Capítulo noveno

La innovación tecnológica como elemento transformador del proceso de inteligencia

Francisco Manuel Vaca Ortega

Resumen

Este trabajo se enmarca en el contexto de una sociedad e instituciones hiperconectadas con el mundo y con capacidad de acceso a datos de todo tipo. En este panorama, tecnologías disruptivas como la IA, hacen que los gobiernos y sus Fuerzas Armadas puedan acelerar su toma de decisiones, pudiendo suponer un cambio de paradigma en la forma de producir inteligencia. El principal propósito del trabajo es estudiar si este cambio de paradigma se va a producir, sobre todo, en lo que respecta en cambios a la doctrina y organización de la inteligencia tal y como la conocemos. Para ello, la metodología empleada consistió en un análisis documental, apoyado en la realización de encuestas a personal de distintos ámbitos, entrevistas y otras herramientas de análisis cuantitativo. Los principales hallazgos encontrados fueron la tendencia continuista, pero acelerada de los procesos actuales de inteligencia, teniendo como principal implicación la necesidad de continuar y mejorar la actual formación de los analistas de inteligencia en tecnologías disruptivas y en seguridad de la información, tanto para para reducir la incertidumbre sobre las herramientas (la caja negra), como para emplearlas. Finalmente, las conclusiones resaltan que aún es pronto para ver un cambio profundo en la forma de producir

inteligencia y que el elemento humano continuara siendo un valor fundamental de la organización, sin embargo, se deja constancia de la necesidad de invertir, tanto en el plano económico como en el formativo, para continuar siendo relevante en el aspecto tecnológico y no poner a la Seguridad Nacional en Riesgo.

Palabras clave

Inteligencia Artificial, Nube, Ciberseguridad, Comunicaciones, Análisis, toma de decisiones y Gestión del dato.

Technological innovation as a transformative element of the intelligence process

Abstract

This work is framed in the context of a society and institutions that are hyperconnected to the world and have access to data of all kinds. In this scenario, disruptive technologies such as AI, allow governments and their Armed Forces to accelerate their decision-making process, which could lead to a paradigm shift in the way intelligence is produced. The main purpose of this work is to study whether this change in thinking will take place, especially regarding changes in the doctrine and organization of intelligence as we know it. To this end, the methodology employed consisted of a documentary analysis, supported by surveys of personnel from different fields and ranks, interviews with experts and other quantitative analysis tools. The main findings were the continuing but accelerating trend of the current intelligence processes, with the main implication being the need to continue and improve the current training of intelligence analysts in disruptive technologies and information security, both to reduce the uncertainty about the tools (the black box) and to use them. Finally, the conclusions highlight that it is still early to see a deep change in the way of producing intelligence and that the human element will continue to be a fundamental value of the organization, however, the need to invest both economically and in training remain as a necessity with the aim to be technologically relevant and not to put the National Security in Danger.

Key words

Artificial Intelligence, Cloud, Cybersecurity, Communications, Analytics, Decision Making and Data Management.

1. Introducción

El avance de las tecnologías asociadas con el Internet de las Cosas (IoT), el procesamiento de datos y, especialmente, la inteligencia artificial (IA), ha generado un amplio abanico de oportunidades en todos los ámbitos de la sociedad, en el que se incluye el militar. Sin embargo, también presentan desafíos significativos: ciberseguridad, gestión de recursos, falta de personal cualificado, etc. (Departamento de Seguridad Nacional, 2019).

Este artículo trata de llamar la atención sobre la aplicación de las innovaciones tecnológicas en el campo de la inteligencia militar. Asumiendo que el conocimiento sobre estas innovaciones, su aplicación práctica y sus riesgos asociados serán la clave para potenciarla (Ministerio de Defensa, 2024). Disponer de un ciclo de decisión más rápido, resiliente y eficaz será clave para acelerar la identificación de amenazas y su neutralización, contribuyendo al mantenimiento de la Seguridad Nacional.

Por todo ello, cabría preguntarse si realmente resulta imprescindible invertir más en estas tecnologías, el impacto sobre los procesos actuales de inteligencia, la incidencia en la seguridad digital e incluso si somos capaces de aceptar estos cambios acelerados, debido a la diferencia generacional en la organización.

Así, el artículo abordará los principales documentos estratégicos de España y sus aliados sobre cuestiones tecnológicas, presentará aquellas tecnologías relacionadas con los procesos de inteligencia y su aceptación por la organización, tratará el impacto en la ciberseguridad de manera general y, expondrá, someramente, los propios procesos de inteligencia, de forma que el lector pueda unificarlo todo.

Finalmente, el artículo tratará de responder si, ante el avance inexorable hacia la transformación digital, será necesario un cambio en el modelo actual de producir inteligencia, en la organización o en su doctrina.

2. Estrategias de innovación tecnológica. España, aliados y otros

En este capítulo se tratarán las visiones estratégicas de España, sus aliados y otros países[1], para observar que tendencia e importancia se arroja sobre las nuevas innovaciones tecnológicas, con

[1] En el caso de las organizaciones a las que pertenecen España y otros países, se hará una descripción somera de los principales documentos consultados, con objeto de obtener la visión sobre su idea de la Transformación Digital.

énfasis en el área de inteligencia. Con este punto de vista, se podrá intuir la presente y futura necesidad de inversión, principalmente por la necesidad de mantenerse relevantes y con cierta «independencia tecnológica», situándonos por delante de competidores y adversarios como Rusia y China (NATO, 2022).

2.1. Estrategia española

En el ámbito nacional, la Estrategia de Seguridad Nacional del 2021 (ESN 2021) expone la necesidad de invertir en tecnología, concienciación en ciberseguridad y retención del talento. Por otro lado, la Estrategia de Tecnología e Innovación para la Defensa (ETID) 2020 destaca la necesidad de cooperación con industria, siendo clave tanto para desarrollar nuevas capacidades, como para la «independencia tecnológica». Por último, el documento Entorno Operativo 2035 (EO 2035) marca los posibles escenarios de actuación (inciertos) en un futuro próximo, reseñando la importancia de disponer tanto de capacidades tecnológicas avanzadas, como de personal cualificado para emplearlas.

2.1.1. ESN 2021

La ESN 2021 destaca la transformación digital (TD) como un proceso imparable que ofrece innumerables oportunidades, pero también desafíos, como una palanca de cambio para continuar el avance de la sociedad, siendo el *dato*, un activo estratégico de primer orden.

Esta TD afecta directamente a la seguridad nacional, con aspectos relevantes y de aplicación directa en las FAS. Por un lado, tendremos elementos tecnológicos digitales y, por otro, acciones facilitadoras, como la colaboración público-privada y la concienciación de la sociedad. Estas últimas afectarán a los factores financieros e intelectuales directamente y sobre los que habrá que poner especial atención al estar relacionados con la operación y mantenimiento de los sistemas, mencionándose, especialmente las siguientes:

– Inteligencia artificial (IA)

La ESN menciona la IA como una función importante para la Seguridad Nacional, sirviendo para el tratamiento eficaz de grandes volúmenes de datos y siendo pilar fundamental de sistemas de alerta temprana, como apoyo para la toma de decisiones y para lucha contra las estrategias híbridas o conflictos en la «zona

gris», facilitando la detección de acciones de desinformación, contrainteligencia o facilitando la ciberdefensa entre otras.

No obstante, también se hace alusión a principios éticos de uso, por lo que será necesario entender el mecanismo por el cual la IA basa sus decisiones, lo que implicará en un control positivo sobre su proceso de aprendizaje, aunque tratando de no limitar sus capacidades (Martínez Millán, 2023).

– Computación en la nube, 5G e Internet de las cosas

Aunque tratados de forma generalista en el documento, la computación en la nube, el Internet de las cosas (IoT) y la adopción del 5G son fundamentales para el almacenamiento, acceso, tratamiento y compartición de datos de forma segura, todo ello con una relativa baja latencia. No obstante, también se reseña cierto aumento de vulnerabilidades en el sistema, debido a este aumento masivo en la conectividad.

– Ciberdefensa

En lo referido a la ciberdefensa, expuesto en el documento e inferido del párrafo anterior, será necesario tomar medidas para prevenir el incremento de acciones hostiles o malintencionadas en el ámbito del ciberespacio, disponiendo de los recursos financieros, humanos, organizativos y de infraestructuras necesarios.

– Tecnología cuántica

La tecnología cuántica se menciona como una tecnología en ciernes, en un intervalo de aplicación del medio-largo plazo y de usos difíciles de prever, pero que se espera que mejoren en lo concerniente al establecimiento de comunicaciones seguras o en lo referente a descifrado/cifrado de datos, aumentando la seguridad en las comunicaciones.

– Colaboración público-privada

La colaboración público-privada se torna esencial como catalizador en el proceso de alcanzar una TD que sea beneficiosa para la Seguridad Nacional, puesto que con ella será más fácil alcanzar las capacidades militares necesarias basadas en tecnologías avanzadas como las citadas en los puntos anteriores, consiguiendo, además, apoyar al sector industrial y tecnológico.

– Concienciación en Seguridad Nacional

La ESN 2021 reconoce la importancia de la concienciación en lo que refiere a Defensa Nacional como objeto que los ciudadanos

dispongan de los conocimientos y habilidades necesarios para afrontar con éxito la TD. La formación y concienciación en ciberseguridad, riesgos/amenazas emergentes y en las propias innovaciones tecnológicas, se tornará fundamental para aumentar la resiliencia de la sociedad española en general. ETID 2020.

2.1.2. EO 2035 y ETID 2020

Ambos documentos abordan las necesidades de investigación, desarrollo e innovación (I+D+I{XE "I+D+I Investigación, Desarrollo e Innovación"}) para los próximos años, de forma coherente con las necesidades militares a largo plazo establecidas por JEMAD.

