Documento
Marco

04/2021 15 de marzo de 2021

Ignacio Nieto Fernández

La capacidad de disuasión estratégica de las operaciones electromagnéticas

La capacidad de disuasión estratégica de las operaciones electromagnéticas

Resumen:

Las operaciones electromagnéticas están en auge, adquieren ahora un creciente protagonismo pues fácilmente hallan su acomodo en la hibridación de los conflictos o en aquellos conflictos que se desarrollan en la zona gris. Las operaciones electromagnéticas se desarrollan en el margen de la ambigüedad y sus efectos suelen estar exentos de atribución, lo que complica el uso del instrumento militar, especialmente con las reglas de juego occidentales, incluso en el ámbito de la autodefensa, tanto individual como colectiva. Son capaces de traspasar el umbral de lo militar y erigirse como una herramienta muy válida para la disuasión estratégica que suelen utilizar los países revisionistas. Se han convertido en una parte esencial de la estrategia que utilizan los países revisionistas, que se ha mostrado del todo eficaz tanto en el combate puramente militar como en la capacidad coercitiva a nivel político de los Estados occidentales.

Palabras clave:

Operaciones electromagnéticas, guerra electrónica, multilateralismo, Gerasimov, zona gris.

The capability of strategic deterrence of the electromagnetic operations

Abstract:

Electromagnetic Operations are on the mend, created more than 12 years ago within the fold of NATO, play an important role in conflict hybridation or in those conflicts so called 'grey zone'. These operations are characterised by a high level of ambiguity and their effects are unattributable by nature, thus the use of the military instrument by western countries is difficult, notably with their rules, even in self-defence, both individual and collective. Electromagnetic operations can cross the threshold of a pure military action and become an outstanding tool for strategic deterrence, carried out by revisionist countries. They have risen to the top of the Russian Federation current strategy that have been proven to be effective, both pure military combat and providing deterrence capability at political level from western countries.

Keywords:

Electromagnetic operations, electronic warfare, multilateralism, Gerasimov, Grey zone.

Introducción

Las operaciones electromagnéticas (OEM) son grandes desconocidas, y siempre van impregnadas de un aura de enigma y novedad. Un misterio rodea esa pegadiza palabra, que se encuentra encima del tablero de los conflictos actuales. Sin embargo, esta apreciación de novedad no guarda consonancia con la historia, puesto que las OEM ya vieron la luz en las Cumbres de la OTAN de Praga y Riga hace más de diez años. El compromiso con la guerra electrónica (EW, por sus siglas en inglés) de las naciones OTAN dio como resultado la promulgación del MCM 0142/2007, que versaba sobre el concepto de transformación para la futura EW. Como su nombre indica, se trataba de hacer evolucionar el concepto de la EW.

Las naciones que conforman la Alianza decidieron impulsar un concepto que debería haber sentado las bases para permitir la transformación de la EW. Una migración que tenía como estadio final las OEM. Una evolución que venía inexorablemente unida a un cambio de cultura sobre el pilar conceptual de pasar de una mera gestión de frecuencias a una gestión del espectro y uso de la energía electromagnética. Una amplitud de miras mayor para la EW, que además debía cubrir todo el espectro electromagnético[1].

Un concepto, que además articulaba las OEM sobre tres de los gremios que se declaraban más relevantes en el espectro: la EW, la gestión del espectro (SM, por sus siglas en inglés) y la inteligencia de señales (SIGINT, por sus siglas en inglés). Estas tres capacidades debían trabajar al unísono sobre la base de la coordinación y la cooperación, centrando los esfuerzos en garantizar tres objetivos: el libre acceso al espectro, la libertad de movimiento que permita efectuar la maniobra electromagnética y dificultar al adversario el uso de este preciado recurso.

Además, indicaba los mecanismos que debían ser utilizados para lograr los objetivos de coordinar y cooperar en el espectro, a todos los niveles del planeamiento y conducción de las operaciones militares. En un primer nivel de integración se encontraba la *electronic warfare coordination cell* (EWCC). En el caso de integrar SIGINT y EW, pasábamos a un nivel de integración superior, en un centro denominado SIGINT and EW Operations Center (SEWOC). Mientras que el primer mecanismo era propio del nivel táctico, el

[1] Conforme a la NATOTerm Database, la definición acordada es: «El espectro electromagnético es la distribución ordenada de ondas electromagnéticas de acuerdo con su frecuencia o forma de onda. Incluye las ondas de radio, microondas, radiación de calor, luz visible, ultravioleta, rayos X, rayos cósmicos y gamma».

SEWOC estaba diseñado para el nivel operacional. Por último, el mecanismo que mejor respondía al reto de la coordinación del esfuerzo en el espectro era el *electroMagnetic battlestaff* (EMB). Un constructo sobre la base de las tres capacidades anteriormente citadas a las que se podían unir otras como navegación, mando y control, espacio ultraterrestre o cualquier otra capacidad que necesitara del espectro para su correcto funcionamiento.

El esfuerzo principal, la amenaza asimétrica

Sin embargo, es cierto que, durante estos años, apenas se volcaron esfuerzos en las OEM, por lo que se precipitaron vertiginosamente al sueño de los justos. Cabría preguntarse el motivo de no haber desarrollado más las OEM, a pesar de tener un respaldo rotundo de las naciones OTAN.

El motivo lo encontramos en la amenaza que convenimos los Estados occidentales confrontar después de la caída del muro de Berlín: la amenaza asimétrica. Esta aproximación es del todo razonable, puesto que los Estados desarrollan sus capacidades militares, en primer lugar, sobre la percepción de la posibilidad de que las amenazas inflijan daños. Posteriormente, atienden a aquellos desafíos que puedan materializarse en amenazas. En este caso, la amenaza asimétrica apenas retaba nuestras capacidades militares. Tampoco cuestionaba el acceso al espectro, lo que, aparentemente, nos hizo dormir en un profundo letargo, sin avanzar en el desarrollo de capacidades asociadas a las OEM.

Un letargo que a la sazón nos resulta gravoso de resolver en la actualidad, puesto que hemos desarrollado numerosas capacidades civiles y militares que tienen una fuerte dependencia del acceso al espectro electromagnético y en la actualidad se encuentra confrontado, disputado y congestionado. Ahora nos encontramos que, lo que antaño era sencillo, por ejemplo, una simple comunicación, ahora se torna complejo.

