Artículo noveno

Transformación del ciclo JISR en la era digital: innovación tecnológica para alcanzar la superioridad informativa

Begoña Rojo Carralero

Resumen

Este capítulo analiza la transformación del ciclo de Inteligencia, Vigilancia y Reconocimiento Conjunto (JISR) en el contexto de la era digital, impulsada por tecnologías emergentes y disruptivas. La integración de capacidades como la inteligencia artificial, los sensores distribuidos, las plataformas no tripuladas, el *edge computing* y los sistemas espaciales está redefiniendo la forma en que se planifica, ejecuta y explota la inteligencia en operaciones cada vez más multidominio.

A lo largo del texto, se examina el impacto de estas tecnologías en cada fase del proceso JISR (TCPED), así como los retos derivados de su uso: desde la necesidad de garantizar la interoperabilidad y la seguridad de los datos, hasta la gestión de riesgos asociados a la automatización, los sesgos algorítmicos o las vulnerabilidades frente a ciberataques.

El capítulo subraya que esta transformación no es únicamente técnica, sino también doctrinal y organizativa. Exige nuevas arquitecturas, un modelo de «dato único» y una cultura orientada a compartir, analizar y decidir con mayor agilidad. La inteligencia artificial no sustituye al factor humano, pero sí lo potencia. En definitiva, la innovación tecnológica aplicada al proceso JISR es una condición necesaria para alcanzar la superioridad informativa en los entornos operativos actuales y futuros.

Palabras clave

JISR, Tecnologías emergentes, IA, Superioridad informativa, Interoperabilidad.

Transformation of the JISR cycle in the digital age: technological innovation to achieve information superiority

Abstract

This chapter examines the transformation of the Joint Intelligence, Surveillance and Reconnaissance (JISR) cycle in the context of the digital age, driven by emerging and disruptive technologies. The integration of capabilities such as artificial intelligence, distributed sensors, unmanned

platforms, edge computing and space-based systems is redefining how intelligence is planned, executed and exploited in increasingly multi-domain operations.

The text analyses the impact of these technologies on all phases of the JISR cycle (TCPED) and highlights some of the main the challenges: the need for interoperability, secure and reliable data sharing, and the risks associated with automation, algorithmic bias and vulnerability to cyber threats.

The chapter emphasizes that this transformation is not only technical, but also doctrinal and organizational. It requires new ISR architectures, a 'single data' philosophy, and a cultural shift towards faster, more collaborative and adaptive intelligence processes. Artificial intelligence does not replace the human factor; it enhances it. Ultimately, technological innovation applied to the JISR cycle is a strategic imperative to achieve information superiority in today's and tomorrow's operational environments.

Keywords

JISR, AI, Emerging Technology, Information Superiority, Interoperability.

«En el siglo XXI, el éxito no será del que más datos obtenga, sino del que más rápido y mejor los convierta en decisiones acertadas».

1 Introducción

La información sigue siendo un factor clave para el éxito en los ámbitos de la seguridad y la defensa. No se trata solo de procesarla, sino también de disponer de ella y trasladarla al nivel de decisión correspondiente, en el momento oportuno y en el formato adecuado.

En un entorno operativo cada vez más digital, automatizado y multidominio, como el de hoy en día, el papel de la inteligencia sigue siendo esencial, pero su forma de generarse, procesarse y aplicarse está cambiando de forma radical. La capacidad de observar, analizar y decidir con rapidez está redefiniendo las reglas del juego. En pleno siglo XXI, el acceso a información precisa y en tiempo real se ha convertido en un factor crítico para obtener ventaja frente a un adversario.

En este contexto, el proceso de inteligencia, vigilancia y reconocimiento conjunto (*Joint ISR o JISR*) se consolida como una herramienta esencial de apoyo al planeamiento y la conducción de operaciones. El volumen, la diversidad y la velocidad de los datos disponibles superan las capacidades de los sistemas convencionales, por lo que la innovación es una herramienta de apoyo para su mejora continua.

Innovar consiste en introducir ideas nuevas o transformar lo ya existente para mejorar los resultados. En el ámbito de la inteligencia militar, esta mejora podría traducirse en la capacidad de tomar decisiones más rápidas, mejor informadas y adaptadas a un entorno operativo cada vez más complejo.

La innovación tecnológica, impulsada por el desarrollo de tecnologías emergentes y disruptivas, está transformando el proceso JISR en profundidad. La inteligencia artificial, el *edge computing*[1], los sensores distribuidos, las plataformas no tripuladas y el uso de fuentes abiertas están dando lugar a un nuevo modelo de arquitectura ISR, más automatizado, interoperable y adaptativo.

La propia OTAN ha reconocido este cambio. En su Concepto Estratégico más reciente, establece el conocimiento superior del entorno como una condición necesaria para mantener la disuasión y responder eficazmente a las amenazas actuales. En este contexto, el enfoque de operaciones

[1] *Edge Computing* o computación en el borde es un paradigma tecnológico que permite procesar los datos cerca de su fuente de generación (sensores, plataformas), lo que reduce la latencia y mejora la capacidad de respuesta en tiempo real.

multidominio (MDO) adquiere especial relevancia como modelo operativo integrado, en el que el proceso JISR permite coordinar capacidades en los ámbitos terrestre, marítimo, aéreo, ciberespacial y cognitivo.

Este capítulo analiza cómo el proceso JISR está evolucionando hacia un sistema más eficiente y multidominio, capaz de operar en entornos altamente digitalizados. A lo largo del texto, se examinarán tanto las oportunidades que ofrecen estas tecnologías como los riesgos y desafíos que plantean.

Innovar en el proceso JISR no es solo una opción tecnológica, sino una necesidad estratégica para anticiparse, adaptarse y decidir con ventaja. En definitiva, el objetivo no es recopilar más datos, sino convertirlos más rápido y de manera fiable en información útil. Y para eso, las tecnologías emergentes y disruptivas, en particular la inteligencia artificial, resultan determinantes.

2 Conceptos básicos del proceso ISR

La Inteligencia, Vigilancia y Reconocimiento Conjunto (JISR) es una capacidad clave para dotar de conciencia situacional al mando y facilitar una toma de decisiones oportuna.

Dentro de la doctrina conjunta de los países aliados, el término JISR se define como el conjunto de capacidades de inteligencia y operaciones que integra las capacidades de recopilación con el procesamiento, explotación y difusión de la información resultante[2].

El proceso JISR se define como un proceso de coordinación a través del cual la recopilación de inteligencia y las actividades de explotación proporcionan datos e información para satisfacer una necesidad de información o inteligencia, en un marco temporal deliberado, *ad hoc* o dinámico, en apoyo de la planificación y ejecución de las operaciones.

Este proceso tiene como objetivo apoyar directamente la planificación, preparación y ejecución de las operaciones, apoyándose en los siguientes elementos constitutivos, los cuales se resumen a continuación:

— Inteligencia: este componente abarca todas las disciplinas de recopilación de inteligencia, incluidas sus capacidades y activos de recolección, procesamiento, explotación y difusión. Las disciplinas de recopilación de inteligencia incluyen: inteligencia acústica (ACINT), inteligencia humana (HUMINT), inteligencia de imágenes (IMINT), inteligencia de medición y firma (MASINT),

[2] Extracto de la definición del proceso JISR según publicaciones y procedimientos de organismos aliados.

inteligencia de fuentes abiertas (OSINT) e inteligencia de señales (SIGINT)

— Vigilancia: la vigilancia consiste en la observación sistemática en todos los ámbitos operativos. Se lleva a cabo mediante medios visuales, electrónicos, fotográficos o de otro tipo y puede abarcar grandes áreas o enfocarse en objetivos específicos.

— Reconocimiento: el reconocimiento permite obtener información mediante observación visual u otros métodos de detección. Su propósito es recopilar datos sobre las actividades y recursos de un adversario o conocer las características meteorológicas, hidrográficas o geográficas de una zona determinada.

