.
3. Simulacros de respuesta (90 min):
    Basados en escenarios: «Tus radios dejan de funcionar de repente. ¿Qué haces?»
    Practica ejercicios de acción inmediata:
        Anuncia «Pérdida de comunicaciones» a las unidades adyacentes (mientras puedas).
        Ejecuta el plan PACE inmediatamente.
        Informa por medios alternativos cuando se restablezca.
        Continúa la misión.
    Rota por múltiples escenarios con diferentes fallos.
    Cronometra cada respuesta, crea memoria muscular.

Evaluación: ¿Puede cada escuadrón reconocer la guerra electrónica y ejecutar la respuesta en menos de 3 minutos?

Notas del comandante:

No se necesitan inhibidores para entrenar esto, basta con simular los efectos.
Haga que la OPFOR grite «ENDEX» en las redes de radio para simular la interferencia.
Céntrese en el reconocimiento y la respuesta, no en el «cómo funciona» técnico.

Día 24 - «Operar con comunicaciones degradadas» (Ejercicio de campo, 4 horas)

Objetivos de entrenamiento:

Mantener la eficacia de la misión con comunicaciones limitadas o inexistentes.
Utilizar el terreno y las acciones planificadas previamente para reducir la dependencia de las comunicaciones.

Fomentar la confianza para operar en un entorno sin comunicaciones.

Ejecución:

1. Planificación (1 hora):
   Misión: Movimiento a nivel de pelotón para establecer contacto.
   Restricción: Suponer que las comunicaciones fallarán en algún momento.
   Enfoque de la planificación:
   ¿Qué decisiones se pueden delegar previamente?
   ¿Qué acciones al establecer contacto son el procedimiento estándar (SOP)?
   ¿Dónde están los puntos de decisión que REQUIEREN comunicaciones?
   ¿Qué señales visuales podemos utilizar?
2. Ensayo (1 hora):
   Repasar toda la misión.
   Identificar cada momento en el que normalmente se utilizaría la radio.
   Desarrollar soluciones alternativas para cada uno: señales manuales, mensajeros, puntos de reunión, etc.
   Practicar hasta que todo fluya con naturalidad.
3. Ejecución (1,5 horas):
   Llevar a cabo el movimiento real.
   Los oficiales al mando (OC) cortan las comunicaciones progresivamente:
   Fase 1: Solo red de la compañía (los pelotones siguen comunicándose internamente).
   Fase 2: Todas las redes de radio caídas.
   Fase 3: Las radios vuelven a funcionar.
   Los pelotones deben continuar la misión en todo momento.
4. AAR (30 min):
   ¿Qué falló cuando se cortaron las comunicaciones?
   ¿Qué funcionó mejor de lo esperado?
   ¿Qué debería incluirse en nuestro procedimiento operativo estándar (SOP) para operaciones sin comunicaciones?

Evaluación: ¿Lograron los pelotones la misión a pesar de la pérdida de comunicaciones?

Lecciones que aprender:

Las acciones planificadas de antemano reducen la dependencia de las comunicaciones.
Las señales visuales funcionan, pero requieren una línea de visión (LOS) clara.
Los mensajeros son lentos, pero fiables.
Algunas tareas requieren realmente comunicaciones; identifícalas.

Día 26 - «Consideraciones sobre el espectro en el ataque» (Ejercicio táctico, 4 horas)

Objetivos de entrenamiento:

Integrar la planificación del espectro en las operaciones ofensivas.
Equilibrar el sigilo (EMCON) con los requisitos de C2.
Comprender cuándo aceptar el riesgo de detección frente a mantener las comunicaciones.