En los documentos se deja patente que nuestras FAS se moverán en entornos volátiles, inciertos, complejos y ambiguos (VUCA), lo que demanda una actualización constante de las necesidades de defensa, así como el suministro del mejor material disponible en términos de avances tecnológicos.

Tanto el EO 2035 como la ETID 2020 se hacen eco de la posibilidad, ventajas y oportunidades que ofrecen las innovaciones tecnológicas en el campo de la defensa y de la forma en que podrían mantener con cierta ventaja operacional a nuestras FAS con respecto a nuestro entorno.

En lo que respecta al aspecto formativo del personal, se establece que será necesario impulsar tecnologías que empleen simulación, elementos *hápticos*, virtualización, salas multiusuario, etc. Todo ello con la intención de una mejora del combatiente, del que se cita, que aún será el eje central de las operaciones en las que participen nuestras FAS. En el mismo sentido de mejora de la formación, el EO 2035 establece la necesidad de potenciar el «liderazgo, la iniciativa y el talento» (CESEDEN, 2022: 108), como instrumento clave en la acción coordinada de las FAS, buscando una mejora en la gestión del talento.

De los combatientes, se reseña que se deberá mejorar con todo tipo de elementos y sensores que, junto a los proporcionados por otros sistemas tecnológicos, dotarán a la Fuerza Militar de una gran cantidad de información, que, analizada de la forma correcta, otorgarán al comandante una conciencia situacional adecuada, con posibilidad de acelerar y mejorar el ciclo de decisión.

Se hace una especial mención a sistemas capaces de gestionar grandes volúmenes de datos, que puedan fusionar inteligencia y

que ofrezcan resultados similares a los del razonamiento cognitivo de un ser humano, con objeto de poder llevar a cabo el análisis de inteligencia de todas las fuentes de información mencionadas con anterioridad.

Independientemente de la mejora cognitiva que supone el disponer de un gran volumen de datos y de sistemas capaces de analizarlos, los documentos también resaltan la necesidad de disponer de redes de comunicaciones capaces de transmitirlos, por ello resalta la importancia de las comunicaciones de amplio espectro 5G y de la necesidad de invertir en ellas.

Estas redes, se enfocarían a la computación en forma de nube (*combat cloud*)[2] que tratarían de que las unidades militares fueran capaces de disponer de la información en todo tiempo y casi cualquier circunstancia, por lo que se destacan que será importante que tengan la flexibilidad, disponibilidad y resiliencia adecuadas.

Por otro lado, y relacionado con el párrafo anterior, estos documentos mencionan las amenazas y los retos derivados de la adopción de todas las innovaciones anteriores, entre lo que se resalta la ciberseguridad/ciberdefensa, con objeto de anular acciones maliciosas que impidan la libertad de acción y la continuidad de las operaciones propias.

En lo que respecta al ámbito presupuestario se resalta que deberemos alcanzar una estabilidad y flexibilidad presupuestaria que permita la adquisición o modernización para alcanzar los requisitos de dotación de nuestras FAS, así como los compromisos alcanzados con nuestros aliados.

2.2. Visión en nuestras organizaciones. La OTAN y UE

> «Promoveremos la innovación y aumentaremos nuestras inversiones en tecnologías emergentes y disruptivas para conservar nuestra interoperabilidad y ventaja militar» (NATO, 2022: 7).

En el plano aliado, tanto la Unión Europea (UE) en su «Brújula Estratégica» (Union Europea, 2022) como la Organización del

[2] «Red interconectada para el intercambio de datos e información dentro del espacio de batalla, donde cada usuario o plataforma aportan y reciben información esencial de forma transparente, que puede ser utilizada en toda la gama de operaciones militares» (CESEDEN, 2022).

Tratado del Atlántico Norte (OTAN) en la Cumbre de Madrid (NATO, 2022), promueven la innovación e inversiones en tecnologías emergentes y disruptivas para conservar la interoperabilidad y la ventaja militar. En ambas estrategias se tiende a mayores inversiones financieras, sobre todo, en coordinación con la industria público-privada. Además, ambas organizaciones destacan como áreas de interés, la Inteligencia Artificial, la computación en la nube, ciberdefensa/ciberseguridad (NATO, 2023d) y, sobre todo, la gestión del dato, el cual se enmarca como activo fundamental (NATO, 2023a).

Con estas estrategias, tanto la UE como la OTAN, demuestran su compromiso con la transformación digital, tomándola como fundamental para su futuro, mejorando su resiliencia, su capacidad de defensa y su competitividad en un entorno global cada vez más digitalizado y más *VUCA*. (Morales Trueba, 2023).

2.3. Otras visiones

El avance tecnológico en los países del entorno impacta directamente en la competitividad de España y de las organizaciones nacionales. Estar al tanto de sus tendencias permite anticiparse, identificar oportunidades y desafíos y adoptar estrategias de inversión e innovación.

Se destacan como amenazas y desafíos, especialmente los relacionados con Rusia y China. (NATO, 2022). El desarrollo de innovaciones tecnológicas duales y disruptivas en estos países tiene implicaciones significativas en el ámbito militar y geopolítico. Estos países son actores clave en el escenario global, por lo que comprender sus estrategias es fundamental para la toma de decisiones en nuestras organizaciones y en nuestro propio nivel.

Asimismo, el conocimiento de las tendencias tecnológicas en el entorno permite identificar posibles socios para la cooperación en I+D y establecer alianzas estratégicas, destacando a Estados Unidos como líder en innovación en IA y tecnología militar de sistemas avanzados, (NATO, 2023c), aunque seguida, no muy de lejos, de países como China.

Por último, se reseñará la tendencia de Israel, quien también se destaca en el campo de la IA, uso de drones[3] y empleo de apli-

[3] En este artículo se empleará el termino *dron*, independientemente si se trata de un vehículo no tripulado o tripulado remotamente, ya sea naval, terrestre o aéreo.

caciones militares con enfoque en ciberseguridad y gestión de datos. (De Spiegeleire *et al*., 2017).

2.3.1. EE. UU.

En la estrategia de Estados Unidos se resalta la importancia de la toma de decisiones, informada y oportuna, para defender el país, disuadir la agresión y prevalecer en los conflictos. (Department of Defense, 2023).

La estrategia enfatiza el enfoque integrado, priorizando velocidad, agilidad, aprendizaje y responsabilidad. Destacando, al igual que las estrategias europeas y de la OTAN, que el éxito no puede lograrse solo, sino que debe buscarse junto con la colaboración de empresas tecnológicas.

La estrategia también establece una jerarquía de necesidades basada en la calidad de los datos, la gestión de su gobernanza, el análisis y las métricas, para finalmente disponer de una IA de uso responsable y ético.

Durante una rueda de prensa, el 2 de noviembre de 2023, la subsecretaria de Defensa Kathleen Hicks, hablaba sobre la dirección de la estrategia de adopción de IA y que representa la importancia e interés que para EE. UU. supone la adopción de las innovaciones digitales (Underwood, 2023):

> «Este es un tema que nos preocupa mucho en el Departamento de Defensa, […] la IA no solo está en la mente de muchos estadounidenses hoy en día, sino que es una parte clave del enfoque global de la innovación centrado en el combatiente que el Secretario [Lloyd] Austin y yo hemos estado impulsando desde el primer día».

2.3.2. Israel

La IA desempeña un papel fundamental en la seguridad nacional de Israel, donde se considera una tecnología estratégica. El término IA en Israel se considera sinónimo de la cuarta revolución industrial (4IR{XE "4IR Cuarta revolución industrial"}) y abarca otras innovaciones tecnológicas como la gestión de datos, el IoT, la automatización, la robótica y los *drones* entre otras. (Antebi, 2021).

Esta estrategia busca agilizar la identificación de objetivos y la toma de decisiones, lo que permite respuestas más rápidas y

precisas, tratando de crear una imagen operativa común para las Fuerzas de Defensa de Israel (FDI{XE "FDI Fuerzas de Defensa de Israel"}) a partir de datos recopilados de diversas plataformas y fusionados con IA.

De nuevo, la colaboración privada resulta fundamental, pero con un valor añadido. Debido al sistema de servicio militar en Israel, la mayoría de los científicos, ingenieros y ejecutivos de las empresas tecnológicas son veteranos de las FDI, por lo que las necesidades de sus FF. AA. les son familiares.

De esta forma, desde el Centro de Transformación Digital de las FDI, se establecen los hitos a alcanzar.

Disponer de infraestructuras físicas por todo Israel para poder proveer de redes de alta velocidad y un sistema de computación en nube.

Establecimiento de un *Data Lake*[4]. Dos arquitecturas: una general y otra local, de mayor velocidad. La última facilitaría el intercambio de información entre las unidades de primera línea, pero continuaría conectada a la general como respaldo.

Factoría de datos: el *core* de la estrategia. Cada servicio de las FDI generaría su propia factoría, mediante procesos de relación y retroalimentación Humanos-Maquina colaborativos.

Finalmente se llegaría a la superioridad informativa, con la interconexión.

Es interesante que se valore como una necesidad el cultivar y retener el talento, el mantenimiento de las infraestructuras y la voluntad emprendedora, todo ello por considerar que únicamente se encuentran en la *punta del iceberg* de este nuevo desarrollo tecnológico (Dagan, 2022).

2.3.3. China

El país asiático está enfocado en alcanzar la primacía tecnológica, reconociendo que las tecnologías emergentes y disruptivas ofrecen tanto oportunidades como riesgos, poniendo de manifiesto,

[4] Repositorio centralizado que permite almacenar, compartir, gobernar y descubrir grandes cantidades de datos estructurados y no estructurados de una organización a cualquier escala. A diferencia de un almacén de datos, puede almacenar datos sin procesar y no requiere un esquema definido para almacenar dato (Fernandez, 2023).

desde el punto de vista de uno de los competidores de la OTAN, su importancia estratégica (NATO, 2022).

