GUERRA ELECTRÓNICA

EL CAMPO DE BATALLA SILENCIOSO DEL FUTURO

Introducción

La **guerra electrónica (EW - Electronic Warfare)** abarca todas las estrategias y tecnologías utilizadas para explotar el espectro electromagnético, incluyendo ondas de radio, microondas, infrarrojos, luz visible, luz ultravioleta y rayos X. El espectro es parte integral de diversas operaciones militares y sirve como columna vertebral para la comunicación, la navegación y la selección de objetivos. La guerra electrónica **tiene como objetivo negar al enemigo el uso del espectro y al mismo tiempo garantizar que las fuerzas amigas puedan operar libremente dentro de é**l.

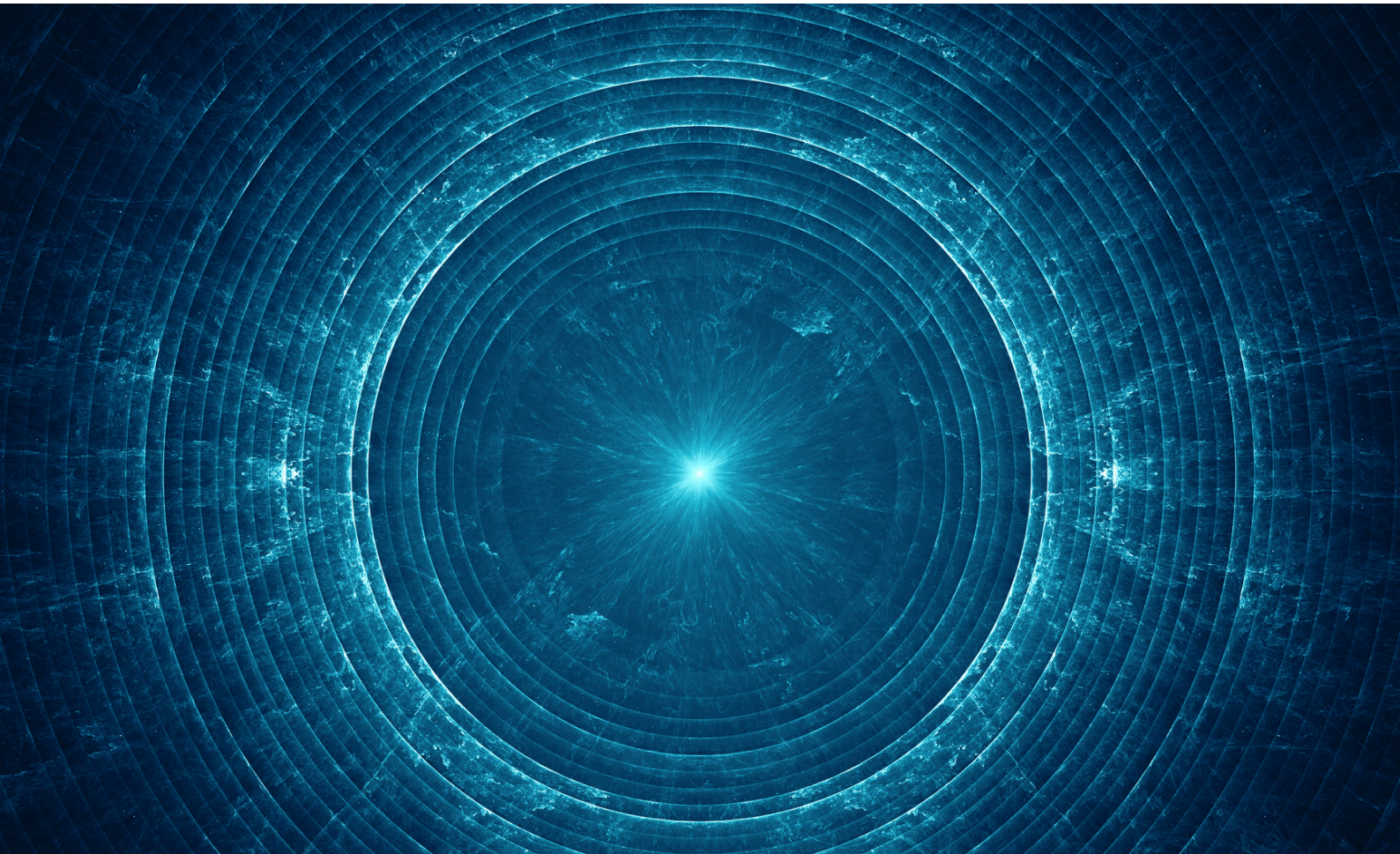
En la actualidad, el espectro electromagnético se ha convertido en un campo de batalla tan crítico como el terrestre, el naval, el aéreo o el espacial. La guerra electrónica representa el **choque de fuerzas invisibles que pueden determinar el resultado de los conflictos** incluso antes de que se efectúe el primer disparo físico.

