MINISTERIO DE DEFENSA

EJÉRCITO DE TIERRA

MANDO DE ADIESTRAMIENTO Y DOCTRINA

EJÉRCITO DE TIERRA
LA FUERZA DE LOS VALORES

EL EJÉRCITO Y LAS OPERACIONES EN EL CIBERESPACIO

RETOS FUTUROS

Jaén, 6 y 7 de mayo de 2024

Aula Magna de la Universidad de Jaén — Campus las Lagunillas s/n 23071

EJERCITO DE TIERRA

https://ejercito.defensa.gob.es/eventos/retos_futuros/index.html

EL EJÉRCITO DE TIERRA Y LOS RETOS FUTUROS 2024

El Ejército y las operaciones en el ciberespacio

Jaén, 6 y 7 de mayo de 2024
Aula Magna de la Universidad de Jaén

Edita:

MINISTERIO DE DEFENSA
EJÉRCITO DE TIERRA

Maquetación: Centro Geográfico del Ejército.

Fecha de edición: julio de 2024.

Las opiniones emitidas en esta publicación son exclusiva responsabilidad de los autores.

Edición no destinada para la venta.

Publicación de uso interno del departamento

Índice

Resumen ejecutivo

El aula magna de la Universidad de Jaén (UJA) fue el marco donde durante los días 06 y 07 de mayo de 2024 tuvo lugar la octava edición de las jornadas de retos futuros del Ejército de Tierra (ET), organizadas por el Mando de Adiestramiento y Doctrina del Ejército de Tierra (MADOC).

Las jornadas "El Ejército de Tierra y los retos futuros" se iniciaron en 2015 como foro de pensamiento del más alto nivel, abierto a instituciones, universidades, empresas y sociedad civil. Convocadas en la actualidad con carácter bienal, se han convertido en uno de los referentes principales de cultura de defensa que realiza el ET. Las jornadas también representan una oportunidad para debatir sobre la necesaria innovación de conceptos, estructuras y procedimientos, aspectos imprescindibles para que el Ejército se adapte con éxito a un mundo esencialmente cambiante.

Con el título "El Ejército y las operaciones en el Ciberespacio", destacadas personalidades del ámbito militar, académico, institucional y empresarial reflexionaron sobre las implicaciones que tienen las operaciones en el ciberespacio (CE). La totalidad del evento se pudo seguir tanto de manera presencial como por *streaming*.

Para el ET, el empleo acertado de las capacidades militares en el CE supone un importante factor de ventaja. Conceptos asociados a la transformación digital como combate multidominio, campo de batalla trasparente, nube de combate, "kill web", integración de actividades ciber-electromagnéticas, guerra de navegación (NAVWAR), criptografía post-cuántica y otros, asociados al empleo de tecnologías como la inteligencia artificial (IA), ya están produciendo cambios en el entorno operativo.

Para profundizar en todos estos temas, estas jornadas se estructuraron en un punto de situación y un panel el primer día y dos paneles el segundo día.

Inició las jornadas **D. Nicolás Ruiz Reyes,** Rector de la UJA, quien dio la bienvenida a los asistentes y agradeció su presencia, así como la elección de la ciudad de Jaén, y en concreto su Universidad, para la celebración de estas jornadas. A continuación, el General de Ejército **D. Amador Enseñat y Berea,** Jefe de Estado Mayor del Ejército de Tierra (JEME), inauguró la octava edición del Ejército y los retos futuros, introduciendo

la elección de la temática por su actualidad e impacto en el proyecto Fuerza 35, de transformación del Ejército de Tierra. Tomó la palabra el Teniente General **D. José Manuel de la Esperanza y Martín-Pinillos,** Jefe del MADOC, quien, tras una ambientación estratégica sobre la evolución del ciberespacio, explicó la estructura de las jornadas, con una somera introducción de los temas, mesas y ponentes.

El punto de situación inicial estuvo a cargo del Teniente General **D. José María Millán Martínez** Director del Centro de Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa (CESTIC), el Vicealmirante **D. Francisco Javier Roca Rivero** Comandante del Mando Conjunto del Ciberespacio (MCCE) y el General de División **D. Guillermo Ramírez Altozano** Jefe de la Jefatura de los sistemas de Información, Telecomunicaciones y Asistencia Técnica del Ejército de Tierra (JCISAT).

Cada panel estuvo compuesto por cuatro ponentes y un moderador que departieron sobre diferentes aspectos del ciberespacio. El primer panel trató el ciberespacio como nuevo entorno de operaciones, el segundo, la convergencia de actividades electromagnéticas y ciberespacio, y el tercero, las tecnologías disruptivas y emergentes en el ciberespacio. Después de cada panel se brindó la posibilidad de plantear preguntas, a través de una aplicación informática, al público asistente en la sala y por *streaming*.

Las jornadas finalizaron con una exposición de las conclusiones más relevantes identificadas, a cargo del General de División **D. Fernando Luis Morón Ruiz**, Director de Investigación, Doctrina, Orgánica y Materiales (DIDOM) del MADOC.

Palabras de D. Nicolás Ruiz Reyes, Rector de la Universidad de Jaén (UJA)

Las primeras palabras del rector fueron para agradecer al ET haber elegido la ciudad de Jaén y su universidad para celebrar las jornadas. Agradeció también el apoyo y respaldo institucional al alcalde de Jaén, al presidente de la diputación, a la caja rural, de forma especial al consejero de universidad, investigación e innovación de la junta de Andalucía presentes en el acto.

Sobre las jornadas afirmó que se han convertido en un espacio de reflexión para colaborar en la modernización de nuestras Fuerzas Armadas (FAS), permitiendo visualizar el futuro, anticipar retos y prever las amenazas en un contexto cada vez más complejo y más digitalizado.

En lo referente al CE puso de manifiesto que se requiere de una colaboración estrecha entre las FAS, el sector privado y la universidad, para la salvaguarda de la información y de las infraestructuras críticas. "La UJA es un referente en la ciberseguridad, en la ciencia e ingeniería de datos y en la IA aplicada a la seguridad informática y a las comunicaciones digitales, pues contamos con grandes profesionales en las dos escuelas politécnicas que tenemos en Jaén y Linares" dijo.

Citó como proyecto de referencia, la llegada del Centro Tecnológico de Desarrollo y Experimentación (CETEDEX) a la ciudad de Jaén. "Ventana de oportunidad" para la que la UJA ha suscrito una cátedra con la empresa pública Ingeniería de Sistemas para la Defensa de España S.A. (ISDEFE), la cátedra ISDEFE-CETEDEX UJA. También se han firmado dos convenios específicos de colaboración con el Instituto Nacional de Técnica Aeroespacial (INTA) para la realización de actividades científico-técnicas. Y se está adaptando la oferta formativa a las necesidades de personal cualificado que va a tener el Centro, así como el ecosistema industrial y de innovación que se genere a su alrededor. El CETEDEX tendrá un gran impacto en el desarrollo y progreso de Jaén si todas las partes implicadas actúan con sentido de estado, lealtad institucional y unidad de acción.

Palabras del General de Ejército D. Amador Enseñat y Berea, Jefe del Estado Mayor del Ejército

Tras saludar a las autoridades y a todos los asistentes, recordó que desde 2015 el Ejército de Tierra viene celebrando las Jornadas sobre Retos Futuros con el propósito de constituirse como un foro de discusión entre diferentes grupos de pensamiento, los medios de comunicación social, el mundo académico y el empresarial, con la aspiración de llegar a ser un referente intelectual y cultural provechoso para la mejora de nuestro Ejército.