China se ha convertido en el segundo mayor actor en el campo de IA tras EE. UU. Sin embargo, existe un incremento, en términos de investigación citada, en el campo del aprendizaje automático, lo que explicaría su interés por avanzar en este asunto (NATO, 2023c).

En este sentido, teniendo en cuenta los principios éticos adoptado por las sociedades occidentales con respecto al empleo responsable de la IA, resulta preocupante la intención de China de estar dispuesta a renunciar a un *control humano significativo* para lograr una velocidad cognitiva cada vez mayor en las decisiones militares (De Spiegeleire *et al*., 2017).

Por último, y con objeto de promover su influencia a través de sus tecnologías digitales, trata de explotar la colaboración con sus socios africanos a través de la denominada Ruta de la Seda Digital. Esta capacidad de influencia le permitiría participar activamente en la gobernanza digital mundial, lo que supondría cierto riesgo por su creciente influencia en el ámbito *ciber* (Rühlig, 2023).

2.3.4. Rusia

Para Rusia, se considera crucial estar a la vanguardia en innovaciones tecnológicas militares, ya que le permitiría mantener su capacidad defensiva y ofensiva en un entorno geopolítico cambiante. Para ello, hace uso, entre otros, de la *Technopolis Militar Era*[5], un centro de investigación, desarrollo y aceleración de tecnologías creado por el Kremlin para suplir la carencia de científicos (Victoria, 2018).

En este sentido, según el Ministerio de Defensa de la Federación Rusa, se están llevando a cabo investigaciones y discusiones sobre la robótica, la IA y otras tecnologías en foros y eventos especializados como el *ARMY-2023*.

En cualquier caso, la OTAN establece que la Federación Rusa es la mayor y más directa amenaza para la seguridad de los aliados en el área euro atlántica. En esta situación, es un hecho que Rusia tiene especial interés en su modernización, en su capaci-

[5] Centro de innovación militar en Rusia que se enfoca en el desarrollo y análisis de tecnologías avanzadas, incluida la inteligencia artificial (IA), para su aplicación en el ámbito militar.

dad balística nuclear y convencional hipersónica, así como en la explotación de tecnologías disruptivas duales (NATO, 2022).

3. Innovaciones tecnológicas aplicadas a la inteligencia

«La tecnología debe tener corazón humano».

Teniente general José María Millán. DICESTIC

Es necesario tener en cuenta que, en el actual panorama tecnológico, cualquier operación tendrá como característica común la saturación de datos. Ante esta situación, una de las tecnologías clave será aquella que permita la gestión masiva de datos, por lo que la capacidad de recopilar, almacenar y analizar grandes volúmenes de datos es una necesidad apremiante (Watling, 2023).

En estos ambientes, será necesario contar con algún apoyo tecnológico para facilitar a los analistas y decisores el manejo de la información, mejorando su comprensión y puesta a disposición del consumidor que la necesite. Este apoyo tecnológico podría venir dado por una IA ya que permitiría, además de mejorar la gestión de cantidades ingentes de datos, la automatización de procesos repetitivos, liberando a los analistas para tareas de mayor valor (Goldfarb y Lindsay, 2022).

Por otro lado, las tecnologías asociadas a la gestión masiva de datos no podrían funcionar sin una capa de comunicaciones de banda ancha, con sus respectivas consideraciones sobre seguridad de la información que se tratarán más adelante. Fundamentalmente, en el caso de España, se tratarán las tecnologías 5G y satelitales, las cuales serán fundamentales para la coordinación y la toma de decisiones en tiempo real o casi real (Garrido García, 2023).

Finalmente, es importante abordar la resistencia al cambio en las distintas organizaciones de las FAS, que surgirá fruto de la inseguridad producida ante esta TD. Solo a través de adecuados programas de capacitación y un liderazgo efectivo, se podrá disminuir esta resistencia, en línea con lo expuesto sobre inversión en formación.

3.1. Gestión del dato. *Data lake* y computación en la nube

«La OTAN posee un fantástico tesoro: una gran cantidad de datos generados por cada una de las 31 naciones de la Alian-

> za, y que cada una gestiona como si fueran de su propiedad» (Lavigne, 2024: 54).

La recolección efectiva de inteligencia requiere la integración de múltiples fuentes de datos, que pueden incluir imágenes satelitales, señales de inteligencia y datos de sensores en el campo de batalla, entre otros.

La interoperabilidad y compatibilidad entre estas diferentes fuentes de datos pueden ser complejos en un entorno operativo, de ahí que cobre importancia el concepto de *Data Lake*, donde se almacenan todo tipo de datos, sin importar si están estructurados o no. Mediante esta forma de almacenamiento se puede acceder a información de una forma más flexible y adaptable a las necesidades de los consumidores.

En este sentido, se reseñan los nodos CSD[6] empleados en la OTAN, nodos sincronizados entre sí, donde se replica la información de los metadatos y sus productos, permitiendo el acceso desde cualquier punto del teatro de operaciones, no solo al originador, sino a toda la coalición (GMV, 2024).

La computación en nube permite la interconexión de plataformas y sensores, hoy potenciada por el continuo aumento del Internet de las cosas militares (IoMT).

Aunque el uso más común de esta tecnología es la de lograr una completa conciencia situacional en todo tipo de situaciones operativas, presenta otro tipo de atributos, como la posibilidad de crear una red escalable, autorreparable, redundante y poco sensible a la degradación (Álvarez, 2022).

En esta red de sensores se incluyen todo tipo de sistemas, desde los personales hasta los específicos, incluyendo satélites, *drones* y cualquier otro sistema conectado. Teniendo en cuenta que, en un escenario de combate, la carestía de medios de obtención suele ser lo habitual, la capacidad de obtener información, de cualquier sistema desplegado, sea o no especifico de inteligencia, es un valor añadido que mejora el conocimiento del entorno y que disminuye la niebla de la guerra (Bellione, 2023).

Por último, la nube combate sería una especie de nexo de todos los niveles de conducción de las operaciones (estratégico, ope-

[6] CSD {XE "CSD Coalition Shared Data"}(*Coalition Shared Data*) Servidores que proporcionan difusión y almacenamiento persistente de productos de inteligencia en formatos estandarizados, con capacidad de *streaming* y que habilita los flujos de trabajo de los procesos de inteligencia.

racional y táctico), permitiendo tanto la conciencia situacional general como la explotación de datos para inteligencia de forma simultánea para la toma de decisiones en todos los niveles (Ministerio de Defensa, 2024).

3.2. Comunicaciones de banda ancha: 5G y satélites

La implementación de los conceptos expresados en apartado anterior requiere una infraestructura de comunicaciones robusta y confiable que pueda absorber los datos y las conexiones necesarias para conducir eficazmente una operación militar. Las características de esta capa de comunicaciones requerirán de una gran capacidad de banda ancha, baja latencia, alta supervivencia y confiabilidad en la transmisión.

3.2.1. Comunicaciones 5G

La tecnología 5G ofrece características que la hacen indispensable para favorecer la toma de decisiones de forma ágil (muy baja latencia), permitiendo la transmisión y recepción de datos en tiempo real o casi real. Además, la tecnología 5G ofrece una gran eficiencia energética, permitiendo una mayor autonomía y resistencia en operaciones.

La supervivencia es otra de las características de comunicación 5G, permitiendo su establecimiento de redes desplegables en entornos altamente degradados, permitiendo la comunicación y la coordinación entre las distintas unidades.

También permite la creación de burbujas 5G entre unidades que operen en teatros lejanos. Estas burbujas permiten a las unidades conectadas acceso y procesamiento de datos almacenados de forma local. Además, mediante sistemas de respaldo satelital sería posible la conexión y acceso a los sistemas basados en territorio nacional o retaguardia, lo que permitiría la actualización de la información, la capacidad de *reachback*[7] o la supervivencia en los peores casos del combate (Ejército de Tierra, 2018).

Sin embargo, ante esta nueva tecnología será necesario establecer las medidas de seguridad adecuadas, teniendo en cuenta

[7] La capacidad *reachback* se refiere a la capacidad de obtener productos, servicios, aplicaciones, fuerzas, equipos o materiales de organizaciones que no están desplegadas en el área de operaciones. (Ejército de Tierra, 2018).

que la mayor superficie de red implica una mayor superficie de exposición a los ataques. Se considera que aún se desconoce todavía mucho sobre los sistemas como para hablar de su *securización*, «aunque es cuestión de tiempo de poder desplegar redes 5G seguras» (De acuerdo con fuentes expertas del MCCE).

3.2.2. Satélites

Los satélites de comunicaciones se usan, principalmente, para permitir la transmisión de señales y, dependiendo de su órbita (la altura donde se coloquen) podrá emplearse en uno u otro cometido.

La orbita típica empleada por los satélites de comunicaciones españoles es la Órbita Geoestacionaria (GEO) (*circa 36 000 km altitud*{XE "GEO Órbita Geoestacionaria"}) que se caracteriza por disponer de una amplia cobertura constante y una vida útil mayor que otros de orbitas más bajas. En el plano negativo, estos satélites disponen de una velocidad de transmisión menor, así como *softwares* no demasiado actuales, debido a la necesidad de emplear tecnología robusta y probada.

En orbitas más bajas, denominadas *Low Earth Orbit* (LEO{XE "LEO Low Earth Orbit"}) (*circa 160-2000 km altitud*{XE "GEO Órbita Geoestacionaria"}), la velocidad y ancho de banda aumenta, sin embargo, son necesarias constelaciones de satélites para garantizar la cobertura de comunicaciones en un área de forma constante, puesto que estos satélites se encuentran en movimiento. Un ejemplo de estos satélites es la red Starlink, Iridium u Oneweb (Rodriguez Collantes y Sanchez Piedra, 2023).