Desde su aplicación masiva en la Segunda Guerra Mundial con la guerra de las radios y el uso del radar, la guerra electrónica ha evolucionado hasta convertirse en una pieza crucial para alcanzar la superioridad en el enfrentamiento en los conflictos modernos.

Para ello, basta señalar el papel relevante que la guerra electrónica juega en la doctrina de las principales fuerzas militares.

Si bien la OTAN, China y Rusia reconocen la importancia de la guerra electrónica, sus **doctrinas divergen** significativamente debido a diferencias en objetivos estratégicos, contextos geopolíticos y prioridades operativas. La **OTAN** se centra en la defensa colectiva y la interoperabilidad; **China** prioriza el dominio de la información y la guerra en red integrada; y **Rusia** enfatiza la flexibilidad estratégica y la integración de la guerra híbrida.

En la actualidad, **Ucrania y Rusia están llevando a cabo un juego del gato y el ratón para interferir mutuamente en sus sistemas hasta un nivel nunca visto**. Ucrania se ha centrado en el uso de la guerra electrónica en apoyo de sus defensas aéreas para hacer frente a los drones y misiles rusos. Rusia, por su parte, se ha centrado en interferir las señales de los satélites del sistema de posicionamiento global que utiliza Ucrania para el guiado de municiones aéreas y de artillería.



El último ejemplo reciente del uso con éxito de las técnicas de guerra electrónica lo podemos encontrar en la ofensiva en marcha lanzada por Ucrania en la región rusa de Kursk.

Tanto Rusia como Ucrania han venido utilizando ampliamente drones de todo tipo para misiones de reconocimiento y ataque. **La innovación introducida por Ucrania ha sido combinar drones de ataque con unidades de guerra electrónica para interferir las señales de los drones rusos, cegándolo**s. Esto ha permitido a los drones ucranianos atacar objetivos y permitir el avance de las unidades terrestres.

Una vez completado el primer avance de las unidades terrestres de unos pocos kilómetros, se ha repetido el proceso (uso de drones más interferencias) a gran velocidad, lo que ha permitido a las fuerzas ucranianas avanzar relativamente intactas, dejando a los mandos rusos con muy poca información sobre los movimientos ucranianos.

Esta innovación, combinada con el uso extensivo de pequeñas unidades de operaciones especiales, altamente móviles, que han podido penetrar tras las líneas rusas y sembrar el máximo caos, ha contribuido a crear confusión en el alto mando ruso forzando a un mal uso de las unidades locales, resultando en su rendición masiva o destrucción.

Sin ánimo de ser exhaustivos, y con una finalidad divulgativa y no técnica, se van a exponer a continuación los principales elementos que configuran la guerra electrónica.

Fundamentos de la Guerra Electrónica

La guerra electrónica reside en el **dominio del espectro electromagnético completo**, desde la banda más baja de los sistemas de comunicaciones tácticas hasta las bandas más altas de los sistemas radar y de comunicaciones satelitales.

Generalmente, se acepta que la guerra electrónica se articula en torno a **tres ejes diferenciados**, que trabajan de forma conjunta para el control efectivo del espectro electromagnético, asegurando que las fuerzas propias puedan comunicarse y operar de manera efectiva mientras niegan o degradan la misma capacidad al enemigo. Cada una de estas categorías tiene sus propias técnicas, herramientas y metodologías, todas ellas fundamentales para las operaciones multidominio actuales.

