Respondiendo a nuevos retos

El planeamiento de defensa en el *siglo XXI*

Federico Yaniz Velasco
General del Ejército del Aire (R)

Don Quijote de la Mancha.

A MODO DE INTRODUCCIÓN

Caído en el campo don Quijote, tras atacar con la lanza en ristre al primer molino que tenía delante, Sancho Panza trata de explicarle que a los que había alanceado eran molinos de viento y no gigantes. don Quijote le respondió "Calla amigo Sancho, que las cosas de la guerra, más que otras, están sujetas a continua mudanza". Don Miguel de Cervantes cuando puso esas palabras en boca de don Quijote tenía un conocimiento de primera mano de las cosas de la guerra pues durante más de cinco años fue soldado encuadrado en varias compañías y había participado en numerosos combates. Entre ellos destacó la batalla de Lepanto en la que don Juan de Austria derrotó a los turcos el 7 de octubre de 1571. En esa gloriosa ocasión, Cervantes combatió embarcado en una de las galeras mandadas por el Marqués de Santa Cruz. Cervantes siempre se mostró orgulloso de aquel lance en el que resultó herido y en sus obras resaltó siempre la importancia de la carrera de las armas. Ese amor por la milicia se refleja en la seriedad con la que Cervantes se pronuncia a través de don Quijote en el "curioso discurso que hizo de las armas y de las letras". Sirvan estas líneas de recuerdo a tan ilustre soldado en el IV Centenario de su muerte en 1616.

La superioridad de las armas empleadas marca la diferencia entre la victoria o la derrota.

Como decía don Quijote con otras palabras, la evolución de las capacidades, las tácticas y las estrategias empleadas en las guerras ha sido continua a lo largo de los siglos. Desde los comienzos de la Historia, una buena organización y moral de las fuerzas combatientes han marcado la diferencia entre la derrota o la victoria. Las falanges macedonias, las legiones romanas o los tercios españoles con su mejor encuadre y gran disciplina superaron a las tropas adversarias. Sin embargo, en muchas ocasiones, la superioridad de las armas empleadas marcó la diferencia entre la victoria o la derrota. Empleando una de las armas más eficaces de la Edad Media, los arqueros medievales fueron capaces de decidir el resultado de muchas batallas. Luego llegaron el arcabuz, las armas de fuego y dando un gran salto, los carros de combate, la artillería pesada y sobre todo los aviones que cambiaron radicalmente el arte de la guerra. En el mar, desde el siglo VII AC, las trirremes griegas y después las romanas controlaron el mar Me-

Bucker 181 de la II Guerra Mundial.

diterráneo. Desechados los remos, las naos, los navíos, las goletas, los galeones, las fragatas y otros barcos de vela dominaron los mares. En el siglo XIX, los barcos de vapor relegaron a los de vela y desde las primeras fragatas acorazadas hasta los portaaviones y submarinos nucleares de hoy, las marinas de guerra con los mejores buques han conseguido imponer su dominio en los mares y controlar las líneas de comunicación marítima. Desde la primera Guerra Mundial (I GM) hasta los últimos enfrentamientos bélicos, las fuerzas aéreas dotadas con los aviones de combate de mejores características, con una logística adecuada y apoyados por los sistemas de mando y control eficaces han sido capaces de tener el dominio del aire o al menos la superioridad aérea esencial para alcanzar la victoria.

Organización de Naciones Unidas.

LA DEFENSA EN EL PRÓXIMO DECENIO

Aunque la evolución de *las cosas de la guerra* ha sido continua a través de la historia, fue en el siglo XX cuando se produjo un cambio dramático en las tácticas y estrategias empleadas en los conflictos bélicos. Incluso la palabra guerra fue prácticamente eliminada del lenguaje políticamente correcto. Además, la aparición del concepto de gestión de crisis ha servido para completar las tradicionales negociaciones diplomáticas en el intento de evitar que conflictos de diversos tipos puedan desembocar en guerras. Los ministerios de la Guerra de los comienzos del siglo XX han pasado a ser ministerios de Defensa y los planes de guerra de los estados mayores han sido sustituidos por los llamados planeamiento de defensa y planeamiento operativo. El dramático sufrimiento y la terrible destrucción causados por la segunda Guerra Mundial (II GM) junto a las consecuencias de la I GM cambiaron el panorama estratégico de Europa y del mundo.