Junto con los elementos descritos con anterioridad, este proceso, consta de cinco fases conocidas como TCPED (T*ask, Collect, Process, Exploit and Disseminate*):

— *Task* (Asignación): recopilación de necesidades ISR y planificación interna de recursos, gestión y asignación de capacidades.

— *Collect* (Recopilación): obtención de datos e información a través de sensores terrestres, aéreos, navales, espaciales, cibernéticos y cognitivos, así como de fuentes humanas o abiertas.

— *Process* (Procesado): organización, filtrado y análisis inicial de los datos. Esta fase puede realizarse mediante personal especializado o algoritmos automatizados.

— *Exploit* (Explotación): interpretación avanzada de la información. También puede dar lugar a nuevas necesidades.

— *Disseminate* (Difusión): entrega de la información a los usuarios adecuados en el momento preciso, a través de canales seguros y adaptados al nivel táctico, operacional o estratégico.

Figura 1. Esquema de fases del ciclo JISR

Este proceso no funciona de forma aislada. Está vinculado con el proceso de gestión de las necesidades de inteligencia y gestión de la obtención, conocido como IRM&CM (*Intelligence Requirements Management & Collection Management*). Su objetivo es garantizar que las necesidades de información sean correctamente formuladas, priorizadas y cubiertas mediante los medios más adecuados y optimizar el uso de recursos ISR.

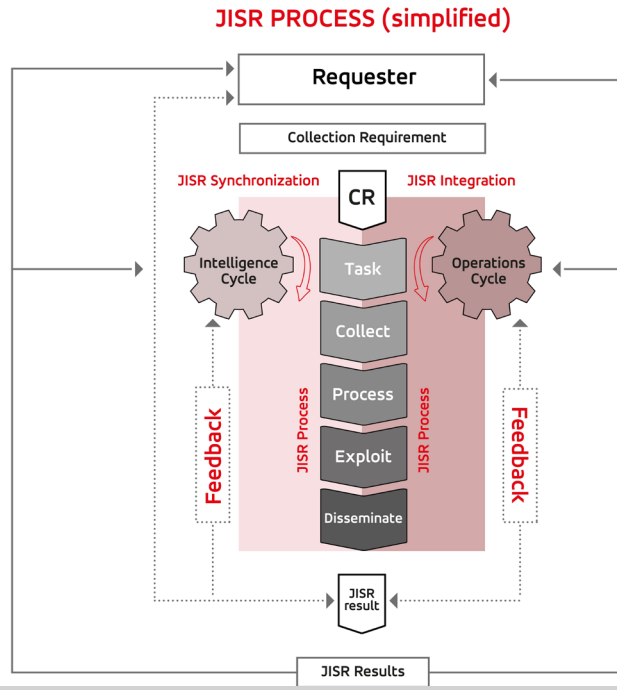

Figura 2. Relación entre el Ciclo de Inteligencia y su Integración en las Operaciones

La figura 2 muestra de manera esquemática la interconexión entre ISR y los ciclos de inteligencia y operaciones.

3 JISR en las operaciones multidominio y el campo de batalla transparente

El concepto de operaciones multidominio (*Multi-Domain Operations*, *MDO*) está ganando un protagonismo creciente como modelo de actuación militar que busca la sincronización de capacidades a través de los dominios terrestre, marítimo, aéreo, espacial, cibernético y cognitivo. Este enfoque permite generar efectos coordinados y simultáneos, de modo que explota sinergias entre dominios y reduce los tiempos de respuesta ante amenazas complejas y dinámicas.

En este nuevo entorno operativo, profundamente digitalizado y caracterizado por una densa malla de sensores y fuentes de información, ha emergido lo que de modo informal se denomina «campo de batalla transparente». Esta nueva realidad no responde tanto a una capacidad deseada, sino al resultado inevitable de la hiperconectividad: sensores militares y civiles, plataformas no tripuladas, redes sociales, dispositivos inteligentes y satélites que generan información constante y multidominio. Todo emite, todo es observado, todo deja rastro.

La consecuencia directa de esta transformación es que el proceso JISR ha tenido que adaptarse a un ecosistema donde la accesibilidad, la veracidad y la velocidad de los datos se han convertido en variables operativas críticas. En un entorno permanentemente observado, cualquier evento relevante puede ser detectado, geolocalizado, interpretado y compartido, por lo que la capacidad de actuar con rapidez es un factor decisivo.

En este contexto, la fusión de información procedente de múltiples fuentes de imágenes (IMINT), señales (SIGINT), fuentes abiertas (OSINT) y combinarla con inteligencia geoespacial (GEOINT) o inteligencia humana (HUMINT), se convierte en el eje central del valor añadido que aporta el sistema JISR. Este nivel de integración se está viendo beneficiado gracias a la inteligencia artificial (IA), que automatiza la explotación, detecta patrones, señala anomalías y facilita decisiones en tiempo real.

La IA, junto con el resto de las tecnologías innovadoras descritas en este capítulo como la «computación en el borde», la sensorización avanzada o los sistemas distribuidos, actúa como catalizador del cambio. El proceso ISR debe ser, por tanto, un sistema distribuido, alimentado por datos de múltiples dominios, orientado a generar información útil, oportuna y verificable.

4 Iniciativas OTAN y europeas relacionadas con el ciclo de inteligencia

La densidad informativa se ha incrementado exponencialmente con la incorporación de sensores comerciales, plataformas autónomas, constelaciones de pequeños satélites, sistemas HAPS (*High Altitude Platform Systems*), sistemas IoT (*Internet of the Things*) y datos abiertos. Todo ello conforma un entorno donde el reto no es solo recoger información, sino organizarla, explotarla y compartirla eficazmente, de modo que garantice coherencia y accesibilidad en tiempo real.

En este entorno, la OTAN ha introducido el concepto de «vigilancia persistente»[3] como un requisito clave para garantizar una respuesta eficaz ante esta nueva realidad operativa. Esta vigilancia exige la integración de medios en múltiples dominios y el desarrollo de nuevas estructuras, procesos y capacidades. La capacidad de utilizar y fusionar distintas herramientas será esencial para lograr este objetivo.

En esta línea, se enmarca la iniciativa *Allied Persistent Surveillance from Space* (APSS), que busca establecer una capacidad aliada de vigilancia persistente desde el espacio e integra activos nacionales y comerciales para proporcionar productos ISR que apoyen la toma de decisiones conjuntas. Esta capacidad incluye la recopilación, análisis

[3] The future of NATO- C4ISR-Assesment and recommendations after Madrid y «The Future of NATO C4ISR» (NCI Agency). JDN 1/23 (UK) y doctrina organismos aliados.

Figura 3. Alliance Ground Surveillance (AGS) RQ-4D «Phoenix». Foto OTAN

y diseminación de datos obtenidos por satélites y sensores espaciales, con el apoyo de herramientas de inteligencia artificial, y bajo estándares compartidos como el STANAG 4559[4], cuyo objetivo es promover la interoperabilidad para el intercambio de productos de inteligencia, vigilancia y reconocimiento entre los sistemas C4ISTAR (*Command, Control, Comunications, Computers, Intelligence, Surveillance Target Acquisiton and Reconnaissance)* accesibles a la OTAN.

Por su parte, la Unión Europea, a través del *Capability Development Plan* (CDP) 2023 de la Agencia Europea de Defensa (EDA), ha identificado como prioridad estratégica el desarrollo de capacidades C4ISTAR persistentes, interoperables y basadas en datos para la defensa colectiva, la gestión de crisis y la resiliencia estratégica.

Además, el Fondo Europeo de Defensa (EDF, por sus siglas en inglés) ha financiado múltiples proyectos de innovación orientados al refuerzo de la arquitectura ISR europea:

— LOTUS, centrado en plataformas terrestres no tripuladas para vigilancia y reconocimiento.

— ODIN'S EYE, orientado a la alerta temprana desde el espacio y sensores de observación estratégicos.

— ABIDE, que explora el uso de inteligencia artificial y *big data* para la toma de decisiones en C4ISR.