- **Ataque electrónico (EA - Electronic Attack)) o contramedidas electrónicas (ECM - Electronic Counter Measures)**: Consiste en el uso de energía electromagnética, energía dirigida o armas anti-radiación para atacar al personal, instalaciones, equipos o sistemas de armas con la intención de degradar, neutralizar o destruir la capacidad de combate del enemigo.

- **Protección Electrónica (EP - Electronic Protection) o Contracontramedidas Electrónicas (ECCM – Electronic Counter Counter Measures)**: Son acciones tomadas para proteger al personal, instalaciones, equipos o sistemas de armas de cualquier efecto del uso propio o enemigo del espectro electromagnético que degrade, neutralice o destruya la capacidad de combate propia.

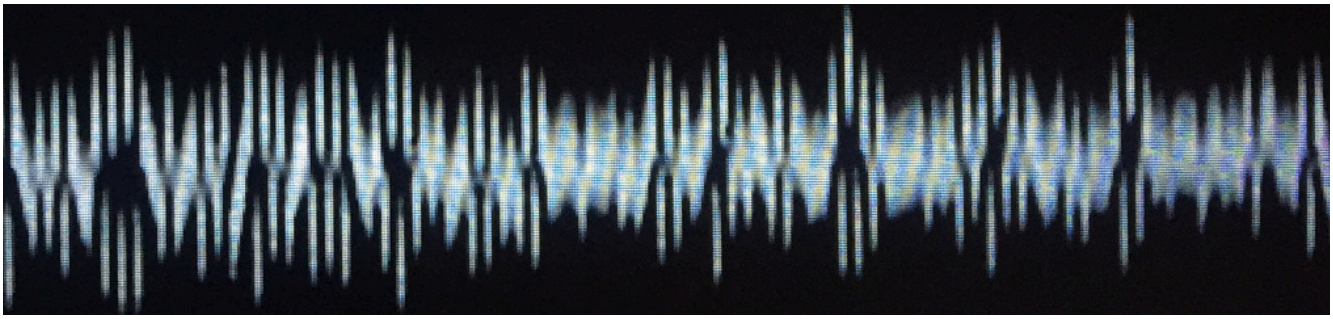
- **Apoyo Electrónico (ES – Electronic Support) o Medidas de Apoyo Electrónico (ESM – Electronic Support Measures)**: Son acciones llevadas a cabo para buscar, interceptar, identificar o localizar fuentes de energía electromagnética radiada intencionalmente o no con el propósito de reconocer inmediatamente amenazas, seleccionar objetivos y planificar y ejecutar operaciones futuras.

Ataque Electrónico (EA) / Contra Medidas Electrónicas (ECM)

Es el **conjunto de técnicas que se utilizan para engañar, confundir o desactivar los sistemas electrónicos del enemigo**. Las técnicas EA/ECM se pueden clasificar en varios tipos, dependiendo de su propósito y método de implementación. A continuación, se describen las técnicas más comunes en cada categoría.

- **Técnicas de Ataque Electrónico**: Las técnicas de ataque electrónico buscan interrumpir, engañar, o destruir los sistemas electrónicos del enemigo. Estos ataques pueden ser tanto ofensivos como defensivos y pueden tener varios objetivos, como la interferencia en las comunicaciones o la neutralización de sistemas de radar.
    - **Interferencia Electrónica (Jamming)**: Consiste en emitir señales de radiofrecuencia para saturar los receptores del enemigo y dificultar o impedir su capacidad de recibir o transmitir información (comunicaciones, radar o sistemas de navegación).
    - **Suplantación (Spoofing)**: Consiste en enviar señales falsas al enemigo para confundir o engañar sus sistemas electrónicos.
    - **Destrucción de Hardware**: Supone la destrucción física de los componentes electrónicos del enemigo mediante el uso de armas de energía dirigida o pulsos electromagnéticos.