Independientemente a los satélites empleados, resultan fundamentales para garantizar la transmisión de datos entre fuerzas proyectadas y desplegadas en teatros alejados y las organizaciones en TN o retaguardia, aun disponiendo de la tecnología 5G.

En lo que respecta a seguridad las comunicaciones satélites, son más vulnerables a nivel transporte, pero están protegidas a nivel información con cifradores, aunque, como se ha mencionado, la tecnología se *desactualiza* rápidamente en el caso de los satélites GEO, volviéndose vulnerable en un corto espacio de tiempo.

3.3. Empleo de herramientas de IA

A la hora de abordar las tecnologías basadas en IA, se debe tener en cuenta que no se trata de un asunto nuevo. Nos podríamos remitir

a los años treinta del siglo pasado, cuando Alan Turing estableció sus teoremas sobre lógica, siendo estos el primer acercamiento a la simulación de una neurona biológica (Baños Abril, s. f.).

Un poco después, en 1943, McCulloch y Pitts formularían matemáticamente el comportamiento de una neurona en lo que respecta a computación y procesamiento (Rodríguez Abril, s. f.).

Sin embargo, aquella tecnología cayó en el olvido hasta que a finales del siglo xx se recuperó de nuevo. Este abandono se produjo por la simple razón de no disponer de la tecnología suficiente hasta explotarla, no obstante, la potencia desarrollada en computación ha facilitado la incorporación de la IA en muchos ámbitos de nuestra vida.

A continuación, se presentarán algunos conceptos básicos sobre la IA a modo de entendimiento básico.

3.3.1. Inteligencia artificial (IA)

La IA es un campo general donde básicamente trata de que las máquinas lleven a cabo tareas (incluidas intelectuales) que normalmente serían llevadas a cabo por la inteligencia humana. Este campo general de IA incluye el aprendizaje automático tales como el *Machine Learning* y el *Deep Learning*, aunque también pudiera incluir otros procesos donde no se incluya nada relacionado con el aprendizaje (El-Hadi, 2022). En resumen, un proceso estaría basado en reglas y lógica, denominada simbólica (por

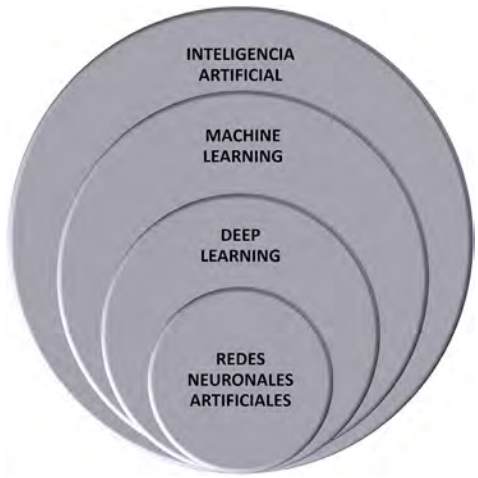

Figura 1. Profundidad de campo IA

ejemplo, controlar la temperatura en una habitación), y el otro en un aprendizaje a partir de datos.

3.3.2. Aprendizaje automático (*machine learning*)

Este es un subconjunto de la IA, centrado en el aprendizaje a través de multitud de datos. Los procedimientos usados en este tipo de aprendizaje son fundamentalmente cuatro: supervisado, semisupervisado, sin supervisión y con refuerzo. Este tipo de aprendizaje se caracteriza por la necesidad de disponer de datos estructurados y de emplear cierta intervención humana (Gómez, 2022). De esta forma, las máquinas aprenden a reconocer patrones, pudiendo realizar predicciones por sí mismas con el objeto de optimizar sistemas.

3.3.3. Aprendizaje profundo (*deep learning*)

El aprendizaje profundo es una subdivisión del ML, basado en las Redes Neuronales Artificiales (RNA), pero con multitud de capas (más de tres capas), permitiendo un mejor modelado y comprensión de los datos complejos (Gómez, 2022). A diferencia de del ML, se necesita una cantidad masiva de datos para entrenar a los modelos y un mayor tiempo de aprendizaje con objeto de evitar falsos positivos o sesgos[8]. Sin embargo, en su entrenamiento no precisa de datos estructurados, disponiendo este modelo de una mayor interpretación de los datos, acercándose a estándares humanos (Xin *et al*., 2018). El *Deep Learning* es responsable de muchos de los avances recientes en IA, como el reconocimiento de voz y de imágenes (Patel, s. f.).

3.3.4. Redes neuronales artificiales (RNA)

Las RNA son un modelo específico de algoritmo, inspirado en las redes neuronales biológicas, es decir, diseñado para actuar como un cerebro humano. Constituyen la base de los algoritmos del *Deep Learning* y su composición es variable, desde estructuras complejas a otras más simples basadas en distintas capas de nodos. El objetivo de este modelo es entrenar y aprender con el tiempo, empleando la experiencia de forma similar al cerebro humano (IBM, s. f.).

[8] Cuando el sistema de reconocimiento facial de Google se puso en marcha, aparecieron errores de identificación por no haber empleado, durante el entrenamiento, la cantidad de datos faciales suficientes (Reese, 2017).

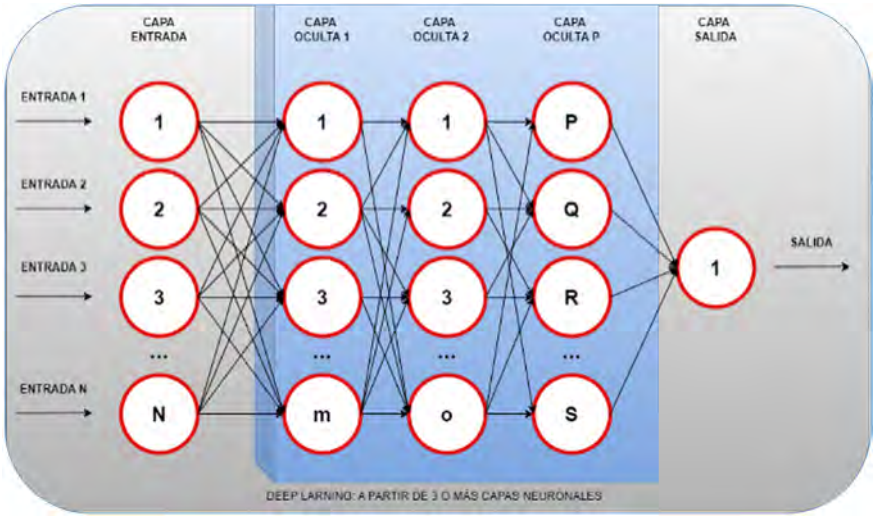

Figura 2. Árbol Inputs-Outputs, red nodal de aprendizaje de IA. A mayor cantidad de nodos, mayor cantidad de procesos internos y posibilidades de respuesta o aprendizaje. Fuente: elaboración propia basada en https://atriainnovation.com/

3.3.5. El ejemplo de la IA conversacional

En los últimos años, aplicaciones de conversación con IA han inundado varios ámbitos de mercado, facilitando la interacción hombre-máquina y la reducción de tareas en algunos colectivos.

Durante la conversación, el usuario usa *prompts*[9] como entradas para la IA, la cual, a través de distintos algoritmos, lo procesa y ofrece una respuesta adecuada. En este proceso, la herramienta puede llegar a comprender la solicitud y su trasfondo, compararla con los datos existentes y adaptarse al cliente.

A esta capacidad se le debe añadir la posibilidad de hacerlo en cualquier idioma, de poder arrojar como respuesta una imagen, audio, texto o incluso video (Chudleigh, 2023).

[9] Un *prompt* es la manera de interactuar entre humanos y una IA (generalmente, modelos de lenguaje), ya sea a través de imágenes, voz o texto para obtener una respuesta específica. En determinados casos, la creación de estos *inputs* se podría considerar un arte, llegándose a denominar *ingeniería de prompts*. Cuanto más claro, especifico y conciso sea el *prompt*, la respuesta de la IA esperada será más relevante y acertada (Hindlekar, 2024).

3.3.6. Empleo militar de la IA

Se podría afirmar que la disponibilidad actual de la tecnología en IA funciona como catalizador para explotar la multitud de datos que se disponen en el actual campo de batalla (Ministerio de Defensa, 2024).

Sin disponer de una IA, los analistas humanos serían incapaces de asumir tal cantidad de datos de forma eficiente, sobre todo, teniendo en cuenta que el cerebro humano necesita procesarlos de forma lineal, mientras que la máquina podrá realizarlo de forma no lineal y a mayor velocidad, gestionando un mayor número de datos y evitando la saturación cognitiva que podría derivar en errores.

Por otro lado, esta tecnología no aplica únicamente al procesado de datos, sino que también abarca a su explotación y difusión. Sin embargo, será necesario desarrollar algoritmos específicos para entrenar a las IA, habilitándolas para detectar, reconocer o identificar, automáticamente, los objetivos de interés que se definan (UK Ministry Of Defense, 2023).

Finalmente, y a modo de ejemplo, el uso de IA permitirá la integración de los datos recibidos por todos los sensores disponibles, que mediante el empleo del 5G y la nube de combate generaría una *Common Operational Picture* (COP{XE "COP Common Operational Picture"}) que abarcaría desde el nivel táctico al estratégico. Esta COP permitiría la toma de decisiones a una velocidad muy superior a la utilizada hoy en día, disponiendo, además, de la capacidad de *reachback,* si se necesitase, desde TN (Ministerio de Defensa, 2024).

3.4. Nuevas innovaciones y resistencia al cambio

«Lo único más difícil que introducir una idea nueva en la cabeza de un militar es cambiar una idea antigua».