[4] STANAG 4559- NATO standard ISR library interfaces and services.

— REACT, enfocado en fusión de datos y arquitectura de sistemas ISR federados.

— SAURON, especializado en vigilancia persistente para protección de infraestructuras críticas.

Estas iniciativas evidencian una apuesta clara por arquitecturas abiertas, distribuidas y colaborativas, capaces de reforzar la innovación y la autonomía tecnológica europea y su integración con las capacidades aliadas.

5 Transformación del proceso JISR: del modelo clásico al digital y multidominio

Las condiciones descritas en los apartados anteriores, junto con la innovación aportada por las tecnologías emergentes y disruptivas, obligan a replantear de forma profunda la organización, ejecución y arquitectura del sistema JISR.

La transición a la era digital ha generado un entorno operativo profundamente transformado, en el que la información de dominio público, procedente de redes sociales, sensores urbanos, dispositivos inteligentes o comunicaciones máquina a máquina, supera en volumen y diversidad a las fuentes militares tradicionales. Este cambio ha desdibujado las fronteras entre lo civil y lo militar.

El volumen, la variedad y la velocidad de los datos superan la capacidad de procesamiento manual y las operaciones actuales se desarrollan de forma simultánea en múltiples dominios. Además, se integran capacidades de aliados y socios, con arquitecturas técnicas diversas y fuentes de información cada vez más descentralizadas. La proliferación de fuentes y formatos exige sistemas capaces de operar en red, en entornos federados y con interoperabilidad semántica, para evitar duplicidades, ambigüedades o sesgos en la producción de la información requerida en el proceso.

Esta evolución plantea retos específicos para el proceso JISR, derivados de las características del *big data*: volumen, variedad, velocidad y veracidad. La capacidad para obtener datos ya no es el principal problema: lo son su validación, priorización, fusión y explotación eficaz en tiempo útil.

Este nuevo escenario exige un sistema ISR distribuido, automatizado y multidominio, capaz de integrar flujos de datos heterogéneos, operar con flexibilidad y generar información útil en tiempo real[5]. La digitalización está reforzando esta tendencia y facilita la convergencia entre capacidades ISR, guerra electrónica, ciberdefensa y plataformas de combate. En este nuevo

[5] Tal y como recogen documentos doctrinales de la OTAN, la JDN 1/23 del Reino Unido y el informe *Science & Technology Trends 2023-2043*, esta es una transformación en curso actualmente.

paradigma, la ISR se consolida como una capacidad funcional central, lo que supera su rol tradicional de apoyo auxiliar y se conecta de forma transversal con los procesos de planificación, ejecución y evaluación de operaciones.

Para operar eficazmente a los desafíos del entorno actual, las arquitecturas ISR deben diseñarse, implementarse y gestionarse conforme a una serie de principios y criterios operativos fundamentales[6]:

- Flexibilidad: para adaptarse rápido a los cambios del entorno operacional. Esto implica reconfiguración dinámica de sensores, priorización automatizada y adaptación a nuevas amenazas o áreas de interés.
- Misión a medida: de modo que cada despliegue ISR responda a las necesidades específicas de la operación, en función de los dominios implicados y el tipo de información requerida.
- Interconectividad: que garantice la integración fluida entre sensores, plataformas, niveles de mando, dominios operativos y socios aliados. Debe facilitarse tanto la conexión vertical como horizontal entre capacidades ISR.
- Compatibilidad: mediante el cumplimiento de estándares técnicos y doctrinales comunes, como los definidos por la OTAN o los marcos de interoperabilidad de la UE. Esto permite compartir productos ISR en entornos multinacionales.
- Automatización: las redes ISR deben operar con el mayor grado posible de automatización y permitir el ajuste autónomo de prioridades y la activación oportuna de sensores.
- Escalabilidad: deben disponer de capacidad suficiente para adaptarse al crecimiento del volumen de datos e incluir recursos de almacenamiento, análisis y diseminación segura.
- Ancho de banda y conectividad: la arquitectura debe garantizar una infraestructura de comunicaciones robusta, segura, capaz de soportar flujos de datos intensivos, minimizar latencias y asegurar la disponibilidad en condiciones adversas.
- Resiliencia y redundancia: de forma que la arquitectura pueda mantener funcionalidad básica incluso en entornos degradados. Cuando la red integrada no esté disponible, deben activarse estructuras alternativas que aseguren la continuidad de la obtención y la diseminación de la información necesaria.

[6] UK Joint Doctrine Note 1/23 (JDN 1/23), que adapta con una exposición más explícita y moderna los principios fundamentos del diseño del proceso JISR según OTAN.

Este conjunto de principios y transformaciones técnicas tiene un objetivo final: garantizar que el sistema ISR no solo responda a las necesidades actuales de las operaciones, sino que esté preparado para adaptarse, anticiparse y operar de forma resiliente en entornos cada vez más interconectados, competitivos y saturados de información.

6 Impacto de las tecnologías emergentes en el proceso JISR

La innovación tecnológica está transformando de manera acelerada el proceso JISR. Esta evolución afecta a toda su arquitectura: desde la expansión de sensores y fuentes de información hasta la automatización de los procesos de análisis y difusión de información.

Tanto la OTAN como la Unión Europea han identificado un conjunto de áreas tecnológicas prioritarias, conocidas como tecnologías emergentes y disruptivas que están redefiniendo los modelos operativos, las capacidades militares y la forma en que se genera inteligencia en los entornos modernos.

En el caso de la OTAN, la clasificación como *Emerging and Disruptive Technologies (EDT)* incluye diez grandes categorías: inteligencia artificial (IA), sistemas autónomos y robótica, *big data* y tecnologías de información, espacio, sistemas hipersónicos, energía y propulsión, materiales avanzados, electrónica y electromagnetismo, tecnologías cuánticas y tecnologías de mejora humana y biotecnología.

Por su parte, la Unión Europea, a través de la EDA y el Fondo Europeo de Defensa ha desarrollado una agenda convergente centrada en el refuerzo de la autonomía estratégica, el entorno electromagnético, la ciberdefensa, el espacio, las plataformas no tripuladas y los sensores colaborativos.

Esta convergencia en las prioridades estratégicas de OTAN y UE evidencia una clara alineación en cuanto al papel esencial que tendrán estas tecnologías para el desarrollo futuro de las capacidades militares.

Este desarrollo tecnológico está transformando de manera acelerada el ciclo de inteligencia. Esta evolución no se limita a la automatización del análisis de datos, sino que afecta a toda la arquitectura ISR, desde la proliferación de sensores hasta la explotación descentralizada en tiempo real.

A continuación, se analiza el impacto de algunas de ellas en las distintas fases y dimensiones del proceso JISR.

6.1 IA y Computación en el borde (edge computing)

Uno de los principales retos del proceso JISR es gestionar de forma eficaz el enorme volumen de datos generado por sensores distribuidos, plataformas no tripuladas y fuentes abiertas. La inteligencia artificial y la

computación en el borde están transformando este proceso, de modo que permite automatizar tareas complejas de análisis, reducir los tiempos de respuesta y optimizar el ciclo de toma de decisiones.

La IA facilita la fusión de datos provenientes de múltiples fuentes (IMINT, SIGINT, OSINT, GEOINT, HUMINT) y permite detectar patrones, anticipar amenazas, clasificar objetos o generar alertas en tiempo real. Además, contribuye a reducir la carga cognitiva del operador, priorizar lo relevante y ofrecer productos listos para la explotación operativa.