Proliferan por doquier los sistemas, dispositivos o aplicaciones que necesitan conectarse gracias y a través del espectro. Un ejemplo es la dependencia de nuestros sistemas a la

señal de sincronismo[2] de algún sistema GNSS[3] (*global navigation satellite system*). Y, para más inri, el futuro se antoja más vulnerable, por ejemplo, con la tecnología inalámbrica de quinta generación, que permitirá velocidades inalámbricas similares o superiores a las conseguidas con cable.

Volvamos a la amenaza asimétrica, aquella que no confrontaba nuestro acceso al espectro. Sin embargo, el adversario lo utilizaba para activar los artefactos explosivos improvisados, que han sido los causantes del mayor número de muertos en la OTAN durante los últimos cuarenta años. Era necesario trabajar para mitigar los efectos de esta amenaza que disfrutaba del acceso al espectro. Se potencian los perturbadores o inhibidores de señales para los dispositivos de controles remotos y en los móviles. Además, se pone especial énfasis en interceptar las comunicaciones.

SEWOC, la fortaleza de trabajar juntos

Para atender a esta necesidad de protección de la fuerza, se forjó uno de los conceptos en los que la OTAN ha puesto más empeño y se ha logrado más consenso, no solamente en el desarrollo doctrinal, sino también en su puesta en práctica, tanto en ejercicios como en operaciones. Nació el concepto SEWOC, reflejado en el MC 515 Concept for the NATO SIGINT & EW Operations Center (febrero de 2012). Concepto que fue modificado varias veces, lo que demuestra el interés de las naciones. Además, fue apoyado por otro concepto más que regulaba los recursos que se debían asumir a este centro[4]. Dos conceptos para una misma idea: el control del espectro.

Los miembros de la Alianza demostraron su compromiso con el concepto SEWOC desplegando múltiples recursos y esfuerzos en conformar células donde trabajaban conjuntamente la EW y la SIGINT. El objetivo primario no era otro que el de salvar vidas humanas en escenarios de alta intensidad como Afganistán.

[2] Se suele tener la tendencia a pensar que lo importante de los sistemas de posicionamiento global es la posición, cuando lo realmente importante es mantener la integridad de la señal horaria que proporcionan sus relojes atómicos.
[3] Por GNSS se entienden los sistemas que proporcionan cobertura satelital global de posición y sincronismo. En la actualidad, existen seis sistemas: el GPS (norteamericano), GLONASS (ruso), BeiDou (chino), Galileo (Unión Europea), IRNSS (indio) y el QZSS (japonés).
[4] En concreto, el MC 521 «Concept for resources and methods to support an operational NATO EWCC/SEWOC».

Se realizaron incluso ejercicios de gran entidad, específicos de SEWOC, como los que se acometieron en el norte de Europa con la denominación MODULEX 2008. Ejercicios que fueron impulsados por dos de los comités asesores al Comité Militar más importantes de la OTAN, el NACSI[5] y el NEWAC[6]. El primero en el ámbito SIGINT y el segundo en el ámbito de la EW.

SEWOC es un concepto orientado a la producción de inteligencia, y en especial la inteligencia de comunicaciones. Su génesis es evitar los largos procesos propios del ciclo de inteligencia. Su finalidad es que las interceptaciones de comunicaciones alimenten, en tiempo real, el proceso de toma de decisiones del comandante de la operación. Básicamente, era la respuesta occidental a la amenaza R-CIED (*radio counter improvised explosives devices*).

La OTAN había promulgado las directrices específicas para prestar la debida atención al espectro. La Alianza apostaba por constructos donde la coordinación era un factor esencial que permitiera obtener sinergias y, a la postre, hacer que el esfuerzo en el espectro no se dilapidara[7]. SEWOC era uno de esos constructos, pero no era el único. Se fomentaba ampliar la capacidad de coordinar con otras capacidades como el espacio ultraterrestre, las relacionadas con la navegación o los sistemas de mando y control. En definitiva, se aconsejaba una disposición específica del estado mayor para afrontar este importante reto. Hablamos del *electroMagnetic battlestaff* (EMB).

La guerra de Chechenia: un cambio de paradigma

El espectro, sin embargo, era un terreno donde otros comenzaban a vislumbrar el potencial que atesoraba en el arte de la guerra. Los más adelantados percibían que no era recurso accesible *per se,* sino un verdadero campo de batalla donde la capacidad militar tenía menos protagonismo que en otros ambientes operacionales. Desde el espectro electromagnético era menos complejo reducir la brecha tecnológica y militar de los Estados Unidos.

[5] NACSI: NATO Advisory Committee to SIGINT.
[6] NEWAC: NATO EW Advisory Committee.
[7] Aparecen conceptos como *fratricidio electrónico*, puesto que el 80 % de las interferencias que se provocaban en Afganistán eran de fuerzas propias.

Esta es la aproximación del jefe de las Fuerzas Armadas de la Federación Rusa, el general de Ejército Yuri Gerasimov. Desde la guerra con Georgia, la Federación Rusa comenzó a modernizar y sofisticar su instrumento militar, especialmente con capacidades como la guerra electrónica. Las lecciones aprendidas condujeron a los rusos a una profunda modernización de las FAS, siendo uno de los pilares la EW[8].

Este plan de modernización se orientaba a dos objetivos: por una parte, potenciar la capacidad de actuar conjuntamente; y, por otra, ser catalizador de otras capacidades, ambas soportadas por un robusto sistema de mando y control. Su finalidad última no era más que adaptar los procedimientos propios de la guerra asimétrica para contrarrestar la superioridad tecnológica de los países occidentales. «Rusia percibió la EW como un capacitador o multiplicador de fuerzas, y utilizó estos conceptos para avanzar diseñando nuevos retos asimétricos para Estados Unidos y la OTAN»[9].

Además, introducía otros elementos, como la ambigüedad, la complejidad en la atribución, el uso de herramientas civiles y un largo etcétera que eran de difícil respuesta con las reglas de juego de Occidente. Elementos que fueron obtenidos después de una observación detenida de nuestra deontología militar, en especial en lo relativo a la aplicación de la fuerza.

El lema *learning by doing* (aprender haciendo) era el motor de la transformación de sus Fuerzas Armadas para convertirlas en competitivas. No hay mejor banco de pruebas para un arma que un escenario real de conflicto. Mantener a Rusia en escenarios de alta intensidad permitía mejorar rápidamente los instrumentos militares rusos. Finalmente, es en los conflictos de Ucrania y Siria donde se despliega el verdadero potencial ruso, que hace despertar a Occidente ante la eficacia de las técnicas rusas. De la mano de la OTAN se comienzan a desarrollar capacidades para confrontar este desafío.

