El Centro Tecnológico de Desarrollo y Experimentación de Jaén dará respuesta a la necesidad de capacidades militares asociadas a las tecnologías disruptivas

La revolución tecnológica del campo de batalla

General de división (R) Jesús Carlos Gómez Pardo
Dr. Ingeniero de Armamento

VIVIMOS en un mundo convulso. Un mundo que, en nuestro afán sistematizador, denominamos VICA (acrónimo de volátil, incierto, complejo y ambiguo), siglas que caracterizan nuestro entorno vital desde la caída del muro de Berlín. En el año 2020, aparece un nuevo cisne negro, la pandemia de la COVID-19, que impacta notablemente en nuestras vidas. Tras la pandemia, se acuña el concepto FANI (frágil, ansioso, no lineal e incomprensible), que hace referencia a lo quebradizo de estos tiempos. Mientras que VICA pone el foco en los factores que causan la incertidumbre y la complejidad, FANI lo hace en los efectos que estas producen en las organizaciones.

El mundo estable de la guerra fría, un mundo de bloques, conocido, parametrizable, de futuro predecible, ha pasado a la historia. En 1989 cae el muro de Berlín, se rompe el equilibrio geopolítico y los acontecimientos se precipitan. En Europa, al euromaidán ucraniano de 2013 le sucede la anexión ilegal de la península de Crimea en 2014 por la Federación Rusa y la posterior invasión en 2022 de otra parte del territorio de Ucrania. El impacto en nuestra sociedad está siendo enorme.

En el resto del planeta la inestabilidad impera. Así, el conflicto de Gaza, las tensiones entre EEUU y China, el deshielo del Ártico o el debilitamiento de los lazos trasatlánticos nos llevan a pensar que el mundo que hemos vivido no volveremos a conocerlo.

España no queda al margen de esta complicada realidad geopolítica que introduce enormes desafíos para la seguridad global. Comprometida con sus socios, nuestras Fuerzas Armadas participan en 17 operaciones en el exterior en las que tenemos más de 3.000 soldados y guardias civiles desplegados en cuatro continentes.

Por otro lado, esta inestabilidad e incertidumbre de la geopolítica global, se ve catalizada por la revolución tecnológica en la que estamos inmersos. Nuestra sociedad evoluciona de manera vertiginosa al compás de la irrupción de nuevas tecnologías emergentes que introducen cambios profundos en nuestra forma de pensar y actuar, y que están acelerando la transición hacia la era digital.

Nuestras Fuerzas Armadas, parte integrante de la sociedad, están sumidas en un proceso de transformación digital que modifica el arte de la guerra. Un campo de batalla transparente, digitalizado e hiperconectado, operaciones en red, combatientes bien pertrechados que se constituyen en nodos de la red de combate y el uso generalizado de vehículos no tripulados, sistemas autónomos, drones y robots armados actuando de manera individual o colaborativa, son ejemplos de una realidad que está modificando sustancialmente los actuales conceptos operativos.

Retos tecnológicos, futuros desconocidos y enormes desafíos para la seguridad ante los cuáles solo podemos actuar creando estructuras ágiles, en permanente adaptación a la rápida evolución del entorno, y dotándonos de organizaciones más flexibles y resilientes que nos permitan sobrevivir y operar en un entorno cada vez más incierto y complejo.

El uso masivo de drones es uno de los cambios fundamentales que se ha puesto de relieve en Ucrania

LECCIONES APRENDIDAS

De la guerra de Ucrania podemos extraer, con cautela, las primeras lecciones aprendidas, recogidas en un documento elaborado por el Centro Conjunto de Desarrollo de Conceptos del Estado Mayor Conjunto (EMACON).

La invasión ilegal de Ucrania por la Federación Rusa nos devuelve, aparentemente, a un conflicto convencional de alta intensidad, pero con algunas salvedades: ambos bandos están haciendo uso extensivo de ciertas tecnologías emergentes y disruptivas, características de un conflicto moderno; existe, además, un claro enfrentamiento entre Rusia y Occidente en la «zona gris»; y todo esto, con el telón de fondo de la amenaza nuclear. Las operaciones se están llevando a cabo en el multidominio que integra los ámbitos de operación físicos (tierra, mar y aire, incluyendo el espacio ultraterrestre) y los dominios no físicos (el ciberespacio y el espacio cognitivo) que establece la doctrina española.

Por otro lado, se han puesto de relieve algunos cambios fundamentales en la batalla, asociados a la digitalización, destacando sobremanera el uso masivo de drones.

De este terrible conflicto, de elevada atrición, podemos extraer, centrándonos en aspectos tecnológicos, las siguientes conclusiones: que las capacidades de inteligencia, vigilancia, reconocimiento y adquisición de objetivos son claves para la superioridad en las operaciones; que en el campo de batalla resulta crítico disponer de fuegos precisos y de largo alcance para batir objetivos, minimizando daños colaterales y alejándonos de las acciones de contrabatería; que es necesaria una gran potencia de fuego para saturar al adversario; que la digitalización del campo de batalla es ya una realidad, habiendo quedado patente que, para que las operaciones en red sean posibles, debe garantizarse la interconexión de los sensores y sistemas de combate con los centros de gestión y elementos productores de fuegos o efectos; y, por último, que para garantizar dicha interconexión es imprescindible disponer de sistemas C2 de mando y control robustos, redundantes y de alta movilidad, así como de capacidades de guerra electrónica para operar en el espectro electromagnético con la necesaria superioridad, de manera que pueda garantizarse la operatividad en entornos degradados y la libertad de acción en los cinco dominios de las operaciones.

