Mi General, señor rector, autoridades civiles, militares y de las Fuerzas y Cuerpos de seguridad del Estado, oficiales, suboficiales y tropa, señoras y señores, queridos alumnos de la Universidad de Jaén.

En las noticias oímos cada día referencias a estar viviendo una nueva guerra fría, si bien con puntos tan calientes como Oriente Próximo o Ucrania. Muchos de los que estamos hoy aquí, por nuestra edad, recordamos bien la verdadera Guerra Fría, de la segunda mitad del siglo pasado, caracterizada por un enfrentamiento bipolar y el permanente temor a un conflicto nuclear.

Una de las características que más diferencia nuestro mundo presente con respecto a aquellos tiempos (marcados por la caída de la Unión Soviética) es la omnipresencia de dispositivos digitales, que prestan todo tipo de información y servicios, con carácter inmediato a través de una Internet cada vez más versátil y accesible.

Se puede considerar que el gran salto se dio en abril de 1993, cuando se entregó la World Wide Web (la “WEB” como se la conoció desde el principio) al dominio público. El siguiente hito fue la firma por el presidente de los EEUU Bill Clinton en 1996 de la “Telecommunications Act”, que permitía a nuevas empresas competir en un mercado naciente que por primera vez incluía también a Internet: así, se pasó de 36 millones de

personas con acceso a la red a casi 250 millones en el año 2000. Todo ello fue clave en la transformación de la economía mundial, pero también en la aparición de nuevos riesgos y amenazas para individuos, empresas y Estados.

De hecho, el Departamento de Seguridad Nacional español advierte cada año de que uno de los mayores riesgos para nuestro país es la vulnerabilidad en el ciberespacio, campo desde el que se puede … “*influir en la opinión pública y en la forma de pensar de las personas a través de la manipulación de la información, las campañas de desinformación o las amenazas híbridas*”.

Los riesgos para la seguridad de desarrollos en ciber tecnologías como la Inteligencia Artificial, el Internet de las Cosas o el almacenamiento en la nube siguen una tendencia al alza, afectando a campos tan diversos como la delincuencia económica, el espionaje, la influencia sociológica y, por supuesto, las operaciones militares.

Haciendo un breve repaso de algunos casos conocidos, podemos recordar que en 2007 se detectó una intrusión en ordenadores de la empresa norteamericana Lockheed Martin; muy poco después, el ejército chino se dotó de dos modernos aviones de combate muy parecidos a modelos de esa empresa: el *Chengdu* J-20 (copia casi exacta del F-22) y el *Shenyang* J-31 (copia del F-35).

Al mismo tiempo, la retirada de un monumento al Ejército soviético se tradujo en el primer ataque cibernético contra todo un país, Estonia, que vivió días de caos por la caída de los servicios informáticos tanto estatales como privados.

Y a comienzos de 2010 se produjeron numerosas averías en las centrifugadoras de uranio de Irán; pronto se descubrió que la red que las controlaba había sido infectada por el gusano informático *Stuxnet:* supuestamente diseñado por Estados Unidos e Israel para frenar el programa nuclear iraní.

Si pasamos al campo estrictamente militar, la invasión rusa de Georgia comenzó en agosto de 2008 con un ciberataque contra los sistemas de mando y control que facilitó las posteriores acciones convencionales. El mismo patrón, ampliado a una extensa gama de acciones de ciberguerra, utilizó Rusia en 2014 durante la crisis ucraniana que derivó en la anexión de Crimea y el conflicto secesionista que persiste en el este de Ucrania.

Estos son sólo algunos ejemplos de cómo el ciberespacio ha ido adquiriendo una relevancia creciente en las últimas décadas como nuevo campo de confrontación.

La realidad es que occidente (personalizado en Estados Unidos) ha perdido la ventaja indiscutible de ser el centro neurálgico de la industria vinculada a Internet. De hecho, la actuación de los servicios de inteligencia rusos y de regímenes como el de Corea del Norte en sucesivos procesos electorales y crisis políticas en países de la Alianza Atlántica han impulsado a éstos a aumentar sus capacidades y cooperación en materia cibernética.

Esta acción se ha materializado en la puesta en marcha en 2019 del Centro de Operaciones en el Ciberespacio de la OTAN. Del mismo modo, la Alianza viene reiterando desde 2016 que un ciberataque malicioso “severo” podría justificar la activación del Artículo 5 del Tratado de Washington. Es cierto que, quizás por su indefinición, tales amenazas no parecen haber hecho reaccionar operativamente a la OTAN, por el momento.

Es preciso tener en cuenta que la ciberguerra puede tener lugar sobre espacios físicos, nada virtuales.

