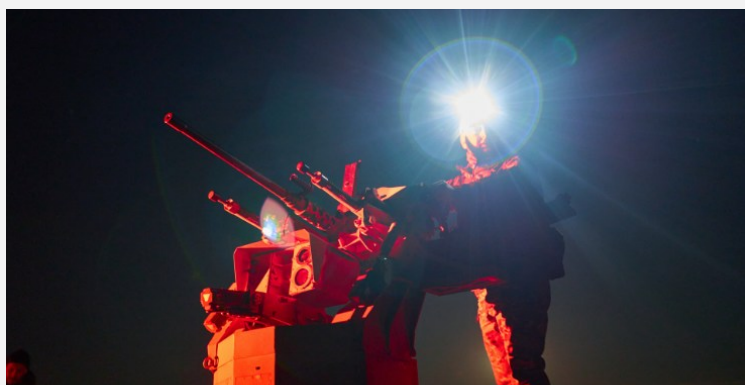


■■■ ESPACIO DE TRANSFORMACIÓN ■■■



Fuego «inteligente» a discreción

Poco a poco, la IA se va incorporando a las capacidades militares con mayor velocidad donde la necesidad es más acuciante. En sistemas complejos, como el avión de combate **Gripen E**, mejora la maniobrabilidad y la identificación de objetivos; pero también permite una mayor eficiencia en la lucha contra los omnipresentes drones. Un buen ejemplo es el **Sky Sentinel** ucraniano, formado por un conjunto de radar y ametralladora. Puesto en posición, sigue a los drones que puedan entrar en su campo de visión y los abate en el punto más propicio de la trayectoria, sin intervención humana alguna. El **US Army**, por su parte, ha conectado un visor inteligente a un fusil **M4A1**. Así, el tirador no tiene más que fijar el dron objetivo en la pantalla y apretar el disparador: el sistema abrirá fuego cuando pueda hacer un mejor blanco. Ante un campo de batalla cada vez más letalizado, estos ejemplos demuestran que la IA puede aportar soluciones más eficaces y eficientes.

Ucrania ha Creado Gracias a un 'Crowdfunding' una Ametralladora que Apunta y Dispara Sola | The Objective



Mosquito espía

En lo que parece un mero alarde tecnológico, China ha presentado un microdrón biónico desarrollado por la **Universidad Nacional de Tecnología de Defensa**. Con apariencia y dimensiones de un insecto, el sorprendente dispositivo ha sido pensado para penetrar en edificios, instalaciones críticas y zonas sensibles sin ser detectado por radares o sensores térmicos. Dado su reducidísimo peso (0,3 g) se le presupone una escasa autonomía y alta sensibilidad a las condiciones ambientales. En cualquier caso, el desarrollo de **micro-UAV** es consecuencia de la necesidad de ganar capacidad de obtención de inteligencia en entornos de compleja volumetría, como las ciudades. Enjambres de drones miniaturizados podrían protagonizar misiones **ISR** en entornos multidominio altamente sensorizados. La miniaturización es una tendencia al alza en un campo de batalla cada vez más transparente, ya que permite reducir la exposición frente al adversario.

China Unveils Tiny Spy Drone that Looks like a Mosquito. What other Small Spy Drones Exist? | Euronews

■■■ ESPACIO DE TRANSFORMACIÓN ■■■



En la mata

Recientemente, en el **frente de Jersón**, se ha detectado la presencia de varios **drones FPV** rusos equipados con paneles solares. Esta adaptación supone un salto cualitativo en el empleo de **tácticas de emboscada** al permitir, gracias a la alimentación de los paneles, que estos aparatos puedan permanecer en espera durante varios días hasta localizar con sus sensores un objetivo a neutralizar. El empleo generalizado de este tipo de drones podría favorecer una sensorización aún mas densa del campo de batalla y dar lugar a la aparición de una especie de «campos de minas» inteligentes y móviles, dificultando, más si cabe, las operaciones móviles y ahondando en el carácter posicional del conflicto. En un **EO** marcado por la proliferación de sistemas letales semiautónomos de bajo coste, preservar la libertad de acción exigirá integrar el desarrollo tecnológico con la continua adaptación de las tácticas, técnicas y procedimientos (TTP) de protección de la Fuerza.