Ejecución:

1. Briefing de la misión (30 min):
   Ataque deliberado de la compañía contra una posición enemiga preparada.
   Inteligencia: El enemigo tiene capacidad de localización de fuentes (DF), puede atacar emisores con artillería.
   Limitaciones: Se necesitan comunicaciones para el fuego de apoyo y la evacuación médica (CASEVAC), pero las emisiones = localización.
2. Planificación (1,5 horas):
   Cada jefe de pelotón planifica su parte.
   Debe abordar:
      Nivel de EMCON durante el movimiento hacia la posición de liderazgo.
      Cómo solicitar fuego de apoyo sin comprometer la posición.
      Ubicación de los repetidores (si los hay)… ¿merece la pena el riesgo?
      ¿Qué pasa si el repetidor es alcanzado?
      Plan de comunicaciones para CASEVAC.
   Explicar el plan al comandante
3. Ejecución (1,5 horas):
   Llevar a cabo el movimiento y el asalto.
   Los oficiales al mando evalúan:
      ¿Mantuvieron las unidades el EMCON cuando era apropiado?
      ¿Rompieron el EMCON cuando fue necesario (fuego de apoyo, evacuación médica)?
      ¿Se ubicaron los repetidores de forma táctica?
      ¿Cómo se adaptaron cuando las cosas cambiaron?
4. AAR (30 min):
   Riesgo frente a recompensa: ¿Cuándo valió la pena el EMCON? ¿Cuándo no?
   ¿Alguien «murió» por una mala disciplina del espectro?
   ¿Qué harías de forma diferente?

Evaluación: ¿Tomaron los líderes decisiones inteligentes sobre el riesgo en relación con las emisiones?

Punto clave de la enseñanza: No hay una respuesta perfecta. A veces se necesita más la comunicación que el sigilo. A veces, el sigilo es más importante. Los líderes deben evaluar y decidir; hay riesgo en cualquier caso.

Día 28 - «Notificación de la actividad de guerra electrónica del enemigo» (Ejercicio práctico, 3 horas)

Objetivos de formación:

Saber qué información notificar sobre la guerra electrónica del enemigo.
Practicar el uso de formatos de notificación estándar.
Comprender por qué es importante la notificación oportuna.

Ejecución:

1. Aula (30 min):
    Por qué es importante informar: Tu contacto ayuda a toda la brigada.
    Qué informar:
        QUÉ: Tipo de efecto (interferencia, DF, suplantación).
        CUÁNDO: Hora del incidente (DTG).
        DÓNDE: Tu ubicación cuando ocurrió.
        DURACIÓN: Cuánto tiempo duró.
        IMPACTO: ¿A qué afectó? (Pérdida de comunicaciones durante X minutos, etc.).
    Formato: Utiliza el formato estándar SALUTE o el de informe puntual.
    Cadena de mando: Informa a S-6 y S-2 (inteligencia).
2. Entrenamiento de escenarios (1,5 horas):
    Las secciones llevan a cabo operaciones.
    Los oficiales al mando introducen eventos de guerra electrónica: «Vuestras radios acaban de dejar de funcionar» o «El GPS indica que estáis a 2 km de vuestra posición real».
    Las secciones deben:
        Reconocer el evento.
        Responder adecuadamente (PACE, etc.).
        Documentar e informar adecuadamente.
    Rotar por múltiples escenarios.
3. Análisis (1 hora):
    Consolidar todos los informes a nivel de compañía.
    Mostrar cómo el análisis de patrones revela:
        Ubicaciones de guerra electrónica del enemigo (¿dónde se concentran los eventos?).
        Capacidades del enemigo (¿qué pueden hacer?).
        Tácticas, técnicas y procedimientos (TTP) del enemigo (¿cuándo y cómo emplean la guerra electrónica?).
    Esto es inteligencia; tus informes contribuyen a la visión global.

Evaluación: ¿Son los informes precisos, oportunos y útiles?

Énfasis del comandante:

Informar no es una tarea administrativa, es recopilación de inteligencia.
Tu informe podría salvar a otra unidad del mismo problema.
5 minutos de un buen informe > 5 horas de especulación.

Día 30 - Evaluación final y validación (Fuerza contra Fuerza, día completo)

Escenario: Operación defensiva de la compañía con guerra electrónica (GE) enemiga simulada.

Configuración:

Utilizar una fuerza enemiga simulada (OPFOR) de otra compañía o unidad externa.
Los oficiales de mando (OC) simulan los efectos de la GE enemiga indicándolos verbalmente (no se necesitan inhibidores reales).