Sir Basil Liddell Hart

Alvin Tofler, en su libro *La Tercera Ola* explora como la sociedad está cambiando debido a la era de la información. La educación, las relaciones, la forma de comunicarse, todo está adaptándose a la nueva realidad que promueven las tecnologías (Toffler, 1993).

Como parte representativa de la sociedad las FAS no son ajenas a este proceso, debiendo adaptarse y evolucionar para emplear estas transformaciones que adelantaba Tofler a su favor.

En lo que respecta a las propias innovaciones, hoy en día, es difícil advertir los límites que pueden alcanzar los desarrollos tecnológicos, especialmente si se trata de la IA, por lo que son fuente de desconfianza continua y, por tanto, un freno a su pleno (y libre) desarrollo en el mundo occidental (Martínez Millán, 2023).

Por un lado, el desconocimiento de herramientas y algoritmos, agrandan esta desconfianza en la tecnología, aumentando a su vez la llamada *caja negra*[10] al no llegar a comprender de forma real los procesos que ocurren en las innovaciones tecnológicas, siendo necesario un modelo más *explicable* (Catalá Lloret, 2022).

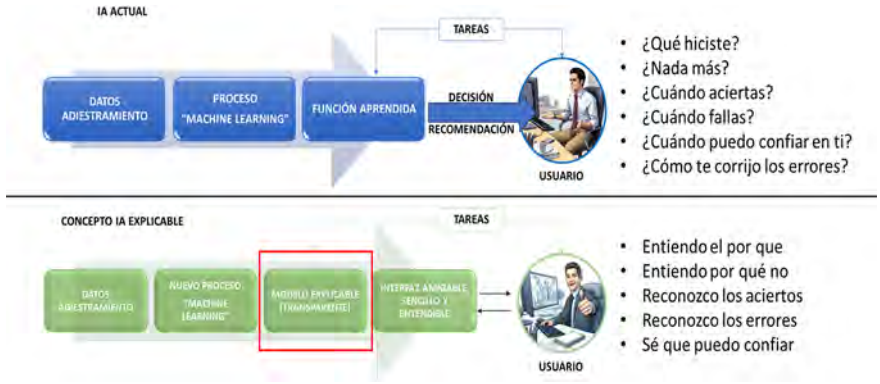

Figura 3. Inteligencia Artificial Explicable. Conociendo los procesos internos de la IA y conociendo el interfaz de la explicación, se comprenderá mejor a la IA y por tanto se tendrá un mayor control y supervisión de esta. Fuente: elaboración propia basado en imágenes de Darpa.mil. Imágenes realizadas con IA

Por otro lado, en las FAS españolas, los cuadros de mandos (empleos directivos y alta gestión) suelen corresponderse con aquellos de mayor edad (por ejemplo, coroneles y generales), por lo que pertenecen a distintas generaciones con vivencias tecnológicas distintas. Esta situación pudiera afectar negativamente a la aceptación de la TD, tal y como propone Rogers en su modelo de adopcion de la innovacion[11]. La curva de Rogers establece

[10] Referido al funcionamiento interno de los algoritmos y que normalmente no son visibles o entendibles.

[11] La curva de adopción de la innovación fue propuesta en 1962 por Everett Rogers en su libro *Diffusion of Innovations*, donde también profundiza en las causas que conducen a la adopción masiva de una innovación, aunque es mayoritariamente utilizada

que la aceptacion de las nuevas tecnologías se reproducira en una gráfica tipo campana de Gauss, distribuida por edades, con la peculiaridad de que existirá un mínimo punto para el cambio, que dependiendo de la organización en la que se tome, sera más o menos amplio (Gil Clemente, 2022).

Por lo tanto, la TD en las FAS podría verse alterada por una adopción tardía, por desconfianza o desconocimiento tal y como se expresa en los modelos de Rogers. Sin embargo, esta TD continúa siendo necesaria para incorporar tecnologías disruptivas que ofrezcan superioridad en el combate, por lo que será necesario recurrir a la formación, el liderazgo y el conocimiento para permitir que se lleven a cabo, salvando las posibles resistencias al cambio por desconfianza o desconocimiento (Ministerio de Defensa, 2024).

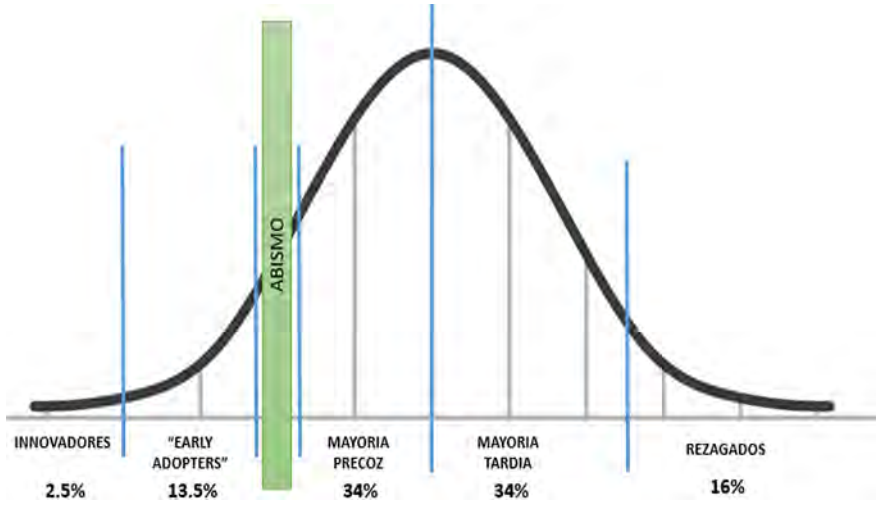

Figura 4. Curva adopción de la tecnología de Rogers. La clave para una adopción temprana de la tecnología se encuentra en la reducción de la franja del «abismo», siendo la estrategia habitual el conocimiento, la publicidad y el liderazgo en su adopción. Fuente: elaboración propia con base en la teoría de Rogers.

3.5. Innovaciones tecnológicas en conflictos recientes

En los últimos años, se han podido observar, en conflictos recientes y algunos, aún activos, el empleo de distintas innovaciones

en el ámbito económico para establecer estrategias comerciales, es interesante su aplicación en el ámbito de estudio para aplicar estrategias de implantación enérgicas.

tecnológicas como las reseñadas en los apartados anteriores. Estos conflictos resaltan la necesidad de disponer de sistemas e innovaciones avanzadas y relevantes, puesto que su empleo demuestra que son tanto un hecho, como una necesidad.

En el conflicto de Ucrania, las innovaciones tecnológicas han permitido a un país inicialmente inferior, tecnológica y militarmente hablando, sobreponerse y resistir los ataques de una potencia que se entendía como superior (NATO, 2023b).

En el caso del conflicto palestino-israelí, y a pesar de que Israel no fue capaz de predecir el ataque del 7 de octubre, Israel empleó el potencial tecnológico tanto en la defensa de su territorio como en las distintas acciones de combate llevadas desde entonces, tanto en la Franja de Gaza como en otras localizaciones.

3.5.1. Conflicto Rusia-Ucrania

Una de las innovaciones que caracterizan la guerra en Ucrania es el empleo a gran escala de UAS[12] (Unmmaned Air System) {XE "UAS Unmmaned Air System"}. Estos sistemas se han utilizado tanto en operaciones ofensivas como en defensivas dentro de lo que se conoce como el concepto de armas combinadas. Otro de los usos principales de estos elementos ha sido la obtención de información para contribuir a una mejor conciencia situacional (Jones *et al*., 2023).

En cuanto al modelo utilizado, se ha observado el efecto que ha ejercido el uso de tecnología civil para empleo militar. Ante la escasez de repuestos y materiales, la tecnología civil de *drones* recreativos ha contribuido al mencionado vuelco en la situación (Greenwood, 2023).

Otro de los aspectos reseñables de la guerra en Ucrania ha sido el empleo de la disciplina OSINT. Existen diversos aspectos que han afectado a la guerra a través del uso de esta disciplina, primeramente, la capacidad de anticipación, antes del inicio del conflicto, tanto agencias como grupos de civiles pudieron, a través del acceso a satélites comerciales, establecer los movimientos preparatorios de las tropas rusas en las fronteras de

[12] Se debe reseñar que Ucrania ha empleado, de la misma forma, sistemas remotamente tripulados marítimos, con un alto grado de eficacia, logrando hundir varios buques rusos.

Ucrania. Además, el OSINT ha acercado el conflicto a la sensibilidad internacional, siendo utilizado entre otros cometidos para corroborar o atribuir supuestos crímenes de guerra. Por otro lado, ha servido tanto para disminuir la niebla de la guerra como para minimizar las campañas de desinformación del adversario (Hockenhull, 2022).

Además, las FAS de Ucrania han podido desarrollar sus propios *softwares*[13] inteligentes que mejoran la conciencia situacional y que son capaces de integrarse con comunicaciones de la OTAN y que gestionan el acceso a mapas electrónicos del área, visualización de la propia posición a través de datos GPS, intercambio de datos con otros usuarios del sistema, cálculos individuales varios, transferencia de datos de reconocimiento de medios y control de fuego automatizado, entre otras funciones (Jones *et al*., 2023).

El ciberespacio se ha empleado constantemente durante el desarrollo del conflicto, desde antes del inicio hasta el presente. Según Microsoft, los ciberataques llevados a cabo contra el gobierno y estructuras de Ucrania se llevaron a cabo en apoyo a las acciones de combate, incrementándose en hasta 35 veces los niveles previos al conflicto (Microsoft Threat Intelligence, 2022).