Comenzó su intervención señalando cómo los dominios, espacios en los que las fuerzas armadas deben ser capaces de operar y que tradicionalmente habían sido los

espacios físicos: terrestre, marítimo y aéreo, ahora incluían dos nuevos no físicos: el cognitivo y el CE, al tiempo que se ampliaba el aéreo con el espacio. También, cómo las fuerzas terrestres, claves en el dominio terrestre, podrán producir efectos y llevar a cabo acciones en los otros dominios.

Definió el dominio ciberespacial como el "espacio artificial compuesto por infraestructuras, redes, sistemas de información y telecomunicaciones y otros sistemas electrónicos, por su interacción a través de las líneas de comunicación sobre las que se propaga y el espectro electromagnético (EEM), así como por la información que es almacenada o transmitida a través de ellos".

En estos nuevos espacios de batalla será el Gobierno de la Nación quien asigne qué responsabilidades les corresponden a las Fuerzas Armadas como elemento esencial de la defensa de España. Al ET se le plantea el reto de desarrollar las capacidades necesarias que nos puedan ser requeridas para cumplir nuestra misión.

En este reto, destacó la función del MADOC y en concreto de la DIDOM como líder en el proceso de elaboración de la doctrina sobre la que desarrollar la organización, los recursos humanos, los materiales, las infraestructuras y finalizar con el adiestramiento. Afirmó que "de la mano del MADOC deben ir la universidad y la empresa porque somos plenamente conscientes de que así lo haremos mucho mejor". El ámbito universitario proporcionará un valioso apoyo desde el conocimiento, mientras que la industria será la responsable de madurar y producir los materiales y el software necesario para equipar a nuestras unidades. Por ello, el General de Ejército agradeció a ambos su apoyo y les pidió que siguieran trabajando con el ET.

Finalizó con agradecimientos a la Diputación de Jaén, a la Fundación Museo del Ejército, a la Fundación Caja Rural de Jaén y a la UJA por sus aportaciones y su absoluta implicación. También agradeció a la ciudad y provincia de Jaén su acogida y el esfuerzo realizado por el MADOC en la organización y coordinación.

Palabras del Teniente General D. José Manuel de la Esperanza y Martín-Pinillos, Jefe del Mando de Adiestramiento y Doctrina (MADOC)

Inició el Teniente General su intervención señalando cómo se ha transformado la economía mundial con la entrega al dominio público de la web y el aumento de la población con acceso a la red, pero también, cómo con ello se ha dado lugar a la aparición de nuevos riesgos y amenazas a la seguridad.

A modo de ejemplo, hizo un repaso de algunos acontecimientos conocidos en los que el CE se ha revelado como nuevo campo de confrontación con una importancia cada vez mayor.

Afirmó que occidente ha perdido la ventaja indiscutible de ser el centro neurálgico de la industria vinculada a Internet. Y que, como respuesta, en el seno de la Alianza Atlántica se trata de adquirir capacidades en esta materia, y se contempla que un ciberataque "severo" podría justificar la activación del Artículo 5 del Tratado. El control de los centros de datos e instalaciones que sostienen internet se ha convertido en una baza geopolítica dado que prestan servicios a cientos de millones de usuarios. Se trata de puntos sensibles y vulnerables a ataques de todo tipo, desde el daño físico, el control remoto o el acceso a la información.

Por otro lado, expuso las posibilidades que da internet para el uso malicioso de técnicas de ingeniería social y manipulación psicológica que facilitan llevar a cabo acciones de desestabilización, tanto para los estados como para organizaciones criminales, destacando la dificultad de articular una respuesta ajustada a derecho para enfrentarlas.

Teniendo en cuenta estas consideraciones, dijo, "se puede comprender por qué se ha elegido el tema 'El Ejército y las operaciones en el ciberespacio' para las jornadas de retos futuros de este año en Jaén".

Continuó su exposición señalando los desafíos que para el ET suponen el escenario actual y el futuro previsible: la filosofía del "mando orientado a la misión", el concepto de "Fuegos en red", la implantación de la IA y el plan de experimentación. Desafíos en los que es obligado integrar el CE como un elemento propio y transversal al de todas de sus actividades.

Tras hacer un repaso de las actividades programadas para las jornadas, finalizó con su agradecimiento a los organizadores de la UJA y del MADOC y su deseo de que los temas resultaran del interés de los asistentes.

Punto de situación

La Primera intervención, con el título "**Capacidades CIS/TIC en apoyo de la estructura operativa de las Fuerzas Armadas",** estuvo a cargo del Teniente General **D. José María Millán Martínez**, Director del Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC) del Ministerio de Defensa.

Centró el ponente su exposición en los retos que, para las Fuerzas Armadas en general y para el Ejercito de Tierra en particular, supone la necesidad de desplegar, en un contexto de hiperconectividad, unas capacidades CIS/TIC cada vez más complejas que permitan: asegurar la libertad de acción en el CE, obtener la superioridad de la información y la ejecución de operaciones multidominio.

El primer reto es admitir que en las operaciones militares y en las actividades de preparación de la Fuerza debe participar CESTIC, que apoya y permite la provisión y gestión de los servicios a través de Infraestructura Integral de Información para la Defensa (I3D), incluidas la capacidad de mando y control y la ciberseguridad. La I3D llega hasta las unidades desplegadas en el terreno, señaló el Teniente General.

Como corolario de este primer reto, añadió los siguientes:

Segundo reto. Integrar plenamente a la Dirección General del CESTIC en el planeamiento operativo de los Ejércitos y Armada en las operaciones y despliegues específicos que lleven a cabo y que requieran de las capacidades tecnológicas del Ministerio de Defensa (MINISDEF).

Tercer reto. Siendo aspectos inherentes al CESTIC las operaciones en el CE de infraestructura y defensivas se hace necesario integrarlas con el resto de acciones, condición indispensable para alcanzar y mantener la libertad de acción de las fuerzas propias. Lo que se conseguirá cuando el MINISDEF en su conjunto comparta una única visión de la situación de seguridad de la información.

Cuarto reto. Como consecuencia del desarrollo de las tecnologías en el ámbito CIS/TIC se produce la necesaria y rápida evolución de la I3D, lo que obliga a CESTIC y a las FAS a mantener una visión compartida y la alineación con las necesidades de la estructura operativa.

Resumió el ponente los cuatro retos anteriores en uno de orden superior transversal, fundamental para responder a las necesidades de apoyo CIS/TIC a la estructura operativa de las FAS: el cambio cultural que permita entender y asumir la Transformación Digital.

Finalizó su intervención con un repaso de los principales aspectos que incluye el cambio digital de los que dijo que "todos tienen un factor común: la consideración de la información como recurso estratégico para todas las actividades del MINISDEF, incluidas las operaciones". Concepto este que afecta no al ET como organización sino a sus miembros, a cada uno desde su puesto en la organización, con sus responsabilidades y sus posibilidades de actuación.

La segunda conferencia **"Lecciones Aprendidas del conflicto ucraniano"** fue presentada por el Vicealmirante **D. Francisco Javier Roca Rivero**, Comandante del Mando Conjunto del Ciberespacio (MCCE).

Comenzó su intervención refiriéndose a la guerra de Ucrania y afirmando que, aunque pudiera parecer otra cosa, estamos siendo testigos de la guerra tecnológicamente más avanzada de la historia debido a la exitosa utilización de un nuevo ámbito de las operaciones: el ciberespacio. El conflicto trascurre paralelamente en el ámbito físico y en el ciberespacial, por lo que en gran medida resulta invisible a los ojos de la mayoría.