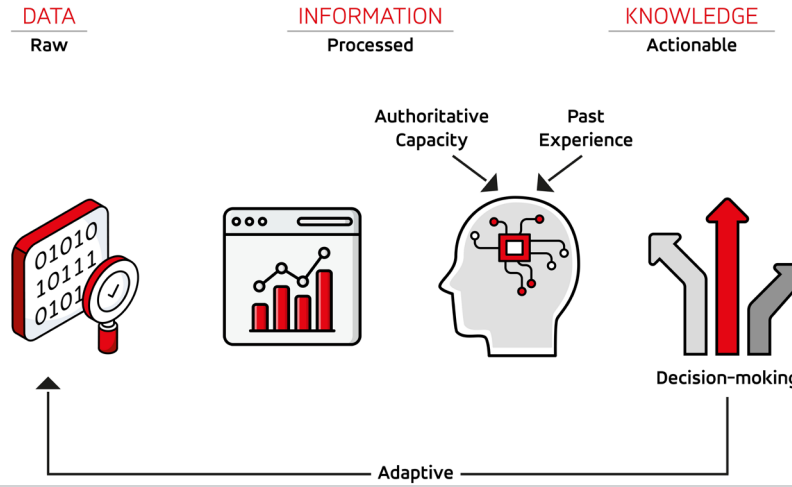

Figura 4. Flujo de datos a información. Fuente: Internetofwater.org

En paralelo, la computación en el borde (*edge computing*) permite procesar la información directamente en el sensor o en plataformas cercanas al punto de obtención, sin necesidad de enviarla a centros centralizados. Esta capacidad mejora la autonomía operativa, aumenta la resiliencia ante interrupciones en la red y es especialmente útil en UAV, sensores desplegados en zonas remotas o sistemas que operan en entornos degradados.

La digitalización impulsada por el Internet Militar de las Cosas (IoMT), genera nuevas exigencias en interoperabilidad, conectividad y gestión de datos. Esta evolución tecnológica está favoreciendo el despliegue de plataformas autónomas o en enjambre, capaces de actuar de forma coordinada, con una supervisión humana más centrada en los efectos que en la gestión técnica del sistema.

Esta transformación tiene también un impacto directo en los perfiles profesionales requeridos. Se demandan operadores con capacidades híbridas, capaces de interactuar con sistemas inteligentes, interpretar salidas automatizadas y tomar decisiones en entornos altamente digitalizados.

Esto obligará a adaptar los programas de formación y entrenamiento en ISR, con un enfoque más técnico, cognitivo y multidominio.

6.2 Expansión y diversificación de sensores

Los sensores son la base del proceso JISR. El avance de la tecnología ha permitido desplegar una gran diversidad de sensores en todos los dominios operativos (terrestre, marítimo, aéreo, espacial, cibernético y cognitivo) con capacidad para recopilar datos ópticos, térmicos, acústicos, electromagnéticos o gravitacionales. La miniaturización y la mejora en eficiencia energética han aumentado la persistencia, adaptabilidad y cobertura de estos sistemas en entornos complejos y multidominio.

El concepto de red de sensores interconectados permite configurar sistemas distribuidos de vigilancia, donde la información se obtiene, transmite y analiza de forma colaborativa. La implementación de procesamiento avanzado en el propio sensor, combinado con *edge computing*, reduce la necesidad de transmitir grandes volúmenes de datos, mejora la fiabilidad de la información y optimiza el uso del ancho de banda.

Además, los sensores civiles y comerciales, como los integrados en redes sociales, dispositivos móviles o sistemas IoT[7], amplían las capacidades del proceso ISR. Estos dispositivos, que recogen vídeo, audio, posicionamiento por satélite o datos de proximidad, proporcionan fuentes complementarias de información con un alto valor operativo, sobre todo, en entornos urbanos o híbridos.

La integración de datos procedentes de redes sociales y sensores tradicionales permitirá avanzar en tareas como el filtrado y resumen de contenido, la detección y seguimiento de eventos, el análisis de dinámicas sociales o la identificación de anomalías en tiempo real. Esta fusión de fuentes y tecnologías mejora la capacidad de respuesta ante amenazas emergentes y consolida un ecosistema de inteligencia más preciso, adaptable y resiliente frente a amenazas electrónicas o cibernéticas.

6.3 Uso de plataformas no tripuladas

El empleo de plataformas no tripuladas (UxV) ha supuesto un cambio cualitativo en las capacidades de inteligencia, vigilancia y reconocimiento. Su integración en operaciones es ya una realidad, impulsada por su capacidad para operar con bajo riesgo, mantener prolongados tiempos de permanencia y posicionarse con flexibilidad en entornos complejos o de difícil acceso.

[7] Internet of the Things.

En particular, los vehículos aéreos no tripulados (UAV) en sus distintas categorías: micro, mini, tácticos o estratégicos, permiten cubrir distintas zonas de interés con sensores ligeros (EO/IR, radar, magnéticos, entre otros), lo que mantiene una vigilancia adaptable y continua. Estas plataformas han demostrado ser especialmente eficaces en operaciones prolongadas, misiones de patrullaje y entornos con escasa cobertura ISR tradicional.

En escenarios urbanos o de combate asimétrico, los micro-UAV desplegables están mejorando de forma significativa la conciencia situacional en tiempo real. Facilitan la adquisición de objetivos, el reconocimiento inmediato y la protección de fuerzas, a la vez que reducen el riesgo para el personal desplegado.

En paralelo, se están desarrollando capacidades de enjambres coordinados de UxV, en los que múltiples unidades cooperan de forma autónoma mediante reparto dinámico de tareas. Estas arquitecturas permitirán ampliar la cobertura ISR, reducir los tiempos de respuesta y optimizar los recursos en operaciones distribuidas y multidominio.

Figura 5. Sistema ISR no tripulado Clase I SEEKER de AUREA Avionics

El uso masivo e inteligente de UxV seguirá creciendo, en especial, cuando se integren con IA, *edge computing* y redes ISR interoperables. Su papel como nodos dinámicos de obtención consolidará su valor dentro del ecosistema JISR.

6.4 Tecnologías cuánticas

Las tecnologías cuánticas, aunque aún en fases de desarrollo incipientes, se perfilan como habilitadores disruptivos claves para el proceso JISR en el horizonte 2030-2040. Su potencial transformador abarca capacidades de

obtención, comunicación, análisis y protección de la información, con implicaciones directas en todos los dominios operativos.

En primer lugar, los sensores cuánticos permitirán detectar con extrema precisión variaciones gravitacionales, geomagnéticas o inerciales. Esta capacidad será especialmente útil en entornos donde los sistemas de navegación por satélite han sido negados o degradados. También se contempla su empleo para mapeo subterráneo, navegación en zonas GNSS-denegadas (entornos donde las señales de navegación por satélite no están disponibles o están limitadas) o seguimiento de objetos submarinos, ampliando las capacidades ISR en entornos difíciles.

En segundo lugar, las comunicaciones cuánticas, en especial mediante técnicas de distribución cuántica de claves (QKD), permitirán establecer enlaces de transmisión prácticamente inmunes a la interceptación o manipulación externa. Estas soluciones reforzarán la seguridad de redes ISR entre plataformas móviles, nodos distribuidos y enlaces espaciales.

Por último, la computación cuántica ofrece una capacidad teórica para resolver problemas complejos no abordables con los sistemas actuales. Su aplicación potencial al análisis masivo de datos, la optimización de misiones, la simulación avanzada de escenarios operativos o la toma de decisiones en tiempo real podría suponer un salto cualitativo para el sistema JISR. Sin embargo, estas aplicaciones aún enfrentan importantes desafíos técnicos, como la estabilidad de los *cúbits*, las condiciones extremas de funcionamiento o la escalabilidad de los sistemas.

Según el informe NATO Science & Technology Trends 2023-2043, los sensores cuánticos son la línea más próxima a una aplicación operativa real, mientras que las comunicaciones y la computación cuántica requerirán más tiempo para alcanzar una madurez funcional. Aun así, su desarrollo anticipado será esencial para mantener la superioridad informativa y la resiliencia frente a actores tecnológicamente avanzados.

6.5 Espacio / satélites

El espacio se ha consolidado como un dominio estratégico crítico para las capacidades ISR modernas. Su valor reside tanto en la obtención de información como en la vigilancia, observación y superioridad informativa en entornos operativos complejos. Durante la próxima década, se espera un aumento exponencial de las capacidades espaciales, impulsado por la miniaturización de plataformas, la reducción de costes de lanzamiento y la madurez tecnológica de sistemas orbitales.