Internet se sostiene gracias a los centros de datos, instalaciones que concentran los ordenadores por los que pasa toda la red. Son cada vez más numerosos y controlarlos se ha convertido en una baza geopolítica, dado que prestan servicios de almacenamiento, procesamiento y computación a cientos de millones de usuarios. Por ello, son puntos muy sensibles y vulnerables a ataques de todo tipo, desde el elemental daño físico a las instalaciones y aparatos, los intentos de control remoto, … o el acceso a información de empresas y potencias extranjeras, que pueden estar incluso autorizadas por la legislación nacional.

Como ejemplo de este último tipo de intervención, la denominada “*Ley de Inteligencia Extranjera*” permite al gobierno estadounidense recopilar información de personas, incluido extranjeros, de sus empresas nacionales. De manera similar, China aprobó en 2017 una “*Ley de Inteligencia Nacional”* que le permite acceder a los datos de sus empresas por motivos de seguridad nacional, sin dejar claro si esta medida puede ser aplicada a centros de datos chinos fuera del país.

Por otro lado, las posibilidades del ciberespacio y las peculiaridades de los hábitos de consumo cultural e informativo han potenciado el uso malicioso de técnicas de ingeniería social y manipulación (o también llamada guerra) psicológica. Estas técnicas son bien conocidas desde largo tiempo atrás, pero han encontrado un vector ideal en las redes sociales y la “internet profunda”.

Desde luego, contribuir a la desestabilización y la división interna de países enteros mediante la alimentación de prejuicios y teorías conspirativas de todo tipo, o extorsionar

con el robo de datos (ya sean correos electrónicos, fotografías, informes, metadatos…) parece más factible que en el pasado, tanto para Estados como para organizaciones criminales.

En todos los casos mencionados, es de resaltar el reto que supone “combatir” en un entorno carente en la práctica de regulación jurídica efectiva. El hecho de que este tipo de acciones escapen al principio de territorialidad que rige, en general, las normas jurídicas, y la inadecuación de las normas de Derecho Internacional Público a esta realidad, hacen difícil articular una respuesta ajustada al Derecho existente y que pudiéramos calificar de “tradicional”.

Por todo lo anterior, los Estados están desarrollando complejas estructuras para dar seguridad a sus sistemas y perseguir prácticas delictivas. En el caso de España, en 2006 se creó en Instituto Nacional de Ciberseguridad (INCIBE), dependiente del ministerio de Economía, y en 2013 se aprobó la primera Estrategia Nacional de Ciberseguridad (renovada en 2019), al tiempo que se creaba el ahora denominado Mando Conjunto del Ciberespacio. Se sumaban así a los servicios del Centro Criptológico Nacional (del CNI) que protege las redes estatales, y las de la Policía y Guardia Civil contra la delincuencia.

Creo que, con estas consideraciones y este recuerdo condensado de algunos momentos de la historia reciente, se puede comprender por qué se ha elegido el tema '*El Ejército y las operaciones en el ciberespacio'* para las Jornada de Retos futuros de este año en Jaén.

En parte puede verse como una continuación de la edición anterior, celebrada en 2022 en Granada con el título de "*El proceso de la decisión en la era digital, marco ético y jurídico*". Si entonces se puso el foco en aspectos morales, casi filosóficos, en estos dos días vamos a entrar más de lleno en el estado de la cuestión desde el punto de vista operativo y tecnológico, ya que el escenario actual y el futuro previsible presentan para el Ejército de Tierra, y para el conjunto de las Fuerzas Armadas en general, importantes retos en este campo.

Podemos destacar algunos de estos retos:

1º. La necesaria alineación con la filosofía del "mando orientado a la misión", tal y como la está desarrollando la Escuela de Guerra y Liderazgo del Ejército. Se trata de un modo de ejercer el mando que otorga a los subordinados el máximo grado de iniciativa posible dentro del propósito del jefe, con la finalidad de acortar los ciclos de decisión, siendo ésta una forma eficaz de alcanzar la superioridad en el enfrentamiento.

2º. El trabajo que se viene realizando en las Fuerzas Armadas para implantar el concepto de "Fuegos en red" en el actual campo de batalla, que podemos calificar de "transparente". Tras procesar el gran volumen de información generada por la multitud de sensores presentes en el campo de batalla, se puede asignar un objetivo de la forma más rápida y precisa a los efectores que correspondan, ya sean propiamente de fuegos, o bien electromagnéticos o cognitivos.

3º. Los trabajos en marcha para la implantación de la inteligencia artificial en las Fuerzas Armadas, en la búsqueda constante de la ventaja en la información y en el apoyo a la decisión. Sirvan como ejemplos cercanos el Grupo de Trabajo permanente de IA del Ejército de Tierra o el Convenio suscrito en febrero con la Universidad de Granada, para la realización de actividades de investigación, docencia y divulgación en este ámbito.