El Almirante centró su presentación en lo que para él son, en lo referente al CE y el nivel estratégico, las 10 lecciones aprendidas de la guerra de Ucrania:

1. Para asegurar en todo momento la libertad de acción en el CE es imprescindible prepararse con tiempo y dotarse de personal y capacidades militares que permitan realizar operaciones defensivas, de inteligencia y de respuesta en el CE.

2. A través del CE se puede atacar a las infraestructuras críticas y servicios esenciales de un país y a su sociedad, influyendo y alterando las actitudes.

3. La conectividad a través del CE favorece la comunicación entre los líderes, su población y sus Fuerzas Armadas, fortaleciendo la voluntad de vencer. También ha permitido mantener la atención de la comunidad internacional y conseguir su apoyo y solidaridad.

4. La superioridad en el CE permite multiplicar la eficacia de las fuerzas propias, en la obtención y difusión de inteligencia, y obstruir la acción del enemigo, especialmente su mando y control.

5. La innovación tecnológica se antoja determinante y resulta necesario captarla donde surja.

6. Al no ser las Fuerzas Armadas el principal cliente de las grandes tecnológicas es fundamental el uso dual de las capacidades civiles en refuerzo o respaldo de las capacidades militares.

7. Las grandes empresas tecnológicas jugaran un papel cada vez más importante en los conflictos futuros. Resultará imprescindible contar con su apoyo. Más del 90 % de nuestro CE de interés es propiedad privada.

8. El CE de interés se puede defender desde cualquier lugar, no requiere "tropas sobre el terreno", operar en el CE requiere de la colaboración civil-militar, público-privada e internacional.

9. Durante el planeamiento, los ciberataques se han integrado con las operaciones cinéticas, pero una vez que se ha declarado la guerra abierta, se han limitado más a la desinformación y el espionaje, adquiriendo un mayor protagonismo las operaciones de gestión del espectro electromagnético y guerra electrónica (EW).

10. En el CE es mucho más difícil defender que atacar.

Finalizó su intervención señalando que: "Ucrania conocía la amenaza ciber y se ha preparado durante muchos años para esta guerra, protegiendo y defendiendo su columna vertebral como país: las infraestructuras y servicios críticos, su Ministerio de Defensa y su Ministerio de Interior.

Concluyó este punto de situación, con la conferencia **"Una visión del presente y futuro de las operaciones terrestres en el ciberespacio",** el General de División **D. Guillermo Ramirez Altozano**, Jefe de la Jefatura de los sistemas de Información, Telecomunicaciones y Asistencia Técnica del Ejército de Tierra (JCISAT).

Comenzó su intervención exponiendo la necesidad de que las FAS se preparen y se doten de medios específicos para combatir en el CE, pues las características de los distintos ámbitos o dominios condicionan las capacidades con las que se opera en ellos.

Del ámbito ciberespacial señaló su transversalidad por lo que las actuaciones

en el mismo influyen directamente en el resto de los ámbitos (terrestre, aéreo, marítimo, espacio y cognitivo). También como el CE es empleado por todas las unidades de las FAS con independencia del ámbito en el que centran su actuación. Y como en el ET, todas las grandes unidades cuentan con personal expresamente dedicado al CE.

De la ciberdefensa señalo los tipos de acciones: de defensa, en la que participan todas las unidades del ET como usuarios de los sistemas, de explotación y de ataque. Estas centralizadas por motivos de eficiencia y disponibilidad de recursos, en el caso del ET, en los dos regimientos de EW. Todas estas capacidades específicas están dirigidas técnicamente desde la JCISAT, de acuerdo a la normativa específica del ET.

La finalidad de la organización descrita es preservar o ganar la libertad de acción en el CE de interés militar, impedir o dificultar su uso por parte del adversario, y contribuir a alcanzar la superioridad en el enfrentamiento en el resto de ámbitos físicos y cognitivos.

En cuanto a las lecciones aprendidas de la guerra de Ucrania en el ámbito ciberespacial, el ponente destacó cuatro de nivel táctico de las operaciones:

1. La necesidad de constituir puestos de mando diferentes. La supervivencia gana peso respecto la eficiencia, exigiendo capacidades de mando y control en movimiento, servicios distribuidos, mayor seguridad de la información y una reducción de la huella humana y electromagnética.
2. El empleo de la EW es clave.
3. El efecto multiplicador en el ámbito ciberespacial de la combinación sinérgica de actividades ciberespaciales y electromagnéticas (CEMA), ciberdefensa y EW, en el ámbito táctico.
4. La combinación de las operaciones electromagnéticas con actividades en el ámbito cognitivo.

Finalizó su intervención señalando las acciones que según su criterio debería llevar a cabo el ET como consecuencia de estas y otras lecciones aprendidas:

1. Implementar una nube de combate integrada en los CIS de los niveles superiores.
2. Llevar a cabo una mayor integración de las operaciones electromagnéticas de EW y ciberdefensa y avanzar hacia un aumento de la capacidad de acciones de ciberdefensa ofensivas en el nivel táctico.

3. Ser capaz de hacer frente a la irrupción masiva de la IA y de la computación cuántica en todos los ámbitos y en el ciberespacial en particular.
4. Adoptar un nuevo liderazgo orientado a misión abierto a las nuevas tecnologías.
5. Disponer de una logística de obtención de recursos tecnológicos que aúne los esfuerzos de los actores militares involucrados en el proceso con las empresas y los expertos del mundo académico.

Primera mesa redonda. "El ciberespacio como nuevo entorno de operaciones"

La mesa estuvo moderada por **D. José de la Peña Muñoz**. Licenciado en Ciencias de la Información por la Universidad Complutense de Madrid y director de la revista española SIC Seguridad en Informática y Comunicaciones.

La primera ponencia titulada **"Ecuación ciberespacio = CIS + CEMA"** fue presentada por el Coronel **D. Francisco José Oliva Bermejo,** Jefe de la Sección de Inteligencia de Señales y Guerra Electrónica de la Subdirección de Actividades en el Ciberespacio y Electromagnéticas del ET.

La ponencia versó sobre tres ideas fundamentales: la primera, cómo el hombre, gracias a la tecnología, ha creado un nuevo ámbito de operaciones que se requiere asegurar; en segundo lugar, cuáles son sus características y composición; y, por último, cual es el impacto que tiene en las operaciones militares.

Con la implantación de los sucesivos avances tecnológicos, se hablaba inicialmente de telecomunicaciones y de EW. Después, del radar y la ampliación del uso del espectro electromagnético, ese elemento tan físico como es el agua del mar. Y más tarde el gran salto, cuando los Estados Unidos buscaron la forma de salvaguardar sus comunicaciones militares mediante redes de comunicación distribuidas (ARPANET, 1962), luego Internet (1983) y la world wide web (1992). El desarrollo de la informática de consumo y la tecnología inalámbrica hicieron el resto, construyéndose de forma abierta y anárquica un nuevo espacio común global por donde discurre nuestra economía, la información o el ocio.