La fundación de la Organización de las Naciones Unidas (ONU) en 1945 y la creación de otras organizaciones internacionales, que pretenden la resolución de los conflictos por métodos pacíficos, han tenido un efecto positivo en favor de la paz. Sin embargo, de 1947 a 1991 durante los años de la llamada Guerra Fría, millones de personas perdieron sus vidas en conflictos regionales en los que en muchas ocasiones las superpotencias dirimían diferencias ideológicas y buscaban el control de territorios estratégica y económicamente importantes. Tras el colapso de la Unión Soviética muchos analistas pensaron que los Estados Unidos y sus aliados iban a ser capaces de establecer y mantener una nueva *Pax Romana* en el mundo. La aparición de potencias emergentes como la República Popular China y la India, la complejidad del panorama estratégico mundial y sobre todo los atentados terroristas del 11 de septiembre de 2001 frustraron esa esperanza. Como consecuencia de los ataques en el corazón de los Estados Unidos y de muchos otros actos terroristas en Europa y en países de todo el mundo, se ha extendido la percepción de que la humanidad se enfrenta a amenazas a la seguridad que son muy diversas, difusas y multidireccionales. Para luchar contra la amenaza terrorista se ha desarrollado una lucha antiterrorista que no ha sido tan exitosa como sería deseable. Por otra parte, algunas organizaciones de defensa como el Pentágono estadounidense han identificado como nuevas amenazas a la seguridad la llamada crisis climática y la carencia de recursos básicos como los hidráulicos y los energéticos en grandes áreas del planeta. El calentamiento global es ya un peligro claro pues si no se consigue frenar, la inestabilidad global se verá exacerbada por la pérdida de cosechas y por la subida del nivel del mar lo que ocasionará millones de refugiados. Aunque el 4 de noviembre de 2016 entró en vigor el Acuerdo de París sobre Cambio Climático habrá que hacer un gran esfuerzo para alcanzar los objetivos marcados.

En los próximos años se hará cada vez más necesario realizar un planeamiento de defensa que tenga en cuenta los retos globales a que se enfrenta la Humanidad y preste especial atención a los malos usos de los avances tecnológicos de todo tipo cuya aplicación práctica ya se vislumbra. También se deberán considerar en ese planeamiento la imparable carrera hacia la conquista del espacio y la posible evolución del uso de la energía nuclear, teniendo siempre en cuenta las oportunidades y riesgos que conlleva su desarrollo. La consideración de esas realidades es una necesidad para lograr tener una defensa adecuada que responda a las necesidades objetivas existentes en el segundo decenio del siglo XXI. Los Estados Unidos, China y la Unión Europea, si consigue superar la crisis, serán actores globales en un mundo multipolar en el que Rusia, la India, Indonesia, Japón, Brasil,

Méjico, Gran Bretaña y otros países jugarán un papel importante. España por su situación estratégica, por su proyección cultural y por su pujanza innovadora puede ocupar un puesto relevante en el mundo del tercer decenio del siglo XXI.

En ese marco, para adecuar nuestra defensa a las necesidades objetivas existentes, es preciso tener en cuenta los posibles riesgos y amenazas contra la seguridad de nuestros ciudadanos e instituciones en un entorno estratégico globalizado y cambiante. En resumen, para que el planeamiento de defensa español en el segundo decenio del siglo XXI sea eficaz, será preciso tener presente, además de los riesgos y amenazas ya tradicionalmente considerados, la realidad del mundo de hoy y del mañana previsible. Dentro de esa realidad, los avances tecnológicos, el cambio acelerado así como la importancia de los espacios cibernético, electromagnético y exterior y de la energía nuclear suponen un reto que es necesario conocer y afrontar. Sólo así será posible preparar de forma rigurosa los presupuestos que deberían ser asignados a la defensa para garantizar la obtención de las capacidades que garanticen la libertad y seguridad de nuestros ciudadanos.

GRANDES RETOS A COMIENZOS DEL SIGLO XXI

La accesibilidad casi universal al conocimiento, la vulnerabilidad de las redes de comunicación y de otras infraestructuras críticas así como la globalización del capital y del comercio, están empezando a hacer posible que actores no estatales tengan acceso a nuevas tecnologías incluyendo aquellas que pueden tener carácter ofensivo.