Centrarse en la RESPUESTA de la Fuerza Azul, no en la capacidad técnica de la Fuerza Roja.

Tareas de la Fuerza Azul (tu compañía):

Defender el sector y mantener el C2.
Reconocer cuándo la guerra electrónica del enemigo está afectando a las operaciones.
Ejecutar simulacros de acción inmediata.
Informar adecuadamente de los incidentes de guerra electrónica.
Continuar la misión a pesar de la degradación de las comunicaciones.

Tareas de la Fuerza Roja (simuladas por los OC):

En los momentos indicados, los OC anuncian los efectos:
- «La red de tu compañía está bloqueada» (las radios se silencian durante 10 min).
- «El enemigo ha localizado su retransmisor» (el retransmisor recibe fuego indirecto).
- «El GPS está falsificado, sus pantallas muestran que se encuentran a 3 km al noreste».

La fuerza de maniobra Roja lleva a cabo un ataque OPFOR normal.

Criterios de evaluación:

1. Reconocimiento: ¿Identificó la Azul rápidamente los efectos de la guerra electrónica? ¿Los notificó?
2. Respuesta: ¿Ejecutó la Azul el plan PACE sin que se le indicara?
3. Adaptación: ¿Continuó la Azul la misión a pesar de la pérdida de comunicaciones?
4. Informes: ¿Se documentaron y notificaron adecuadamente los incidentes de guerra electrónica?
5. Éxito de la misión: ¿Logró Blue cumplir la misión defensiva?

Estándares para «GO»:

Reconocimiento de los efectos de la guerra electrónica en menos de 5 minutos.
PACE ejecutado en los 3 minutos siguientes al fallo primario.
Todos los incidentes de guerra electrónica notificados. utilizando el formato adecuado.
Misión cumplida a pesar del deterioro de las comunicaciones.
Sin fallos catastróficos (p. ej., retraso en la evacuación médica debido a una planificación deficiente).

AAR (2 horas):

AAR completo de la compañía centrado en:
- ¿Qué ha cambiado en 30 días? Comparar con el día 1
- ¿Qué habilidades relacionadas con el espectro se han adquirido? Ser específico
- ¿Qué carencias persisten? Evaluación honesta
- ¿Cómo mantendremos esto? Integración en el entrenamiento futuro
- ¿Qué haríamos de forma diferente en combate? Aplicación en el mundo real

Evaluación final del comandante:

¿Tienen en cuenta los líderes el espectro en la planificación?

¿Tienen los soldados la confianza necesaria para operar en un entorno sin comunicaciones?
¿Forma ahora parte el espectro del ADN táctico de la compañía?

Reflexión final del día 30:

No se necesita equipo caro para entrenar la conciencia del espectro. Se necesita:

1. Un pensamiento disciplinado sobre la firma electromagnética.
2. Procedimientos ensayados para cuando fallen las comunicaciones.
3. Líderes que entiendan que la amenaza es real.

El equipo puede llegar más tarde. La mentalidad empieza ahora.

El sargento dice que tienes que firmar esta lista.

Post-entrenamiento: Mantener la capacidad

Has creado una compañía consciente del espectro. Ahora mantén esa capacidad.

Entrenamiento de repaso mensual:

Semana 1: Repasar los fundamentos del espectro (1 hora).
Semana 2: Ensayo del plan PACE (2 horas).
Semana 3: Recorrido por el terreno del espectro (2 horas).
Semana 4: Integración con fuego real o FTX.

Integrar en todo el entrenamiento:

Cada problema de campo incluye consideraciones sobre el espectro.
Cada OPORD incluye un apartado de guerra electrónica.
Cada AAR aborda el rendimiento del espectro.

Desarrollo de líderes:

Leer y comprender el ATP 3-12.3, especialmente el Apéndice A.
Mantener una biblioteca de TTP de guerra electrónica y lecciones aprendidas.