La protección de las infraestructuras críticas y de la información militar sensible es un tema principal tratado en las lecciones aprendidas del conflicto, estableciéndose conclusiones de importancia en el nivel estratégico y operacional como la necesaria evaluación de riesgos, la compartición de datos ante ataques, la concienciación y el adiestramiento. A nivel táctico, se focaliza en disponer de planes de contingencia, redes securizadas (y segmentadas), así como incidir en el adiestramiento y concienciación (NATO, 2023b).

Finalmente, ninguno de los éxitos se habría conseguido sin un sistema banda ancha que permitiera el enlace entre sistemas y unidades (Hockenhull, 2022). En este sentido, se pudo disponer e integrar la red de Starlink, tanto para conducción de operaciones (comunicaciones de baja latencia, banda ancha y cifrada) como para mantener una moral elevada en sus combatientes y población (servicio telefónico e Internet).

[13] El *software* Kropyva es un ejemplo que entre otros medios de financiación se ha empleado el *crowdfunding*, siendo otra característica de este conflicto (ARMYSOS, s. f.).

3.5.2. Conflicto Hamás-Israel

Israel está a la vanguardia en la integración de la IA y la ciberseguridad en sus operaciones militares y estrategias de seguridad nacional, reflejando una fuerte necesidad y compromiso con la innovación tecnológica que lo posicionan como líder del sector (Antebi, 2021).

A pesar de los recursos tecnológicos, el 7 de octubre de 2023 Israel fue atacado sin haberlo podido prever y siendo sorprendidos a través de sus fronteras terrestres. No obstante, durante los ataques, y con el transcurso del conflicto, también se produjeron ataques a distancia con cohetes, desde la Franja de Gaza Líbano, Siria, Yemen e incluso Irán (Carl, 2023).

En lo que respecta a los ataques a distancia, el sistema de defensa antiaéreas israelí ha funcionado con garantías. Este sistema denominado Iron Dome consiste en varios componentes, entre los que se incluyen los lanzadores de misiles y los centros de mandos, pero lo que sin duda marca la diferencia es el *software* de IA, que permite predecir la trayectoria, evaluar el punto de impacto, sus consecuencias y, en caso necesario, lanzar la contramedida (Parra, 2023).

Para análisis y selección de objetivos, las FDI emplean un *software* denominado *Habsora* (una IA*)* cuya función es proponer objetivos rentables a través del análisis de multitud datos de inteligencia recogidos por todo tipo de disciplinas, como: IMINT (satélites y UAS), GEOINT, HUMINT o SIGINT (registros de redes telefónicas), entre otros (Sierra, 2023). Desde el inicio del conflicto, el sistema ha ayudado a identificar más de 12 000 objetivos (IDF, 2023a).

Israel también es una potencia en la fabricación y empleo de UAS, los cuales aportan información y datos continuos al sistema *Habsora* y que permiten disponer de una conciencia situacional elevada para los comandantes en el campo de batalla (Mimran *et al*., 2024).

Por último, a través de unidades denominadas *Adan,* Israel fusiona todos los datos disponibles del campo de batalla, los analiza y los pone a disposición de los mandos tácticos casi en tiempo real. Estas unidades tienen la misión de gestionar la información proveniente tanto de inteligencia estratégica como del propio campo de batalla, gestionarla y distribuirla a los mandos que la necesiten (IDF, 2023b).

4. Impacto en ciberseguridad y ciberdefensa[14]

La creciente interconexión de dispositivos y sistemas digitales como: el IoT, el 5G o la IA amplían, significativamente, la superficie exposición a los ciberdelincuentes (Di Santo, 2024), lo que hace que las amenazas del ámbito «ciber» sean cada vez más sofisticadas y peligrosas. Según el Instituto Nacional de Ciberseguridad (INCIBE{XE "INCIBE Instituto Nacional de Ciberseguridad"}), en el 2023, se gestionaron un 9 % de incidentes más que el año anterior, muchos de ellos de riesgo alto. Además, se menciona el aumento en más de un 40 % de *ransomware* en el 2022, así como una preocupación creciente en el ámbito ciber (Centro Criptológico Nacional, 2023).

En este sentido, la mejora tecnológica, en especial la IA, se espera que supondrá tanto un aumento, como una sofisticación en las campañas que se podrían llevar a cabo con todo tipo de *malware* (Centro Criptológico Nacional, 2023), poniendo en valor el concepto de *Crime as a service*[15], el cual permite al programador quedar impune y con posibilidad de volver a atacar.

En este contexto de transformación digital, los órganos de ciberseguridad/ciberdefensa de la AGE, del ámbito privado y del Ministerio de Defensa desempeñarán un papel crucial en este escenario, velando por la protección de las redes, la documentación sensible y la incorruptibilidad de los datos.

En el segundo apartado, se presentarán las generalidades de la Estructura de Ciberseguridad del Ministerio de Defensa. De la misma forma, se tratará la Red Nacional Centro de Operaciones de Seguridad (SOC{XE "SOC Centro de Operaciones de"}) y Plataforma Nacional de ciberincidentes, como un exitoso modelo

[14] La ciberseguridad y la ciberdefensa son campos íntimamente relacionados, pero claramente diferenciados. En algunos casos se han empleado indistintamente. Se aclara que la ciberseguridad se centrará en la prevención de ataques cibernéticos y la protección de sistemas y redes e incluiría la propia resiliencia de los sistemas. En el caso de la ciberdefensa consistiría en salvaguardar los intereses nacionales en caso de verse amenazados, abarcando operaciones activas o pasivas realizadas por el Estado (Pontijas Calderón, 2023).

[15] El *Crime as a Service* (CaaS), en el caso que nos aplica, *Malware as a Service*: es un modelo en el que los ciberdelincuentes ofrecen ataques prefabricados, como *ransomware*, DDoS y *phishing*, que el usuario puede controlar desde una interfaz o con instrucciones sencillas, sin necesidad de conocimientos en ciberseguridad o *hacking*.

español que integra SOC de entidades públicas y privadas[16], con la posibilidad de extenderse a la UE.

4.1. Soberanía digital y seguridad

El concepto de soberanía digital se refiere a la capacidad de un estado de tener el control sobre el propio destino digital, con objeto de proteger, controlar el acceso, uso y la gestión de datos e información, además de *hardware* y *software*. Esto implica que las personas y entidades tengan el control y la propiedad de su información, evitando depender en exceso de terceros para su gestión y protección. (Faba de la Encarnación y Simón Canal, s. f.)

La soberanía de los datos está relacionada con la capacidad de decidir cómo se recopilan, almacenan y utilizan los datos personales, lo que influye en la privacidad y la seguridad digital, que tanto se pretende en los documentos nacionales (Departamento de Seguridad Nacional, 2019). España y sus socios europeos ven con preocupación que la gran cantidad de información generada a partir del uso de servicios tecnológicos se almacene y gestione en otros países, en especial EE. UU. (Snowden, 2019).

En relación con lo anterior, es posible preguntarse sobre la necesidad de disponer de soberanía digital. Para una mejor figura, se tratará de explicar con un ejemplo cotidiano: es muy común que, al conversar con miembros de una comunidad, al final de la conversación, el *smartphone* muestre artículos o anuncios relacionados con ese tema de conversación, ¿verdad? Esta situación, en ciertos ámbitos, se explica con el tópico «tu *smartphone* no es un teléfono, es un dispositivo de escucha y localización»[17].

En la misma línea, Shoshana Zuboff, en su libro *La era del capitalismo de la vigilancia,* se refiere a cómo las empresas, sobre todo las más potentes, se valen de todo tipo de datos personales con el fin de crear productos anticipando el propio comportamiento humano. Si bien, remarca que sus fines son propiamente comerciales, pero el excedente que se genera permanece en propiedad de las empresas, siendo usado para otros fines (incluido la venta en el mercado a terceros) (Zuboff, 2019).

[16] Actualmente, actúan únicamente como proveedoras de servicios, pretendiéndose incorporarlas.

[17] Autor desconocido. La expresión se utiliza, normalmente, en ambientes relacionados con espionaje, ciberdefensa, ciberseguridad o asuntos digitales.

Pero ¿cómo es posible que esto ocurra? De acuerdo con los datos aportados por la firma de Oliver Wyman y reproducidos por Expansion.com, el 92 % de los datos del mundo occidental se almacenan en servidores de EE. UU., siendo probablemente utilizados por las agencias de inteligencia locales (Snowden).

En este sentido, no solo se trata del almacenamiento, sino también de la infraestructura (*hadware*) y *software*. Torres de comunicaciones, cables submarinos, ordenadores e inclusos cifradores y enrutadores son de propiedad (mayoritariamente) norteamericana, de la misma forma que lo es el *software* de las plataformas de correo, Oracle, Windows, Office y otros paquetes conocidos. Como contraargumentación se podría plantear que EE. UU. es un aliado, pero, en este sentido, es necesario recordar que en el ámbito de la información y la inteligencia solo existen los intereses[18].

Un ejemplo sobre los intereses nacionales son las escuchas ilegales a Ángela Merkel (Pereda, 2013) y a otros líderes europeos reveladas hace algunos años. Y que, con el tiempo, resultó que se trataba de una práctica empleada, con normalidad, por la NSA desde los años noventa (EC/Agencias, 2021) y apoyados en la posterior Ley Patriótica (*USA Patriot Act*).

> «En el año 2000, Duncan Campbell, el mayor experto en la red Echelon[19], expuso su informe ante la Eurocámara, en una sesión abierta a los medios de comunicación. Lo que los presentes escucharon aquel día en la sala removió los mismos cimientos de la Unión Europea. Echelon era una realidad. No era una película de espías, ni el producto alocado de una imaginación paranoica. Echelon era la red de espionaje más grande del mundo y tenía capacidad para interceptar 2000 millones de comunicaciones privadas diarias» (Suárez Sánchez-Ocaña, 2015: 40).

