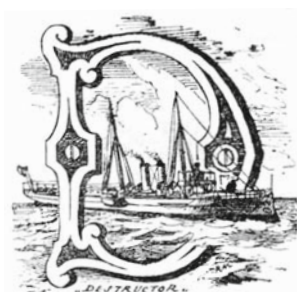


LA GUERRA ELECTRÓNICA Y EL MEWGA

Ignacio NIETO FERNÁNDEZ



Introducción



ESDE hace varios años la OTAN viene promulgando una serie de documentos que esbozan la necesidad de prestar la debida atención a lo que ocurre en el espectro electromagnético (1). A nadie se le escapa que el espectro es el vehículo conductor de diferentes tipos de señales, no solo las propias de radares (2), y es el nexo de unión de los escenarios de operaciones con los centros de mando. En el ámbito marítimo es más acuciante la necesidad de poder operar en el espectro, pues no goza de los enlaces terrestres.

Los recientes acontecimientos en los conflictos de Siria y Ucrania dejan vislumbrar el potencial de la Guerra Electrónica (GE) como potenciador y catalizador de otras capacidades. La Federación Rusa ha desarrollado la GE de tal forma que es capaz de comprometer la eficacia de las tropas de la OTAN.

En el Grupo de Trabajo de Guerra Electrónica de la OTAN (3), hace algunos años se acuñó el acrónimo de MEWGA que significa *Make Electronic Warfare Great Again*, apelando a encumbrar, de nuevo, la GE a un sitio preferente dentro del campo de batalla. En la actualidad algunos la tildan como la

(1) Destacar el MCM-0142-2007 sobre *Transformation Concept for Future NATO Electronic Warfare*, el MC 64/11 sobre *NATO EW Policy* y el MC 515/1 sobre *SEWOC, SIGINT and EW Operation Center*.

(2) Por regla general, en nuestra cultura se tiende a pensar que el oficial de Guerra Electrónica solo tiene competencias en el rango de frecuencias radar.

(3) *El NATO Electronic Warfare Working Group (NEWWG)* se reúne al menos cuatro veces al año. España participa en las reuniones. Es un grupo de trabajo dependiente del *NEWAC (NATO Electronic Warfare Advisory Committee)*.

bella durmiente a la que se acude en conflicto pero queda en el ostracismo en tiempos de paz (4).

La Guerra Electrónica

Al convertirme en especialista de Electrónica en la maravillosa ETEA (Escuela de Transmisiones y Electricidad de la Armada), embarqué a bordo de un escolta de la Armada, donde rápidamente aprendí mis tres roles fundamentales como especialista en electrónica: el equipo de detección de señales, la gestión integral de los radares del barco y la misión más trascendental, ocuparme de que el sistema de televisión funcionara debidamente, incluyendo una extensa gama de películas en formato VHS (los más jóvenes quizás no entiendan este acrónimo).

De esta forma, mi trabajo, con carácter general, quedaba acotado al margen de señales radar en el campo de detección. Mientras la Armada formaba especialistas en Electrónica, su misión en el barco no se limitaba solo a esto, sino también a la GE. En la práctica, mi principal misión era adiestrar en las lecciones aprendidas y en la doctrina que se desprendía de la Guerra de las Malvinas. A todos nos traen recuerdos los famosos ejercicios de lanzamiento de *chaff* como medida a tomar ante un Zippo (5) promulgado por la fuerza ante un lanzamiento de misil.

La misión se centraba en el equipo de GE, bien el Neptunel, el Deneb y los principios del Aldebarán. Poco margen se dejaba a técnicas de perturbación, decepción o abrir el rango de trabajo de los especialistas de GE a otras esferas que implicaran un dominio del espectro electromagnético. El especialista en Electrónica entendía su trabajo como una mera identificación de parámetros ayudado por la base de datos de emisores de la OTAN (6). En ningún caso entendía el espectro como un campo de batalla o se sentía guardián de él. Su labor era autárquica, pues apenas atendía a las demandas de los otros gremios, que también necesitaban del espectro para conducir sus operaciones con éxito.

