Ciberdefensa, elemento clave en la guerra de Ucrania

EN principio pudiera parecer que la guerra de Ucrania es una vuelta a las guerras de trincheras y artillería que asolaron Europa en el siglo pasado, pero nada más lejos de la realidad. Estamos siendo testigos de la guerra tecnológicamente más avanzada de la historia de la Humanidad, y ello es debido a la exitosa utilización en el conflicto de un nuevo ámbito de las operaciones: el ciberespacio.

Contralmirante Javier Roca
Segundo Comandante del MCCE

Durante milenios, las guerras se libraban solo en el mundo físico y eran sangrientas, brutales, pero visibles. La guerra en Ucrania, aunque sigue siendo brutal, a menudo es invisible, al menos a los ojos de la mayoría. En Ucrania, el conflicto transcurre paralelamente en el ámbito físico y en el ciberespacial, y aunque solo podemos ver la punta del iceberg, la gente real sufre y muere a consecuencia de lo que ocurre en el ciberespacio.

A lo largo de la historia, la superioridad tecnológica ha sido una ventaja clave en los conflictos, pero en la actual era digital en la que vivimos, la superioridad en el ciberespacio se antoja determinante para el empleo de las nuevas Tecnologías Emergentes y Disruptivas (EDT) que transformarán el «espacio de batalla» y la forma en la que se combatirá: la inteligencia artificial, los vehículos y armamento autónomos, la computación en la nube, la sensorización, etcétera. Aunque para esto último todavía faltan unos años, la realidad del actual ciberespacio se le acerca bastante.

De nada sirve tener los mejores sistemas de armas si no conoces la ubicación, las capacidades y las intenciones del enemigo para poder emplearlas eficazmente. Y tampoco sirve de nada disponer de la mejor inteligencia del mundo (proporcionada incluso por tus aliados) si no puedes hacerla llegar en tiempo y forma al lugar donde se necesita. La enorme diferencia en la precisión, rapidez y eficiencia en el empleo de la artillería rusa y ucraniana es solo una muestra de ello. Podría decirse que el ciberespacio sustenta gran parte de capacidades militares, y por ello, como requisito previo al éxito militar, debes tener libertad de acción para operar en y a través del ciberespacio.

En Ucrania, si bien ha tenido lugar el mayor número de ciberataques destructivos que jamás haya existido a redes e infraestructuras críticas (*computer network attacks*), el uso del ciberespacio para los fines de la guerra ha ido muchísimo más allá de los tradicionales ciberataques a los Sistemas de Información y Telecomunicaciones (CIS). El mantenimiento heroico de la conectividad en el país (Internet y telefonía móvil), el empleo magistral de las Redes Sociales (Telegram, Twitter, etcétera) y el innovador desarrollo de aplicaciones móviles (App's) y herramientas web (*bots*) para apoyar el esfuerzo militar y la resiliencia de la población, están siendo fundamentales en la defensa de Ucrania y un ejemplo para las guerras del futuro. El uso de satélites de baja órbita como *Starlink*, la aplicación del *roaming* nacional, la batalla en las redes de telefonía móvil y las aplicaciones Diia, AirAlarm, Bachu, ePPO, o @eVorog_bot, entre otras muchas, son ya parte de la historia militar.

El conflicto transcurre paralelamente en el ámbito físico y en el ciberespacial


Rafa Navarro / Foto: Hélène Gicquel

Ucrania sabía que, sin el acceso seguro y confiable al ciberespacio, hubiera caído en las primeras semanas y por tanto se había preparado a conciencia en los últimos años. Muestra de ello es que desde 2019, el nuevo gobierno de Zelenski comenzó una ambiciosa transformación digital del país y de sus Fuerzas Armadas, fomentando la innovación y el desarrollo de *software*, como el creado en su Centro de Innovación y Desarrollo de Tecnologías de Defensa del Ministerio de Defensa. De este centro surgió la aplicación Delta, el «google maps» de la guerra, que ofrece unas posibilidades antes inimaginable en el combate. GIS Arta, el «uber de la artillería» es otra muestra de la capacidad innovadora de Ucrania, donde la capacidad de fusionar y compartir la información en tiempo casi real para organizar, optimizar y priorizar los ataques artilleros está siendo el factor diferenciador en el frente.

Además, el ciberespacio de interés (sus redes, sistemas y servicios) se puede defender en gran medida desde cualquier lugar y Ucrania esta recibiendo una extraordinaria ayuda tanto de países amigos como de grandes empresas tecnológicas occidentales (Space-X, Microsoft, Google, Maxar, Clearview AI, etcétera.), que aportan unas capacidades excepcionales, tanto económicas, como tecnológicas, o de influencia social. Para operar en el ciberespacio es fundamental la colaboración civil-militar, público-privada e internacional.

Mantener la conectividad en el país y desarrollar herramientas informáticas destinadas a combatir digitalmente en primera línea de batalla, ha permitido a Ucrania obtener cuatro ventajas: mantener la moral y comunicación con su población y sus Fuerzas Armadas, sosteniendo la voluntad de vencer y la fe en la victoria; multiplicar la eficacia de sus propias fuerzas, en especial en la obtención y difusión de inteligencia; obstruir la acción del enemigo, especialmente su Mando y Control, obligando a los rusos a usar frecuencias de radio abiertas y teléfonos civiles, que pueden ser interceptados; y, por último, ha logrado llamar la atención de la comunidad internacional y conseguir su apoyo y solidaridad. En tiempo record fueron capaces de crear una marca que ya es sinónimo de libertad, democracia y lucha por la independencia. Esa marca se llama «Ucrania» y el mundo occidental la adora.

Ucrania ha demostrado que incluso contra una de las potencias cibernéticas con mejores recursos del planeta, es posible defenderse siempre que se posea Unidad de Mando y una Fuerza de Operaciones en el Ciberespacio bien adiestrada y preparada para operar en el ámbito ciberespacial, coordinándose con el resto de operaciones cinéticas en el resto de ámbitos físicos.

Por todo ello, la principal conclusión de lo que estamos viendo en Ucrania en este ámbito es que, en un futuro muy próximo, en el que las operaciones se desarrollarán en un entorno multidominio donde todo va a estar interrelacionado, el control del ciberespacio bajo el concepto de un mando único será imprescindible para poder operar eficazmente en el resto de los ámbitos. Quien domine el ciberespacio y limite la libertad de acción del oponente en este ámbito, dominará la contienda.

Desgraciadamente, aunque no lo queramos o busquemos, hoy en día vivimos en permanente competencia, confrontación y, a veces, conflicto. En Ucrania hemos visto lo frágil que es la paz y la seguridad. Hay que invertir y trabajar todos los días para mantenerla. Ucrania ha demostrado que haber invertido en ciberdefensa fue un gran acierto. La ciberdefensa no es cara; lo realmente caro, a veces incluso concluyente, es no tenerla y lamentarse cuando sea «demasiado tarde».