De esta forma, se entiende que EE. UU. considere la soberanía digital como un problema de seguridad nacional, destinando gran cantidad de recursos a mantenerla, sobre todo en relación con competidores como China y Rusia. (Faba de la Encarnación y Simón Canal, s. f.)

---

18 Lord Palmeson, primer ministro inglés del siglo XIX: «Inglaterra no tiene amigos ni enemigos, Inglaterra tiene intereses».

19 Red formada por EE. UU., Reino Unido, Australia, Canadá y Nueva Zelanda. También conocida como *los cinco ojos*.

En el caso de España y sus socios, los documentos analizados en el capítulo I tienden a un mayor porcentaje de tecnologías propias o, al menos, del ámbito europeo con objeto de disponer del mayor control e independencia en el mundo tecnológico y de la información.

En este aspecto, se han realizado propuestas por la Unión Europea que abordan medidas para proteger tecnología y economía frente a potencias extranjeras, buscando reforzar el control de inversiones extranjeras en sectores críticos y crear un escudo económico frente a China, Rusia y Estados Unidos (Esteller, 2024; Alarcón, 2024). Estas propuestas están en línea con el concepto de soberanía digital, ya que buscan mantener la autonomía tecnológica y económica de la UE, reduciendo su dependencia extranjera (Union Europea, 2022).

Por otro lado, y centrados en España, el EMAD y Telefónica E. han acordado impulsar proyectos tecnológicos de alto impacto, para contribuir a la creación de capacidades nacionales en el ámbito digital (EMAD, 2024). Además, siguiendo la estrategia de colaboración público-privada, están apareciendo iniciativas, de fondos de inversión, dirigidas al fomento de tecnologías propias en pymes, mayormente españolas (Servimedia, 2024).

Desafortunadamente, y siendo realistas, es utópico aspirar a ser 100 % soberanos digitales, aunque España ha dado ya pasos para mejorar en este aspecto, sobre todo en la intención de ser dueño del dato, evitando que ese dato no pueda ser empleado por un tercero no confiable.

> «Esta situación no es tan utópica y es factible de conseguir, además de extremadamente valiosa desde el punto de vista de la Inteligencia militar (es necesario una arquitectura del dato y un gobierno del dato a nivel conjunto)» (Fuente especializada del MCCD).

Puesto que es extremadamente difícil ser totalmente soberano en el ámbito digital, ¿cómo podemos aspirar a ser dueño del dato? Desde el punto de vista técnico, preservando su integridad y fiabilidad con un cifrado apropiado, robusto y que perdure en el tiempo. Teniendo en cuenta que los sistemas son manejados por personas, estas deberán de estar acreditadas, por lo que será necesario la implementación de procedimientos de seguridad enfocados, de la misma forma, a controlar el dato y el acceso a la información.

4.1.1. Cifrado. Tecnología cuántica y poscuántica

Además de disponer de un grado elevado de soberanía digital, es necesario proteger los datos, de forma que, aunque existan intrusos o vigilantes en nuestros sistemas, podamos disponer de un sistema de cifrado adecuado. De esta forma, nos aproximamos al concepto del dato como activo estratégico creciente, pero no lo será solo por sí mismo, sino también toda la infraestructura digital que lo contiene [Lorenzo Avello López (CNN, 2023)].

De la misma forma que cualquier *hardware*, es conveniente que las FAS cuenten con sus propios sistemas y algoritmos de cifrado, con objeto de preservar la inviolabilidad de los datos sensibles con los que trabaja. De la misma forma, las organizaciones de inteligencia necesitan gestionar datos para cumplir su misión principal, poner a disposición del decisor de forma oportuna información de inteligencia que disminuya la incertidumbre y permita la toma de decisiones.

En este sentido, Defensa ha invertido, en el 2022, en la mejora y adquisición de cifradores a la empresa española EPICOM (Duro Felguera) (InfoDefensa, 2023), con objeto de mejorar la seguridad en las comunicaciones.

Del mismo modo, en el mismo año se invirtió en un sistema *Flying Ad hoc NETwork & distributed mobile Tactical Cloud* (FANET-C{XE "FANET-C Flying Ad-hoc NETwork & distributed mobile Tactical Cloud"}) para comunicaciones tácticas y nube de combate del Ejército de Tierra, también enfocado hacia la mejora e implementación de tecnologías disruptivas basadas en 5G (Ministerio de Hacienda, 2023b).

– Cifrado simétrico, asimétrico y cuántico.

En lo que se refiere a cifrado, se explicarán someramente cómo funcionan los sistemas clásicos de cifrado (simétrico y asimétrico) y el cifrado cuántico.

Los sistemas clásicos funcionan con distintos algoritmos de cifrados que, en función de su longitud o complejidad, hacen que el sistema sea más o menos seguro, sus principales diferencias se basan, además de los algoritmos, en la longitud y el número de claves.

En el cifrado simétrico, el emisor y el receptor usan la misma clave para cifrar y descifrar los datos. Este método es rápido y eficiente, pero se requiere que las partes tengan conocimiento de la clave, lo que supone un riesgo a la seguridad. Uno de los algoritmos más comunes es el AES con longitud de 128, 192 o 256 bits.

Por otro lado, el cifrado asimétrico utiliza un par de claves: la pública y la privada. La clave pública se conoce, mientras que la clave privada es secreta. Este sistema es el mismo que se dispone en los documentos nacionales de identidad en España. Al enviar un mensaje, el emisor cifra con la clave pública del receptor, y el receptor lo descifra con su clave privada. El principal problema de este sistema es que es más lento que el cifrado simétrico. El algoritmo más común es el RSA de al menos 2048 o 4096 bits.

El cifrado cuántico es una forma avanzada de encriptación que se basa en los principios de la mecánica cuántica para proteger la información. A diferencia del cifrado clásico, que emplea algoritmos matemáticos, el cifrado cuántico utiliza partículas subatómicas para transmitir claves de forma segura.

Básicamente, la criptografía cuántica utiliza el principio de superposición[20] para dotar de seguridad a las transmisiones. De acuerdo con este principio, cualquier intento de interceptación sería detectado, lo que convierte a esta tecnología en un sistema altamente seguro (López, 2024).

Aunque se trate de una innovación prometedora para cifrar, esta tecnología presenta una serie de problemas técnicos, especialmente los relacionados con la infraestructura necesaria para su funcionamiento, sobre todo, en términos de costo y equipos especiales, que la hacen inviable actualmente, según la Agencia de Seguridad Nacional de los EE. UU. (NSA{XE "NSA Agencia de Seguridad Nacional"}) (National Security Agency/Central Security Service, s. f.).

– Cifrado poscuántico

La criptografía poscuántica (PQC{XE "PQC La criptografía pos-cuántica"}), también conocida como criptografía resistente al *quantum*, es una evolución de la criptografía simétrica actual. Su principal diferencia radica en el empleo de algoritmos y cadenas de cifra más resistentes y complejas que las anteriores, incluso para ordenadores cuánticos.

Aunque no existe garantía de seguridad total, la fortaleza se basa en que aún no existen ordenadores cuánticos que puedan

[20] Una partícula cuántica puede existir en múltiples estados al mismo tiempo y, al ser observada, su estado se colapsa a una sola posibilidad. Por lo tanto, si se intenta interceptar la información, se alteraría el estado de las partículas cuánticas de la transmisión, lo cual sería detectado. (Paradoja de Schrödinger) (Sanz Romero, 2020).

efectuar los cálculos necesarios para romper dicha cifra en poco tiempo. En pocas palabras, se podría tratar como un parche de seguridad de las tecnologías existentes, pero requiriendo de sistemas (*hardware*) de mayor potencia.

De acuerdo con recomendaciones en EE. UU., la Casa Blanca instó en 2022 a toda su administración a migrar sus sistemas, completamente, a tecnologías PQC para 2035 (Krelina y Dúbravčík, 2023).

En lo que respecta a tecnología cuántica nacional, existe un proyecto *Quantum Spain*, que nace de la Estrategia Nacional de Inteligencia Artificial, con el objetivo de disponer de construir un ordenador cuántico de 30 qubits para el año 2025. Este ordenador es íntegramente español, con participación de empresas que actualmente se relacionan con las FAS, por lo que representaría una oportunidad de contar con el *Know How* en esta materia (Gobierno de España, 2023).

A pesar de no existir aún ordenadores cuánticos plenamente desarrollados, existen empresas, en la actualidad, que están haciendo copias de páginas web cifradas para poder descifrarlas para cuando estén operativos (Concepto roba ahora, descifra después) (López, 2021).

4.2. Pasar de la confianza total a confianza cero (*Zero Trust*)

Para entender mejor el concepto *Zero Trust* es conveniente explicar el contrario: el concepto de *Full Trust*: cuando un miembro de la organización gana el acceso a la red ya no es necesaria ninguna supervisión o verificación. Este sistema tiene numerosos inconvenientes, sobre todo al tratar con enemigos dentro de la propia institución, personal que cambia su comportamiento o, simplemente, personal que tiende a extraer recursos de la red sin intención de hacer el mal (Mishra, 2023).

Ahora bien, durante las V Jornadas de Ciberdefensa, el representante de Teldat reseñó que se destacaban siete aspectos fundamentales para la seguridad en entornos de tecnología 5G: uso de *firewalls* y filtrado de tráfico, autenticación sólida, gestión de identidades y accesos basados en el principio de mínimo acceso, detección de amenazas con IA, actualizaciones automáticas, monitorización continua y políticas de respuesta a incidentes [Antonio García (CNN, 2023)].