Para el análisis de las características y composición de este espacio, estableció un interesante paralelismo entre el CE, dominio físico artificial y global y el mar, dominio físico, global e inicialmente común en este caso natural. El CE se compone de elementos físicos de información y telecomunicaciones, su interconexión y la información almacenada o transmitida a través de ellos. Es decir, los ordenadores, servidores, dispositivos, radares son los componentes físicos (los barcos, submarinos), que se interconectan a través del espectro electromagnético (el mar) y transportan información (mercancías) con capacidad de generar efectos en otros dominios físicos y/o cognitivos. En este sentido, afirmó que, si las acciones sobre los barcos son las operaciones en el CE y la actuación sobre el mar las electromagnéticas, parece necesario coordinar las acciones sobre los barcos y sobre el agua. Su equivalente es la sincronización y coordinación de las actividades ciberespaciales y electromagnéticas (CEMA).

Finalmente, sobre la influencia del CE en las operaciones, señalo que la libertad de acción, imprescindible para combatir en la nube, no se alcanza sin superioridad en el espectro electromagnético, lo que hace que CEMA sea vital para el éxito de las operaciones multidominio. Sin olvidar que el poder de alcanzar las mentes gracias a la hiperconectividad permite modificar el curso de la guerra que se desarrolla en los espacios terrestres, marítimos, aéreos o espaciales, pero que sobre todo es de naturaleza cognitiva.

La segunda ponencia fue **"El papel del Ciberespacio en los últimos conflictos"** del Coronel **D. Ignacio Javier Simón Andújar**, jefe de la Jefatura de Telecomunicaciones y Guerra Electrónica del Mando Conjunto del Ciberespacio del Estado Mayor de la Defensa.

Inició señalando la importancia del control del CE, tal y como ha quedado patente en los últimos conflictos, entendiendo por CE que nos referimos a capacidades de ciberdefensa (CD), de sistemas de comunicaciones e información (CIS), de gestión del espectro electromagnético (EEM) o *Spectrum Management* (SM), de navegación e identificación (NAVID) y, por último, de EW o electromagnética (EW), que es como se la denomina ya en OTAN.

Para este control efectivo del CE es esencial desarrollar adecuadamente las operaciones electromagnéticas (EMO) y en el espacio (comunicaciones posicionamiento y observación). Los CIS y las capacidades de CD también están directamente relacionadas con estas EMO.

Estas capacidades de las EMO vinculadas a la transformación digital permitirán: 1) conducir operaciones multidominio, 2) asegurar la interoperabilidad en todos los dominios, 3) mejorar la conciencia situacional y 4) facilitar las consultas políticas y acelerar la toma de decisiones basadas en una muy eficiente gestión de los datos.

Afirmó también, que los recientes conflictos bélicos han puesto de manifiesto la importancia de la explotación, tanto de nuevas tecnologías, como el mantener las capacidades que ya se venían empleando en el CE.

Hizo a continuación un repaso del empleo de algunas de estas capacidades (PNT/NAVWAR[1], SATCOM[2], SEOT[3], EW, comunicaciones tácticas, sistemas de identificación) en los últimos conflictos señalando acciones llevadas a cabo, procedimientos empleados, efectos producidos, uso combinado de las mismas, importancia de las interacciones publico privadas, etc.

La tercera Ponencia de esta mesa trató de las **"Operaciones Multidominio y Ciberespacio"** y fue presentada por el Coronel **D. Bonifacio Gutiérrez de León,** subdirector de Investigación y Lecciones Aprendidas del Mando de Adiestramiento y Doctrina del Ejército de Tierra.

Comenzó su disertación afirmando que nos encontramos en un punto de inflexión entre la forma en que se libran actualmente las guerras y cómo se librarán en el futuro, como consecuencia de dos factores fundamentales:

Primero: la utilización para ejercer su poder, por parte de determinados regímenes, de tácticas y actividades, por debajo del umbral de un conflicto armado abierto, basadas en gran medida en el uso imaginativo del CE y del espectro electromagnético.

Segundo: tecnologías de sensorización, misiles de precisión de largo alcance, armas hipersónicas, municiones controladas remotamente, robótica, sistemas autónomos, computadoras cuánticas, la conexión en red o la IA permitirán localizar objetivos con precisión a mayor distancia, permitiendo atacarlos con rapidez desde más lejos.

Como consecuencia de la necesidad de enfrentarse a un enemigo capaz de aunar ambos factores, la Alianza Atlántica ha puesto en marcha el concepto de operaciones multidominio (OMD) para integrar los nuevos espacios de operaciones con los tradicionales y definir las capacidades que necesarias.

---

1 Posicionamiento, navegación y sincronismo/guerra de navegación.

2 Satélites de comunicaciones.

3 Sistemas espaciales de observación de la tierra.

Las OMD son una evolución de las operaciones conjuntas hacia otras centradas en operar más eficazmente las capacidades espaciales, ciberespaciales y cognitivas y en las que se debe contar con otros actores no militares que pueden contribuir al éxito. Los elementos clave en que se apoyan son: la integración de los nuevos ámbitos, un necesario cambio de mentalidad, la irrupción masiva de las tecnologías emergentes y disruptivas (EDT), un mando y control colaborativo, ágil y capacitado, una mayor conectividad e interoperabilidad.

A continuación, abordó el CE como fuente de oportunidades para las fuerzas terrestres en las OMD. Entre ellas mencionó las siguientes:

— Garantizar unas comunicaciones globales seguras, una *Common Operational Picture* (COP) compartida y la seguridad de las operaciones.

— Mantener la libertad de acción en el campo de batalla y restringir la del adversario.

— Ejercer el mando y control en ambientes electrónicamente degradados.

— Actuar sobre las audiencias autorizadas a través de las redes sociales y otras aplicaciones, para realizar operaciones de influencia específicas.

— Disponer de un conocimiento exacto de la situación logística propia en tiempo real, interoperable con otros ejércitos y organismos.

En contraposición, y para cerrar su intervención, también dijo que no disponer de libre acceso al espectro electromagnético y al CE constituye una importante vulnerabilidad.

La cuarta y última ponencia de la primera mesa titulada **"El marco jurídico del ciberespacio. Su incidencia en materia de Defensa"** estuvo a cargo de **D. Manuel Medina Guerrero,** catedrático de Derecho Constitucional de la Universidad de Sevilla.

Al inicio de su intervención el ponente habló de la normativa que la Unión Europea ha introducido, en el marco del Tratado, dado el potencial riesgo que entraña la utilización de estas tecnologías para los derechos de los ciudadanos. Esta normativa tiene por finalidad introducir restricciones, condicionantes y garantías en el uso de estos sistemas automatizados. Es el caso del Reglamento General de Protección de Datos (Reglamento 2016/679), que consagra el derecho a no ser objeto de decisiones automatizadas y reconoce un amplio catálogo de derechos sobre el tratamiento de datos personales y, de mayor relevancia aún, el Reglamento de Inteligencia Artificial, dedicado a la regulación de los sistemas algorítmicos, que prohíbe determinadas prácticas de IA y delimita la categoría de "sistemas de IA de alto riesgo".

Sin embargo, las actividades relativas a la defensa y seguridad nacional de los estados miembro de la Unión, así como la IA de uso militar, están excluidas de la aplicación de ambos reglamentos.

La razón de ser de esta exclusión en el ámbito militar y de defensa se justifica por el propio Tratado de la Unión Europea, que subraya que "la seguridad nacional seguirá siendo responsabilidad exclusiva de cada Estado miembro", y queda fundamentado por las especificidades de las políticas de defensa de los Estados miembros y de la Unión "que están sujetas al Derecho Internacional Público, que es, por tanto, el marco jurídico más adecuado para la regulación de los sistemas de IA en el contexto del uso de la fuerza letal y de otros sistemas de IA en el contexto de las actividades militares y de defensa".

