CIBER ELECTROMAGNETIC ACTIVITIES,

LA NUEVA VERSIÓN DE LA GUERRA DIGITAL

Me despierta la claridad de la mañana que entra con fuerza por la ventana del dormitorio, señal inequívoca de que me he dormido. Rápidamente me dirijo a la ducha maldiciéndome por no haber configurado la alarma del dichoso móvil.

Entro al baño y segunda sorpresa del día, no hay luz. Aunque entra claridad del vecino dormitorio, toca ducha fría ya que la caldera precisa de la energía eléctrica para funcionar.

Con un pésimo humor y poco tiempo que perder, me encamino a oscuras hacia la calle –la opción de usar mi vehículo queda descartada ya que la puerta del garaje se acciona mediante corriente eléctrica y parece que el corte afecta a todo el bloque–.

Mientras me dirijo a pie hasta la cercana parada de autobuses, tiro de móvil para llamar al trabajo y avisar de que voy de camino, pero para mi sorpresa, recibo la alocución de que no hay línea.

Aún a pesar de tener la cabeza pesada por la ausencia de cafeína y de la ducha reglamentaria, una extraña sensación empieza a cobrar presencia en mi cabeza, tanto corte eléctrico no puede ser casual.

Sirenas de coches patrulla ululan cada poco tiempo en las calles aledañas, aumentando mi sensación de que algo no está bien. Ya en la parada de autobuses, los cariacontecidos usuarios buscando cobertura para sus móviles confirman mis sospechas de que algo grave pasa…

Semejante obertura que podría resultar ideal para un guion de Hollywood o para la siguiente novela de Dan Brown, no hace sino poner de manifiesto la gran dependencia que tiene nuestra sociedad de la energía eléctrica y todas las tecnologías que la usan, representadas de forma significativa en la dependencia de los *smartphones* y sus múltiples funcionalidades –despertador, enlace de comunicaciones voz, aplicaciones vía Internet etc– que usamos de forma diaria y profusa.