    - **Engaño Electrónico (Deception)**: Se utiliza para manipular las percepciones del enemigo sobre la situación táctica, mediante la manipulación de señales o la falsificación de información.
- **Técnicas de Contramedidas Electrónicas**: Son técnicas defensivas que buscan proteger los propios sistemas electrónicos de los ataques enemigos.
    - **Resistencia a la interferencia (Jamming)**: Se centran en mantener la funcionalidad de los sistemas de comunicación y radar incluso bajo condiciones de interferencia.
    - **Detección y Localización de inhibidores (Jammers)**: Es crucial para identificar y neutralizar las fuentes de interferencia mediante el análisis de espectro y localización de origen.
    - **Encriptación y Seguridad de Comunicaciones**: Protegen la información transmitida contra la interceptación y la suplantación (spoofing).
    - **Emisión Controlada de Señales**: Es una técnica que busca minimizar la firma electromagnética de los sistemas propios para evitar la detección y la interferencia por parte del enemigo.
    - **Contramedidas Activas**: Implican el uso de sistemas que pueden responder directamente a las amenazas de guerra electrónica, ya sea eliminando o bloqueando las señales enemigas.



Protección Electrónica (EP) / Contra-Contra Medidas Electrónicas (ECCM)

Son las técnicas de guerra electrónica que mediante una variedad de prácticas intentan reducir o eliminar el efecto de las ECM del enemigo en los sensores electrónicos propios de las plataformas terrestres, navales y aéreas, y de los misiles. Existen varias técnicas comunes de EP/ECCM. Estos son algunos ejemplos:

- **Aumento de la potencia de transmisión de radio**: Esta es la técnica más básica. Implica aumentar la potencia de las transmisiones de radio para "quemar" el intento de interferencia del enemigo.
- **Armas de detección de radiación y detección de ECM**: Consiste en el uso de sensores que pueden reconocer los intentos enemigos de engañar a los radares e ignorarlos. Es el caso de los misiles antirradiación (ARM - anti radiation missile), que pueden detectar y apuntar a las emisiones de radio con sus propios sensores e incluso redirigirse hacia la fuente de la señal de interferencia enemiga si la interferencia hace imposible alcanzar su objetivo original.

- **Uso de tecnología de baja observabilidad:** Consiste en alterar la reflexión de una plataforma terrestre, naval o aérea mediante la aplicación de una capa absorbente de radar para debilitar la señal de retorno, dificultando su detección por el radar enemigo.
- **Software avanzado:** Consiste en el uso de software avanzado que puede discriminar mejor entre objetivos reales y señuelos.

Apoyo Electrónico (ES) – Medidas de Apoyo Electrónico (ESM)

Las técnicas de ES/ESM se pueden clasificar según su funcionalidad y aplicación, siendo la principal la **Inteligencia de Señales (SIGINT – Signals Intelligence)**, que es una forma de recopilación de información que se realiza mediante la interceptación de señales. Aquí hay algunos puntos clave:

- **Interceptación de comunicaciones**: SIGINT comprende la interceptación de comunicaciones directas entre personas (conversaciones telefónicas, mensajes de texto, llamadas de radio y canales de señalización), conocida como Inteligencia de Comunicaciones (**COMINT - Communications Intelligence**), o la interceptación de emisiones electrónicas de distintos medios que no son de comunicaciones, conocida como Inteligencia Electrónica (**ELINT – Electronic Intelligence**).
- **Análisis de información**: Los equipos SIGINT analizan las comunicaciones interceptadas para conocer mejor al adversario o enemigo, así como autoproteger las comunicaciones propias para evitar que puedan ser monitorizadas, analizadas e intervenidas.
- **Uso en investigación y espionaje**: Las técnicas SIGINT se utilizan habitualmente para conocer información sobre determinados objetivos tales como la información secreta presente en las comunicaciones de otro país, sus servicios de inteligencia, sus infraestructuras críticas u otras entidades de interés.

Futuro de la guerra electrónica

A medida que la tecnología continúa avanzando a un ritmo rápido, las fuerzas militares se enfrentan a diversos desafíos en el ámbito de la guerra electrónica. La congestión del espectro, las vulnerabilidades de la ciberseguridad y el desarrollo de contramedidas por parte de los adversarios plantean obstáculos continuos.

De cara al futuro, el campo de la guerra electrónica encierra un inmenso potencial. Los avances en el dominio del espectro, la integración con la inteligencia artificial y el aprendizaje automático, las actividades cibernéticas ofensivas, las armas de energía dirigida, las tecnologías cuánticas y fotónicas, y las capacidades espaciales darán forma a la evolución de la guerra electrónica.