¿Y realmente qué comprende la GE? Abreviado en inglés EW, *Electronic Warfare*, consiste en una actividad tecnológica y electrónica con el fin de determinar, explotar, reducir o impedir el uso hostil de todos los espectros

(4) No solo de paz, sino de conflictos de baja intensidad o aquellos en lo que la amenaza no considera el espectro como un campo de batalla, a pesar de que durante los últimos años la clara amenaza se materializaba en artefactos explosivos improvisados, *Counter Improvised Explosives Devices* (C-IED), que tienen su vertiente de remotos que utilizan el espectro para detonarlos.

(5) Zippo no es más que una palabra clave para advertir a la fuerza de que existe una amenaza de misil.

(6) Denominada NATO *Emitter Data Base* (NEDB).

de energía, por ejemplo, el electromagnético, etc., por parte del adversario y a la vez conservar su utilización en beneficio propio (7).

La OTAN adopta la definición consensuada de *Military action that exploits electromagnetic energy to provide situational awareness and achieve offensive and defensive effect* (8).

En ambas acepciones se contempla que la GE es la encargada de explotar el espectro electromagnético sin acotarlo a ningún margen de frecuencias. Es decir, las frecuencias de las bandas de comunicaciones, láser o infrarrojas también deben ser asumidas por la GE. Dentro de esta definición también se incluye su explotación.

Ahondando un poco más en las capacidades, nos encontramos con las manidas acciones que podemos llevar a cabo dentro del amparo de la GE que en general son bien conocidas. Estas se catalogan como las medidas de apoyo electrónico, las contramedidas electrónicas y las medidas de protección electrónica.

Medidas de apoyo electrónico

Denominadas en inglés las ESM, *Electronic Support Measures*, consisten en el análisis del espectro electromagnético, encaminado a interceptar e identificar las emisiones y localizar su procedencia. Básicamente están pensadas para proporcionar alerta temprana, reconocimiento de las actividades del enemigo y obtención de datos para el Orden de Batalla Electrónico (OBE).

Se abre un interesante debate sobre realmente qué deben asumir los equipos de ESM y si dentro de sus competencias debe entrar la elaboración de inteligencia. En algunos foros se habla de la GE como proveedor de productos de inteligencia, puesto que el operador de EW con facilidad puede elaborar un análisis que enriquezca el proceso de toma de decisiones al mando (9). Este importante escollo ha sido sorteado, en el ámbito nacional, al acotar las actividades ESM dentro del corto plazo, dejando el medio y largo plazo, y por lo tanto la elaboración de inteligencia, a otros gremios dentro del amplio marco del mundo de la inteligencia.

En principio, las actividades de ESM cubren todo el espectro, incluidos los márgenes de frecuencia de comunicaciones infrarrojos o electroópticos. Esto nos lleva a otro debate sobre las competencias de ESM y las de las actividades de inteligencia de señales (SIGINT, *SIGnals INTelligence*) y sus dos áreas: la

(7) <http://www.ejercito.mde.es/unidades/Madrid/rew31/Organizacion/index.html>.

(8) MC 64 NATO EW Policy.

(9) Existen multitud de definiciones de inteligencia, pero sin duda la diferencia entre información e inteligencia está consensuado en que la segunda aporta un valor añadido al proceso de toma de decisiones.

inteligencia de comunicaciones (COMINT, *Communications Intelligence*) y electrónica (ELINT, *Electronic Intelligence*), que se mantienen bajo el amparo de las actividades reservadas, y por lo tanto desconocidas, para la mayoría de los mortales.

Las ESM pueden explotar, atendiendo a la definición, el campo de las comunicaciones y puede generar productos derivados que, si bien es complejo tildarlos de inteligencia, no se alejan mucho de un producto genérico de Intel. De esta forma, cuando en la Armada a las fragatas se las dota de un equipo de interceptación de comunicaciones, no está claro si la explotación entra dentro del ámbito de COMINT o simplemente de GE. Este punto es importante, pues los productos derivados de la explotación de COMINT deben tener clasificación *Cosmic Top Secret Bohemia* (CTS-B), lo que desde luego dificulta sobremanera no solo la gestión de la información, sino incluso la misma elaboración de los productos o la propia ubicación del equipo.

Otras naciones son más claras en este aspecto y no encuentran diferencia entre la explotación del espectro y engloban todas las actividades dentro de la GE. Dejan en el terreno de la clasificación de seguridad la separación de las actividades (GE-SIGINT), lo cual parece más lógico que la postura nacional, aunque solo sea por el mero hecho de aunar esfuerzos y economía de recursos.