Miguel Antonio Castro Arjona
Capitán del Ejército del Aire

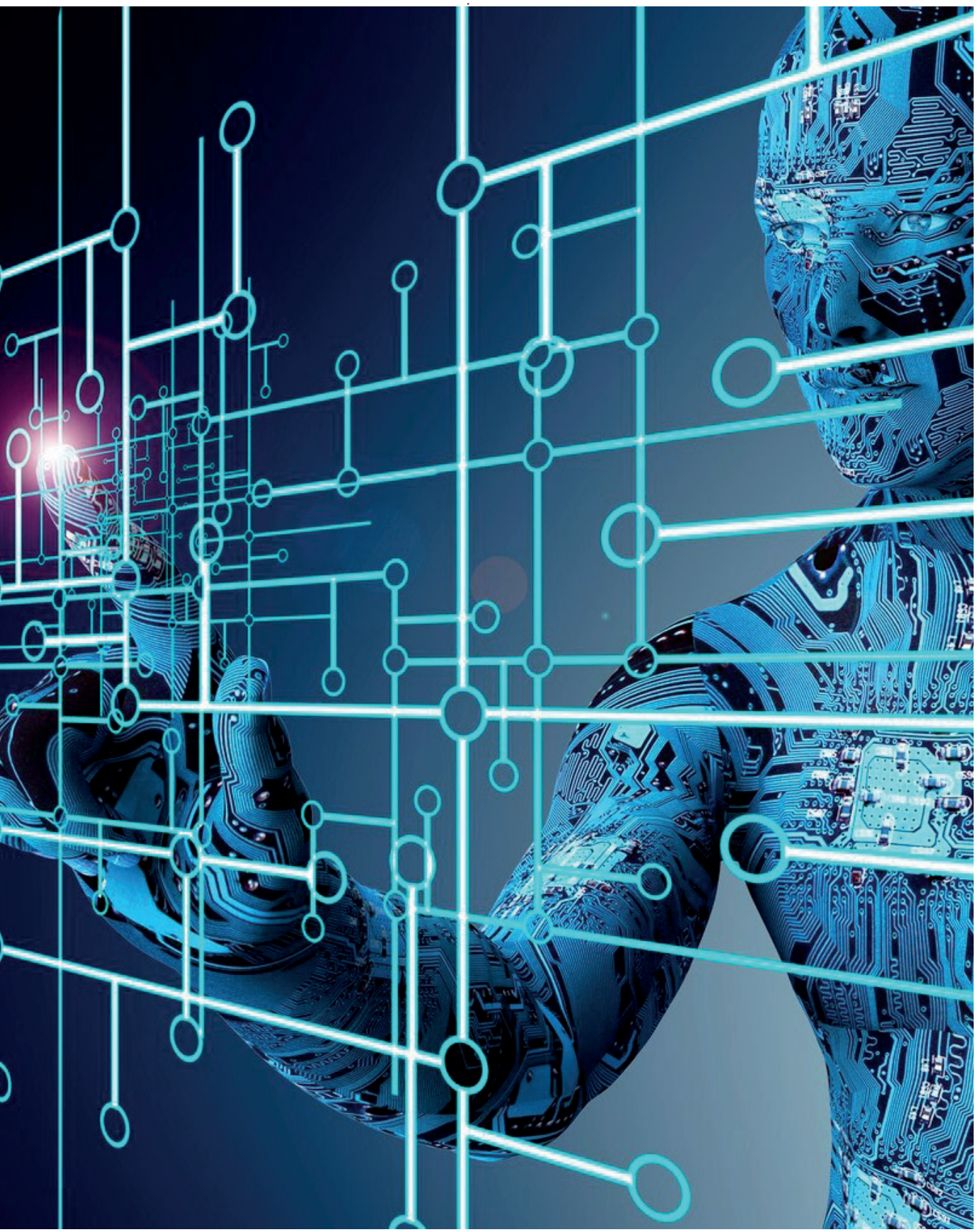
A las tradicionales dimensiones, tierra, mar, aire y espacio, se les ha unido recientemente la quinta, el ciberespacio, dimensión que es transversal a todas las anteriores y sobre la que se constituye el dominio cognitivo, pieza fundamental para crear la adecuada Situation Awarenes (SA) que todo comandante o responsable de un sistema de Mando y Control (civil o militar) precisa tener en todo momento.

Finalmente, el Internet de las cosas ha posibilitado acceso remoto a cualquiera de los dispositivos de los que nos facilitan la vida cotidiana y, lo que es más peligroso, a las infraestructuras y servicios que sustentan nuestra sociedad, centrales energía/agua, telecomunicaciones, banca etc. Tal es la demanda de conectividad a Internet, que se precisa del constante desarrollo de las tecnologías de telecomunicación –sirva como ejemplo el desarrollo de la tecnología 5G para telefonía móvil– que permitirá incrementar el número de elementos conectados por área de servicio y la velocidad de transmisión.

Pero toda esta ingente demanda de servicios se enfrenta a una realidad inapelable, el medio físico usado para sustentarlos –el espectro electromagnético– es un medio finito, que podemos segmentar o multiplexar hasta un límite.

Una prueba evidente que cualquier lector ha sufrido en su vida cotidiana es la constante necesidad de resintonizar los canales de televisión digital, ya que sus bandas de trabajo originales son necesarias para nuevos servicios de telecomunicaciones, lo que obliga a migrar aquellas en beneficio de éstos últimos. Un buen ejemplo será la próxima entrada en servicio de la tecnología 5G ya mencionada.

Pero a buen seguro que llegados a este punto el lector ya se está preguntando que tiene que ver el espectro electromagnético (en adelante EMS, que corresponde a sus siglas en inglés) con el ciberespacio y la lucha que en él se está librando. La respuesta es sencilla, el EMS es la vía sobre la que discurre el ciberespacio ya que



tarde o temprano, todas las comunicaciones electrónicas tienen que hacer uso de esta capa física.

Ya sea mediante las comunicaciones inalámbricas de corto alcance (*wifi, bluetooth*), las microondas de medio alcance o los enlaces satelitales, los diferentes elementos que constituyen los modernos sistemas de información precisan del acceso a este medio físico para comunicarse entre sí.