De cara al futuro, la integración entre guerra electrónica y acciones cibernéticas será aún mayor a la hora de detectar y responder a amenazas exteriores.

Una de las consecuencias de esta integración es la dificultad en el futuro para garantizar la seguridad e integridad de los servicios públicos de los que depende la población civil.

Analizamos brevemente a continuación la aplicación de las tecnologías disruptivas y diferenciadoras como la fotónica y la cuántica al desarrollo futuro de la guerra electrónica.

Ventajas de la tecnología fotónica en los sistemas de guerra electrónica

La tecnología fotónica tiene un gran potencial en este campo, desde la **transmisión** de señales de microondas a través de fibras ópticas hasta la **medición** de la frecuencia de las señales en tiempo real y el **procesamiento** de múltiples canales de señales simultáneamente.

La RF fotónica es una de las tecnologías habilitadoras para la nueva generación de sistemas de guerra electrónica en aplicaciones de radar y comunicaciones, tanto en medidas ES/ESM como de EA/ECM.

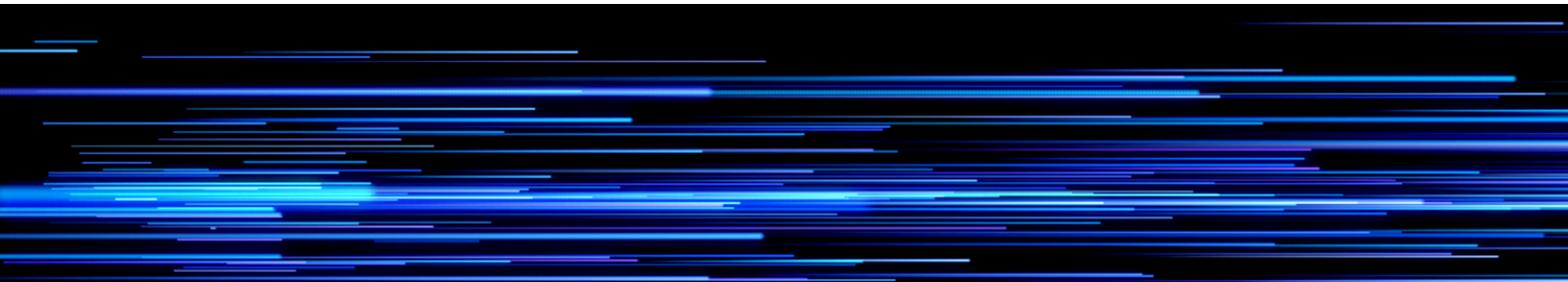
Las **principales ventajas** de los sistemas de guerra electrónica basados en tecnología fotónica frente a las tradicionales basados en RF son las siguientes:

- **Enorme ancho de banda instantáneo** (sin barrido) con capacidad de procesar instantáneamente anchos de banda muy grandes (> 40 GHz) y con envolventes de tamaño, peso y consumo (SWaP) muy reducidas. Esto permite hacer frente a radares de baja probabilidad de interceptación (LPI) que operan con gran agilidad en frecuencia y complejas formas de onda.
- **Procesamiento ultrarrápido con muy baja latencia** (< 10 ns), al sustituir los electrones por fotones.

- **Ataque electrónico más efectivo**, con gran capacidad para hacer frente a las ECCM del adversario (alta agilidad de frecuencia) y generar señales de alta fidelidad para engañar al radar.
- **Reducción de las cadenas de RF** con equipos (LRU – Line Replaceable Unit) de reducido factor de forma y bajo consumo (SWaP), maximizando la potencia por Gz más allá de los límites de la RF.
- **Libre de interferencias electromagnéticas**, debido a la naturaleza de la luz y su falta de interacción con campos eléctricos y magnéticos.
- **Bajo coste comparado con los sistemas basados en RF**, debido a su eficiencia energética, menor necesidad de mantenimiento, capacidad de transmisión de datos más alta y menor impacto ambiental.
- **Tecnología disponible en muy pocos países**, ya que sólo EE.UU., China, Rusia, Francia, Reino Unido e Israel disponen de sistemas de guerra electrónica operativos basados en tecnología fotónica.