Creeping Doom: Russia Deploys Solar Powered Ambush Drones
| Forbes



La cámara indiscreta

Las escenas de película en las que *hackers* utilizan dispositivos ajenos para acciones de espionaje no son tan ficticias como cabría pensar. Durante la «**Guerra de los Doce Días**», Irán ha utilizado cámaras de seguridad privadas en Israel para recopilar información en tiempo real sobre los impactos de sus misiles y mejorar la precisión de posteriores ataques. En otros contextos, actores estatales y no estatales se han servido de cámaras de seguridad privadas, de uso extendido por su bajo coste y fáciles de piratear, para obtener información sobre ubicación de objetivos o tropas. De hecho, se estima que las imágenes en directo de 40.000 cámaras de seguridad de todo el mundo son accesibles en Internet. Este es solo un ejemplo del posible doble uso de tecnologías ampliamente utilizadas, por lo que es vital instruir, también a la población civil, acerca de medidas de protección adecuadas para mejorar la resiliencia ante amenazas en el ciberespacio.

Irán Ataca a Israel 'Desde Adentro': Reportan que 'Secuestra'
Cámaras de Seguridad para Espiar | El Financiero

■■■ ESPACIO DE TRANSFORMACIÓN ■■■

Dron²

En una reciente **operación frente a las costas de Crimea**, al menos un USV ucraniano desplegó varios cuatrirrotores para atacar componentes de un avanzado sistema de radar de alerta temprana ruso **Nebo-M**. Dicha operación, en la que Ucrania ha combinado el empleo de medios navales y aéreos no tripulados, representa un avance sustancial en su empleo táctico y habilita la ejecución de **operaciones distribuidas** con un alto grado de autonomía. Esta innovación, de marcado carácter multidominio, aporta versatilidad en el entorno litoral y podría adaptarse tanto a misiones **ISR** como de ataque, en función de la carga de pago y del objetivo designado. El empleo de sistemas no tripulados en el campo de batalla es una realidad cada vez más extendida. No obstante, el desafío a futuro será lograr la operación de dispositivos autónomos, provenientes de distintos dominios, de forma coordinada e integrada, tanto entre ellos como con las fuerzas combatientes.

Ukraine's Uncrewed Surface Vessels Are Now Launching Bomber Drones To Attack Crimea | The War Zone



Laboratorio para la desinformación

Parece que Burkina Faso se ha convertido en un «laboratorio de desinformación», con acciones de propaganda ya vistas por cientos de miles de personas en todo el mundo. Circulan **videos deepfake** en los que estrellas internacionales como Beyoncé, Justin Bieber o el nuevo papa alaban al presidente militar del país, el **capitán Ibrahim Traoré**. Otros montajes muestran imágenes falsas de multitudes en varias capitales europeas apoyando al que dice asumir, en primera línea, el papel de líder panafricanista, antioccidental y prorruso. Esta alternativa digital contrasta con la realidad: Burkina Faso es el epicentro del terrorismo global, sufre elevados niveles de violencia, pérdida de control estatal y propaganda gubernamental. Las estrategias de desinformación suponen una amenaza desde el punto de vista cognitivo, máxime allí donde existen «**cámaras de eco**» de resentimiento que podrían conducir al colapso social y al fallo de un Estado.

Burkina Faso, the World's Disinformation Lab
| FPRI Insights

■ ESPACIO DE TRANSFORMACIÓN



Mar de China Espacial

En la «zona gris» se establece una pugna en la que los adversarios mantienen, sin traspasar el umbral del conflicto armado y mediante acciones híbridas, una actitud coercitiva que persigue objetivos propios de una guerra. En este sentido, algunos autores creen que China podría utilizar en el espacio **estrategias similares a las ya empleadas en el mar de China Meridional** contra sus rivales. Así, ciertas maniobras agresivas, lanzamientos, colocación estratégica de constelaciones, apropiación de trayectorias orbitales o sus ambiciones sobre la Luna podrían equipararse a sus tácticas marítimas de desbordamiento, desgaste, acoso o hechos consumados tipo «**salami**» en la región. Viéndose amenazado, Taiwán va a emplear la IA para vigilar esta situación. La apertura a otros dominios de operación abre posibilidades de confrontación a las que habrá que anticiparse, analizar y contrarrestar, desde una ventaja tecnológica que facilite la superioridad en la decisión.