La Federación Rusa diseña una serie de acciones que producen efectos que no se corresponden con la tradicional praxis en el uso del instrumento militar. En el campo de batalla, se difuminan las fronteras entre lo militar y lo civil y se genera una confusión que complica el racional y juicioso uso de la fuerza por parte de las FAS occidentales. La

[8] MCDERMOTT, Roger. «N. Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum», *Center for Strategic and International Studies*, enero de 2018.
[9] «Russian Electronic Warfare», *American Security Project*, abril de 2020. Disponible en: https://www.americansecurityproject.org/wp-content/uploads/2020/04/Ref-0236-Russian-Electronic-Warfare.pdf (Consultado el 13/1/2021).

dificultad de operar en estos entornos fue expuesta en una conferencia de más de 2000 especialistas en inteligencia por parte del general Raymond A. Thomas, antiguo general jefe del Mando de Operaciones Especiales de los Estados Unidos, cuando expresó: «Ahora en Siria estamos operando en el más agresivo ambiente de EW del planeta. Cada día nos ofrecen un nuevo reto, tiran nuestras comunicaciones o inhabilitan nuestras aeronaves de EW, etcétera»[10].

De esta forma, crea una nueva forma de confrontarnos, mucho más sutil y sibilina. Nace una forma diferente de contrarrestar el tremendo potencial de los Estados Unidos en lo que se refiere a las capacidades militares. Los occidentales codificamos esta forma de friccionar como los conflictos propios de la zona gris y/o estrategias híbridas. El doctor Jordán define la zona gris como «un espacio intermedio en el espectro de conflicto político que separa la competición acorde con las pautas convencionales de hacer política, del enfrentamiento armado directo y continuado»[11].

Los países que pertenecen a la Alianza se afanan, promulgando sesudos estudios, en explicar ese comportamiento de la Federación Rusa. Aplican el método analítico de lo ocurrido para desglosarlo en partes menores y comprenderlo mejor, considerando que es rígido y estático. Sin embargo, nuestros adversarios modifican esa misma forma de friccionar y migran a otros modelos más sofisticados, adaptados al entorno al que van a combatir, aplican las lecciones aprendidas y mejoran sus procesos con mucha agilidad. Esta forma de actuar les permite adquirir ventaja táctica; la prospectiva y la actitud proactiva se antojan esenciales para poder dominar este escenario.

Las operaciones electromagnéticas

Las OEM hallan perfecto acomodo en este tipo de conflictos, que las habilitan como un instrumento adecuado para alcanzar los objetivos estratégicos que los Estados persiguen. La razón esencial de esta afirmación es que estas operaciones participan de muchas de las características que conforman los conflictos que transcurren en la zona

[10] CLARK, Colin. «Russia Widens EW War, 'Disabling' EC-130s OR AC-130s In Syria», *Breaking Defense - Defense industry news* (análisis y comentario), mayo de 2018. Disponible en: https://breakingdefense.com/2018/04/russia-widens-ew-war-disabling-ec-130s-in-syria/ (Consultado el 13/1/2021).
[11] JORDÁN, Javier. «El conflicto internacional en la zona gris: una propuesta teórica desde la perspectiva del realismo ofensivo», *Revista Española de Ciencia Política*, mayo 2018. Disponible en: https://ugr.es/~jjordan/Conflicto-zona-gris.pdf (Consultado el 13/1/2021).

gris, como por ejemplo la ambigüedad o la dificultad en la atribución de las acciones electromagnéticas.

Por otra parte, el abanico de capacidades que aglutinan las OEM es inmenso, en especial porque se conforma por un conjunto de factores que no solo satisfacen la demanda de seguridad más allá de la tradicional guerra regular, sino que cubren otros campos como los híbridos o los propios de la mencionada zona gris. Es, por lo tanto, un instrumento ideal para aplicar en los entornos operativos actuales (y con más intensidad en los futuros) que se describen tanto a nivel nacional como a nivel OTAN[12].

La definición de las OEM ha llevado a muchas horas de discusión en el seno de los grupos de trabajo de la OTAN. Este documento no pretende explicar las numerosas aristas conceptuales de la definición oficial sino simplificar el concepto en aras de una mejor comprensión de este término en los legos de la materia. Por ello, utilizaremos la siguiente definición para las OEM: «El uso de la energía electromagnética para fines ofensivos y defensivos». Aunque no es la oficialmente aceptada, es la que mejor captura la esencia de las operaciones electromagnéticas[13] para una audiencia no experta.

Con la energía del espectro, la panoplia de acciones que se pueden llevar a cabo es innumerable, por eso el ámbito de actuación de las OEM es muy amplio. Este ámbito abarca cualquier uso que pretendamos dar de la energía electromagnética[14] que se encuentra presente en el espectro.

Además, y de forma sencilla, las OEM se pueden entender como la traslación de los efectos y acciones[15] propios de la tradicional EW a los diferentes ámbitos de operación:

[12] Por ejemplo, el documento de ACT de la OTAN *Framework for Future Alliance Operations*, que describe los escenarios futuros en los que la OTAN debe desenvolverse y que, como una de las conclusiones, propugna potenciar la guerra electrónica. Disponible en: https://www.defensa.gob.es/ceseden/Galerias/ccdc/documentos/2018_NATO_FFAO_Report.pdf (Consultado el 13/1/2021).
[13] La definición acordada por los países OTAN en el AJP 3.6.Ed C Ver 1 es: «All operations that shape or exploit the electromagnetic environment, or use it for attack or defence including the use of the electromagnetic environment to support operations in all other operational environments». En castellano se puede traducir por: «Todas aquellas operaciones que modelan o explotan el entorno electromagnético, o lo usan para atacar o defender incluyendo el uso del entorno electromagnético en apoyo a las operaciones».
[14] Es importante apreciar cómo esta nueva concepción del espectro que se centra en energía cambia el modelo cultural que hasta ahora se había mantenido, que se centraba en frecuencias, básicamente en gestionar las frecuencias.
[15] Las acciones propias de la EW son la *electronic attack* (EA), *electronic defence* (ED) y *electronic surveillance* (ES), conforme a la doctrina ratificada e implementada de España AJP 3.6. Ed. C Ver. 1 sobre *Allied Doctrine for EW*.

el terrestre, el marítimo, el aeroespacial, el cognitivo y el ciberespacial, sin olvidar los ámbitos mixtos[16].