La proliferación de las nuevas tecnologías

La proliferación de las nuevas tecnologías a escala global presenta retos que serán duraderos. Es un hecho incontestable el crecimiento del comercio global, la existencia de unos mercados cada vez más abiertos y el uso creciente en el sector de defensa y seguridad de innovaciones promovidas con fines comerciales. El acceso al conocimiento y la globalización del capital está produciendo la transferencia de las nuevas tecnologías y de su producción a las economías en desarrollo. Todo ello facilitará que esas tecnologías proliferen y permitan a nuevos actores el acceso a técnicas que antes estaban sólo al alcance de unos pocos estados. Esos actores, incluyendo posibles adversarios "menos avanzados", podrían emplear las tecnologías comerciales existentes o las de doble uso de una forma innovadora que les permita ocultar el conocimiento de sus actividades.

Visión gráfica del espacio cibernético.

La fabricación aditiva puede permitir que individuos, actores no estatales y estados fallidos tengan la capacidad de producir grandes cantidades de armas de alta tecnología a bajo coste.

La fabricación por adición (*additive manufacturing*) y la ingeniería inversa son avances tecnológicos importantes que son accesibles a nuevos actores que podrán adoptar e integrar esas nuevas tecnologías a un ritmo que hará difícil a los países más avanzados mantener su ventaja tecnológica.

La fabricación por adición o impresión en tres dimensiones es considerada por los expertos como una tecnología que puede ser especialmente significativa en este contexto. Las ventajas de la fabricación por adición están mundialmente reconocidas siendo una de las 10 tecnologías emergentes del año 2015 según el Consejo del Foro Económico Mundial sobre Tecnologías Emergentes. Como el nombre lo sugiere, la fabricación por adición es lo opuesto a la fabricación por sustracción que es la manera tradicional de fabricación (se empieza con una pieza de material (madera, metal, piedra, etc.) y se quitan o sustraen capas hasta que se llega a la forma deseada]. La fabricación por adición, en cambio, empieza con material suelto, líquido o en polvo, y luego se construye en una forma tridimensional con una plantilla digital. La fabricación por adición puede hacer más corta la cadena logística y puede ayudar en las operaciones en entornos no permisivos sobre todo cuando la cadena logística es larga, es cara o está amenazada. En su aspecto negativo, la fabricación aditiva puede permitir que individuos, actores no estatales y estados fallidos tengan la capacidad de producir grandes cantidades de armas de alta tecnología a bajo coste.

La ingeniería inversa facilita el acceso a la tecnología avanzada a actores diversos que pueden obtener con ella la información necesaria para fabricar equipos o sistemas partiendo del análisis de un ejemplar del mismo. En efecto, lo que se pretende con la ingeniería

inversa es obtener información a partir de un producto acabado con el fin de determinar de qué está hecho, qué lo hace funcionar y cómo fue fabricado. Hoy día, los productos más comúnmente sometidos a ingeniería inversa son los programas de los ordenadores y los componentes electrónicos pero la ingeniería inversa puede emplearse en prácticamente todos los campos de la industria y de la investigación. En ocasiones, se recurre a la ingeniería inversa cuando se quieren desarrollar nuevos productos que sean compatibles con otros, sin conocer detalles del desarrollo de éstos últimos. En informática tanto en los equipos como en los programas se emplea con frecuencia la ingeniería inversa. Con relativa frecuencia se utiliza esta técnica para recuperar el código fuente de un programa porque se ha perdido, para estudiar cómo realiza ciertas operaciones, para mejorar su rendimiento, para corregir un error cuando no se dispone del código fuente, para identificar contenido malicioso (un virus) o para adaptar un programa informático escrito de un procesador para poder ser usado por otro. De los ejemplos mencionados es fácil deducir el campo de posibilidades que la ingeniería inversa puede abrir a ciertos grupos.

El acelerado ritmo de cambio tecnológico dejará obsoletos los sistemas de armas cada pocos años.