En consecuencia, el ponente señaló al Derecho Internacional Público como regulador de los sistemas de IA diseñados y utilizados para fines militares y de defensa, pero también planteó el debate que produce la necesidad de aclarar cómo han de interpretarse estas reglas y principios al proyectarse en un contexto (el cibernético) desconocido cuando los mismos se formularon, como, por ejemplo, cuándo nos hallamos ante un supuesto de "ataque armado", premisa para el ejercicio del derecho de legítima defensa. Asimismo, han de tenerse presentes los problemas de atribución inherentes a los ciberataques.

Finalizó su intervención señalando el encendido debate en torno a los denominados sistemas letales de armas autónomas, aquellos que seleccionan y atacan objetivos sin intervención humana, con el riesgo de que una defectuosa configuración del sistema algorítmico pueda suponer la vulneración de los principios del citado Derecho Internacional Humanitario. Y aunque no faltan voces que propugnan la prohibición, parece que la fórmula más razonable sea la de establecer una regulación específica.

Segunda mesa redonda. "Convergencia de actividades electromagnéticas y ciberespacio"

La catedrática del Departamento de Informática de la UJA **D. María Teresa Martín Valdivia** se encargó de moderar esta mesa. En ella, la primera ponencia titulada **"La seguridad de la información"** corrió a cargo de **D. Manuel José Lucena López,** Profesor Titular de Ciencias de la Computación e Inteligencia Artificial de la UJA.

Comenzó el ponente poniendo de relieve la importancia que

ha tenido, en el éxito evolutivo de la humanidad, la capacidad de obtener, procesar e intercambiar información. Señaló los principales hitos que a lo largo de la historia han hecho posible llevar a cabo estas tareas de forma eficiente: la escritura, la imprenta y finalmente la informática y las telecomunicaciones que han dado lugar a un nuevo escenario, el CE. Esta importancia de la información convierte en crucial su seguridad, mucho más en el mundo de las telecomunicaciones y más aún, de la información relacionada con la defensa.

Para poder identificar algunos de los retos que presenta la seguridad de la información, D. Manuel analizó las tres características que debe cumplir ésta: la confidencialidad, la disponibilidad y la integridad:

1. Confidencialidad: hacer llegar la información a sus destinatarios e impedir que otros agentes puedan acceder a la misma. Históricamente, para esta tarea se ha combinado el uso de la criptografía con la protección de los medios físicos de comunicación. En la actualidad, al no tener la certeza de los medios físicos por los que viaja nuestra información (internet), la criptografía es un elemento crítico.

2. Disponibilidad: garantizar que nosotros mismos vamos a poder acceder a nuestra información. Aquí los retos son más complejos ya que existen múltiples métodos, propios del CE como el secuestro y destrucción de datos o del espectro electromagnético como generación de interferencias e inutilización de los enlaces físicos. Pero el verdadero reto es la saturación de información inútil que viaja por las redes de telecomunicaciones.

3. Integridad: garantizar que la información viaja sin errores. Quizás el reto más acuciante para la seguridad de la información se encuentra en esta característica y es la información falsa.

Con esta reflexión, para finalizar, el profesor planteó la hipótesis de un nuevo hito en la historia del uso de la información: la IA. Estamos desarrollando dispositivos capaces de igualar habilidades que se creían exclusivas de los seres humanos y, con ello, la generación de información falsa indistinguible de la realidad.

La segunda ponencia de esta mesa **"La Coordinación y sincronización de las operaciones en el ciberespacio y las operaciones electromagnéticas"** fue impartida por el Coronel **D.Manuel Sasot Oliván,** Subdirector de Actividades en el Ciberespacio y Electromagnéticas de la Jefatura de los sistemas de Información, Telecomunicaciones y Asistencia Técnica del Ejército de Tierra (JCISAT).

Comenzó el Coronel dejando claro que el CE está constituido por tres capas. Una física, compuesta por los sistemas hardware, incluidos los sistemas de telecomunicaciones y su interacción con el soporte de transmisión. Otra capa lógica, compuesta por software, datos, en definitiva, por información digitalizada. Y una tercera constituida por las ciberpersonas o identidad virtual de las personas u organizaciones reales. Como consecuencia, en un ámbito con capas físicas y virtuales, a la vez, se requiere de la coordinación de las acciones en todas estas capas del CE.

Con relación a las operaciones en la capa física afirmó que el espectro electromagnético se ha convertido en el principal soporte de transmisión. Se trata de un recurso finito cada vez más escaso y donde la demanda aumenta sin cesar.

Por su parte, las operaciones en el CE centran sus actividades en la capa lógica y sus efectos pueden producirse sobre las ciberpersonas.

El acceso a la capa lógica requiere actuar sobre la capa física. Los niveles más altos se encuentran en las grandes redes de comunicaciones basadas en fibra óptica y en internet. Pero a niveles inferiores, la capa física es el espectro electromagnético, principal soporte de transmisión.

Las operaciones en el CE hacen necesario sincronizar y coordinar las actividades en ambas capas. Así nace el concepto de CEMA, actividades que tratan de conseguir efectos complementarios que no podrían alcanzarse mediante su empleo por separado, impidiendo conflictos e interferencias mutuas que reduzcan o anulen su efectividad, para garantizar la superioridad y mantener la libertad de acción en el CE y el espectro electromagnético, mientras se niega o degrada su uso por parte del adversario.

Para finalizar, el ponente puso de manifiesto que es preciso crear en el seno de los cuarteles generales desplegables un órgano capaz de sincronizar y coordinar estas operaciones e integrarlas en el resto, así como mejorar los medios, tácticas, técnicas y procedimientos.

La tercera ponencia versó sobre **"Convergencia de Actividades Electromagnéticas y Ciberespacio. Concepto CEMA en OTAN"** y fue presentada por el Coronel **D. Víctor Valero García,** Adjunto CIS del Cuartel General Terrestre de Alta Disponibilidad de OTAN en Valencia (CGTAD).

Inicialmente el ponente introdujo el concepto de la estructura militar de la OTAN con la finalidad de encuadrar la estructura de fuerzas que aportan las naciones, en concreto el caso del CGTAD en su faceta de Cuerpo de Despliegue Rápido Español de la OTAN (NRDC-ESP).

Examinó a continuación cómo la OTAN ha ido adaptando la organización de sus estructuras y desarrollando las actividades de los Sistemas de Comunicaciones e Información (CIS), de las Operaciones en el Ciberespacio (CO) y de la EW, pero por ahora, sin aplicar el concepto CEMA. De momento, dijo, en la doctrina de alto nivel el CE es un dominio mientras que el espectro electromagnético es un entorno. Además, tanto las CO, como los CIS y la EW tienen sus propias doctrinas, relacionadas, pero distintas.

En cambio, Estados Unidos y el Reino Unido sí han abrazado el concepto CEMA. Estados Unidos ya ha creado a nivel "Combatant Command" las llamadas "Multidomain Task Forces", que incluyen compañías CEMA, y el Reino Unido ha anunciado la organización de un Grupo de Efectos CEMA que va a agrupar dos regimientos de EW y uno de transmisiones bajo un mando común. España reconoce la necesidad de una coordinación más estrecha, pero todavía no lo refleja en su doctrina. Podemos decir que es un reto futuro.