Resulta, por tanto, fundamental disponer de potentes sistemas de guerra electrónica con capacidad para interferir las señales PNT (acrónimo de posición, navegación y tiempo) del adversario, pero sin afectar a los sistemas propios. Así, en el conflicto de Gaza la situación es similar. La omnipresencia de la guerra electrónica israelí impide el uso adecuado de los sistemas de armas de *Hamás*, *Hezbolá* y de cualquiera que opere en la zona y que no tenga superioridad PNT. Esto es lo que se conoce como guerra de navegación, NAVWAR (*Navigation Warfare*).

NUEVAS CAPACIDADES MILITARES

De estas lecciones aprendidas se deriva la necesidad de dotar a nuestros soldados de nuevas capacidades militares asociadas a la aparición en el campo de batalla de las tecnologías disruptivas que pasamos a describir a continuación.

• Guerra de navegación

La mayoría de los sensores y sistemas empleados en el campo de batalla (sistemas de mando y control, comunicaciones o subsistemas de navegación y guiado) utilizan la señal de navegación por satélite

para disponer de una PNT precisa. Sin embargo, presentan graves vulnerabilidades relacionadas con la degradación del rendimiento o la denegación de la señal de navegación por satélite. Al tratarse de sistemas muy dependientes de esta señal resultan muy sensibles a los ataques de denegación (*jamming*) y de suplantación (*spoofing*). Si tenemos en cuenta que el uso de perturbadores (*jammers*) se ha generalizado en todo tipo de conflictos por su eficiencia, bajo coste y facilidad de implementación podemos comprender la enorme vulnerabilidad de estos sistemas.

La pérdida de la señal de navegación por satélite hace que los errores de posición se incrementen y que, por tanto, los sistemas de armas que utilizan la navegación por satélite en entornos no estructurados (señal denegada o degradada), queden anulados para el combate. Entendemos por guerra de navegación al conjunto acciones y medidas técnicas que permitan asegurar la superioridad de la información PNT. La NAVWAR se encarga de proteger los sistemas de navegación propios, los que proporcionan posición geográfica y aquellos que facilitan señales horarias de referencia, y de degradar la información de posición, navegación y tiempo del adversario.

Para garantizar una señal PNT robusta, podemos actuar de tres maneras: protegiendo los sistemas propios de navegación por satélite mediante diversas técnicas, generando una referencia de tiempo independiente y utilizando sistemas de navegación alternativos, como los sistemas de navegación basada en terreno.

En el conflicto de Ucrania hemos visto que los equipos de guerra electrónica de última generación empleados por el ejército ruso, en particular sus bloqueadores de la señal GPS (*Global Positioning System*), son capaces de actuar a más de 500 km, permitiendo interferir las señales de orientación y posicionamiento de los satélites ucranianos, impidiendo así el empleo de municiones guiadas de precisión, dotadas de un guiado terminal GPS-inercial, o la operación de los drones ucranianos. Estas capacidades de Guerra Electrónica (EW), de las más importantes del mundo, han obstaculizado seriamente las acciones del ejército ucraniano. El asunto es de tal relevancia que el departamento de defensa americano creó en 2004 el Centro Conjunto de Guerra de Navegación.

Debemos, por tanto, trabajar en el desarrollo de tecnologías que nos permitan, por un lado, garantizar una señal PNT robusta a los sistemas propios que utilizan la navegación por satélite, como la munición de precisión *Excalibur,* en pantalla, o los sistemas de navegación de vehículos de combate, y, por otro lado, denegar la del adversario.

• Defensa antidron

Otro aspecto importante del conflicto de Ucrania ha sido que, por primera vez, hemos observado el empleo masivo de drones en tareas de inteligencia, vigilancia, adquisición de objetivos, reconocimiento o para la destrucción de objetivos tácticos, empleados como armas baratas de precisión o para colapsar las defensas antiaéreas mediante ataques en enjambre.

El ejército ruso está utilizando en sus operaciones drones sencillos, como el *Orlan-10*, para misiones de vigilancia, reconocimiento o guerra electrónica. Asimismo, dispone de drones de mayor capacidad, como el *Shahed-136* de procedencia iraní, cuyo empleo en enjambre y como dron kamikaze produce efectos físicos y psicológicos devastadores.

El ataque de un enjambre de drones se constituye, por tanto, en una verdadera amenaza para la que actualmente no estamos adecuadamente preparados. En este sentido, la OTAN exige unas capacidades mínimas a los sistemas antidron o C-UAS (*Counter-Unmanned Aerial System*).