Inversión en equipamiento:

Solicitar analizadores de espectro a través del batallón.
Adquirir SDR económicos para el entrenamiento (entre 50 y 300 dólares cada uno).
Construir emisores señuelo a partir de radios viejas.

Notas finales del comandante

Este plan de 30 días es ambicioso, pero factible. Así es como se ve el éxito:

Antes del entrenamiento:

Los soldados piensan que el espectro es tarea de otros.
Los líderes de pelotón no tienen en cuenta la guerra electrónica en la planificación.
La compañía no tiene un procedimiento operativo estándar (SOP) de EMCON.
Las radios son «cajas negras» que o bien funcionan o bien no.

Después del entrenamiento:

Los soldados piensan instintivamente en la firma electromagnética.
Los líderes integran el espectro en todas las órdenes de operación.
La compañía puede operar en entornos con denegación de espectro.
Las radios se consideran herramientas que pueden emplearse tácticamente.

El espectro electromagnético es un espacio de maniobra al igual que el terreno. Tus soldados no necesitan ser ingenieros de RF, sino que deben ser tácticamente competentes en este ámbito. Este plan les permite alcanzarlo.

Ahora ve a entrenar a tu compañía. La próxima batalla se ganará o se perderá en el espectro antes de que se dispare el primer tiro.

Apéndice A: Recursos de formación

Aplicaciones gratuitas o de bajo coste:

WiFi Analyzer (Android/iOS): visualiza el espectro Wi-Fi.
RF Signal Tracker (Android/iOS): ubicación y potencia de las torres de telefonía móvil.
SDR Touch (Android): si dispone de hardware RTL-SDR.

Lecturas recomendadas:

ATP 3-12.3 *Técnicas de guerra electromagnética*.
ATP 6-02.70 *TÉCNICAS PARA OPERACIONES DE GESTIÓN DEL ESPECTRO*.

Recursos en línea:

Publicaciones del Army Cyber Institute sobre el espectro.
Recursos de la División de Guerra Electrónica de la NDIA.
Lecciones de guerra electrónica del conflicto de Ucrania (informes del RUSI y el ISW).

Lista de equipos deseados (si el presupuesto lo permite):

HackRF One (300 $): SDR básico para formación.
Analizador de espectro TinySA (100 $): visualiza el entorno de RF.
Antenas direccionales para ASIP: amplían el alcance y reducen la firma.

Apéndice B: Ejemplos de escenarios de entrenamiento

Escenario 1: «Simulacro de recuperación de comunicaciones perdidas»

Duración: 30 minutos.
Configuración: Durante cualquier evento de entrenamiento, la red de la compañía/batería queda en silencio.
Tarea: Los pelotones ejecutan el plan PACE sin que se les indique.
Estándar: Todos los pelotones pasan al plan alternativo en 5 minutos.

Escenario 2: «Retransmisión bajo fuego»

Duración: 1 hora.

Configuración: Establecer el sitio de retransmisión y recibir un informe de «contacto».
Tarea: Mantener las comunicaciones mientras se desplaza la retransmisión bajo fuego.
Estándar: <3 min de interrupción de las comunicaciones durante el desplazamiento.

Escenario 3: «Búsqueda de DF»

Duración: 2 horas.
Configuración: El equipo Rojo transmite desde una ubicación oculta.
Tarea: El equipo Azul utiliza técnicas de DF para localizar el emisor Rojo.
Estándar: Determinar la ubicación del equipo Rojo con una precisión de 500 m en menos de 30 minutos.

EMS 2025 ha sido escrito y producido por un oficial de carrera del Ejército que ha pasado la última década y media trabajando en múltiples formaciones y organizaciones centradas en la modernización, las operaciones multidominio y las tecnologías emergentes. Explora: cómo se comportan las señales y por qué es importante; el uso práctico de los SDR y las herramientas de EM accesibles; la intersección entre la guerra electrónica, la ciberseguridad y los efectos de largo alcance; los fundamentos de la energía electromagnética, explicados de forma sencilla; y cómo los líderes pueden tomar mejores decisiones en entornos técnicos complejos. Puedes contactar con él a través de su página de Substack.