En lo que se refiere al NRDC-ESP, el coronel dijo que para el acceso al CE en el nivel táctico es imprescindible que disponga de las capacidades ciberespaciales y electromagnéticas que necesita y que las pueda gestionar de la forma más rápida y eficaz. Para lograrlo y ante la necesidad de aplicar el concepto CEMA, el NRDC-ESP diseñó e implementó a

lo largo del año 2021 el Centro de Operaciones CEMA (CEMOC) sobre la base de los elementos existentes en la División CIS (DIVCIS) (CIS; Ciberseguridad, EW y FM) y en G2 el SEWOC (SIGINT and EW Operations Center) y G3 (Cyber Force Protection). Todos estos elementos se pusieron bajo la dirección de la célula de planes de la DIVCIS para incardinarlos directamente con el planeamiento de las operaciones.

Finalizó su ponencia señalando el próximo reto al que se enfrenta el NRDC-ESP, adoptar las CO como parte de su combate, en lugar de considerarlas como un apoyo a sus operaciones. El CEMOC es un primer paso para conseguirlo.

La cuarta y última ponencia de la segunda mesa titulada **"Implementación de la ciberdefensa y la guerra electrónica"** la expuso el Coronel **D. Miguel Angel San Segundo,** Jefe del Regimiento de Guerra Electrónica nº 31 del Ejército de Tierra.

Igual que desde los primeros aviadores, Ingenieros del Ejército, hasta la creación del Ejercito del Aire trascurrieron casi 30 años, "considero que estamos en un momento similar, donde las operaciones en el dominio ciberespacial están en tránsito hacia su futuro" comenzó afirmando el Coronel.

Sobre las capacidades de Ciberdefensa militar y refiriéndose al Regimiento de Guerra Electrónica nº 31 (REW31) bajo su mando, dijo llevar desde 2018 implementándola a través de Centros de Operaciones Desplegables en todas las redes tácticas y operacionales instaladas por el ET y en redes no clasificadas y de moral y bienestar desplegadas en ZO.

También comentó su participación activa junto con el Mando Conjunto de Ciberdefensa (MCCE) que lidera las operaciones ofensivas y con el Centro de Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa (CESTIC) y la Jefatura de los sistemas de Información, Telecomunicaciones y Asistencia Técnica del Ejército de Tierra (JCISAT) junto con quien el propio REW 31 asume el liderazgo de las defensivas. "Mi Regimiento, mediante un proceso de formación permanente,

aportando un recurso humano cualificado y capacidades modulares y transportables, realiza monitorización, inspección y *pentesting*, análisis de *malware*, análisis forense y gestión."

Respecto a la EW dijo que actualmente ponen estas capacidades al servicio de los escalones más bajos con equipos ligeros y equipos móviles y a través del Sistema "Gesta" para los escalones división y superior. Dispone de capacidades vinculadas al uso del espectro electromagnético más clásico de localización, interceptación y escucha (ESM) y las de perturbación. Por otra parte, se debe seguir avanzando para obtener capacidades de vigilancia y perturbación/intrusión sobre la telefonía móvil y comunicaciones satelitales; capacidades de perturbación sobre los sistemas de navegación, las municiones guiadas, los UAV y los UGV o en el diseño de perturbadores dispersables o desplegables, de pequeño tamaño y bajo coste, incluso de un solo uso que generen interferencias por tiempo limitado y a demanda.

Finalizó con una reflexión de como la IA puede colaborar a implementar la EW en el medio plazo sobre los tres pilares, ESM-Vigilancia, ECM-perturbación y EPM-Protección. En una inmensidad de datos, estas ayudas deben estar orientadas a acortar el ciclo de la decisión propio y a generar un espectro degradado que ralentice al adversario.

Tercera mesa redonda. "Tecnologías disruptivas y emergentes en el ciberespacio"

Esta mesa fue moderada por el Coronel **D. Javier Bermejo Higuera,** Subdirección General de Sistemas Terrestres del Instituto Nacional de Técnicas Aeroespaciales (INTA)**.**

La primera ponencia titulada **"Ciberseguridad en la Era Cuántica: Desafíos y Oportunidades para el Ejército de Tierra"** corrió a cargo del Teniente Coronel **D. Carlos Herrero Santos**, Jefe de Sistemas de Mando y Control y Simulación de la Sección de Ingeniería de Tecnologías de la Información, Telecomunicaciones y Simulación de la Jefatura de Ingeniería del Mando de Apoyo Logístico del Ejército de Tierra.

En su introducción sobre la física cuántica y sus posibles aplicaciones, el Teniente Coronel puso de manifiesto que la computación cuántica constituye una amenaza, a corto plazo, para los algoritmos de cifrado más robustos utilizados en la actualidad.

Frente a este desafío, afortunadamente, dijo, existen planteamientos y posibles soluciones en la nueva era post-cuántica de las comunicaciones y la seguridad de la información.

Señaló soluciones híbridas que emplean, junto con los algoritmos actuales, nuevos algoritmos frente a la computación precuántica inicialmente y a la computación postcuántica en el medio plazo. O bien la migración paulatina de todos los sistemas criptográficos hacia otros con algoritmos criptográficos postcuánticos.

Continuó el ponente citando los servicios de seguridad más relevantes que se verán influidos en materia de comunicaciones cuánticas y finalizó subrayando la exigencia de que la industria, las universidades y el Ejército participen en la detección de necesidades y la búsqueda de soluciones que permitan mantener la soberanía en el demandante campo de las tecnologías cuánticas en el ámbito de la Defensa.

A continuación, para hablar de **"Tecnologías de Guerra de Navegación (NAVWAR)"** intervino **D. Manuel Pérez Cortés,** Director General de Defensa y Seguridad de la empresa GMV.

Comenzó hablando de la alta dependencia de las operaciones militares con respecto de los sistemas de Posición, Navegación y Tiempo (PNT) que a su vez usan como fuente

primaria los *Global Navigation Satellite System* (GNSS). De ahí que la capacidad de degradar o imposibilitar la recepción de señales GNSS por parte del adversario y asegurar la recepción propia resultan de vital importancia. Esto es lo que se denomina *Navigation Warfare* (NAVWAR).

Dijo en relación a los ataques NAVWAR que son exitosos y proporcionan una muy buena relación eficacia-coste al atacante. Del NAVWAR defensivo, afirmó que pasa por poder identificar las señales en las que se puede confiar, al mismo tiempo que se detectan y descartan aquellas que están comprometidas.

Habló de la Integridad de los GNSS como la medida de la confianza que se puede poner en que la información proporcionada por el sistema es la correcta. Esto incluye la capacidad para detectar errores y alertar al usuario. Al hablar de los riesgos, resaltó que:

— El *jamming* es una interferencia genérica que anula la capacidad del receptor de seguir las señales GNSS.

— El *spoofing* (suplantación) es una señal que reemplaza la de los satélites. Es más difícil de detectar que *jamming y meaconing.*

— El *meaconing* es una repetición de la señal recibida.

Es posible disponer de equipos que detectan señales de j*amming* y *spoofing* contra sistemas GNSS. Estos sistemas registran anomalías en las señales recibidas mediante técnicas avanzadas de procesado de señales. La IA se aplica actualmente a situaciones de NAVWAR entrenando algoritmos para detectar la presencia de *jamming* y *spoofing*, así como para alertar al sistema de la existencia de amenazas.

Finalizó recomendando la concienciación sobre la vulnerabilidad de los sistemas PNT, así como de la obtención de capacidad para monitorizar y evaluar la eficacia de los sistemas propios, para mantener una adecuada adaptación a los desafíos NAVWAR.

La tercera ponencia de esta mesa trató de **"La convergencia de sistemas IT/OT/IoT: Nuevos retos y amenazas en las Operaciones en el Ciberespacio"** y la impartió **D. Roberto Amado Giménez,** Director de Servicios Especiales de la compañía S2Grupo.