Por otro lado, la inteligencia que controla y administra estas infraestructuras de telecomunicaciones está conformada por un *core* de complejos sistemas de información, los cuales, mediante diversos algoritmos y protocolos, conmutan circuitos físicos y virtuales, exprimiendo cada *slot* de tiempo y cada frecuencia del EMS para sustentar esta maraña de servicios que demandamos.

Así pues, esta simbiosis tecnológica es el corazón que alienta nuestro modo de vida, al igual que los actuales teatros de operaciones que evolucionan al ritmo de la moderna sociedad de la información y de las tecnologías que esta demanda.

En esta línea, la última revisión de la estrategia del poder aéreo conjunto de la OTAN (junio 2018) hace especial hincapié en que, para poder operar con éxito en los actuales escenarios multidominio, es preciso disponer de una infraestructura tecnológica que posibilite el planeamiento y conducción de las operaciones con agilidad y seguridad, y que posibilite adquirir una superioridad en la información.

Para ello pone el acento en varias cuestiones:

- Disponibilidad y resiliencia: se debe garantizar el acceso al EMS, implementando los medios necesarios para asegurar la con-

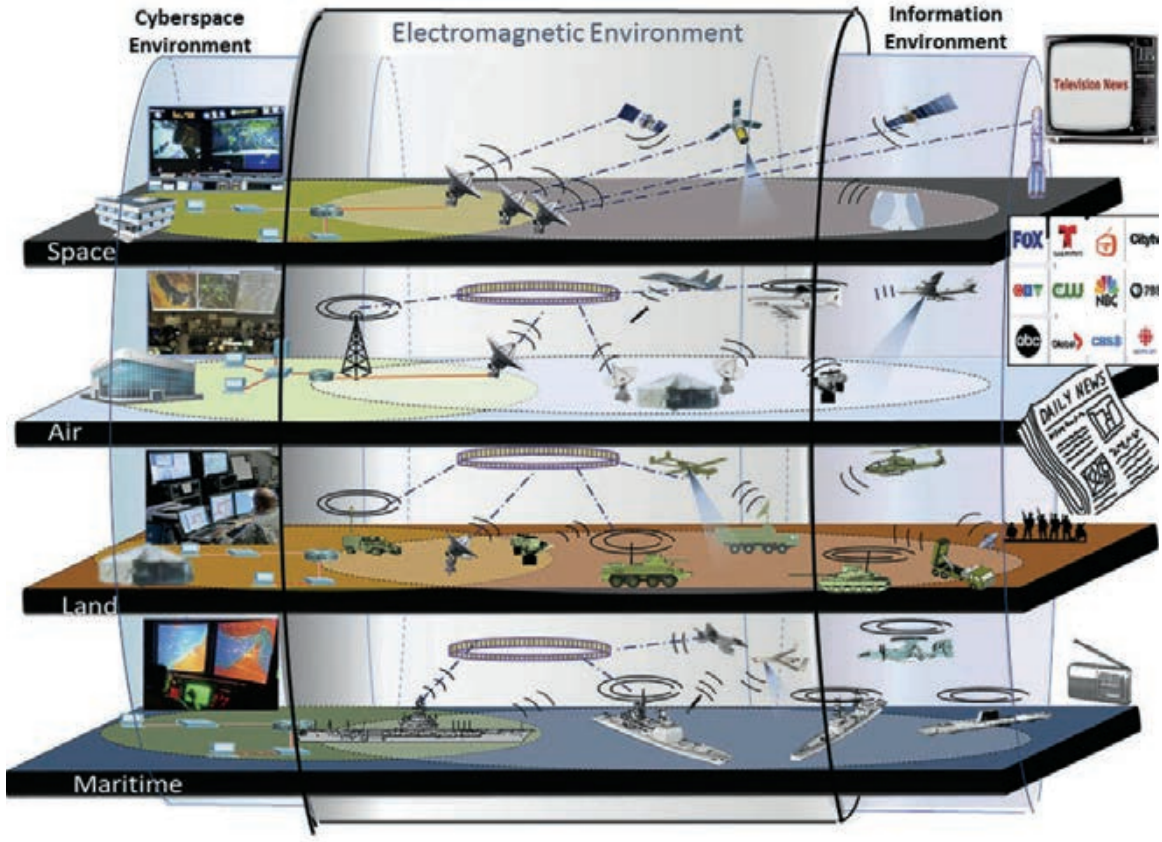
tinuidad de su uso y la resiliencia de los enlaces que lo propician, para garantizar un servicio 24H o, al menos, durante el transcurso de las operaciones militares. Esta circunstancia es especialmente preocupante en el entorno civil por las consecuencias que, para una sociedad hiperconectada, supondría un apagón digital.