Uno de los desarrollos más significativos es la proliferación de pequeños satélites (*smallsats*) en órbitas bajas (LEO) y medias (MEO). Estas plataformas, más económicas y flexibles que los grandes satélites tradicionales, permiten una vigilancia más frecuente, mayor resiliencia frente a amenazas

antisatélite y una capacidad de observación más ágil. Las constelaciones de *smallsats*, equipadas con sensores ópticos, infrarrojos o radar de apertura sintética (SAR), ofrecen una resolución y latencia cada vez más competitivas.

En este contexto, la iniciativa *Allied Persistent Surveillance from Space* (APSS) de la OTAN, mencionada en apartados previos, impulsa el desarrollo de una arquitectura aliada de vigilancia permanente desde el espacio. Esta capacidad integrará activos nacionales y comerciales para proporcionar productos ISR basados en satélites y sensores embarcados, combinados con herramientas de procesamiento avanzado, fusión de datos e inteligencia artificial. Todo ello bajo estándares OTAN como el STANAG 4559, que garantizan la interoperabilidad entre aliados.

Paralelamente, se están desarrollando soluciones intermedias como los HAPS (*High-Altitude Pseudo-Satellites*). En el marco de la PESCO (Permanent Structured Cooperation) y el Fondo Europeo de Defensa, el proyecto EuroHAPS está experimentando con dirigibles estratégicos, plataformas híbridas y globos estratosféricos, diseñados para operar durante largos periodos de tiempo. Estas plataformas ligeras ofrecen una vigilancia persistente en escenarios donde los satélites pueden tener limitaciones.

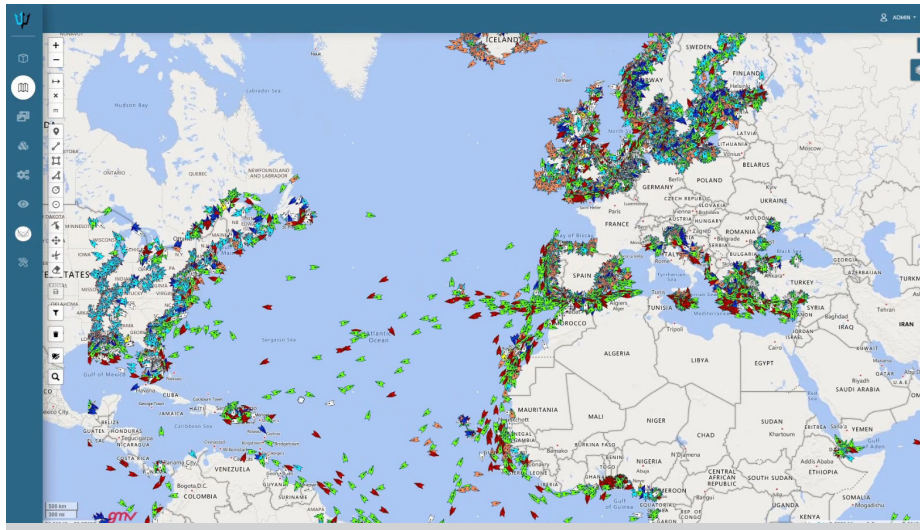

Figura 6 Sistema C2 SOCRATES de GMV para la detección y clasificación de buques

Por último, los programas de satélites de comunicaciones militares de nueva generación, como SPAINSAT *Next Generation* (SPAINSAT NG), están diseñados para reforzar la conectividad segura y la resiliencia de los flujos de información en operaciones conjuntas y multidominio. Su integración en arquitecturas ISR interoperables será esencial para asegurar el dominio informativo y la continuidad operativa en todo el espectro de misiones.

6.6 Sistemas hipersónicos

Actualmente, se están explorando las posibilidades de emplear plataformas hipersónicas con fines ISR y aprovechan su alta velocidad y baja detectabilidad para realizar misiones de reconocimiento estratégico a gran altitud. Este tipo de plataformas permitiría una recolección de datos e información más ágil y flexible que la ofrecida por los satélites tradicionales, sobre todo, en escenarios donde se requiera una cobertura puntual, rápida y de difícil detección.

Desde el punto de vista de la amenaza, los sistemas hipersónicos representan un desafío tecnológico emergente de primer orden. Su combinación de velocidad extrema, capacidad de maniobra y baja firma los hace difíciles de detectar, seguir e interceptar. Estas características obligan a rediseñar las arquitecturas actuales de alerta temprana, seguimiento y respuesta, ya que reducen drásticamente los márgenes temporales para la toma de decisiones.

Para enfrentarlos, será necesario integrar redes de sensores distribuidos, tanto terrestres como espaciales, apoyadas en capacidades de análisis automatizado e inteligencia artificial. Solo una arquitectura ISR adaptativa, con detección en múltiples dominios y capacidad de respuesta en tiempo casi real, podrá ofrecer cobertura efectiva frente a este tipo de amenazas.

6.7 Tendencias transversales en tecnologías emergentes aplicables a ISR

Además de las tecnologías específicas ya analizadas, existen líneas de desarrollo que están impactando de forma transversal en el ecosistema JISR y aportan capacidades complementarias que refuerzan su precisión, adaptabilidad y resiliencia.

Los nuevos materiales, como metales avanzados, recubrimientos inteligentes o superficies autolimpiables, permiten fabricar antenas más potentes, estructuras más ligeras y resistentes y componentes capaces de operar en condiciones extremas. La «fabricación aditiva», por su parte, está revolucionando la logística militar, al posibilitar la producción *in situ* de piezas críticas para sensores o plataformas ISR.

En el ámbito de la biotecnología, se están incorporando sensores biométricos al equipamiento del combatiente, lo que permite el monitoreo en tiempo real del estado físico y cognitivo del operador. Estas tecnologías, combinadas con interfaces avanzados y realidad aumentada, contribuyen a mejorar la conciencia situacional y la toma de decisiones bajo presión.

Las tecnologías de energía avanzada, como baterías de nueva generación, sistemas de propulsión eléctrica o armas de energía dirigida (láseres, microondas), permitirán desplegar plataformas ISR más sostenibles,

silenciosas y autónomas. Esto cobra especial relevancia en misiones prolongadas, entornos denegados.

Finalmente, la convergencia entre inteligencia artificial y computación cuántica abre nuevas posibilidades para el análisis de datos complejos, la simulación de escenarios y la gestión segura de comunicaciones. Estas capacidades permitirán conectar redes ISR distribuidas en todos los dominios (terrestre, marítimo, aéreo, espacial, cibernético y cognitivo), con mayor precisión, velocidad y resiliencia.

Estas tendencias no solo ampliarán las funciones tradicionales de la ISR, sino que contribuirán a consolidar un entorno más distribuido, robusto y adaptativo. Su adopción deberá realizarse bajo principios éticos, marcos normativos aliados y criterios de interoperabilidad que garanticen su eficacia operativa y su integración segura en entornos multinacionales.

7 Posibles mejoras en cada una de las fases del proceso JISR

Como ya se ha visto con anterioridad, el proceso JISR se organiza en torno a cinco fases conocidas como TCPED (Task, Collect, Process, Exploit, Disseminate). Cada una de ellas ha sido clásicamente abordada mediante procedimientos secuenciales y sistemas especializados. Sin embargo, la transformación digital y la introducción de tecnologías disruptivas están permitiendo avances concretos que podrían favorecer la eficacia de cada etapa.

A continuación, se describen estas mejoras con un enfoque basado en la aplicación de las tecnologías descritas previamente, de una manera realista y con base en el conocimiento disponible en GMV gracias al desarrollo de la suite de herramientas JISR SAPIIEM[8]. Estas herramientas se han probado con excelentes resultados en distintos ejercicios de la OTAN, como Unified Vision, Steadfast Cobalt, MAJEX, OPTIMAX, Trident Juncture, entre otros.