Comenzó afirmando que la convergencia de sistemas de tecnología de la información (IT), tecnología operativa (OT) e internet de las cosas (IoT) y su interconexión, genera nuevas vulnerabilidades que pueden suponer para el enemigo una ventana de oportunidad para tomar ventaja estratégica en el CE. Detectar de forma exitosa estas amenazas utilizando las actuales medidas de ciberseguridad supone un reto a abordar.

Los atacantes generan y protegen sus operaciones mediante *Operation Security* (OpSec) que no es otra cosa que la identificación y protección de la información crítica durante una operación, la cual, si fuera descubierta, pondría en riesgo la misión. De tal manera, si el proceso de OpSec falla es muy probable que la operación también lo haga. Por lo tanto, habrá que conseguir interferir en ellas mediante el uso de tecnologías disruptivas.

En las operaciones en el dominio del CE, el proceso de OpSec del adversario comienza desde una etapa temprana de pre-ataque y continúa durante todo el ciclo de su ataque. Por lo tanto, conocer aspectos de la OpSec de la amenaza puede ayudarnos a interferir en ella.

Las tecnologías para interferir en la OpSec del adversario se llevan a cabo mediante ciber aplicaciones basadas en IA que tratarán de detectar el *malware*, la intrusión en la red, la detección de *phishing/spam* y otros.

Dentro de las tecnologías disruptivas para interferir en las OpSec del adversario se encuentra el concepto de agente generativo, que consiste en la aplicación de la IA mediante un ciclo de *Large Language Model* (LLM): observación, pensamiento/razonamiento, toma de acción y mantenimiento de una memoria del ataque recibido.

Finalizó afirmando que las nubes de combate van a estar llenas de agentes de IA cuya finalidad es la protección de dichas nubes.

La cuarta y última ponencia de esta tercera mesa **"Uso de tecnologías 5G en el entorno táctico"** estuvo a cargo de **D. José Martínez Valenzuela,** Director de Ciberseguridad de la compañía Innovaciones Tecnológicas del Sur (INNOVASUR).

Las comunicaciones tácticas, que tienen lugar en el campo de batalla han evolucionado desde simples sistemas de radio hasta redes de comunicaciones avanzadas, capaces de soportar una amplia gama de servicios y aplicaciones.

El espectro 5G, que abarca una amplia gama de frecuencias electromagnéticas, es la base tecnológica que impulsa la próxima generación de redes de comunicaciones móviles. A diferencia de las generaciones anteriores el 5G utiliza un espectro más amplio y diversificado, lo que permite alcanzar velocidades de transmisión de datos significativamente más rápidas y una capacidad de red mucho mayor, lo que resulta crucial en aplicaciones que requieren baja latencia y alta fiabilidad, como la telemedicina, los vehículos autónomos y las operaciones militares. Además, el 5G facilita la conectividad masiva de dispositivos de la Internet de las cosas (IoT).

Otra característica clave del espectro 5G es su capacidad para ofrecer una cobertura uniforme y confiable en áreas densamente pobladas, así como en entornos remotos o de difícil acceso. Esto es posible gracias a la utilización de tecnologías avanzadas de antenas y la implementación de redes de células pequeñas, que permiten una distribución eficiente de la señal y una mayor capacidad de penetración en interiores.

El uso militar de tecnología 5G simplifica el proceso de adquisición y despliegue de nuevos sistemas al aprovechar las economías de escala y los procesos de fabricación ya establecidos en la industria civil, reduciendo costes de producción, de mantenimiento y de soporte a lo largo de su ciclo de vida.

Concluyó, exponiendo que las necesidades de I+D+i para el uso militar de tecnología 5G son:

— Robustez y resiliencia, deben ser capaces de soportar condiciones adversas y de recuperar rápidamente cualquier interrupción en el servicio.

— Cifrado y seguridad de la información.

— Las operaciones militares entrañan movimiento, lo que requiere la movilidad de las redes 5G.

— Priorización del tráfico en función de la misión y calidad de servicios para aplicaciones críticas como la voz, el video y el intercambio de datos tácticos.

— La capacidad de integrar el 5G con sistemas heredados, así como con redes civiles y aliadas.

Conclusiones finales

Una vez finalizada la tercera mesa redonda y respondidas las preguntas planteadas a través de la aplicación informática, el General de División **D. Fernando Luis Morón Ruiz**, Director de Investigación, Doctrina, Orgánica y Materiales (DIDOM) del Mando de Adiestramiento y Doctrina (MADOC) llevo a cabo la siguiente exposición de las conclusiones más relevantes.

Comenzó destacando la perspectiva complementaria que desde los tres niveles, estratégico, operacional y táctico se había proporcionado en las tres ponencias del punto de situación. Tras ellas, la primera mesa de ponentes, nos enfocó en el CE como nuevo entorno de operaciones y se explicó, con profusión de ejemplos, el papel que ha tenido el CE en los últimos conflictos; en la segunda mesa, se abordó en detalle la coordinación y sincronización de las operaciones en el CE y las operaciones electromagnéticas y finalmente, descendiendo de lo general a lo particular, la tercera mesa redonda trató de las tecnologías habilitadoras que más están influyendo en el uso militar del CE.

Consideró que en estas jornadas sobre el Ejército de Tierra y las operaciones en el CE se había puesto de manifiesto que cualquier actividad operativa necesita desplegar unas capacidades en sistemas y tecnologías de información y comunicaciones cada vez más complejas, interoperables y resilientes, porque éstas se han convertido en un habilitador imprescindible.

A continuación, afirmó que el Ejército de Tierra está inmerso en un profundo proceso de transformación, Ejército 2035, que nos debe permitir hacer frente a las amenazas y retos en el entorno operativo futuro. En este proceso, integrar el CE como un elemento propio y transversal al resto de actividades es una prioridad ineludible que ya se está plasmando en acciones a todos los niveles, como la alineación con la filosofía del "Mando orientado a la misión", desarrollo de conceptos como el

de las Operaciones Multidominio, "Fuegos en red", integración de actividades ciberespaciales y electromagnéticas, implantación de tecnologías como la IA o el 5G, con un enfoque eminentemente ágil, práctico y de aprendizaje que se plasma en el Plan de Experimentación que el Ejército de Tierra está desarrollando.

Todos estos cambios e innovaciones tienen un factor común: la consideración de la información como recurso estratégico para las operaciones militares, y son en realidad reflejos de otro cambio de orden superior, transversal y más profundo: la Transformación Digital, como cambio cultural y organizativo.

Por eso, tanto la Transformación Digital como el Mando Orientado a la Misión son pilares fundamentales de la visión del GE JEME para el Ejército 2035 que, junto a la tecnología, nos permitirán alcanzar esa Fuerza de Ventaja en el horizonte temporal de 2035.