Contramedidas electrónicas

Vulgarmente conocidas como ECM (*Electronic Counter Measures*), abarcan las acciones encaminadas a evitar que el adversario utilice el espectro mediante el uso de la energía electromagnética. Dentro de ellas se contempla la perturbación, la neutralización y la decepción.

Las ECM han tenido un desarrollo impresionante que da cuenta del verdadero potencial de la GE. Comenzado por la perturbación, la verdad es que a los más veteranos se nos viene a la cabeza la imagen de la pantalla radar con un sector ciego por la perturbación o con la pantalla con la detección degradada. Quizás nuestra comprensión de la perturbación se haya quedado aquí, sin conocer el potencial de la perturbación en las actividades que se vienen desarrollando en Ucrania o en Siria.

Pongamos el ejemplo de la perturbación de las señales del GPS (*Global Positioning System*) que lejos de ser complejas se han convertido en sencillas, y al alcance de todo el mundo. Basta con realizar una búsqueda por internet para encontrar perturbadores o inhibidores de la señal GPS. Resulta difícil determinar hasta qué punto nuestras fuerzas están preparadas para afrontar unas operaciones en un ambiente carente o deficitario de señal GPS. Hay que considerar la importancia que tiene no solo el perder la posición, sino también la señal horaria o *timing* que proporciona el sistema GPS a multitud de equipos.

La sencillez en perturbar la señal GPS produce fascinación. Por ejemplo, el aeropuerto de Newark sufrió varios días de interferencias en el sistema de seguimiento de los aviones que estaba gobernado por GPS. La cuestión es que un simple trabajador, en aras de evitar el seguimiento por parte de su jefe de la furgoneta que usaba de trabajo, compró un perturbador de señal que ocultara sus movimientos. Al final, al dejarlo encendido cerca del aeropuerto provocó un importante incidente de carácter nacional.

Recientemente, el presidente de la Federación Rusa amenazaba a los Estados Unidos con que podría derribar o perturbar sus misiles Tomahawk. En los dos *strikes* lanzados sobre Siria por los estadounidenses, solo una parte de los Tomahawk llegaron a su destino y del resto se desconoce su paradero. Rusia aboga que fueron o bien perturbados o bien destruidos por el sistema de defensa aérea sirio de procedencia rusa.

No me cabe la menor duda de que un Tomahawk es perturbable y, sin querer ser agorero, no creo que sea ni incluso complicado, pero entra dentro del terreno de lo clasificado. La pregunta que debemos hacernos es si en un ambiente saturado de perturbación podemos lanzar un misil, a sabiendas de que puede ser perturbado y por lo tanto perder la posición y dirigirse a otro blanco no deseado, pongamos por ejemplo un hospital.

Pero qué es lo que puede ser perturbado debería llevarnos a la reflexión. Recientemente, asistí a una conferencia en la que los representantes de Ucrania manifestaban que en ciertos escenarios la congestión del espectro era de tal entidad que era imposible volar los drones. Muchas operaciones, o la recolección de inteligencia, quedan seriamente mermadas sin poder operar drones.

Si la perturbación es fascinante, mucho más la decepción, pues está al alcance de todo el mundo decepcionar la señal de GPS y tomar control de aquellos dispositivos o unidades que estén gobernadas por este sistema.

Y vuelve a mi cabeza la misma pregunta en relación a qué es decepcionable. En diciembre de 2011 uno de los más avanzados drones de Estados Unidos, el *RQ-170 Sentinel* operaba en Afganistán. El dron se perdió y se declaró oficialmente que se había quedado sin combustible cayendo en las montañas de Afganistán. Poco tiempo después, Irán declaraba que había tomado su control y le había forzado a tomar tierra en una de sus bases. Posteriormente, declararon haber realizado ingeniería inversa, y ahora Irán, en una fabulosa campaña psicológica, muestra su poderío de drones *Sentinel*.

Nos queda la tercera división de las ECM: la neutralización o el uso de esa energía electromagnética para inutilizar o destruir las capacidades del enemigo que utilizan el Ambiente Electromagnético (10) (AEM). En este campo se

(10) Utilizaré este término, AEM, definido en la doctrina OTAN (*Electromagnetic Environment*, EME) sustituyendo al de espectro electromagnético, aunque a los efectos de este artículo viene a ser lo mismo.

necesitaría un artículo entero para explicar la amalgama de armas, instrumentos y equipos que actualmente están en uso o en vías de desarrollo. Cubren el campo letal y el no letal y su uso reduce significativamente los daños colaterales, lo cual es, sin lugar a duda, uno de los factores más a tener en cuenta en el uso de la fuerza militar.