• Organización: se debe regular el uso del EMS, para que todos los servicios que lo precisen puedan convivir sin interferencias. Para ello hay que actualizar las estructuras de mando en aras de posibilitar una gestión ágil e integral de este recurso compartido.

• Integridad: es vital garantizar que la información que transita por estas infraestructuras (voz o datos), lo haga de forma inalterada. La base para ejercer el mando y control (C2), reside en la confianza en los datos que ofrecen los diferentes sensores y demás flujos de datos que conforman la RAP (*Recogniced Air Picture*, visión situación operativa Aérea)o COP (*Common Operational Picture*, visión operativa Conjunta).

En semejante entorno, la ciberdefensa juega un papel trascendental ya que, al estar gestionados de forma remota, tanto los sistemas de gestión de las infraestructuras de telecomunicaciones, como los de gestión de infraestructuras críticas (luz, agua, gas, etc.), sistemas bancarios y bursátiles, así como los medios de difusión social (periódicos y foros de opinión) están expuestos a la acción de *hackers*, siendo el blanco preferente de los continuos ataques que se vienen registrando a diario por las agencias de seguridad de todos los países.

Igualmente y haciendo uso de las telecomunicaciones, el arma ciber puede potenciar y



extender nuestras acciones más allá que cualquier otro medio convencional –terrestre, marino o aéreo– sirviendo para la preparación y el apoyo de las misiones de estos.

Así, los tradicionales medios CIS (*Communications Information Systems*), ya no son solo medios de apoyo, sino las modernas armas con las que tendremos que garantizar la seguridad de las naciones, tanto en su vertiente civil como en la militar.

Llegados a este punto, es preciso prestar atención a otro elemento fundamental de la seguridad y defensa íntimamente relacionado con lo anterior, ya que comparte el mismo medio físico, la guerra electrónica (EW).

Como ya expuse en las conclusiones de mi anterior artículo «Los nuevos escenarios de la EW y sus retos tecnológicos» (*Revista de Aeronáutica y Astronáutica* n.º 876 de septiembre de 2018) «Los nuevos escenarios y la evolución de las TIC desplegadas en ellos, nos plantean un nuevo entorno en el que las fronteras son cada vez más difusas y en el que desde el combatiente de a pie, hasta la más moderna de las plataformas, dependerá de señales electro-ópticas para desarrollar su misión como parte integrante de una comunidad completamente interconectada».

Así pues ya tenemos las tres patas que sustentan el moderno tablero de juego y que se materializan en el concepto CEMA, Ciber Electromagnetic Activities.

Este concepto, actualmente implementado en varios de los países de nuestro entorno, nace de la constatación de que, para poder tener éxito en los modernos teatros multidominio, es preciso conseguir una superioridad en el dominio cognitivo de dichos entornos operacionales, que normalmente se obtiene y distribuye mediante una infraestructura tecnológica con fuerte dependencia electrónica. Así lo reconoce el JEMAD en su concepto de ciberdefensa de 2018 (solución: elementos centrales; integración en las operaciones conjuntas).

En consecuencia, es preciso disponer de una superioridad –o al menos la necesaria disponibilidad– en el uso del EMS, no solo para sustentar dicha infraestructura, sino para poder planificar, conducir y ejecutar las operaciones militares.

Por ello las operaciones ciber, junto con las EMO (Electromagnetic Operations), en un objetivo conjunto para conseguir y garantizar el uso del EMS para nuestras fuerzas y denegárselo en caso necesario al adversario, deberían estar presentes mediante células CEMA –equipos de técnicos multidisciplinares expertos en las ramas de telecomunicaciones, EW y ciber–, en todas las fases de las operaciones, ya que sin una mínima superioridad en este medio físico, difícilmente podremos desarro-

llar operaciones con medios convencionales contra un adversario tecnológicamente avanzado.