Destacó que nada mejor que volver al principio, a las palabras de bienvenida del GE JEME que sintetizaban el por qué y el para qué de estas jornadas:

> *"Ante nosotros se plantea el reto de desarrollar las capacidades necesarias que nos puedan ser requeridas para cumplir la misión del Ejército de Tierra. Para ello es clave acometer el proceso de análisis de los factores MIRADO, cambiando el orden del acrónimo, pues la D de la doctrina, como elemento de comunidad de ideas y cohesión, debe ser la base. En este aspecto, el rol del MADOC es claro, liderar el ciclo del conocimiento en el Ejército de Tierra, elaborando una doctrina sobre la que continuar con la organización, los recursos humanos y materiales, las infraestructuras para finalizar con el adiestramiento, en el que el MADOC volvería a cerrar el círculo, para que el Ejército sea una Institución que aprende, innova e incorpora lo aprendido con la agilidad que requiere el ritmo de cambio actual.*
>
> *De la mano del MADOC deben ir el ámbito universitario y el de la empresa. Se trata de un entorno de colaboración que el Ejército trata de impulsar y mejorar con Jornadas como estas, además de otras como el Foro Ejército – Empresa – Innovación. Lo hacemos porque, aunque podríamos hacerlo en solitario, somos plenamente conscientes de que lo haremos mucho mejor con su colaboración. Por eso, dijo el GE JEME, se lo agradezco, y les pido que sigan trabajando con nosotros.*
>
> *El ámbito universitario y de la investigación proporciona un apoyo desde el conocimiento que será muy valioso en todo el ciclo de conocimiento, aprendizaje y transformación."*

Finalizó su intervención afirmando que "de esta manera, codo a codo con ustedes, sigamos construyendo ese Ejército 2035 que requiere la Seguridad y Defensa de España".

Clausura

Las jornadas finalizaron con unas palabras de **D. Nicolás Ruiz Reyes**, Rector de la UJA, que destacó el valor de estas jornadas de retos futuros para avanzar en los objetivos que se habían propuesto.

Estos son, en primer lugar, fomentar la cultura de la seguridad y la defensa nacional en el mundo universitario, e inculcar en nuestra sociedad la necesidad de contar con unas Fuerzas Armadas preparadas y vigorosas.

En segundo lugar, contribuir desde la Universidad, es decir, desde el conocimiento, la investigación y la innovación, al proceso de modernización y de transformación que deben afrontar las Fuerzas Armadas para dar adecuada respuesta a los retos y desafíos que se plantean en un contexto geopolítico complejo, cambiante y no exento de dificultades, especialmente en el ámbito que nos ocupa, que es el de la ciberseguridad.

Y, en tercer lugar, fomentar e impulsar un espacio de cooperación entre el Ejército de Tierra, la Universidad de Jaén y el sector productivo de Jaén.

Señaló que los tres objetivos se habían alcanzado de forma satisfactoria, volvió a agradecer al Ejercito de Tierra por elegir esta universidad y esta provincia para el desarrollo de estas jornadas y destacó que:

"Durante dos días hemos podido debatir y reflexionar sobre cómo marcarán las tecnologías vinculadas al CE la labor de nuestras FAS en un futuro ya muy cercano. Hemos escuchado conceptos nuevos como EW, ciberdefensa, operaciones multidominio, nube táctica de combate, concepto CEMA, etc... Hemos visto cómo se despliegan todos estos conceptos en el conflicto de Ucrania.

Cualquier desarrollo tecnológico va a crear nuevos escenarios de riesgo a resolver y en el entorno digital donde vivimos, dado que estos avances son cada vez más rápidos y más globales, su impacto va a ser cada vez más elevado. Por lo tanto, si no estamos preparados todos los sectores, no podremos dar una respuesta adecuada a lo que nos demandan las necesidades de seguridad y defensa de España.

La preparación en el ámbito de las FAS requiere la adquisición de nuevos conocimientos y competencias, proceso que se ha de realizar de una forma ágil y eficaz, lo que exige un esfuerzo en formación y un contacto permanente con los centros donde se genera el conocimiento, las universidades. En la Universidad de Jaén siempre van a encontrar un aliado".

Por último, el Teniente General **D. José Manuel de la Esperanza y Martín-Pinillos**, Jefe del MADOC dio por finalizadas estás jornadas, clausurando las mismas.

EL EJÉRCITO DE TIERRA Y LOS RETOS FUTUROS 2024

El Ejército y las operaciones en el ciberespacio

Jaén, 6 y 7 de mayo de 2024
Aula Magna de la Universidad de Jaén

Programa

Día 1 (06MAY24)

12:00 h **Inauguración**

General de Ejército D. Amador Enseñat y Berea. Jefe de Estado Mayor del Ejército de Tierra.

Teniente General D. Jose Manuel de la Esperanza y Martin-Pinillos. Jefe del Mando de Adiestramiento y Doctrina del Ejército de Tierra.

D. Nicolás Ruiz Reyes. Rector de la Universidad de Jaén.

12:35 h **Punto de situación / visión**

Teniente General D. José María Millán Martínez. Capacidades CIS/TIC en apoyo de la estructura operativa de las FAS.

Vicealmirante D. Francisco Javier Roca Rivero. Lecciones aprendidas del conflicto ucraniano.

General de División D. Guillermo Ramírez Altozano. Una visión del presente y futuro de las operaciones terrestres en el ciberespacio.

Almuerzo de trabajo

16:00 h **Mesa 1: El ciberespacio como nuevo entorno de operaciones**

Moderador: D. José de la Peña Muñoz. Director de la revista SIC/Ediciones CODA.

Coronel D. Ignacio Javier Simón Andújar. Jefe de la Jefatura de Telecomunicaciones y Guerra Electrónica del Mando Conjunto de Ciberespacio.

Coronel D. Bonifacio Gutierrez de León. Subdirector de Investigación y Lecciones Aprendidas de la Dirección de Investigación, Doctrina, Orgánica y Materiales del Mando de Adiestramiento y Doctrina del Ejército de Tierra.

Coronel D. Francisco José Oliva Bermejo. Jefe de Sección de Inteligencia de Señales y Guerra Electrónica de la Jefatura de los Sistemas de Información y Telecomunicaciones y Asistencia Técnica del Ejército de Tierra.

D. Manuel Medina Guerrero. Catedrático de derecho Constitucional de la Universidad de Sevilla.

Día 2 (07MAY24)

09:00 h **Mesa 2: Convergencia actividades electromagnéticas y ciberespacio**

Moderadora: Dña. María Teresa Martín Valdivia. Catedrática de Lenguajes y Sistemas Informáticos de la Universidad de Jaén.

D. Manuel José Lucena López. Profesor Titular de Ciencias de la Computación e Inteligencia Artificial de la Universidad de Jaén.

Coronel D. Manuel Sasot Oliván. Jefe Subdirección de Actividades en el Ciberespacio y Electromagnéticas de la Jefatura de los Sistemas de Información y Telecomunicaciones y Asistencia Técnica del Ejército de Tierra.

Coronel D. Victor Valero Garcia. Cuartel General Terrestre de Alta Disponibilidad.

Coronel D. Miguel Ángel San Segundo Campo. Jefe del Regimiento de Guerra Electrónica nº 31.

11:30 h **Mesa 3. Tecnologías disruptivas y emergentes en el ciberespacio**

Moderador: Coronel D. Javier Bermejo Higuera. Jefe de Comunicaciones y Seguridad Informática TICS INTA.

Teniente Coronel. D. Carlos Herrero Santos. Jefe del Negociado de Simulación del Mando de Apoyo Logístico del Ejército de Tierra.

D. Manuel Perez Cortes. Director general de Defensa y Seguridad de GMV.

D. Roberto Amado Giménez. Director de Servicios Especiales de S2Grupo.

D. José Martínez Valenzuela. Cybersecurity and Compliance Business Manager de Innovasur.

13:30 h **Conclusiones**

General de División D. Fernando Luis Morón Ruiz. Director de Investigación, Doctrina, Orgánica y Materiales del Mando de Adiestramiento y Doctrina del Ejército de Tierra.

14:00 h **Clausura**