4º. Por último, hay que mencionar y destacar el Plan de Experimentación del Ejército de Tierra, con el que se pretende validar los nuevos conceptos de combate y adaptarnos progresivamente a los nuevos escenarios, con el objetivo de disponer de una Fuerza de Ventaja en 2035.

En este profundo proceso de transformación en que está inmerso el Ejército de Tierra, que le debe permitir hacer frente a las amenazas y retos en el entorno operativo futuro, supone una obligación y, a la vez, un desafío integrar el ciberespacio como un elemento propio y transversal al resto de sus actividades.

Conceptos como combate multidominio, el campo de batalla transparente, la nube de combate y "kill web", la integración de actividades ciber electromagnéticas, la guerra de navegación, la criptografía post-cuántica y otros asociados al empleo de tecnologías tan vigentes como la inteligencia artificial, ya están marcando el camino hacia el Ejército 2035. De ahí la pertinencia y oportunidad de dedicar estas jornadas al tema que nos ocupa.

Así que, llegados a este punto, vamos a centrarnos en el programa que hemos preparado.

Comenzaremos esta mañana con un punto de situación sobre las capacidades CIS/TIC ya existentes y la previsión de operaciones militares en el ciberespacio, con mención especial a las lecciones aprendidas de la actual guerra en Ucrania. Estoy seguro de que las charlas del teniente general José María Millán, el vicealmirante Francisco Javier Roca y el general de división Guillermo Ramírez centrarán el tema de una forma completa y precisa.

Esta tarde asistiremos a una mesa redonda sobre '*El ciberespacio como nuevo entorno de operaciones*' moderada por José de la Peña, director de una revista de referencia en este ámbito. Los coroneles Ignacio Javier Simón, Bonifacio Gutiérrez y Francisco José Oliva, junto con el catedrático Manuel Medina disertarán sobre el ciberespacio, cómo se está empleando en los conflictos bélicos en marcha, su dimensión multidominio, cómo se conjuga con las tecnologías y el espectro electromagnético, así como su marco jurídico.

Creemos que de esa forma terminaremos la jornada de hoy con una visión bastante completa de cómo se ha desarrollado en los últimos años este ámbito bélico, que se añade a los tradicionales de tierra, mar y aire (y, ahora, espacio).

Mañana empezaremos abordando la necesaria '*Convergencia entre actividades electromagnéticas y ciberespacio*', con la moderación de la catedrática María Teresa Martín. El profesor Manuel José Lucena y los coroneles Manuel Sasot, Víctor Valero y Miguel Ángel San Segundo nos mostrarán cómo las operaciones de guerra electrónica de las últimas décadas se complementan ahora con las realizadas en el ciberespacio y en el

conjunto de las actividades electromagnéticas. También veremos cómo se debe dar seguridad a la información dentro del nuevo concepto CEMA.

Y terminaremos con la mesa dedicada a las '*Tecnologías disruptivas y emergentes en el ciberespacio*', moderada por el coronel Javier Bermejo, en la que nos asomaremos a un futuro que ya tenemos inmediato. Nos van a hablar de la era cuántica, de las acciones para asegurar (o interferir) los sistemas de navegación, de la inteligencia artificial y del internet de las cosas. El teniente coronel Carlos Herrero, junto con Manuel Pérez, Roberto Amado y José Martínez nos van a abrir los ojos sobre la forma en que nuestra vida diaria está inmersa en el ciberespacio, con lo que ello supone de amenaza, pero también de oportunidad.

Sin duda alguna, este apretado programa con conocimiento y opiniones de primera fila será de gran utilidad para los asistentes, tanto los que provenimos de una experiencia militar de largo recorrido, en la que hemos debido adaptarnos a una creciente carga tecnológica, como para los jóvenes estudiantes de esta Universidad, que en el futuro habrán de afrontar situaciones en las que la ciberseguridad sea vital.

Quiero terminar agradeciendo el trabajo realizado por el personal organizador tanto de la Universidad de Jaén como del Mando de Adiestramiento y Doctrina, que han dedicado muchas semanas a sacar adelante estas jornadas.

Espero que todos los temas a desarrollar sean de su interés y que estas Jornadas '*El Ejército de Tierra y las operaciones en el ciberes*pacio' sean fructíferas para cuantos nos encontramos aquí, mejoren nuestro conocimiento sobre estas materias y, sobre todo, sobre sus riesgos y sus posibilidades.

Todo ello para que en este ámbito podamos realizar el mejor servicio posible a España.

TG DE LA ESPERANZA Y MARTÍN-PINILLOS