Destacan entre todas ellas la utilización del pulso electromagnético como arma, es decir poder generar una cantidad de energía importante contra un equipo electrónico que le infrinja daños. Una bomba de estas características dejaría muchos de los equipos electrónicos del enemigo inoperativos con un daño colateral a los seres humanos nulo o muy reducido. Ni que decir tiene la fascinante posibilidad de generar un pulso electromagnético de gran altitud que podría causar daños devastadores a, incluso, una nación entera. Estados Unidos considera esta arma como una amenaza y ya en el 2001 formó una Comisión para el estudio de esta amenaza (11).

Merecen también atención las armas de energía dirigida que emiten energía altamente condensada al objetivo para dañarlo. Entran dentro del abanico de las letales y no letales pues gobernando la cantidad de energía que deseas poner en el AEM el efecto es o no letal

El abanico de armas no letales es muy variado, están en pleno auge pues en los conflictos asimétricos actuales, donde el uso de la fuerza letal es siempre muy cuestionado, estas armas tienen un espacio insustituible. Además de las armas de energía dirigida nos encontramos con otras como la utilización del sonido para dañar al enemigo, denominado dispositivo acústico de largo alcance.

Medidas de Protección Electrónica

Y nos encontramos con el patito feo de la GE, que no menos importante, pero sí son las que menos comprensión tienen. Las denominadas EPM, *Electromagnetic Protection Measures*, son las acciones encaminadas a eludir las ECM y las ESM. Se pueden clasificar en activas y pasivas. El Plan de Control de las Emisiones o EMCON Plan, los alertadores o los *chaff* entran dentro de las ESM.

Merece especial atención la importancia de los señuelos, como un método eficaz de defensa contra misiles. Ya viene de lejos, de la Guerra de las Malvinas, la importancia del uso de estos dispositivos. Actualmente pocos recursos tiene un piloto al defenderse de un misil que no sea lanzando el *chaff*.

Pero las EPM no se quedan en eso solamente; los desarrollos en técnicas de enmascaramiento dan resultados sorprendentes y las nuevas tecnologías radar hacen muy complicadas las detecciones por parte del adversario.

(11) En su página web existen numerosos informes <http://www.empcommission.org/>.

La necesidad de estar en permanente transformación

En el 2007, la OTAN promulgó un interesante documento, a nivel Comité Militar, el MCM-0142-2007, que establecía las líneas maestras de la transformación necesaria para la futura GE en la OTAN. Básicamente se modificaba su concepto, que pasaba de una gestión del espectro y de las frecuencias a uno nuevo: las operaciones electromagnéticas, entendiendo como tales todas aquellas que ocurren en el AEM.

En el mismo se apuntaba lo siguiente:

- Se declaraba el AEM como un ambiente operacional, esto es, que afecta a todos los niveles de la guerra. No hablamos de un dominio, pero el paso era importante, pues implicaba contar con las secciones de GE en cualquier ámbito de la guerra o de la crisis.
- Por otra parte, y al amparo del *Effects Based Approach to Operations* (EBAO), se establecieron los tres efectos asociados a la GE: el ataque electrónico, la vigilancia electrónica y la protección electrónica. Estos están íntimamente ligados a las tres medidas anteriormente explicadas.
- Por último, se convenía que se debían buscar mecanismos que permitirán coordinar el esfuerzo en el AEM, de tal forma que por ejemplo se evitaran fratricidios electromagnéticos. Se apuntaba la conveniencia de trabajar de forma mancomunada entre las secciones de Guerra Electrónica e Inteligencia de Señales (SIGINT *and* EW Operations Center SEWOC) y de migrar a mecanismos de coordinación más ambiciosos, integrando no solo las secciones de Gestión del Espectro (*Electromagnetic Battle Staff*), sino todas aquellas áreas que trabajen con el AEM.