Pongamos algunos ejemplos que nos permitan alcanzar el potencial de las OEM en el ámbito militar. En el campo de la información, muchas de las comunicaciones se desarrollan por el éter gracias a circuitos que aprovechan las microondas. Casi la totalidad de las comunicaciones militares en operaciones utilizan el espectro. La información se transmite por las ondas y está disponible para cualquier usuario que disponga de tecnología para interceptar esa comunicación. En muchas ocasiones, esta comunicación está exenta de dispositivos que la cifren o que simplemente la codifiquen, lo que simplifica el acceso a la información. Conocer lo que habla el adversario proporciona automáticamente una sustancial ventaja a todos los niveles, desde el táctico al estratégico. El futuro nos hace incluso más vulnerables, puesto que los avances tecnológicos, como la capacidad de procesamiento de la inteligencia artificial, ponen en jaque circuitos encriptados o decodificados.

Incluso seríamos capaces de traspasar las fronteras de lo militar e introducirnos en las comunicaciones en el ámbito civil, como las redes sociales o incluso los mensajes de WhatsApp de los soldados que luchan en el frente. En principio, basta con colocar un poste de comunicaciones en sus cercanías que capture las señales de nuestros móviles. En el conflicto de Ucrania, las familias de los generales reciben atentos mensajes de las redes sociales, algunos hasta utilizan Telegram[17], desarrollado por dos empresarios rusos. También podemos adoptar un perfil ofensivo perturbando las comunicaciones, los radares o utilizando la energía para realizar interferencias provocadas sobre dispositivos electrónicos, o incluso podemos radiar energía centrada en las frecuencias que gobiernan los autómatas de esos sistemas para dejarlos inoperativos.

La eficacia de estas operaciones se ha podido comprobar en los conflictos de Ucrania y Siria, con el comportamiento de la Federación Rusa, que nos adelanta una nueva morfología de los conflictos, donde el espectro electromagnético juega un papel esencial. No es solo el conocido problema de la congestión del espectro, sino también la confrontación de este. La facilidad que antaño teníamos en el acceso y en el libre uso

[16] Los ámbitos de operación vienen determinados en la PDC 01 (A). Existen zonas de contacto o de intensa interacción entre ámbitos, físicos y no físicos, que dan lugar a ámbitos mixtos, como el litoral, el aeroterrestre, el aeronaval o los que generan el ámbito ciberespacial y el cognitivo, como las redes sociales, transversales al resto de ámbitos.
[17] Telegram es una plataforma de mensajería y VOIP desarrollada por los hermanos Nikolái y Pável Dúrov.

del espectro se ha desvanecido. Esta amenaza ha llevado a pensar en países del norte de Europa, a la necesidad de militarizar el espectro para garantizar su uso por parte de la población civil.

A nadie se le escapa que la libertad de maniobra en el espectro electromagnético es un prerrequisito para la conducción de las operaciones. En estos escenarios, su acceso está confrontado de tal manera que se ha convertido en un verdadero campo de batalla. Un entorno, el electromagnético, que condiciona al resto de ámbitos declarados en la doctrina nacional: el terrestre, el marítimo, el aeroespacial, el ciberespacial y el cognitivo[18].

Este nuevo espacio de confrontación, el entorno electromagnético, lleva sus operaciones asociadas, las OEM. Mientras nuestra aproximación al espectro siempre fue de la mano de las frecuencias, en este caso el término de referencia es la energía electromagnética, pues captura mejor la naturaleza de este tipo de operaciones.

Hablamos de energía anteriormente y dejamos de referirnos a frecuencias. El uso de la energía en el éter puede también convertirse en una herramienta ofensiva interesante, por ejemplo, con las armas de energía dirigida que proliferan en la actualidad y que tienen un uso multifacético. Armas que viajan a la velocidad de la luz, sin daños colaterales gracias a su tremenda precisión, muy económicas en el uso, con complicada atribución al no ser visibles ni apenas detectables. Son incluso ecológicas, puesto que no dejan residuos al llevar a cabo la acción ofensiva.

La fragilidad de la arquitectura de seguridad y defensa occidental

Los efectos de las OEM desbordan los ámbitos puramente militares y adquieren una dimensión mucho mayor, entrando de pleno a condicionar las esferas políticas. En especial porque son capaces de degradar algo tan preciado en las sociedades occidentales como el bienestar de los ciudadanos. Adquieren relevancia como un instrumento ideal dentro de lo que se ha venido denominando *political warfare*. Un término pasado que vuelve a adquirir protagonismo. Para definirlo me adhiero a un

[18] Estos ámbitos son los declarados por la PDC 01 A sobre la doctrina para el empleo de las FAS de 27 de febrero de 2018.

reciente informe de Rand Coorporation[19] que indica que «la guerra política consiste en el uso intencionado de uno o más instrumentos de poder (diplomático, información, militar y económico) para condicionar la composición política o el proceso de toma de decisiones a nivel político en un Estado».

Los Estados occidentales son unos consumidores compulsivos de seguridad. Una vez tienen garantizados aspectos fundamentales como la libertad o los derechos, se aferran a garantizar otros más complejos de proteger como el bienestar, que, en clave nacional, también entra dentro del concepto de seguridad nacional[20].

Una vez definidas y parcialmente comprendidas las OEM, la cuestión es saber cómo pueden influir estas operaciones al proceso de toma de decisiones a nivel político. Pero antes es conveniente analizar someramente la arquitectura de seguridad en la que confiamos los países occidentales, en especial a lo relativo al uso de la fuerza. Una arquitectura de seguridad y defensa que está cuestionada por muchos e incluso se afirma que podría estar cerca de su colapso[21].

Los Estados responden ante las amenazas y riesgos a la población mediante un sistema de asignación de competencias a las diferentes autoridades y Administraciones públicas. Para hacer frente a los desafíos y amenazas, el Estado debe articular mecanismos para responder ubicándolos en dos cestos. Por un lado, los retos compartidos; y, por otro, los exclusivos, pues tienen diferente resolución. Por regla general, las amenazas compartidas se resuelven en los foros de las Organizaciones Internacionales de Seguridad y Defensa (OISD) aplicando estrategias multilaterales gracias al firme compromiso de sus miembros, mientras que las amenazas no compartidas es necesario atenderlas en el ámbito local o, en el menor de los casos, regional.