Tanto si se trata de una campaña contra un adversario tecnológicamente avanzado, como si se trata de un conflicto asimétrico, debemos estar vigilantes a las actividades que se desarrollan en este medio ya que, si bien es caro y difícil adquirir modernas plataformas de combate, llevar a cabo actividades de *hacking*, COMJAM o GPS JAMMING, resultan sumamente baratas y sus efectos pueden ser devastadores.

Sirva como ejemplo ilustrativo la captura por parte de fuerzas iraníes de un dron RQ 170 Sentinel de los EE.UU. mediante interceptación GPS y hackeo de sus sistemas –con un equipo cuyo coste estimado era de 26 dólares– haciéndolo aterrizar con todos sus sistemas intactos. Una vez en tierra y mediante ingeniería inversa, la industria iraní tuvo acceso a la más avanzada tecnología de defensa estadounidense, lo que supuso un gran salto cualitativo con un mínimo coste de tiempo y recursos, que les ha permitido fabricar su propia versión de dicha plataforma y poner dicha tecnología en manos de terceros países.

Otro claro ejemplo, es la lucha que se mantiene en el campo de la información pública y los medios de difusión social para controlar las noticias relacionadas con las operaciones militares.

Una campaña de *fake news* puede dar al traste con meses de planificación y multitud de recursos movilizados, llegando incluso a poner en duda la legitimidad de procesos electorales, como se ha visto recientemente.

Una vez constatada la realidad tecnológica que impera en los modernos teatros de operaciones, es preciso adoptar una solución integral para prevalecer en una dimensión que no tiene fronteras, en la que operan desde el más pequeño equipo portátil hasta el más sofisticado satélite.

Semejante tarea se antoja titánica, por lo que, para abordarla, precisamos desglosarla en varios aspectos fundamentales que permitan dotarnos de las estructuras, tecnologías y personal necesarios:

1.º Operativo: es preciso adaptar las actuales estructuras de mando y control y sus ciclos de planeamiento para dar cabida a esta nueva realidad.

Si tenemos en cuenta que las actividades CEMA afectan a todas las fases del combate, desde la preparación a nivel estratégico, hasta la ejecución a nivel táctico, habrá que diseñar una estructura escalable que permita contar con personal y medios CEMA en todos estos niveles de planeamiento y conducción, para llevar a cabo la planificación de sus actividades y los efectos que se pretenden conseguir con ellas, la integración con el resto de acciones de la campaña y la sincronización de todas ellas para generar sinergias y apoyos mutuos que multipliquen los respectivos efectos, evitando interferencias o duplicidad de esfuerzos.

Los perfiles de cada célula CEMA, cubiertos por personal con empleos, formación y experiencia acordes a cada nivel, compondrían los eslabones de la una cadena que ejercería un control efectivo de todas las actividades CEMA, ya sea para cumplir con misiones propias o para apoyar al resto de misiones de la campaña.

2.º Tecnológico: estar al día de los últimos avances tecnológicos es una tarea harto complicada, dada la cantidad de tecnologías disponibles en el actual mercado. La feroz competencia existente, obliga a las empresas del sector a buscar diferentes soluciones que se traducen en multitud de equipos y plataformas con sinfín de funcionalidades. Al ser diseños independientes y no disponer de organismo regulador que genere estándares, la integración de cada equipo con el resto de los medios existentes es toda una odisea, inabordable por si solos, para las fuerzas y cuerpos de seguridad de la mayor parte de los países.

Al formar parte de organismos de defensa multinacional, España tiene acceso a programas de I+D que dan solución a algunos de estos problemas de integración, lo que posibilita que nuestras plataformas se integren en las operaciones multinacionales en que estamos presentes; no obstante, para ser competitivo en un entorno tan dinámico y crítico, se precisa de una solución más ambiciosa.