El cambio tecnológico acelerado

Otro aspecto que es necesario considerar al realizar el planeamiento de defensa en el próximo futuro, es el *tempo* acelerado de los cambios tecnológicos. Esta aceleración obliga a una revisión de los métodos y procesos de obtención de equipos y sistemas de armas dado que, movidos por las demandas de los mercados de masas, los ciclos de desarrollo de nuevos productos han dejado atrás los modelos tradicionales. En efecto, hasta hace pocos años el ciclo de obtención de los sistemas de armas podía tener una duración de 10 a 20 años y su ciclo de vida estaba entre los 30 y 50 años. Parece muy probable que en los próximos años, el ciclo de vida de los sistemas se reduzca significativamente como consecuencia del acelerado ritmo de cambio tecnológico que los dejaría obsoletos en unos pocos años. Para responder a esa situación será necesario reducir los tiempos de los ciclos de planeamiento de defensa, adoptar procedimientos de obtención muy ágiles y disponer de dotaciones presupuestarias plurianuales adecuadas para poder renovar los equipos y sistemas con mayor frecuencia.

La computación en red

Otro elemento de carácter tecnológico que también es preciso considerar de cara al futuro inmediato es el avance imparable de la computación en red. Según estudios fiables en un plazo de 10 a 20 años los ordenadores estarán frecuentemente conectados recogiendo información y compartiéndola sin solución de continuidad, sin intervención ni conocimiento humano en algunos casos. Por otra parte, se dispondrá de ilimitada capacidad de almacenamiento de datos en dispositivos de tamaño micro. Esta realidad obligará a prestar atención en el planeamiento de defensa al impacto que tendrá en la privacidad, el aseguramiento, la jurisdicción y la seguridad de los datos el hecho de que puedan ser almacenados en cualquier servidor ubicado en el extranjero. Estos servidores serán parte importante de la infraestructura crítica nacional pero no estarán protegidos por la soberanía nacional.

La computación en red ha hecho posible los avances producidos en la analítica de grandes volúmenes de información es decir la habilidad para recoger, procesar y analizar de forma rápida grandes cantidades de datos. Dado el creciente volumen de datos aumentarán las oportunidades para extraer de ellos información de interés. Diversas organizaciones, incluidos actores no estatales, intentarán obtener una ventaja informativa usando la analítica de grandes datos para crear predicciones probabilísticas. Esta posibilidad tendrá que ser considerada por los servicios de inteligencia que deben evitar que nuestros datos críticos puedan ser fuentes de información para posibles adversarios incluidos actores no estatales hostiles.

Las capacidades defensivas y las nuevas armas

Los últimos avances tecnológicos y las capacidades que hacen posibles dichos avances deben de tenerse en cuenta en el planeamiento de defensa de cara al segundo decenio del siglo XXI. En efecto, la rápida aparición de

Computación en red (recreación artística).

Cañón láser europeo.

nuevos sistemas de armas como consecuencia de nuevas tecnologías debe considerarse al hacer el planeamiento de defensa. Sin embargo, deben evitarse decisiones precipitadas basadas en análisis superficiales sobre las posibilidades que ofrece la tecnología punta.

Un caso digno de mención es la rapidez con que en los últimos años se han hecho presentes los sistemas no tripulados y en especial los vehículos aéreos no tripulados (*UAV*). Entre todos ellos destacan los *RPAS* o aviones pilotados remotamente. En un solo fabricante estadounidense[5], la demanda de estos sistemas pasó de 500 en el año 2001 a 6.900 en 2016. Pero no sólo está aumentando el número de RPAS sino también las capacidades que tienen. En efecto, se están desarrollando sistemas que podrán ser certificados para poder operar en el espacio aéreo civil. De esa forma se ampliarán dramáticamente sus posibilidades de uso pues se podrán emplear en misiones de control de fronteras, vigilancia de pesquerías, control del medio ambiente, etc. Para responder a los requisitos de aeronavegabilidad exigidos para operar en el espacio aéreo europeo será necesario introducir cambios en la ingeniería y en el software de los *RPAS* e incluir equipos –*sense and avoid*– apoyados en radar y transpondedores que hagan posible su vuelo en espacios aéreos no segregados.

Está aumentando de manera muy significativa en los últimos años el número y las capacidades de los RPAS.

Actualmente es posible que organizaciones terroristas, estados fallidos y otros grupos hostiles tengan acceso a vehículos aéreos no tripulados (*UAV*) que pudieran ser usados contra nosotros y contra países aliados y amigos. La amenaza de los *UAV* se ha hecho global pudiendo afectar también a nuestras fuerzas no sólo en su territorio sino también a unidades desplegadas en misiones lideradas por la OTAN o la ONU. En este caso, se debe evitar que *UAV* hostiles puedan conseguir información de nuestras fuerzas mediante operaciones de inteligencia, vigilancia, adquisición de

Un RPAS MQ-9 Reaper.

objetivos y reconocimiento (ISTAR). Por todo ello, los *UAV* en manos de elementos hostiles constituyen una seria amenaza para la seguridad nacional y para el mantenimiento de la ley y el orden dentro y fuera del territorio nacional. Sin entrar en detalles sobre cómo contrarrestar la amenaza de los *UAV*, baste señalar que es fundamental disponer de sistemas de detección que sean capaces de discriminar entre los diversos elementos que aparecen en las pantallas de vigilancia como son pájaros, aviones civiles o militares, etc.