De esta forma, la *political warfare* debe atender a ambas lógicas, la nacional y la exterior, puesto que los objetivos de las FAS se determinan considerando ambos prismas, en particular en el segundo, de acuerdo con nuestros compromisos y vocación internacional

[19] ROBINSON, Linda *et al. Modern. Political Warfare: Current Practises and posible responses*. Santa Monica: Rand Corporation.
[20] De acuerdo con la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, en su artículo 3 define la seguridad nacional como la «acción del Estado dirigida a proteger la libertad, los derechos y bienestar de los ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos».
[21] YESTE, Miguel P. *Defensa europea: fin del paradigma y los riesgos de dejarse llevar*. Documento de Opinión IEEE 71/2018. Disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2018/DIEEEO71-2018_DefensaEuropea_MPecoYeste.pdf

y la promoción de un multilateralismo eficaz; es decir, tiene que ser capaz de condicionar el proceso de toma de decisiones a nivel nacional y a nivel de las organizaciones internacionales, que han cobrado un protagonismo mucho mayor de la mano de la globalización.

Aunque el instrumento militar puede ser utilizado como una medida coercitiva, no siempre puede condicionar la toma de decisiones. Traigo como ejemplo las operaciones de defensa colectiva contempladas en el artículo 5 del Tratado de Washington[22], que crea la Alianza. La defensa colectiva de la OTAN ha sido durante estos años el verdadero azote de cualquier intento de uso del instrumento militar contra algún país miembro de la Alianza. Agresiones de esta naturaleza no son aceptadas por el Consejo de Seguridad de las Naciones Unidas (CSNU), y para la mayoría de los países sería causa de una fuerte represalia.

Se habla con frecuencia de este artículo 5, pero muy poco del artículo 4, sobre consultas, que dice textualmente: «Las Partes se consultarán cuando, a juicio de cualquiera de ellas, la integridad territorial, la independencia política o la seguridad de cualquiera de las Partes fuese amenazada». Se ha invocado cuatro veces a petición de Turquía, en tres ocasiones con las guerras de Irak y de Siria, y también por parte de Polonia, en marzo de 2014, al considerar que los acontecimientos en Ucrania amenazan la integridad territorial, la independencia política y la seguridad de los Estados vecinos que eran miembros de la Alianza.

Artículo 4, que es esencial para activar el artículo 5 de defensa colectiva. En las consultas se proporcionarán las razones de suficiente calado para que los países adquieran un compromiso en tomar una acción colectiva, normalmente de carácter militar. Con independencia de las razones que se aduzcan, la cuestión es que el proceso vendrá condicionado por las capitales, que habrán predeterminado su posición después de un estudio meticuloso de las implicaciones que tiene emprender una acción militar contra determinado adversario. Especialmente complejo sería si el agresor es un país miembro del CSNU con derecho a veto, o simplemente un país amparado por alguno miembro permanente del CSNU.

[22] NATO. *The North Atlantic Treaty, 04-Apr.-1949*. Disponible en: https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=es (Consultado el 13/1/2021).

En las organizaciones internacionales, la toma de decisiones se suele gobernar por consenso después de un proceso complejo y proceloso. Incluso la OTAN, que, *a priori*, es de las organizaciones internacionales con más agilidad en el proceso de toma de decisiones, tiene verdaderos problemas en adoptar decisiones de calado con el compromiso unánime de sus miembros, «pues no todos los aliados, a pesar de ser aprobadas por ellos, participarán con la intensidad y capacidades requeridas»[23].

Juega en franca desventaja que nuestros procedimientos en el uso del instrumento militar guardan un escrupuloso respeto a la legalidad internacional y también a la nacional. Los militares no gozan del derecho ilimitado de la aplicación de la fuerza, sino que su aplicación es controlada por instrumentos que se gobiernan desde el nivel político. Por ejemplo, las reglas de enfrentamiento, las restricciones o *caveats*, las propias órdenes operativas o directrices o por la propia cultura de los ejércitos occidentales.

De esta forma, en el proceso de la decisión relativa al uso del instrumento militar juegan factores como la certeza en la atribución de la agresión o la determinación clara del objetivo, con una reducción de los daños colaterales y minimizar los potenciales efectos que la acción pudiera tomar en los intereses de nuestro país. Además, la ambigüedad durante el proceso de consultas no suele dar como resultado una firme posición común solidaria con el que sufre la agresión. Estas características son especialmente relevantes en el uso de las OEM en los conflictos. Las acciones electromagnéticas pueden tener un impacto estratégico, en muchas ocasiones no es posible determinar la fuente de la agresión y se mueven en la niebla propia de la guerra, en la ambigüedad, escenario que los occidentales tenemos aversión a darle una respuesta con el instrumento militar.

Las OEM, una navaja multiusos

Las OEM explotan las vulnerabilidades que dejan los avances tecnológicos, un pilar fundamental de nuestro desarrollo y de nuestro estado de bienestar. De esta forma, la tecnología es capaz de perfilar la morfología de los conflictos además de erigirse como en elemento esencial en los nuevos escenarios de confrontación, como por ejemplo el electromagnético. Existe un cambio sustancial con respecto a las campañas de Irak,

[23] BLASCO, F. Javier. «Las dificultades de la OTAN actual a la hora de tomar decisiones», *Kosmos-Polis*. Disponible en: https://sites.google.com/site/articulosfjavierblasco/las-dificultades-de-la-otan-actual-a-la-hora-de-tomar-decisiones (Consultado el 13/1/2021).

donde la supremacía tecnológica fue un factor decisivo y asentó el concepto de Revolución en los Asuntos Militares. En este caso, la diferencia estriba en que la tecnología proporciona herramientas para confrontar esa superioridad tecnológica de los países occidentales y se reduce la brecha tecnológica entre los Estados Unidos y las naciones revisionistas. Se ha demostrado que el problema se acucia cuando esos desarrollos tecnológicos están al alcance de cualquiera, también de los actores no estatales.

La cuestión es que las sociedades son cada día más dependientes del espectro, gran parte de la globalización se soporta gracias a la tecnología inalámbrica[24]. Con la llegada de la tecnología de quinta generación o 5G se multiplicará la capacidad de las autopistas de la información, se alcanzará en poco tiempo el mito de las ciudades hiperconectadas. Las nubes alojarán una cantidad ingente de datos que nos proporcionará saber, por medio de nuestro móvil y en tiempo real, la temperatura de nuestra nevera, la posición del móvil de nuestro hijo, de nuestro automóvil o de la cantidad de amperios que consume nuestra casa. Un mundo inmenso de bienestar y desafortunadamente repleto de vulnerabilidades.