7.1 Tasking – *Planificación y asignación de recursos*

La fase de asignación de tareas y gestión de necesidades de inteligencia ha sido tradicionalmente un proceso lento, manual y muy dependiente de la experiencia del operador. Sin embargo, la integración progresiva de inteligencia artificial está transformando esta etapa y permite automatizar tareas como la identificación de zonas o áreas de interés donde operaran los medios de obtención, la asignación óptima de medios ISR o la priorización de requerimientos en función de criterios operativos, disponibilidad y contexto.

[8] SAPIIEM, es la suite de productos JISR, compatibles con las iniciativas de interoperabilidad de la OTAN (STANAG) y la doctrina de la OTAN, desarrollada por GMV.

Ejercicios como el JFX[9] han demostrado que establecer dinámicas de trabajo más flexibles, apoyadas en herramientas como SAPIIEM, mejora significativamente la planificación y la trazabilidad de la obtención de la información. Interfaces adaptadas y asistentes inteligentes permitirán en el futuro realizar simulaciones de escenarios, identificar redundancias en los requerimientos o proponer alternativas de asignación según cambios en el entorno operativo.

7.2 Collection – *Obtención de información*

La fase de recogida de datos se beneficia directamente de la proliferación de sensores terrestres, navales, aéreos, espaciales y cibernéticos. El despliegue de UAV de última generación, sensores distribuidos y redes IoT permite una recolección de información más persistente, diversa y automatizada, adaptada a entornos operativos cada vez más complejos.

El uso de inteligencia artificial en esta fase permite programar dinámicamente sensores, redirigirlos ante eventos imprevistos o activar de forma autónoma plataformas de observación. Este tipo de automatización mejora la eficiencia del sistema y permite responder con mayor rapidez a nuevas necesidades de obtención.

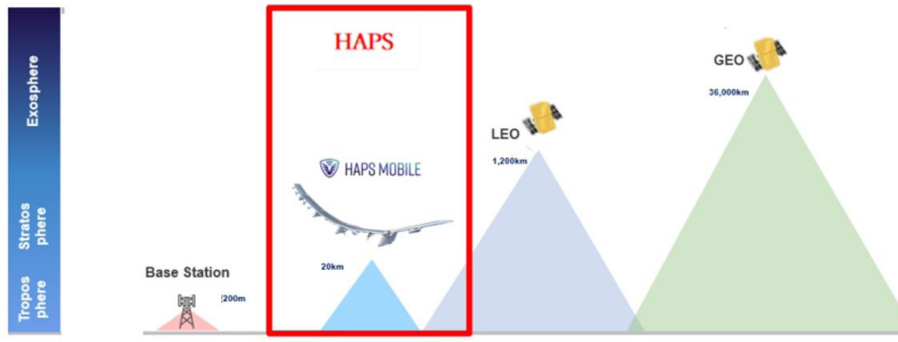

Figura 7. Altitudes operación HAPS. Fuente HAPS Alliance

En particular, esta lógica resulta especialmente útil en entornos urbanos densos, donde tecnologías como los micro-UAV desplegables a nivel táctico facilitarán la vigilancia, la protección de fuerzas y la recopilación de datos en tiempo real, incluso en condiciones adversas o degradadas.

[9] Joint Force Exercise (Ejercicio de la Fuerza Conjunta), un ejercicio militar nacional español organizado por el Estado Mayor Conjunto de las Fuerzas Armadas (EMACON). Su objetivo es adiestrar a la estructura operativa de las FAS en la planificación y conducción de operaciones conjuntas e integrar sistemas ISR, C2, etc. Su ejecución es anual.

7.3 Processing – *Tratamiento y clasificación de datos e información*

El procesamiento de datos es una fase crítica, donde se organiza y estructura la información recopilada. Gracias al uso de *edge computing*, muchas tareas de procesamiento pueden realizarse ahora en el propio sensor o en nodos cercanos, lo que reduce la latencia y mejora la resiliencia ante cortes de red.

Además, técnicas de reconocimiento de objetos mediante IA permiten catalogar de forma automática la información de sensores, imágenes satelitales o vídeos. Estas herramientas pueden detectar anomalías, etiquetar datos e incluso generar metadatos útiles para su explotación posterior.

7.4 Exploitation – *Análisis de los datos y la información*

La explotación de datos ha sido tradicionalmente una tarea intensiva en recursos humanos. En la actualidad, gracias al *big data*, al aprendizaje automático y a nuevas técnicas de análisis automatizado, es posible realizar explotaciones más rápidas de grandes volúmenes de datos, de modo que se detecten patrones ocultos y genera información que pueda servir a la elaboración de inteligencia en menor tiempo.

La inteligencia artificial ya permite realizar búsquedas inteligentes mediante lenguaje natural (NLP), elaborar resúmenes automáticos o incluso generar contenido directamente a partir de la información estructurada mediante sistemas de tipo RAG (*Retrieval-Augmented Generation*). Estas capacidades permiten al analista concentrarse en las tareas de validación, contraste y contextualización y deja a los algoritmos las funciones repetitivas de análisis primario.

El objetivo de esta fase sigue siendo el mismo: generar la información relevante, oportuna y adaptada al nivel de decisión, pero con un grado de automatización que acelere los procesos dentro de esta fase, mejore la trazabilidad y permita reaccionar con mayor agilidad ante escenarios en evolución.

7.5 Dissemination – *Difusión y uso de la información*

En esta fase, el objetivo es asegurar que la información y los datos lleguen al usuario adecuado, en el momento oportuno y en el formato más útil. Para lograrlo, es esencial contar con sistemas interoperables, redes seguras y una arquitectura basada en la filosofía del «dato único».

Herramientas como SAPIIEM permiten sincronizar los nodos ISR y garantizar la trazabilidad desde la necesidad hasta la difusión de la información. Al mismo tiempo, plataformas más recientes introducen productos

de inteligencia interactivos, adaptativos y reutilizables, que se ajustan dinámicamente al perfil del usuario y al contexto operativo.

La inteligencia artificial contribuye también en esta fase mediante funciones como la generación automática de resúmenes personalizados o la clasificación automática de productos según su propósito (planeamiento, *targeting*, operaciones). Estas capacidades ayudan a evitar la sobrecarga cognitiva del usuario y a asegurar que la información se entrega en condiciones óptimas para ser explotada.

7.6 Lecciones aprendidas y condiciones de éxito

Para aprovechar plenamente el potencial de las tecnologías emergentes aplicadas al proceso JISR, es fundamental combinar una estructura organizativa clara y flexible, personal, formado en herramientas ISR, procesos revisados y orientados a la automatización, y una cultura de interoperabilidad real entre niveles y dominios.

Ejercicios como el JFX-22, organizado por el Estado Mayor Conjunto (EMACON), han demostrado que estas condiciones no son solo teóricas. En ese contexto, se emplearon herramientas como SAPIIEM para gestionar el proceso IRM&CM y la explotación de la información. Los resultados evidenciaron una mejora sustancial en la trazabilidad, la coordinación entre niveles y la rapidez en la generación de productos útiles.

Asimismo, la suite ATENEA ha demostrado su potencial para integrar planeamiento, asignación y explotación en una única plataforma digital, aumenta la coherencia del proceso y facilita su adaptación a distintos escenarios. La formación anticipada de los operadores y la unificación de criterios doctrinales fueron elementos clave para su implementación eficaz durante los ejercicios.

Estas experiencias en ejercicios muestran que la transformación tecnológica del proceso JISR requiere tanto soluciones técnicas como cambios culturales y doctrinales, orientados a una explotación más eficaz de la información.

8 Interoperabilidad y filosofía del «dato único»

Uno de los desafíos principales del proceso JISR es asegurar que la información generada sea accesible, coherente y utilizable por todas las unidades y actores implicados en un entorno de operaciones conjuntas. En escenarios multidominio y en operaciones multinacionales, la interoperabilidad ha dejado de ser un ideal deseable para convertirse en una condición imprescindible.