Conviene recordar también que se está produciendo una mejora muy notable de las características de los misiles con el empleo de nuevas tecnologías diseñadas para permitirles burlar avanzadas contramedidas electrónicas y para operar a velocidades supersónicas o superiores.

Los cañones electromagnéticos, los explosivos híbridos y las armas de energía dirigida, como los laser de alta potencia, así como las armas de microondas, obligarán en el próximo decenio a buscar protecciones adecuadas para el personal y los equipos propios. Otros avances tecnológicos como sistemas biomecánicos, las drogas para mejorar la memoria y los componentes sintéticos biológicos, cuyo desarrollo presentan riesgos añadidos, tardarán más tiempo en estar disponible pero es necesario seguir su desarrollo para evitar sorpresas tecnológicas.

El componente nuclear en el siglo XXI

Como es conocido, en el año 2016 son nueve los estados que poseen armamento nuclear: Corea del Norte, China, Francia, los Estados Unidos, India, Israel, Pakistán, Rusia y el Reino Unido. Hay muchos otros países con la posibilidad de conseguir ese tipo de armamento en un plazo más o menos corto. Actualmente existen en el mundo 17.300 cabezas nucleares aunque sólo los Estados Unidos y Rusia tienen más de 300 cabezas. Entre los estados con armas nucleares hay diferencias en la apreciación de las causas que justificarían una respuesta con ese armamento. Sin embargo, parece que los expertos están de acuerdo en que es cada vez más probable que

El Secretario General de la OTAN delante de un Gobal Hawk del AGS de la OTAN. Varsovia, 8 de julio de 2016.

algún estado pudiera usar armas nucleares tácticas para responder a amenazas convencionales incluyendo graves ataques cibernéticos. La respuesta nuclear seguirá siendo controvertida y de muy difícil ejecución cuando las amenazas, incluso nucleares, provengan de grupos terroristas o de criminales cibernéticos con localización dispersa. En los próximos años se necesitará una mayor voluntad política y el consenso internacional para luchar contra la muy peligrosa proliferación del armamento nuclear.

TRES ESPACIOS PARA LA DEFENSA

La defensa del siglo XXI está en evolución y tiene por escenario principal tres espacios que en gran parte se solapan y que se superponen a los tradicionales teatros de operaciones terrestre, marítimo y aéreo. Esos tres espacios son el cibernético, el electromagnético y el exterior. La importancia que ya tienen y que tendrán esos tres espacios para la defensa es trascendental y decisiva. En efecto, sin conseguir un dominio o al menos una superioridad local suficiente en esos espacios no será posible asegurar una defensa eficaz. Para ello se necesita realizar un planeamiento conjunto que tenga en cuenta esos tres espacios y los retos que los avances tecnológicos asociados presentan. Lograr la superioridad en esos espacios únicamente con capacidades propias será difícil y en ocasiones será conveniente la cooperación con aliados para conseguirla.

El espacio cibernético

Una preocupación mayor en la era de la información es la vulnerabilidad de los sistemas de almacenamiento y transferencia de datos a los ataques cibernéticos. Los expertos señalan que las operaciones cibernéticas serán consideradas como componente principal del espacio de combate interarmas. Dado que los sistemas de armas dependerán cada vez más de las redes de información, especialmente para integrar sensores y sistemas de mando y control, será esencial la protección cibernética y la resiliencia de nuestra defensa ante los ataques cibernéticos.

En este marco, es preciso ser consciente de que cualquier uso del espacio cibernético que impacte infraestructuras críticas nacionales e internacionales puede dar lugar a respuestas militares de difícil valoración, incluyendo

el uso de armamento nuclear táctico. Los retos a afrontar en el campo de la seguridad de la información y de las infraestructuras seguirán creciendo durante los próximos veinte años pues los ataques cibernéticos aumentarán en alcance, frecuencia e impacto. Además es previsible que los posibles adversarios sean capaces de usar esos ataques para golpear en el nivel estratégico, operacional y táctico y no sólo a las infraestructuras críticas.