Este conjunto de ventajas convierte la tecnología fotónica en una opción atractiva para aplicaciones de guerra electrónica.

Además, la tecnología fotónica permite el desarrollo de soluciones tanto para la interconexión con fibra óptica dentro de las plataformas terrestres, navales y aéreas, así como satélites, y para el diseño y fabricación de transpondedores, elevando la capacidad de proceso por 10 sin aumento de peso tamaño o consumo.



La tecnología cuántica y su potencial para revolucionar la guerra electrónica

La tecnología cuántica puede revolucionar la guerra electrónica de forma sustancial, pero **su aplicación práctica todavía está en etapas de desarrollo y prueba en muchos casos.** La implementación generalizada y efectiva de estas tecnologías en entornos operativos reales requiere superar aún varios **desafíos técnicos y de infraestructura**. A continuación, se presentan las principales áreas donde la tecnología cuántica puede tener un impacto significativo:

- **Ordenadores cuánticos**: Aprovechan las propiedades de las partículas cuánticas para realizar cálculos complejos a velocidades mucho más rápidas que los ordenadores clásicos, lo que puede permitir, por ejemplo, decodificar muy rápidamente señales cifradas o complejas utilizadas del enemigo, así como la optimización de operaciones de guerra electrónica.
- **Sensores cuánticos**: Utilizan las propiedades de las partículas cuánticas, como la superposición y el entrelazamiento, para realizar mediciones más precisas que los sensores convencionales, consiguiendo detecciones más precisas, de mayor alcance y la operación en entornos altamente congestionados, así como el desarrollo de ECCM avanzadas.

- **Comunicación cuántica**: Utiliza fenómenos como el entrelazamiento cuántico para transmitir información de manera segura y eficiente mediante enlaces de comunicación seguros, ya que cualquier intento de intercepción alteraría el estado cuántico de la señal, alertando a los usuarios.
- **Criptografía Cuántica**: Utiliza principios cuánticos para crear métodos de cifrado que aseguran que las comunicaciones militares no puedan ser interceptadas ni descifradas por el enemigo, protegiendo los datos críticos y la información estratégica. Además, la criptografía cuántica será crucial para la protección contra posibles ataques cuánticos. Los sistemas de cifrado cuántico han sido probados y están comenzando a implementarse en entornos de defensa.
- **Radar cuántico**: Utiliza propiedades cuánticas para detectar objetos con mayor precisión y a mayores distancias, posibilitando la detección temprana de amenazas y de objetivos sigilosos, y la detección no lineal de vehículos ocultos o enemigos que usan camuflaje.

Grupo Oesía como garante de la soberanía nacional en guerra electrónica

Desde Grupo Oesía tenemos el propósito de ayudar a crear un mundo mejor, más eficiente, seguro y sostenible para las generaciones futuras.

Un elemento clave dentro de esta misión es la de incrementar la **soberanía nacional**, contribuyendo a la **autonomía estratégica de Europa,** que nos permita hacer frente a desafíos tan importantes como la guerra electrónica. Para ello, estamos contribuyendo con desarrollos basados en tecnología fotónica y en tecnología cuántica.

Actualmente, se está llevando a cabo el desarrollo de **Sistemas de Guerra Electrónica** tanto en banda radar como en banda de comunicaciones basados en procesamiento fotónico, cuyas ventajas se han descrito anteriormente y que proporciona una capacidad de detección de señales muy superior.

Tecnobit-Grupo Oesía está trabajando en el proyecto GEFOT del Ministerio de Defensa, que incluye el suministro, instalación y pruebas de un sistema ELINT/COMINT basado en basado en tecnología fotónica para el Ejército de Tierra. Este proyecto constituirá el germen para el desarrollo de un nuevo sistema táctico de guerra electrónica terrestre.

Asimismo, Tecnobit-Grupo Oesía ha participado en el proyecto europeo SIGNAL para el desarrollo de una suite de guerra electrónica (SIGINT) embarcada en UAS.

Por otro lado, nuestras capacidades de **ciberseguridad y cifra** contribuyen a proteger la integridad de los sistemas y las comunicaciones. Nuestras soluciones cuentan con las certificaciones del Centro Criptológico Nacional (CCN) y la OTAN e incorporan elementos de última generación como la criptografía cuántica.

