EL EJÉRCITO Y LAS OPERACIONES EN EL CIBERESPACIO

LA GUERRA INVISIBLE

Ana Vercher / Jaén

La primera vez que se utilizó el término ciberespacio fue en el año 1984, en la novela *Neuromancer,* de William Gibson. El sector de la informática acogió esta denominación, dado el parecido de la obra con las tecnologías de redes de comunicaciones actuales. Se trata de un concepto que ha trascendido a la literatura para convertirse en realidad.

Hoy día, el ámbito del ciberespacio permea todos los aspectos de nuestra vida, cada vez con una mayor dependencia de los dispositivos digitales, y las operaciones militares no son una excepción. Por ello, integrarlo como un elemento propio y transversal dentro del Ejército de Tierra se ha vuelto imprescindible, constituyendo un factor de ventaja. Conceptos como combate multidominio, *kill web* o guerra de navegación ya están marcando el camino hacia el "Ejército 2035".

Para profundizar en estos aspectos tecnológicos clave, el Ejército ha dedicado sus jornadas "El Ejército de Tierra y los retos futuros" de 2024 al conflicto en este entorno virtual y sus implicaciones para las fuerzas terrestres. Bajo el título "El Ejército y las operaciones en el ciberespacio", este ciclo de conferencias tuvo lugar los días 6 y 7 de mayo, en el aula magna de la Universidad de Jaén.

Bgda. J. M. Dueñas (DECET)

Las jornadas fueron inauguradas por el JEME, al que acompañaron otras autoridades como el rector de la Universidad de Jaén o el jefe del MADOC

Inauguradas por el Jefe de Estado Mayor del Ejército de Tierra (JEME), general de ejército Amador Enseñat, se contó además con la presencia de numerosas autoridades civiles y militares, entre las que destacan el rector de la citada universidad, Nicolás Ruiz, y el jefe del Mando de Adiestramiento y Doctrina (MADOC), teniente general José Manuel de la Esperanza.

Estructuradas en distintas mesas de trabajo, las jornadas trataron el impacto del ciberespacio en las operaciones militares a todos los niveles, con énfasis en el nivel táctico y las operaciones multidominio, concluyendo que la obtención de la superioridad en el citado ciberespacio y en la guerra de la información está asociada a la transformación digital en curso, uno de los cuatro pilares del "Ejército 2035".

PUNTO DE SITUACIÓN Y VISIÓN DE LAS OPERACIONES EN EL CIBERESPACIO

Las jornadas comenzaron con un punto de situación de las conocidas como capacidades CIS (Sistemas de Información y Comunicaciones, por sus siglas en inglés) en apoyo a la estructura operativa de las Fuerzas Armadas. Se hizo hincapié en la amenaza omnipresente que suponen los ciberataques. Estos, sin previo aviso, pueden afectar gravemente tanto a las infraestructuras como a la población, y ya se encuentran plenamente integrados en las operaciones militares —como se está demostrando en el conflicto ucraniano—. Igualmente, se ofreció una visión del presente y futuro de las operaciones terrestres en el ciberespacio, resaltando la importancia de la preparación para realizar también acciones ofensivas en este entorno, así como la integración de las operaciones electromagnéticas y las tecnologías emergentes disruptivas, como Inteligencia Artificial (IA) y computación cuántica, entre otros aspectos.

MESA 1:

EL CIBERESPACIO COMO NUEVO ENTORNO DE OPERACIONES

Se realizó un repaso del papel que ha tenido el ciberespacio en los últimos conflictos, desde la guerra electrónica tradicional hasta la "guerra de navegación", y los mecanismos de defensa frente a la misma. El concepto CEMA (Actividades Ciberespaciales y Electromagnéticas) une de manera indisoluble el ciberespacio y el espectro electromagnético como su principal capa física. La superioridad en operaciones multidominio constituye un multiplicador para la fuerza, ya que acelera la toma de decisiones, obstruye la capacidad de mando del enemigo y permite compensar una inferioridad de efectivos con superioridad tecnológica. Por su parte, la inteligencia artificial, con un carácter completamente transversal, afecta a todas las funciones del combate. No obstante, también se pusieron de manifiesto los riesgos del uso no regulado de la misma, en una ponencia sobre el marco jurídico aplicable.

MESA 2:

CONVERGENCIA DE ACTIVIDADES ELECTROMAGNÉTICAS Y CIBERESPACIO

La seguridad de la información se fundamenta en su confidencialidad, disponibilidad e integridad. Las técnicas criptológicas actuales se están viendo comprometidas por los avances en computación cuántica, al tiempo que continuamente se crea información falsa, generada por IA, que hace cada vez menos confiable la información disponible. Para la protección de dicha información, negarla al adversario y mantener la libertad de acción, se requiere actuar coordinadamente sobre la capa física (el espectro electromagnético), la capa lógica (ciberespacio), y sobre las "ciberentidades" que pueden ser personas, organizaciones o incluso sistemas autónomos. Por último, desde el Cuartel General Terrestre de Alta Disponibilidad, se manifestó que el concepto CEMA se encuentra en rápido desarrollo en el entorno de la OTAN, repasando algunas iniciativas que actualmente están tomando forma.

MESA 3:

TECNOLOGÍAS DISRUPTIVAS Y EMERGENTES EN EL CIBERESPACIO

Se puso sobre la mesa la amenaza de la computación cuántica a la criptología actual, y la urgencia de incorporar algoritmos de cifrado postcuántico. Asimismo, se llevó a cabo un repaso de los riesgos sobre los navegadores por satélite y los mecanismos de protección contra los mismos. De igual modo, se presentaron los retos que supone la convergencia del "internet de las cosas", en las tecnologías de la información y las operacionales, destacando que la Inteligencia Artificial es una gran amenaza, a la vez que una gran aliada. Por último, se hizo una introducción de la implementación de la tecnología de comunicaciones 5G y *edge computing* en infraestructuras militares, y su aplicación en la nube táctica de combate. T