La solución se presenta en forma de colaboración a tres bandas de los actores implicados en la seguridad y defensa; Minisdef, universidad y empresas del sector a través de uniones temporales de empresas creadas para cada proyecto, en las que cada empresa aporte sus tecnologías para obtener un resultado final totalmente integrado e interoperable.

El sistema educativo español está generando un gran capital humano altamente cualificado que está ahíto de proyectos en los que volcar dicho conocimiento. Captar y orientar dicho capital al servicio de la seguridad y defensa no puede sino dar generosos beneficios en forma de tecnologías y prototipos que sirvan de base a la industria nacional. Finalmente, y para evitar la multiplicidad de soluciones y el problema de la integración de los mismos, el Minisdef –como usuario preferente de estas tecnologías– debe ejercer un papel armonizador, definiendo las necesidades operativas que se deriven de los análisis estratégicos elaborados por sus organismos.

Aunque diferenciados por sus misiones y medios, los ejércitos y el resto de fuerzas y cuerpos de seguridad del Estado confluyen en la misma dimensión tecnológica, de modo que ambas organizaciones pueden y deben compartir tecnologías que permitan generar sinergias y mejorar la interoperatividad de medios y plataformas, ya que cada día son más las ocasiones en que deben aportar medios combinados para responder a crisis de seguridad del Estado.

Teniendo en cuenta las características del entorno social en que nos movemos, ya descrito en mis primeras líneas, no es descartable que

para conseguir efectos militares, se busque desequilibrar los centros de gravedad de un país a través de acciones de base digital de diversa índole.

Debemos estar atentos para dar cumplida respuesta a esta amenaza, y la mejor manera es compartir información, tecnología y procedimientos que ayuden a contener las amenazas en un escenario tan amplio.

3.º Humano: tanto las estructuras de mando como los equipos y tecnologías que las sirven, necesitan de personal técnico altamente cualificado que las nutran y operen. Algunos de estos perfiles pueden ser cubiertos con personal egresado del sistema educativo general o bien del militar.

Sin embargo, dada la extensión y complejidad del dominio digital, se precisa de algunos perfiles específicos que no se pueden obtener por estos medios convencionales, ya que lo que se busca es precisamente personal poco convencional, que piense en las posibilidades y recursos que se escapan al común de los mortales, y que sean capaces de detectar y explotar las vulnerabilidades de los sistemas digitales.

Los cibercamps y demás ejercicios patrocinados por los diferentes organismos implicados en este campo, son el mejor estadio para detectar y captar el talento necesario para ocupar dichos perfiles. Tan solo se precisa definir las trayectorias de este personal para explotar al máximo sus capacidades y fidelizarlo, evitando futuros problemas de seguridad.

Un paradigma inalterable en la historia de la guerra, es que la altura ofrece una ventaja táctica sobre el adversario, que permite actuar sobre sus fuerzas con una menor exposición de las propias. Esta, junto con la velocidad, agilidad y proyección, hacen del poder aéreo un elemento indispensable y decisivo en el combate moderno.

Teniendo en cuenta que, desde la dimensión terrestre hasta la espacial, y pasando por todas las intermedias, el EMS se configura como un medio que nos rodea como una suerte de atmósfera digital por la que, vía aérea o a través de cables, discurren las señales electro-ópticas que sustentan nuestras modernas sociedades. Y quien mejor para liderar la conquista de este entorno que el arma aérea, con quien el medio digital comparte el mismo medio físico, el aéreo, que a ambos les ofrece las ya mencionadas cualidades de altura, proyección y dinamismo.

Como colofón y resumen a todo lo anterior, citaré las reflexiones de sir Stuart Peach, ilustre aviador que actualmente ocupa el puesto de máxima responsabilidad militar en la OTAN: «Comprender, gestionar y controlar el entorno electromagnético juega un papel fundamental en la guerra en todos los niveles de intensidad. El resultado de futuras operaciones será decidido por aquél que tome una ventaja decisiva en este campo». ■

BIBLIOGRAFÍA

– Concepto estratégico OTAN.
– Estrategia Aérea OTAN.
– CEFAS Cambio 2.
– PDC-01 Doctrina de empleo de las FAS