Ningún sistema ISR opera hoy de forma aislada. La integración de capacidades nacionales, aliadas y comerciales requiere que sensores,

plataformas, sistemas de mando y herramientas de análisis compartan no solo datos, sino también formatos, protocolos y lenguajes comunes. Esto es especialmente crítico en el marco de operaciones OTAN o UE, donde el éxito depende de generar una imagen operativa común basada en inteligencia compartida y validada.

La interoperabilidad debe abordarse en tres niveles: técnico (*hardware*, *software* y conectividad), semántico (coherencia en la interpretación de datos) y organizativo (procesos y doctrina). La ausencia de interoperabilidad genera fragmentación, retrasos y pérdida de eficacia en la toma de decisiones.

En este contexto, la filosofía del dato único se convierte en un principio rector. Consiste en que un dato obtenido por un sensor, generado por un analista o producido por una IA, se registre una sola vez y quede disponible, de forma segura y trazable, para todos los usuarios autorizados. Este enfoque evita duplicidades, mejora la calidad del análisis y permite:

— Trazabilidad y control de versiones.

— Reducción de la carga sobre redes tácticas.

— Explotación cruzada mediante herramientas de IA.

— Coherencia y velocidad en el ciclo de decisión.

Su implementación exige arquitecturas distribuidas, redes seguras, normas técnicas comunes y una cultura organizacional basada en la necesidad de compartir, no solo en la necesidad de conocer.

La OTAN ha desarrollado estándares como el STANAG 4559, que regula el funcionamiento del *Coalition Shared Data* (CSD). Plataformas como INTEL-FS y BICES permiten compartir inteligencia de forma estructurada entre centros de análisis aliados.

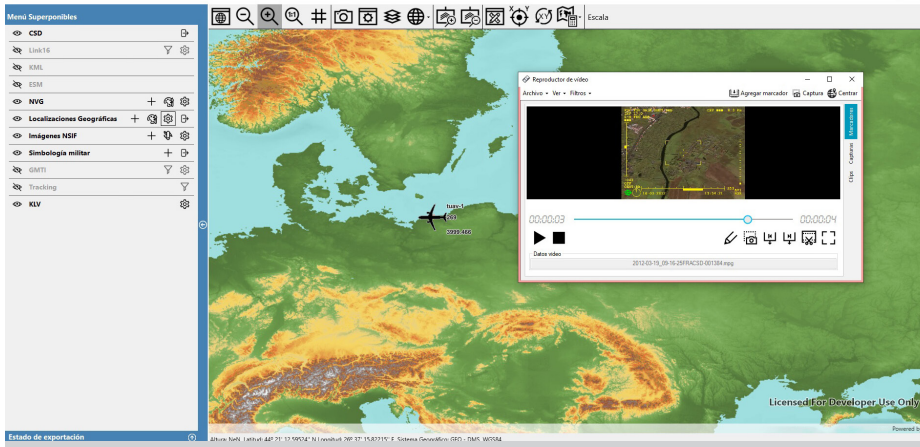

Figura 8. Sistema SEISMO de GMV

En el ámbito nacional, el sistema SAPIIEM ha demostrado su compatibilidad con estas estructuras internacionales, tanto en ejercicios conjuntos[10] como en operaciones reales. Estas infraestructuras permiten que el proceso JISR funcione de forma federada, de modo que aumente la eficacia colectiva y acelere la generación de inteligencia útil.

9 Innovación tecnológica como amenaza al proceso JISR

Hasta este punto, el capítulo ha expuesto las oportunidades que las tecnologías emergentes ofrecen para transformar el proceso JISR. Sin embargo, esa misma innovación tecnológica también genera nuevas vulnerabilidades que no pueden ser ignoradas. En muchos casos, las mismas herramientas que potencian la eficacia del sistema (IA, sensores inteligentes, automatización, computación en el borde) también amplían la superficie de exposición a riesgos operativos, cibernéticos o cognitivos.

En este apartado, se analizan dos de los aspectos más críticos en los que la innovación puede actuar como amenaza: la ciberseguridad del proceso JISR y las vulnerabilidades de la inteligencia artificial.

9,1 La importancia de la ciberseguridad en el Proceso JISR

La digitalización del proceso JISR ha multiplicado sus capacidades, pero también ha incrementado su exposición a amenazas cibernéticas. La incorporación de sensores distribuidos, redes de intercambio de información, plataformas diversas, herramientas de análisis automatizado y sistemas de mando y control interconectados ha convertido a los entornos ISR en un objetivo prioritario para actores hostiles. En este contexto, ya no se trata solo de proteger la infraestructura física, sino de asegurar la integridad, disponibilidad, trazabilidad y confidencialidad de la información a lo largo de todas las fases del ciclo.

El ecosistema JISR depende de una interconexión segura entre sensores, nodos de procesamiento, plataformas de explotación y usuarios finales. Cada uno de estos elementos puede convertirse en un vector de ataque. Por ejemplo, los sensores pueden ser objeto de suplantación o manipulación (*spoofing*), las redes pueden ser saturadas o intervenidas, los algoritmos pueden sufrir ataques mediante técnicas de *adversarial AI*[11] y los productos de inteligencia pueden ser interceptados o alterados durante su transmisión.

[10] Se ha mencionado previamente el JFX.

[11] *Science & Technology Trends 2023-2043*, volumen 2. Este documento describe el uso adversario de la inteligencia artificial y el aprendizaje automático como una colección de técnicas diseñadas para obstaculizar o engañar a los sistemas inteligentes, impactando sensores militares, sistemas de armas y sistemas de apoyo a la decisión.

Estas amenazas no son hipotéticas. En ejercicios y operaciones reales, se han identificado múltiples vectores de ataque: inserción de datos falsos, interceptación de flujos de información, denegación de servicio a plataformas ISR críticas o incluso alteraciones en la lógica de los sistemas de procesamiento automatizado. Todo ello pone de manifiesto que el entorno JISR debe ser activamente protegido frente a las ciberamenazas.

En contextos multinacionales, como los marcos OTAN o UE, el intercambio de información entre aliados exige especial atención a la seguridad de red, el cifrado, la autenticación y la trazabilidad. Un fallo en un solo nodo puede comprometer la seguridad de toda la red. Por ello, la interoperabilidad debe ir acompañada de garantías de ciberseguridad comunes, robustas y auditables.

La arquitectura de los procesos y sistemas JISR debe diseñarse desde el inicio bajo el principio de *security by design*[12] e integrar la ciberseguridad como parte estructural del sistema y no como un complemento posterior. Esto incluye controles de acceso, detección de intrusiones, auditoría de procesos, validación de datos y resiliencia ante fallos a lo largo de todo el ciclo.

Además, es fundamental reforzar la cultura de seguridad entre operadores, analistas y gestores del ciclo de inteligencia. El factor humano sigue siendo uno de los vectores de riesgo más relevantes, en especial, por errores involuntarios. La concienciación, la formación continua y los protocolos de buenas prácticas son elementos clave para mitigar estos riesgos.

Finalmente, el desarrollo de capacidades de ciberdefensa activa específicas para entornos JISR debe considerarse una línea de acción prioritaria. Esto incluye la protección dinámica de sensores y enlaces, la supervisión constante de plataformas de procesamiento y explotación y la capacidad de recuperación rápida ante incidentes. Todo ello requiere una estrecha colaboración entre responsables de ciberdefensa, desarrolladores de sistemas y analistas de inteligencia.

9.2 Sesgos y vulnerabilidades de la inteligencia artificial en el proceso JISR

El despliegue de tecnologías de inteligencia artificial en el proceso JISR promete una mejora sustancial en la velocidad, precisión y adaptabilidad de las operaciones. No obstante, esta transformación conlleva también nuevos riesgos operativos que deben ser considerados con rigor. Entre los más relevantes, destacan los sesgos algorítmicos, la opacidad de los modelos de decisión y la vulnerabilidad frente a manipulaciones o ataques cognitivos.