La disputa por gobernar esta tecnología es frenética, pues el dato se erige como el nuevo petróleo del futuro y está conformando por sí solo un nuevo escenario de confrontación entre los Estados más poderosos. Para abordar este reto, los Estados Unidos han promulgado recientemente una estrategia específica que le garantice la superioridad en el espectro electromagnético[25].

Es quizá la vulnerabilidad de los sistemas GNSS el paradigma de que la tecnología ofrece extraordinarios beneficios, pero conlleva un nivel de vulnerabilidades que son fácilmente explotables por parte de cualquiera, lo que convierte a casi cualquier ciudadano en un potencial terrorista.

[24] Con tecnología inalámbrica no solo hay que pensar de las redes wifi que gobiernan muchos sistemas actuales, por ejemplo, las casas domóticas, los sistemas de detección mediante cámaras; también hay que incluir las diferentes constelaciones de satélites que día a día proporcionan más capacidades. También todos aquellos elementos que son capaces de transmitir datos, como los teléfonos o puntos de acceso o dispositivos en hospitales. En un mundo hiperconectado, el ritmo de datos por el éter se incrementa exponencialmente.

[25] La estrategia se promulgó en octubre del pasado año con la denominación Electromagnetic Superiority Spectrum Strategy. Nota de prensa, así como la estrategia, se encuentran disponibles en: https://www.defense.gov/Newsroom/Releases/Release/Article/2397850/electromagnetic-spectrum-superiority-strategy-released/ (Consultado el 13/1/2021).

La denegación del sistema de posicionamiento global (GPS, por sus siglas en inglés) es un claro ejemplo de los efectos que se pueden conseguir con estas operaciones. Los perturbadores de la señal GPS imposibilitan la llegada al receptor de la señal de posición y la de sincronismo, que provoca un efecto nocivo impredecible en otros sectores, pues gran parte de los equipos digitales disfrutan de esta señal.

Esta vulnerabilidad a los sistemas GNSS ha sido cuantificada por varias naciones. Los informes públicos que ofrecen más detalle de las pérdidas económicas, en los diferentes sectores, por una denegación del GPS, son los que proporcionan los Estados Unidos[26] y el Reino Unido[27].

Las tablas I y II son un extracto de ambos informes, que dan muestra de las numerosas pérdidas que la ausencia de señal GPS provoca en las sociedades más avanzadas.

Infrastructure	Aspect	RAG	Loss of GVA (direct+secondary) (five days)	Loss of utility benefits (five days)
Space	Satellite communications		£22.5m	*See Maritime transport infrastructure*
Transport infrastructure	Maritime transport infrastructure		£1,069.3m	*See Maritime usage applications*
Application	**Aspect**	**RAG**	**Loss of GVA (direct+secondary) (five days)**	**Loss of utility benefits (five days)**
Surveying	All applications		£344.8m	£-
Rail	Automatic train doors			£2.8m
	Train cancellations		£77.7m	£12.7m
Road	Navigation		£-	£1,869.7m

Tabla 1. Pérdida económica en determinados sectores ante una denegación de GPS de UK. Fuente. *London Economic*. «GVA: Gross Value-added».

La realidad es que vivimos en un mundo progresivamente dependiente del espectro. Existen iniciativas ambiciosas, como la financiada por la UE denominada AUToSHIP[28] (Autonomous Shipping Initiative for European Waters), que tiene como objetivo una flota

[26] El informe es del Instituto Nacional de Tecnología de los Estados Unidos. Disponible en: https://www.rti.org/sites/default/files/gps_finalreport.pdf (Consultado el 13/1/2021).
[27] El informe es de la Coorporación London Economics. Disponible en: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/619544/17.3254_Economic_impact_to_UK_of_a_disruption_to_GNSS_-_Full_Report.pdf (Consultado el 13/1/2021).
[28] Disponible en: https://www.autoship-project.eu

de barcos no tripulados. Durante este año se han realizado dos pruebas con diferentes barcos. La primera, más simple, se acometió en aguas interiores, y la segunda a mar abierto entre países del norte de Europa.

Sector	Specific Analytical Focus	Potential Losses ($ million)
Electricity	Electrical system reliability and efficiency	$275
Finance	High-frequency trading	Negligible
Location-based services	Smartphone apps and consumer devices that use location services to deliver services and experiences	$2,859
Mining	Efficiency gains, cost reductions, and increased accuracy	$949
Maritime	Navigation, port operations, fishing, and recreational boating	$10,411
Oil and gas	Positioning for offshore drilling and exploration	$1,520
Surveying	Productivity gains, cost reductions, and increased accuracy in professional surveying	$331
Telecommunications	Improved reliability and bandwidth utilization for wireless networks	$9,816
Telematics	Efficiency gains, cost reductions, and environmental benefits through improved vehicle dispatch and navigation	$4,137

Tabla 2. Pérdida por denegación de GPS, durante un mes, en determinados sectores en los EE. UU. Fuente. RTI Internacional.

España tiene el compromiso de adherirse a esta iniciativa que, en unos años, permitirá que proliferen barcos sin dotación. Llama poderosamente la atención que se deje en manos del espectro electromagnético la navegación de decenas de mercantes, pues a través del espectro se remiten las órdenes de gobierno de los buques.

La inhibición de los GNSS se ha convertido en una herramienta más encuadrada dentro de lo que el jefe de Estado Mayor ruso, Valery Gerasimov, explicaba[29] para alcanzar los objetivos de la campaña, mediante otros medios, sin recurrir al tradicional uso de la fuerza: «El papel de los medios no militares para conseguir objetivos políticos y estratégicos ha crecido y, en muchos casos, su eficacia es mayor que el poder de las armas».

En este terreno las OEM proporcionan un sustento a lo que la Federación rusa denomina disuasión estratégica[30] pues los efectos que se pueden conseguir con las OEM son coercitivos para cualquier nación y es compleja la respuesta incluso en el formato de la autodefensa.

[29] GERASIMOV, Valery. «The Value of Science is in the Foresight», *Military Review*, vol. 96, 2016.
[30] LABOIRE, Mario. *La estrategia de seguridad nacional de la Federación Rusa*. Documento de Opinión IEEE 25/2016. Disponible en: http://www.ieee.es/en/Galerias/fichero/docs_opinion/2016/DIEEEO25-2016_ESN_Rusia_MLI.pdf (Consultado el 13/01/2021).