Esta nueva aproximación a la GE dio como fruto un esfuerzo por parte de las naciones en aras de explotar estos nuevos conceptos y se llevaron a cabo ejercicios orientados a la GE y en concreto a coordinar el esfuerzo en el AEM. Destaca el realizado en el norte de Europa en 2008, denominado MODULEX, orientado a explotar el concepto SEWOC, que se convirtió en un completo éxito y dio lugar a mejoras sustanciales en la doctrina de coordinación entre los tres principales gremios que trabajan en el espectro: EW, SIGINT y SM (Gestión del Espectro, *Spectrum Managment*).

Este impulso inicial se ha visto frenado y hemos entrado en un letargo, imprudente desde mi punto de vista, el cual ha sido aprovechado por otras naciones para avanzar en capacidades de GE.

Toda esta iniciativa de la OTAN viene aparejada con un cambio de mentalidad, que pasa de una gestión y recolección de paramétricas a un ámbito superior, que se denomina Operaciones Electromagnéticas. Sería necesario dedicar varios artículos para explicar en profundidad este ambicioso concepto y concretar la amenaza actual.

¿Estamos en el camino del MEWGA?

Las naciones modelan su esfuerzo en el desarrollo de capacidades confrontando la amenaza que perciben. La guerra híbrida es un claro ejemplo del tipo de motivación que necesitan las naciones para desarrollos doctrinales, estrategias, capacidades y un sinnúmero de acciones que rodean la tan manida guerra híbrida.

Sin embargo, en GE no parece que existan un vibrante desarrollo de capacidades o doctrinal; más al contrario, se tiene una percepción de abandono o por lo menos de actitud laxa. Esta aproximación no contrasta con la inseguridad de las tropas occidentales cuando se refiere a lo que ocurre en escenarios como Siria o Ucrania. Atender a una sola de las conferencias que las autoridades ucranianas vienen impartiendo sobre lo que ocurre en Ucrania suele ser un antes y un después en la percepción de la GE y, por supuesto, de la amenaza.

El presidente ruso Vladímir Putin es sin duda un genio de la EW y la utiliza con profusión por el binomio coste-eficacia. El Ejército ruso viene utilizando la GE como un facilitador de las acciones que otros sectores acometen. Recientemente se ha publicado un informe por parte del Centro Internacional de Seguridad y Defensa de Estonia (12) que habla del uso que hace la Federación Rusa de la GE, que ha llevado a muchos estamentos a recapacitar sobre si este ostracismo es beneficioso.

Hay que considerar que en Ucrania se perturba el GPS de forma masiva, lo que dificulta sobremanera el uso de dispositivos electrónicos. En muchas ocasiones no es posible volar los drones. Las comunicaciones están sujetas a permanente decepción, no solo las de HF/UHF, sino también las que corren por internet con enlaces satelitales, por ejemplo, la mensajería por ordenador o por telefonía móvil.

Pero ahora el AEM es un campo de batalla donde los que menos recursos tienen lo utilizan para poner en jaque a las fuerzas más poderosas. Las operaciones electromagnéticas dentro del AEM no están garantizadas, ni mucho menos; se llega incluso a afirmar que en conflictos de media intensidad se ha perdido el control del AEM y, perdido este, las actividades militares no tienen viso alguno de poder ser efectivas.

Lamentablemente la percepción de esta amenaza no motiva el MEWGA, quizás porque es complejo entender las actividades asociadas en el espectro. Siempre hemos visto el espectro como ilimitado y libre en el uso, afirmación que ya dejó hace mucho tiempo de ser cierta, pues es limitado y desde luego está congestionado. Tampoco ayuda que siendo un ambiente físico, al contra-

(12) El autor es Roger N. MacDermott; el informe es de carácter abierto, disponible en <https://www.icsd.ee/publications/article/russias-electronic-warfare-capabilities-to-2025-challenging-nato-in-the-electromagnetic-spectrum/>.

rio del cibernético, no es visible y por lo tanto cuesta llevarlo al terreno de la comprensión.

Por otra parte, es complejo marcar un terreno común de entendimiento, pues la GE es diferente no solo desde el abanico táctico al estratégico, sino que también para los que trabajan en el marítimo, terrestre o aéreo su concepción es también distinta. Por último, los marcos nacionales suelen divergir del de la OTAN y conforman una GE del todo diferente en muchas ocasiones.