La rápida evolución de los drones y de sus tácticas de empleo fuerza a que el desarrollo de tecnologías para hacerles frente sea absolutamente prioritario. Es crítico disponer de sistemas C-UAS con capacidad para la localización, identificación y seguimiento de la amenaza dron o enjambre de drones, desarrollando distintos tipos de tecnologías, como radares bi o tridimensionales, detectores de IR/VIS (Infrarrojo-visible), sistemas para la detección y localización de emisiones de RF de drones o sistemas para la localización e identificación de amenazas que utilicen el protocolo *Mavlink*. Además, deberán disponer de capacidad de neutralización, bien con medios de guerra electrónica, que actúen sobre el radioenlace o la señal de geolocalización del dron, lo que se conoce como *soft kill* (técnicas de *jamming* o *spoofing*), o bien con medios físicos de destrucción, como efectores cinéticos (proyectiles, cohetes o sistemas de protección activa), redes, pulso electromagnético, arma láser, enjambres defensivos, etc., lo que conocemos como *hardkill*.

CETEDEX será referente en las áreas de vehículo autónomo y conectado, defensa antidron e IA

Además, será necesario desarrollar aplicaciones de inteligencia artificial, para una simulación completa del entorno de batalla y para un sistema de gestión integral del combate C-UAS eficaz que garantice la seguridad de cualquier operación.

• Vehículos autónomos

En el conflicto ucraniano se está haciendo, asimismo, un uso extensivo de vehículos autónomos terrestres, pero sobre todo navales, dominio en el que Ucrania está teniendo notables éxitos en sus operaciones en el mar Negro.

Es, por tanto, necesario desarrollar tecnologías en los campos de la robótica y de los vehículos autónomos que permitan automatizar los sistemas heredados (*drive-by-wire*), así como desarrollar interfaces avanzados conductor-vehículo y tecnologías para la interacción

entre vehículo no tripulado terrestre y aéreo o UGV-UAV (*Unmanned Ground Vehicle, Unmanned Aerial Vehicle*). Además, se han identificado otras tecnologías críticas que, para su maduración, necesitan de modelos y algoritmia de IA (Inteligencia Artificial), entre las que se encuentran la fusión de sensores, el posicionamiento preciso en entornos complejos, la navegación autónoma en entornos no estructurados, el desarrollo de algoritmos de automatización, la planificación de itinerarios o el funcionamiento colaborativo.

• La transformación logística y la IA

De la mano de la enorme capacidad de computación actual surgen herramientas tecnológicas como la IA, los sistemas ciber físicos, el *machine learning*, los sistemas cloud, el *Big Data*... Y, así, las doce tecnologías asociadas a la industria 4.0 que optimizan los procesos logísticos. Los mandos de apoyo logístico de los Ejércitos y de la Armada están inmersos en una profunda transformación de sus estructuras, evolucionando de una logística reactiva-preventiva (logística 3.0), a una predictiva (logística 4.0), basándose en la transformación digital. Los nuevos procesos logísticos permitirán maximizar la disponibilidad operativa de los sistemas de armas, fin último de la logística militar. Es por tanto prioritario disponer de capacidades para el desarrollo de tecnologías y herramientas orientadas al mantenimiento predictivo de edificios y sistemas de armas, mediante el empleo de las tecnologías de la industria 4.0.

La IA se concibe como una herramienta transversal, capacitadora. Hemos visto que tanto las tecnologías asociadas a la NAVWAR como al desarrollo de vehículos autónomos y sistemas antidron necesitan del concurso de aplicaciones de IA. De esta manera, los desarrollos de IA deberán orientarse en este campo al análisis automático e inteligente de grandes volúmenes de datos procedentes de sensores de sistemas de armas, al desarrollo de tecnologías para el mantenimiento predictivo de plataformas y al análisis inteligente de fuentes de información en apoyo a la decisión.

PROYECTO CETEDEX

Estamos siendo testigos de terribles conflictos que están afectando a la seguridad global y que suponen enormes desafíos para nuestra forma de vida. En estos conflictos hemos visto el empleo de tecnologías disruptivas que han modificado sustancialmente las operaciones en el campo de batalla. Las lecciones aprendidas ponen de manifiesto la necesidad de dotar a nuestros soldados de capacidades militares inicialmente no previstas. Debemos por tanto desarrollar tecnologías, en forma de sistemas de armas avanzados, que proporcionen al combatiente una ventaja operativa clara en el campo de batalla. Y es en este ámbito de actuación en el que se plantea la actividad del Centro Tecnológico de Desarrollo y Experimentación de Jaén, CETEDEX, concebido como un Centro para el desarrollo ágil de aquellas tecnologías de la seguridad y la defensa que nos permitan afrontar con éxito las nuevas amenazas a la seguridad global.

CETEDEX nace para dar respuesta a esta necesidad; con la misión de desarrollar, certificar y experimentar tecnologías duales que ofrezcan soluciones innovadoras y transformadoras en las áreas de vehículo autónomo y conectado, defensa antidron e IA. Un proyecto de oportunidad que empezará a operar a finales de 2026 y estará totalmente operativo a finales de 2028.