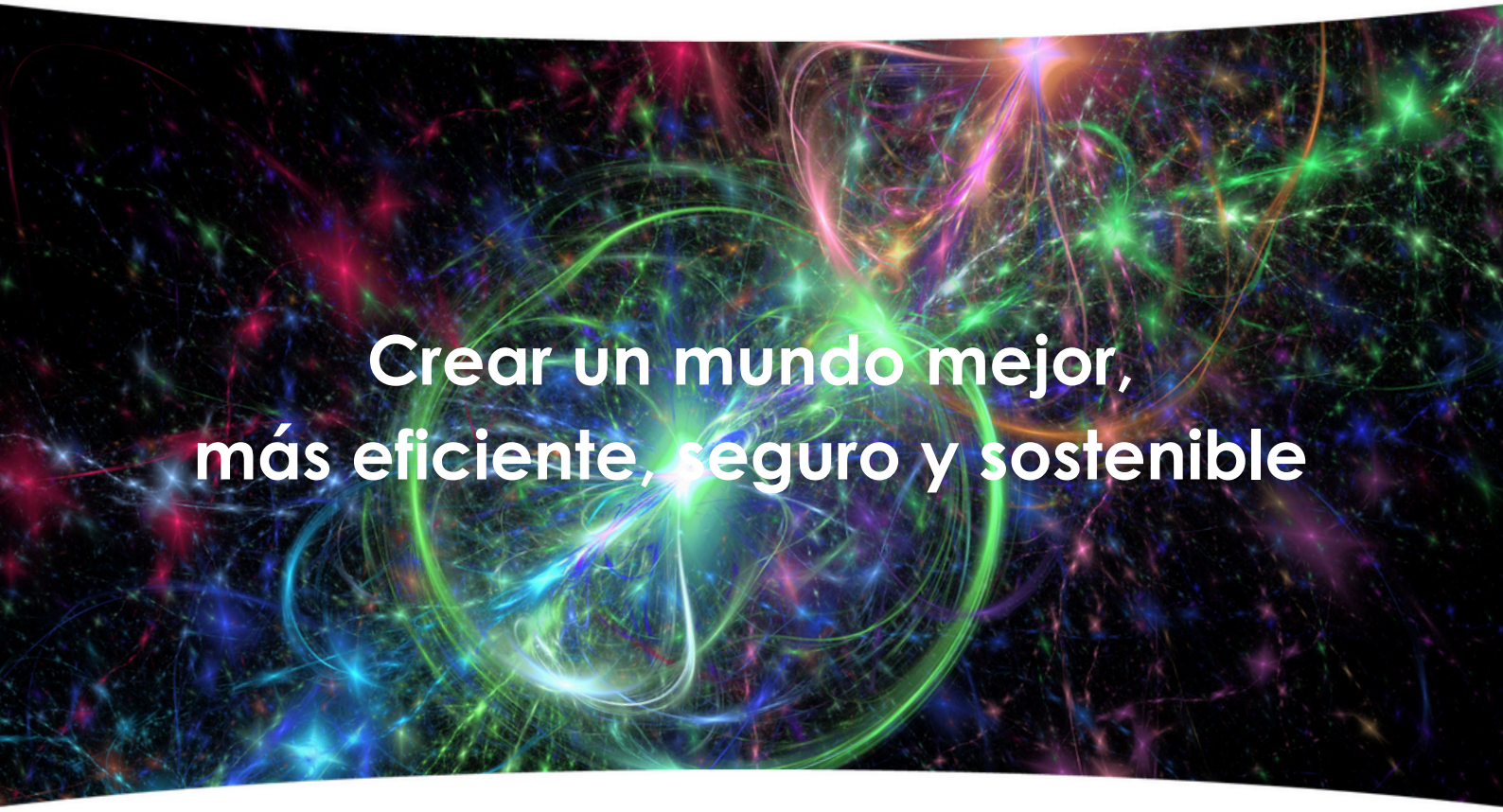
Por

Salvador Álvarez

Director de Estrategia
de Grupo Oesía

oesia grupo

tecnobit grupo oesia cipherbit grupo oesia UAV Navigation grupo oesia inster grupo oesia



grupooesia.com