Uno de los desafíos clave es el sesgo de entrenamiento. Los modelos de IA utilizados para la clasificación de imágenes, la detección de amenazas o el análisis de comportamiento se entrenan con conjuntos de datos

[12] *Science & Technology Trends 2023-2043* – OTAN

previamente definidos. Si estos datos están incompletos, mal etiquetados o reflejan prejuicios históricos o contextuales, el sistema puede reproducir o amplificar errores, lo que genera falsos positivos o falsos negativos críticos en entornos operativos. Esto podría implicar decisiones erróneas, priorizaciones defectuosas o incluso consecuencias no deseadas.

Además, muchos modelos de aprendizaje profundo funcionan como «cajas negras», difíciles de auditar o explicar. Esta falta de transparencia afecta de forma directa a la confianza del mando en los sistemas automatizados, especialmente cuando las decisiones deben tomarse con rapidez y bajo alta presión.

Otro punto crítico es la vulnerabilidad a ataques adversarios. Existen técnicas (*adversarial AI*) capaces de manipular los resultados de un sistema de IA las cuales modifican mínimamente los datos de entrada (imágenes, señales, texto). Estas técnicas podrían utilizarse para confundir algoritmos y generar errores en la fase de explotación del proceso JISR. Este riesgo es, en especial, relevante en conflictos híbridos, donde actores hostiles pueden contar con capacidades cibernéticas sofisticadas.

La integración de IA en arquitecturas distribuidas, como *edge computing* o plataformas autónomas, amplía la superficie de exposición del sistema JISR a ciberataques o fallos sistémicos. La proliferación de sensores inteligentes y la automatización de procesos hacen que cualquier error no detectado en la IA pueda replicarse y escalar rápido en toda la red.

La inteligencia artificial puede ser un multiplicador de capacidades sin precedentes en el entorno JISR, pero solo si se gestiona de forma responsable. Frente a los riesgos mencionados, se hace imprescindible desarrollar e implementar soluciones de IA bajo principios de seguridad, explicabilidad y gobernanza robusta, de modo que se incorporen entre otras medidas como las siguientes:

- Validación continua de los datos de entrenamiento.
- Evaluación de sesgos y explicabilidad de modelos.
- Simulación de escenarios para robustecer los sistemas.
- Supervisión humana en decisiones críticas (*Human-in-the-loop* / *Human-on-the-loop*).
- Gobernanza de algoritmos bajo marcos normativos OTAN/UE.

10 Conclusión

Las innovaciones que derivan de las tecnologías emergentes y disruptivas, identificadas como prioritarias por la OTAN y la Unión Europea, están redefiniendo de forma transversal las capacidades militares, los ciclos de inteligencia y los procesos de toma de decisiones. Sensores inteligentes,

plataformas no tripuladas, *big data*, computación cuántica, materiales avanzados o tecnologías espaciales forman ya parte de un ecosistema ISR cada vez más interconectado, automatizado y distribuido.

Esta revolución tecnológica no afecta solo al plano técnico, sino también al doctrinal y organizativo. Las arquitecturas ISR deben adaptarse a un entorno en el que la información es abundante, diversa y generada desde múltiples fuentes, muchas de ellas fuera del ámbito militar tradicional. En este escenario, el proceso JISR se convierte en una capacidad continua, horizontal y multidominio, que debe ser capaz de operar en tiempo real y de integrar datos útiles desde el nivel táctico al estratégico.

Dentro de este conjunto, la inteligencia artificial se ha consolidado como el motor de cambio más inmediato, innovador y transformador. Su aplicación a lo largo de las fases del proceso TCPED permite automatizar la asignación de medios, elaborar planes dinámicos, anticipar amenazas, procesar grandes volúmenes de datos y proporcionar información de manera más rápida. La inteligencia artificial no sustituye al factor humano: lo ha de potenciar, liberándolo de tareas repetitivas y permitiéndole su enfoque en el análisis crítico, la validación y la toma de decisiones.

Esta transformación alcanza también a las plataformas, que se convierten además de sensores ISR avanzados, en elementos capaces de recolectar e incluso procesar información de manera previa en tiempo real. Su integración con sistemas de ciberdefensa, *targeting* o guerra electrónica refuerza la coherencia operativa y la eficacia en entornos complejos.

En este sentido, la arquitectura ISR del futuro deberá ser:

— Flexible, para adaptarse a escenarios cambiantes;

— interconectada, para integrar sensores y dominios;

— automatizada, para acelerar el ciclo de decisión;

— escalable y segura, para gestionar el volumen de datos y proteger su integridad.

Además, este ecosistema más conectado, automatizado e inteligente debe sustentarse en una estrategia de ciberseguridad transversal y adaptativa, que garantice la continuidad operativa y la protección de la ventaja informativa frente a amenazas sofisticadas y persistentes.

En definitiva, innovar en ISR es anticiparse, adaptarse y decidir con ventaja. El éxito no dependerá de quién obtenga más información, sino de quién sepa protegerla, compartirla, explotarla y convertirla en decisiones oportunas y acertadas más rápido y con mayor fiabilidad.

La transformación constante del proceso JISR no es solo un desafío tecnológico, es una necesidad estratégica ineludible.

Bibliografía

España. (2021). Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021. *Boletín Oficial del Estado*. 31 de diciembre, núm. 314, pp. 167795-167830.

European Defence Agency. (2023a). *Enhancing EU military capabilities beyond 2040. Main findings from the 2023 Long-Term Assessment of the Capability Development Plan*. European Defence Agency (EDA). DOI: 10.2836/360180.

European Defence Agency. (2023b). *The 2023 EU Capability Development Priorities*. European Defence Agency (EDA).

Gómez Gómez, Juan de Dios. (2025). ESFAS. La inteligencia de comunicaciones contra el crimen organizado: un arma fundamental ante la amenaza híbrida. *Noticia IEEE 09/2025*. [Consulta 24 marzo 2025).

Gómez González, Á. S. (2021). Tendencias de evolución de la inteligencia militar. *Documento de Opinión IEEE 35/2021*. [Consulta: 5 febrero 2024).

Gordon B., D. Jr. (2023).The future of NATO C4ISR after Madrid summit. Assessment and Recommendations. NCI Agency. ISBN-13 978-1-61977-273-1.

Kerth, C., Klotz, P. y Essendorfer. (2019). *A new approach for information dissemination in distributed JISR coalitions*. Proc. SPIE 11015, Open architecture / Open Business Model Net-Centric Systems and Defense Transformations 2019. Fraunhofer IOSB. 110150N. [Consulta: 10 marzo 2025]. Disponible en: https://publica-rest.fraunhofer.de/server/api/core/bitstreams/e23811eb-b3a6-432f-8250-64cc94c02b99/content

Kerth, C.; Klotz, P. y Essendorfer, B. (2020). *A new approach for information dissemination in distributed JISR coalitions*. Karlsruhe, Fraunhofer IOSB.

Ministry of Defence (UK). (2023). *Joint Doctrine Note 1/23 Intelligence, Surveillance and Reconnaissance*. Gov.uk. [Consulta: 2025]. Disponible en: https://www.gov.uk/government/publications/intelligence-surveillance-and-reconnaissance-jdn-123

NATO. (2022) *Strategic Concept for the Alliance at the Madrid Summit on 29 June 2022*. NATO.

NATO Science & Technology Organisation. (2023). *Science & Technology Trends 2023-2043. Across the Physical, Biological, and Information Domains*. Volume 1. NATO Science & Technology Organisation.

Pérez-Breva, L. (2018). Innovar: un manifiesto de acción. Deusto. ISBN 978-84-234-2933-2.

Sánchez Sánchez, J. L. (2025) Inteligencia artificial en apoyo a la inteligencia militar. Eje fundamental del éxito o fracaso en la competición estratégica entre grandes potencias. *Documento de Análisis IEEE 09/2025*. Ministerio de Defensa, Instituo Español de Estudios Estratégicos.