Asimismo, las capacidades en GE apenas son ofrecidas, pues residen en el terreno de lo clasificado, y por lo tanto se desconocen y por supuesto no son ofertadas a la OTAN en los procesos de generación de fuerzas, con lo que es complejo avanzar mediante el *Learning by doing*.

Por último, y quizás más importante; la mentalidad de la EW es deficiente y con un claro desenfoque de la realidad. Seguimos enclavando al oficial de GE como un oficial con competencias exclusivas radar sin formarle con una visión más amplia. La GE solo se puede entender como una capacidad transversal al resto y que tiene jurisdicción en las demás áreas, puede ejercer un resultado catalizador y multiplicador de los efectos de otras disciplinas o capacidades.

Desde mi humilde perspectiva, se necesita un cambio de cultura de la organización que permita comprender y entender el peso específico de la GE en los conflictos actuales. No solo se tiene que vigorizar la aproximación de arriba-abajo, *top-down*, con esfuerzos en la concienciación de lo que viene ocurriendo en Siria y Ucrania y la facilidad en poner en jaque fuerzas militares occidentales. También precisamos de una fortaleza conceptual en la aproximación de abajo-arriba, *bottom-up*, que permita expandir en entendimiento del potencial de la GE que estimule debates y resulten en procedimientos de coordinación y cooperación con el resto de disciplinas.

En el ámbito del NEWAC se está potenciando la mentalización de los mandos de la estructura de la OTAN sobre la importancia que en las operaciones actuales tiene el AEM como una de las medidas encaminadas a dotar de peso específico la aproximación *top-down* que consiga el MEWGA.

En cuando a la *bottom-up*, desearía destacar los cursos que se vienen realizando en la Escuela de la OTAN de Oberammergau (13) y muy especialmente el catalogado como N3-152 Operaciones Electromagnéticas, donde se logra concienciar a un máximo de 30 alumnos sobre la importancia de coordinar el esfuerzo en el AEM.

(13) El catálogo de los cursos, así como las normas de inscripción, se encuentran disponibles en <http://www.natoschool.nato.int/Academics/Resident-Courses/Course-Catalogue>.

Conclusiones

El rango de responsabilidades de los destinos de GE es, como se ha visto, abrumador. Todo ello solo si nos ceñimos a nuestra labor como electrónicos a bordo. Si nos trasladamos al ámbito de las operaciones electromagnéticas, que es donde debiéramos trabajar, el abanico se amplía hasta límites inabordables.

En la actualidad, todas las actividades propias de las marítimas son demandantes del AEM y necesitan de la GE, aunque solo sea por la protección que esta les puede proporcionar. Las operaciones actuales demandan, con ansiedad, el acceso al espectro como un prerrequisito para poder conducir las operaciones.

La coordinación y/o la cooperación en el AEM pasan a ser un elemento esencial en la confrontación bélica actual; la potenciación de las capacidades de GE es esencial si queremos tener alguna oportunidad de éxito en conflictos de media intensidad. El espectro es un campo de batalla muy complejo donde se necesita mucho adiestramiento avanzado para poder recuperar el AEM y conseguir MEWGA.

Comprender que el espectro no es un mero recurso físico, sino un campo de batalla donde es sencillo infligir daños a naciones poderosas, es una línea de acción que debe ser emprendida cuanto antes a todos los niveles, de tal forma que nos permita estar preparados para tener la supremacía en el espectro electromagnético.

Debemos empezar por explicar, en todos los estratos, el uso que se hace de la tecnología en escenarios de crisis, sin focalizarlo en la Federación Rusa, sino en aprender lo que viene haciendo la GE para conseguir sus objetivos. Estas capacidades son baratas y tienen mucho potencial y pueden ser utilizadas por cualquier otro adversario con el mismo éxito que en Ucrania o Siria.

Quizás estas medidas deban ser encuadradas dentro de una campaña de concienciación de las Fuerzas Armadas que nos permita conformar una respuesta de entidad que fortalezca nuestra defensa colectiva, piedra angular del tratado fundacional de la OTAN. Es el principio consagrado en el artículo 5 del Tratado del Atlántico Norte, que establece el espíritu de solidaridad dentro de Alianza que debemos preservar con capacidad de respuesta ante escenarios previsibles. Tenemos que prepararnos para un escenario de características similares a los actuales en Siria y Ucrania, y ello pasa por la potenciación de la GE o, mejor dicho, de las operaciones electromagnéticas.