Hemos analizado tan solo una de las vulnerabilidades, derivada del uso masivo de la tecnología aplicada al espectro que proviene de los sistemas de posicionamiento global, pero las vulnerabilidades en el espectro de las sociedades occidentales son innumerables. Hablemos, por ejemplo, de la energía electromagnética para usos ofensivos. Nos encontramos ante el suculento mercado de las armas de energía dirigida, armas que viajan a la velocidad de la luz, no dejan trazabilidad y es complicada su atribución, se mueven en ese oscuro terreno de la ambigüedad.

Existen también, dentro de este mercado, dispositivos que permiten inutilizar los procesadores que se encuentren a su paso. No es ciencia ficción, sino que se vende por parte de la empresa americana BOEING[31]. Se denomina CHAMP (*counter-electronics high-powered microwave advanced missile project*). Consiste en un haz de energía dirigida, es inocuo para el ser humano, pero inutiliza los procesadores que se encuentra a su paso. Utilizar este dispositivo en un aeropuerto o en una ciudad puede, desde luego, producir efectos devastadores. La atribución de la acción sería realmente compleja. Es, por lo tanto, una posibilidad muy a tener en cuenta[32].

El abanico de posibilidades que presenta el uso de la energía electromagnética es desbordante, solo hace falta apelar a la imaginación de cada uno para advertir las numerosas vulnerabilidades que las sociedades occidentales presentan en el espectro. En clave de conflicto militar, hay que simplemente seguir las indicaciones de Gerasimov[33] y apelar a la creatividad: «En conclusión, quería decir que no importan las fuerzas de que disponga el enemigo, no importa lo bien preparadas que estén ni los conflictos armados que sean, maneras y métodos de vencerles pueden ser encontrados. Siempre tendrá vulnerabilidades, lo que nos indica que existen medios adecuados para confrontarlo».

CHAMP es lo que se denomina un *game changer*, pues cambia sustancialmente la forma de combatir. Es una capacidad extraordinariamente compleja de confrontar que genera un daño económico de dimensiones dantescas. Una mera pasada por la ciudad de

[31] Disponible en: https://www.boeing.com/features/2012/10/bds-champ-10-22-12.page
[32] CASTRO, Jose Ignacio. *El impulso electromagnético y las armas de radiofrecuencia: La vulnerabilidad de las sociedades evolucionadas*. Documento de Análisis 16/2018. Disponible en: http://www.ieee.es/Galerias/fichero/docs_analisis/2018/DIEEEA16-2018_Impulso_Electromagnetico_JICT.pdf (Consultado el 13/1/2021).
[33] *Ibid.*

Madrid sería capaz de cerrar el aeropuerto de Madrid Barajas Adolfo Suárez o la estación de Atocha. Un elemento más que contribuye a la disuasión estratégica.

Aunque siempre podemos pensar que este escenario no va a tener lugar porque la respuesta de la comunidad internacional sería de tal calado que ahuyente al agresor a tomar esa medida. Algo similar a la destrucción mutua asegurada que tanta estabilidad proporcionó en los tiempos de la Guerra Fría. Sin embargo, es del todo diferente, pues la atribución del ataque es mucho más compleja y la herramienta (en menor escala) puede estar en manos de actores no estatales, o un actor estatal decidir realizar una agresión mediante un *proxy*. Las OEM se convierten en un paradigma perfecto alineado con la Estrategia Nacional de Seguridad de la Federación Rusa[34]: «La utilización de la fuerza militar para proteger los intereses nacionales es posible solo si adoptando todas las medidas de naturaleza no violenta se han mostrado ineficaces».

Supongo que esta deducción era similar a la que adoptó Estonia en 2007 cuando sufrió el mayor ciberataque de la historia, que paralizó por completo el país báltico.

Las alarmas han saltado

La prospectiva es, sin lugar a duda, complicada. Adivinar qué es lo que puede ocurrir en un mundo gobernado, en las relaciones internacionales, por la anarquía es, sin duda, arriesgado, por no decir imprudente. Tras la caída del muro de Berlín, una de las conclusiones es que las fronteras ya no serían modificadas, puesto que existían instrumentos internacionales para poner orden y concierto en el sistema internacional. Todo ello respaldado por el hegemón único y todopoderoso de los Estados Unidos.

La realidad del desmembramiento de Yugoslavia, la independencia de Kosovo —reconocida por algunos países, entre los que no se encuentra España— y los recientes sucesos de Crimea o el Donbás demuestran lo aventurado y arriesgado de la prospectiva en las relaciones internacionales.

La cuestión es que países de Europa perciben a la Federación Rusa[35] como una amenaza, mientras que los Estados ribereños del Mediterráneo consideramos esa

:[34] Disponible en: http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf (Consultado el 13/1/2021).
[35] NORBERG, Johan. «Training for war- Russian's strategic Level military exercises 2019-2017», *Swedish Defence Research Agency FOI*. Disponible en: https://www.foi.se/report-summary?reportNo=FOI-R--4627--SE

percepción como una evaluación exagerada. Este artículo no pretende ahondar en el proceloso mundo de la prospectiva, pero invita a reflexionar sobre la aproximación que adoptan algunos países como Suecia, que eleva el gasto militar en un 40 % y que, además, incrementa sus Fuerzas Armadas de 40 000 hombres a 90 000[36].

Recientemente, la OTAN ha promulgado un interesante documento[37] donde refleja el tanto por ciento de gasto en defensa de los diferentes países de la Alianza. Refleja que solo ocho países cumplen los criterios de la Cumbre de Gales de la OTAN de asignar un 2 % del PIB. Estos son: Noruega, Francia, Polonia, Rumanía, Letonia, Lituania, Estados Unidos y Reino Unido. Si a estos les unimos Suecia y Finlandia, tenemos una clara indicación de qué países geográficamente sienten necesidad de incrementar su potencial militar.

Estos países no parece que confíen en la eficacia del multilateralismo derivada de la cohesión de los miembros de las organizaciones internacionales a las que pertenecen. La arquitectura de seguridad de los europeos tiene mucho con ver con el neoliberalismo institucional, que considera que el multilateralismo aporta estabilidad en las relaciones internacionales. Desafortunadamente, no parece que estemos en este caso.

Y la cuestión no debe ser si un determinado país va a sufrir una agresión de una potencia mundial, que no parece probable. El debate debería atender otras consideraciones, por ejemplo, si capacidades que engloban las OEM pueden ser utilizadas por organizaciones terroristas o por países que no entran dentro del término *amenaza compartida* desde el prisma nacional.