Sin embargo, el dominio cibernético también ofrece oportunidades como la integración del señalamiento de objetivos que contribuya a una postura de disuasión de amplia base. Por otra parte, la cibernética puede ofrecer medios creíbles para conseguir un efecto disuasorio amenazando las infraestructuras críticas de un posible adversario que queda así sujeto a coerción.

Otro riesgo que es preciso considerar en el espacio cibernético es la posibilidad del acceso desde dentro a información sensitiva almacenada y el consiguiente riesgo de que sea compartida de forma no autorizada. Los casos de Manning y Snowden han demostrado que un individuo desleal con acceso apropiado puede causar grave daño a la seguridad de la información.

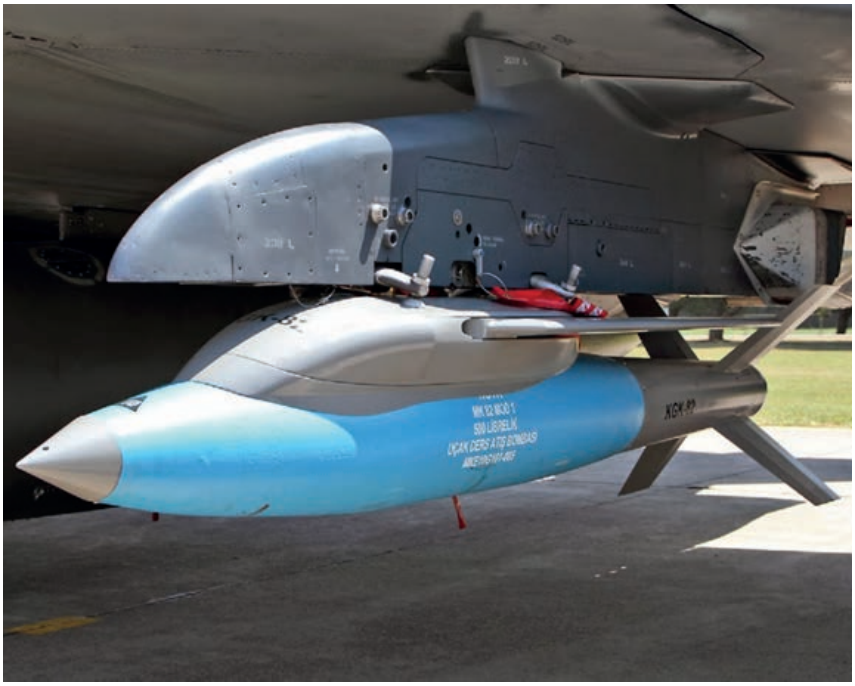
El espacio electromagnético

La guerra electrónica tuvo ya un papel protagonista en el planeamiento de defensa y operativo durante los últimos años de la guerra fría. Los responsables de esos planeamientos, tanto a nivel nacional como en la OTAN, dedicaban gran atención a los aspectos relacionados con el espectro electromagnético. El acceso y la libertad de acción dentro de ese espectro se siguen considerando como vitales en la prosecución de una efectiva acción conjunta en los próximos años. La capacidad de navegar, comunicarse, usar efectos cinéticos y no cinéticos así como de obtener información y comprensión de la situación depende del acceso al espectro electromagnético. Donde el ancho de banda es limitado, el acceso al espectro puede estar constreñido por operadores comerciales que buscan aumentar su propio uso. El creciente uso de tecnologías basadas en el espacio exterior incrementará la vulnerabilidad de nuestro espectro electromagnético.

La capacidad de comunicarse, navegar, usar efectos cinéticos y no cinéticos así como de obtener información y comprensión de la situación depende del acceso al espectro electromagnético.

En todo caso, en los próximos años parece que las capacidades de guerra electrónica avanzada serán ubicuas y, cuando proliferen, adversarios no especialmente preparados serán capaces de crear un amplio espectro de amenazas electrónicas. En este escenario nuestras plataformas y sistemas necesitarán una protección adecuada para poder resistir los ataques electrónicos y ser capaces de operar en entornos electrónicos hostiles. Las medidas de defensa electrónica seguirán siendo necesarias para contrarrestar la amenaza de los artefactos explosivos improvisados así como para mitigar los efectos de armas guiadas por radio frecuencia, rayos infrarrojos o rayos laser. Medidas de protección activa o pasiva serán también necesarias para proteger nuestros sistemas y redes de datos de ataques cibernéticos realizados a través del entorno electromagnético.