China is Bringing Gray-Zone Warfare to Space
| Defense One



«Y2Q»: el próximo gran reto

La tecnología plantea a veces desafíos existenciales a nivel global. Muchos recordarán la preocupación a finales de los 90 en torno a la programación del **software** y sistemas ante el «**efecto 2000**» o «Y2K». Años de medidas preparatorias y atención pública precedieron a la llegada del temido 01/01/2000. Hoy día, **sin una fecha fija en el horizonte**, se presenta el gran reto de la **criptografía poscuántica (PQC)**, que con inusitada facilidad es capaz de romper los cifrados actuales. Entre ambas situaciones existen grandes diferencias en cuanto a la complejidad de la solución técnica y al interés global por colaborar. Entre otras, el adversario tratará de apropiarse ahora de información crítica para descifrarla llegado el momento. De la experiencia pasada se pueden extraer lecciones, ya que la aplicación de medidas preventivas y la concienciación pública juegan un papel clave en la preparación. Planificación y protección anticipadas serán recetas de éxito ante el temible «Y2Q» .

From Y2K to PQC: Preparing for the Next Great IT Challenge
| Government Executive

■■■ ACTIVIDADES DEL CCDC ■■■



PROSPECTIVA ESTRATÉGICA

Strategic Foresight Analysis Workshop III septiembre 2025

Entre los días 16 y 18 de septiembre, el *Allied Command Transformation* (ACT) celebrará en Virginia (EE. UU.) la reunión para la última revisión del *Strategic Foresight Analysis* (SFA). En ella se debatirán y, posteriormente, se validarán los escenarios, las evidencias y las implicaciones previstas, a fin de emitir la versión 2025 del documento. Cerrado el SFA-25, en la misma reunión, se abrirá el ciclo de redacción del *Future Operating Environment* 2026. En ambos procesos de elaboración participa la SEAYP.



CONCEPTOS Y EXPERIMENTACIÓN

FOC del Centro de Wargaming del EMAD

Un año después de su establecimiento y tras un proceso de formación teórico-práctica, el Centro de *Wargaming* del EMAD (CWGEMAD) ha alcanzado su capacidad final operativa (FOC). El CWGEMAD, que se organiza según la **Instrucción Comunicada IC 01/25**, ha distribuido recientemente un oficio a toda la organización solicitando que le sean remitidas **propuestas de trabajo** para el curso 2025-2026. Estas propuestas, una vez validadas por el centro y priorizadas por el JEMAD, constituirán su plan de trabajo.



DOCTRINA

TTPC Empleo conjunto de las unidades aéreas buques de la Armada

Sancionadas por el JEMAD las orientaciones para el desarrollo doctrinal, se iniciará la elaboración de una nueva doctrina conjunta de 3^{er} nivel, la TTPC-3.1.2 "Empleo conjunto de las unidades aéreas de las FAS en los buques de la Armada". Esta publicación incluirá las TTP comunes y los principios básicos de seguridad de vuelo, que deben ser conocidos por las unidades aéreas de las FAS capaces de operar en los buques de la Armada para que se garanticen unas operaciones aeronavales seguras.

■■■ CoE DEL MES ■■■



JOINT CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR DEFENCE
CENTRE OF EXCELLENCE

■■■ PUBLICACIONES ■■■



ENTORNO OPERATIVO 2035



PUBLICACIONES DEL CCDC

Las imágenes pertenecen a las noticias y organismos referenciados y relacionados, al fondo propio del EMAD y a bancos de imágenes (Freepik y Pixabay) y algunas han sido generadas utilizando técnicas de IA.

Este boletín ofrece una visión no oficial de asuntos de interés relacionados con la Transformación de las FAS y el entorno operativo futuro.

El CCDC no se hace responsable de los enfoques y opiniones vertidos en los artículos y las publicaciones ajenas enlazados.

Suscribirse

Darse de baja



ESTADO
MAYOR
DE LA
DEFENSA



INTEGRACIÓN EN
EL MULTIDOMINIO