La cuestión sería determinar si existe un nivel suficiente de concurrencia de los aliados en una respuesta contundente contra un adversario que realiza una agresión desde el espectro con fuertes dosis de ambigüedad y compleja atribución. Y también debería llevarnos a una profunda reflexión si nuestro Sistema de Seguridad Nacional está preparado para una combinación de esta agresión con otras medidas coordinadas en el ámbito político, diplomático, militar, económico o informativo.

[36] MAIZ, Julio. «El mar Báltico cada vez más caliente, la escalada militar del norte de Europa». *Defensa.com*, diciembre de 2020. Disponible en: https://www.defensa.com/otan-y-europa/mar-baltico-cada-vez-mas-caliente-suecia-aprueba-aumento-40 (Consultado el 13/1/2021).
[37] Disponible en: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/10/pdf/pr-2020-104-en.pdf (Consultado el 13/1/2021).

En la madrugada del 20 de septiembre del 2018, el puerto de Barcelona recibió un ciberataque contra los servidores que gestionan el tráfico marítimo de uno de los principales puertos de España y de Europa. El plan de contingencia permitió superar el teórico desastre que hubiera supuesto cerrar el puerto al tráfico de mercancías. No se conoce hasta ahora respuesta de la comunidad internacional ni tampoco sanciones a ninguna organización. La falta de atribución complica los procesos judiciales o simplemente los imposibilita.

Habría que plantearse el impacto operativo del puerto con la señal GPS denegada que anulara las señales de posición y de sincronismo que gobiernan muchos equipos y sistemas de puerto. Parece una entelequia, pero ha ocurrido en Estados Unidos, en un aeropuerto de Newark donde un trabajador se dejó por error un dispositivo inhibidor de la señal de GPS en el aeropuerto[38]. Un simple dispositivo de 40 euros deja en jaque un aeropuerto. Más de 38 000 dólares de multa para el autor de esta pequeña torpeza.

Los países nórdicos y eslavos tienen otra percepción porque sufren a diario injerencias en su territorio que demuestran su vulnerabilidad. Aunque consideremos que pueden entrar en lo que denominamos *amenaza compartida*, es complejo que los mecanismos de toma de decisiones en el uso de la fuerza les proporcionen protección suficiente. El CSNU está condicionado por el voto particular con derecho a veto de los miembros permanentes. En clave de la OTAN, es complejo que exista consenso en una respuesta contundente con el instrumento militar cuando la ambigüedad o falta de atribución de la agresión es significativa.

El uso de la fuerza demanda una clara atribución de la acción del adversario que permita ganar consenso sobre la acción a tomar cuando se active el artículo 4 del Tratado de Washington. La maraña de cuestiones legales y de intereses políticos complicará la decisión de activar el artículo 5 y nos veremos atrapados en nuestro laberíntico proceso de toma de decisiones para autorizar la aplicación de la fuerza. Nos sumergiremos a entablar interminables diálogos jurídicos y los árboles no nos dejarán ver el bosque, mientras que el adversario se moverá rápidamente, con un catálogo de normas diferentes, dejando nuestra respuesta en la inoperancia.

[38] La noticia está disponible en: https://www.nj.com/news/2013/08/man_fined_32000_for_blocking_newark_airport_tracking_system.html (Consultado el 13/1/2021).

La Doctrina Gerasimov, recurrentemente utilizada por los *scholars* occidentales, simplemente no existe como la presentamos en Occidente, encorsetada en un diseño específico, sino que se adapta al entorno buscando las debilidades y vulnerabilidades del adversario utilizando todos los instrumentos del Estado en aras de conseguir alcanzar los objetivos políticos. Tan simple como eso, pero tan complejo de confrontar con nuestra deontología occidental.

Es tan antigua como el arte de la guerra, que encuentra en el ingenio y la creatividad una de las herramientas que nos lleva a doblegar al enemigo a pesar de tener dominio militar. Ya lo dice Gerasimov: «Una aproximación hacia nuevas ideas, no comunes, hacia otros puntos de vista, es inaceptable en la ciencia militar. E incluso es más inaceptable que tengan esa actitud hacia la ciencia para los que se incorporan al mundo militar».

Conclusión

Las operaciones electromagnéticas, de la mano de los avances tecnológicos, diseñan una nueva morfología de los conflictos y modelan un escenario de confrontación dinámico y muy complejo. Un campo de batalla muy difícil de confrontar, básicamente motivado por la disimetría de normas en la utilización del instrumento militar de ambos contendientes.

La ambigüedad de las operaciones electromagnéticas, su complejidad en determinar la atribución de una acción ofensiva, así como la capacidad de alcanzar efectos estratégicos sin el uso de la fuerza, hallan perfecto acomodo en las estrategias híbridas o en los conflictos que se desarrollan en la zona gris. Un arte de la guerra que cuenta con las operaciones electromagnéticas y que logra reducir la importante brecha en capacidades militares con respecto a los Estados Unidos.

Las OEM participan de estrategias diseñadas *ad hoc*, que se basan en el ingenio y la creatividad en la utilización de todos los instrumentos de poder del Estado. Y dentro de ellos, las OEM se han demostrado muy eficaces para alcanzar los objetivos políticos. El verdadero problema es que esta capacidad está al alcance de cualquier Estado y, también, de los actores no estatales.

La resolución de los conflictos por vía del multilateralismo, auspiciado por las OISD, está en franca decadencia por diversos motivos.

En primer lugar, por el auge de los intereses nacionales; en segundo, por la falta generalizada de compromiso de los miembros de las OISD en garantizar una sólida actuación común; y en tercer lugar, por la disuasión estratégica, que condiciona el proceso de toma de decisiones política en todos los ámbitos, tanto nacional como internacional.

El resultado final es que se resquebraja la solidaridad entre las naciones que soportan el sistema internacional liberal, con el consiguiente debilitamiento del multilateralismo. Debilitar el multilateralismo tiene su impacto en la gobernanza global, que se materializa en la incapacidad de utilizar los mecanismos necesarios para confrontar a los Estados revisionistas.

En este escenario corren malos tiempos para aquellos que piensan que disponer de capacidades militares es un gasto superfluo. En un sistema internacional, de carácter hobbesiano, aproximaciones cándidas al pensar que no existe interés en debilitar a España pueden pasar factura. Quizá otras naciones se estén equivocando en incrementar sustancialmente sus gastos en defensa, pero esta aproximación, al menos, debe invitar a la reflexión. Pero, una vez más, lo importante es que juntos somos más fuertes, pero poco más; lo mejor es estar unidos y seremos invencibles.

*Ignacio Nieto Fernández**
Jefe del Centro de Operaciones Electromagnéticas
Mando de Operaciones