La revigorización y explotación de las capacidades de ataque electrónico pueden asegurar una ventaja operativa. Sin embargo, parece oportuno considerar la conveniencia de que nuestra defensa reduzca en lo posible su dependencia del espectro electromagnético dado que la proliferación de esa tecnología dotará a posibles futuros adversarios con capacidades diseñadas para impedir nuestro acceso a los entornos marítimos, terrestres, aéreos, espaciales, ciberespaciales y electromagnéticos.



Sistema de armas EMP Boeing CHAMP.

El espacio exterior

Las infraestructuras críticas de defensa de los países occidentales descansan de algún modo en capacidades espaciales y esta dependencia se incrementará a lo largo de los próximos 20 años. Esa dependencia del espacio exterior no es siempre evidente y en muchos casos las capacidades necesarias son proporcionadas por proveedo-

Amanecer desde espacio exterior.

res de servicios no nacionales, lo que aumenta la vulnerabilidad. El acceso al espacio exterior es ya muy competitivo tanto en capacidad orbital como en ancho de banda. Naciones emergentes en el campo espacial, en ocasiones con intereses opuestos a los nuestros, buscarán cada vez más un acceso equitativo al espacio exterior. Es muy posible que esos nuevos actores espaciales se opongan al orden "espacial" establecido disputando los tratados y los acuerdos y compitiendo por las mejores órbitas para los satélites artificiales. Acordar la asignación de órbitas será un problema creciente como también lo será la proliferación de basura espacial y las colisiones en el espacio. La posibilidad de realizar lanzamientos a un coste reducido hará más fácil el acceso al espacio, incluso para actores no estatales hostiles y para organizaciones criminales. Un cada vez mayor número de lanzamientos tratará de responder a las necesidades de los usuarios de un mercado masificado como el de los satélites de comunicaciones (demandando creciente ancho de banda) o el de la obtención de imágenes geográficas. Los usuarios militares del espacio continuarán confiando, al menos en parte, en empresas civiles para operar misiones en el espacio exterior y para conseguir equipos y vehículos espaciales.

EPÍLOGO

Los avances tecnológicos son a estas alturas del siglo XXI cada vez más rápidos afectando de una manera directa tanto al planeamiento de defensa como al planeamiento operativo. Esos avances afectan a los sistemas de armas pues su ciclo de vida operativa puede verse reducido por la rápida aparición de nuevas técnicas que proporcionen mejores capacidades. Por otra parte, la globalización del capital y la proliferación de las nuevas tecnologías ponen al alcance de terroristas y otras organizaciones hostiles nuevas capacidades ofensivas. Esas capacidades pueden constituir una amenaza contra nuestra población, territorios e intereses y al mismo tiempo emplearse en la guerra híbrida. A todo lo anterior, hay que añadir la importancia creciente para la defensa de tres espacios: el cibernético, el electromagnético y el exterior. Por ello, parece necesario un planeamiento de defensa que tenga un enfoque integral, que sea conjunto y combinado con nuestros aliados, que tenga en cuenta los retos que presentan las nuevas tecnologías y que preste especial atención a los tres espacios (cibernético, electromagnético y exterior) que van a ser escenario principal de nuestra defensa en los próximos años del siglo XXI.

NOTAS

[1]Don Quijote de la Mancha, de Miguel de Cervantes; Primera Parte, capítulo VIII, página 91. Edición Planeta, revisada por Martín de Riquer. Barcelona, España. Año 2005.

[2]Don Quijote de la Mancha, edición ya citada. Primera Parte, capítulo XXXVIII, página 410 y siguientes.

[3]Convención Marco sobre el Cambio Climático. Distribución limitada. París, 12 de diciembre de 2015
Ver URL http://unfccc.int/resource/docs/2015/cop21/spa/l09s.pdf

[4]Consejo del Foro Económico Mundial sobre Tecnologías Emergentes.
Ver URL https://www.weforum.org/es/agenda/2015/03/las-10-tecnologias-emergentes-de-2015/

[5]*Aircraft Systems Group, General Atomics Aeronautical Systems Inc*.