La afirmación anterior coincide con el concepto de *Zero Trust*, o confianza cero, donde se asume que no se puede confiar en nada dentro o fuera de una red. Para llevarlo a cabo es necesario verificar constantemente la identidad y la seguridad de cualquier persona o dispositivo que trate de acceder a los recursos de la red, empleando las medidas anteriormente citadas. (Pinedo Lapeña, 2022)

Este concepto, aunque relativamente innovador en el ámbito civil, no lo es tanto en el ámbito militar por disponer un sistema dual, basado en la *necesidad de conocer* y en la disponibilidad de una Habilitación Personal de Seguridad (HPS{XE "HPS Habilitación Personal de Seguridad"}). No obstante, en un mundo muy interconectado, donde se dan situaciones de comprometimiento de seguridad desde la propia estructura interna de las organizaciones, el concepto *Zero Trust* podría tener cabida en las FAS.

Aplicando el concepto de *Zero Trust* en el mundo militar, los avances en *software* de seguridad y tecnologías de inteligencia artificial (IA) podrían reforzar la verificación constante de la identidad de los usuarios, así como monitorizar sus patrones habituales de búsqueda, manteniendo un registro constante de toda la información cargada, descargada o consultada (INCIBE, 2023).

Esto se alinea con el principio militar de *necesidad de conocer*, donde, además, el sistema estaría habilitado para cortar el acceso, o enviar alertas de seguridad al administrador ante comportamientos/patrones maliciosos o inusuales de los usuarios.

4.3. Gobernanza ciberseguridad. Red nacional SOC

El modelo español actual es un modelo plural y disperso en el que los principales actores en este ámbito serían el Departamento de Seguridad Nacional (DSN{XE "DSN Departamento de Seguridad Nacional"}), la Oficina de Coordinación de Ciberseguridad (OCC{XE "OCC Oficina de Coordinación de Ciberseguridad"}), el Centro Criptológico Nacional (CCN{XE "CCN Centro Criptológico Nacional"}-CERT), el INCIBE-CERT y el Mando Conjunto Ciberespacio (MCCE{XE "MCCE Mando Conjunto Ciberespacio"}), además del CESTIC, de otros órganos de distintos ministerios y distintas secretarías de Estado.

El Ministerio de Defensa de España cuenta con una estructura de ciberseguridad que se encuentra bajo la responsabilidad del MCCE y la jefatura de Ciberseguridad. El MCCE, con sus órganos,

se encargará de las respuestas ante incidentes mientras que su jefatura será responsable de apoyar al CESTIC en la gestión de las políticas de seguridad de la información, así como controlar su cumplimiento.

Uno de los grandes problemas que se presenta es el poder acceder a todos los sistemas clasificados, que son de distintos niveles de clasificación y distintos dominios, por lo que se hace necesaria la creación de un SOC central.

Por otro lado, la OCC, perteneciente a la Dirección general de Coordinación y Estudios (Ministerio del Interior), lleva a cabo la coordinación y el intercambio de información con el resto de los organismos de la Unión Europea. Por otro lado, también funciona como canal especifico con los otros CERT nacionales de referencia (Oficina C, 2022).

Uno de los principales problemas que se encuentra es la necesidad de atender a numerosos sistemas y no disponer de los medios materiales, humanos y conocimientos para atenderlos a todos. Por esta razón se trata de buscar Centros de Operaciones de Seguridad (SOC{XE "SOC Centros de Operaciones de Seguridad"}) que atiendan a más de un sistema, tendiendo hacia un sistema más o menos centralizados.

Un ejemplo de la tendencia a la centralización es la Red Nacional de SOC, donde la iniciativa del CCN-CERT está evolucionando hacia un sistema más integrado y colaborativo, intercambiando información automáticamente para una respuesta más rápida y eficaz a las amenazas. [Carlos Córdoba (CNN, 2023)].

En este sentido, el CCN establece el Esquema Nacional de Seguridad a través del el Real Decreto 3/2010, y su actualización del Real Decreto 311/2022. Con ellos se busca homogeneizar en la administración digital los principios, requisitos y medidas de seguridad comunes, facilitando la gestión de riesgos, las brechas de seguridad y la comunicación de ciberincidentes (*Esquema Nacional de Seguridad*, s. f.).

En la presentación de las V Jornadas de Ciberdefensa, tanto la directora del CNI como la ministra de Defensa y la secretaria de Estado de Digitalización e Inteligencia Artificial coinciden en que la colaboración, el intercambio de conocimientos y la acción colectiva son los elementos clave para enfrentar los desafíos del ciberespacio. No en vano, el lema de dichas conferencias es *compartir para ganar* (CNN, 2023).

Es de reseñar que, en el ámbito europeo, hay países que trabajan hacia una gobernanza de la ciberseguridad más centralizada, a través de agencias únicas de ciberseguridad, las cuales unificarían los criterios, metodologías y actuaciones en esta materia en cada miembro Estado.

Reflejo de esto será el escenario que dibuje la Directiva UE NIS2[21]. La adopción de esta norma supondrá una gestión mucho más eficiente de la gestión de amenazas de seguridad y de la metodología de notificación, con un sistema de trabajo sencillo y un único ente con quien tratar (sistema centralizado).

4.4. Casos de estudio Snowden y Teixeira

A continuación, se presentarán dos casos de estudio y aplicación del concepto *Zero Trust* donde, por el hecho de disponer de la más alta clasificación de seguridad, no es óbice para dejar de controlar el acceso y uso de la información, especialmente, pero no exclusiva, la dedicada al uso de la Defensa Nacional.

4.4.1. E. Snowden

Edward Snowden fue un trabajador y analista de los servicios de inteligencia estadounidense que denunció y reveló la existencia de programas secretos de recopilación de información masivos en 2013. Antes de los veintinueve años, Snowden ya disponía de un buen sueldo y de un nivel de acreditación de seguridad que le permitía acceder a información sensible de EE. UU.

En 2013, reveló la existencia de programas secretos de vigilancia, como PRISM, que daban a la NSA acceso directo a los servidores de empresas como Facebook, Google y Apple. Tras las filtraciones, Snowden viajó a Hong Kong y luego a Rusia, donde es de suponer que ha vivido desde entonces.

> «Lo que estoy definiendo como fundamentalmente estadounidense no es solo la infraestructura de internet, sino también el software (Microsoft, Google, Oracle) y el hard-

[21] La Directiva NIS2, también conocida como Directiva (UE) 2022/2555, es una normativa europea que establece medidas para garantizar un alto nivel común de ciberseguridad en toda la Unión Europea. Esta directiva tiene como objetivo mejorar las medidas destinadas a garantizar un adecuado nivel común de ciberseguridad y se aplica a diversos sectores, dividiéndolos en sectores de alta criticidad y otros sectores esenciales (Gobierno de España, 2022).

> ware (HP, Apple, Dell) de los ordenadores. Es todo, desde los chips (Intel, Qualcomm) hasta los enrutadores y los módems (Cisco, Juniper), los servicios web y las plataformas de correo electrónico, redes sociales y almacenamientos en nube (Google, Facebook y Amazon que es el más importante en cuanto a estructura, aunque permanezca invisible, ya que ofrece servicios en nube al gobierno estadounidense, aparte de a la mitad de internet)» (Snowden, 2019: 225).

En 2019, se publicó su libro *Vigilancia Permanente* y en 2020, un tribunal federal de EE. UU. dictaminó que el programa de vigilancia masiva expuesto por Snowden era ilegal y posiblemente inconstitucional.

La motivación expresada por Edward Snowden, para filtrar los datos que finalmente derivaron en el fallo de seguridad, aludían a conflictos éticos generados por este programa de vigilancia masiva (Snowden, 2019; Suárez Sánchez-Ocaña, 2015).

> «Los archivos filtrados por Snowden dan cuenta de que la NSA ha espiado el correo electrónico y los teléfonos de 35 dirigentes políticos extranjeros, entre ellos, la canciller alemana Angela Merkel, la presidenta de Brasil, Dilma Rousseff, el papa Francisco, el mandatario mejicano Peña Nieto y diversos miembros del gobierno de España, además de algunas grandes empresas, como la brasileña Petrobras» (Suárez Sánchez-Ocaña, 2015: 37)».

Sea como fuere, es un hecho que existió un fallo de seguridad llevado a cabo por personal de la organización que en un determinado momento sus lealtades cambian y, al disponer de las credenciales suficientes, se produce el robo de documentación sensible.

4.4.2. Jack D. Teixeira

Jack D. Teixeira fue un miembro de la Fuerza Aérea de los Estados Unidos destinado en la 102.ª Ala de Inteligencia de la Guardia Nacional Aérea de Massachusetts. Teixeira saltó a las noticias al ser acusado de retener y transmitir información de defensa nacional sin autorización en 2022, con veintiún años.

Según datos del informe, Teixeira comenzó a publicar información clasificada en febrero de 2022, siendo arrestado por el FBI en abril de 2023. En ese momento, Teixeira se enfrentó a medi-

das penales por compartir información clasificada y fotografías a través de la plataforma Discord[22] a terceros no autorizados.

En el auto de su investigación se destaca que ingresó en las Fuerzas Aéreas en 2019 y que en 2021 (veinte años) se le acreditó un tipo de clasificación *Top Secret*. Debido a su puesto como técnico de mantenimiento, disponía de acceso tanto a locales como sistemas clasificados, entre otros, al Joint Worldwide Intelligence Communication System (JWICS), incluyendo sus contenidos y análisis.

Según los informes, Teixeira fue advertido hasta en dos ocasiones de llevar un comportamiento inadecuado. De la misma forma, la investigación señala la falta de guía de conceptos como *la necesidad de conocer, la falta de supervisión y la ocultación de factores negativos en las investigaciones iniciales* (The Inspector General of the Air Force, 2023).

De acuerdo con lo expuesto anteriormente, y en relación con el caso de E. Snowden, a Teixeira se le concedió un alto nivel de acreditación y acceso a la información en instalaciones de seguridad cuya falta de supervisión continua provocó el fallo de seguridad.

4.4.3. Otros casos recientes

A lo largo del 2024, se han producido una serie de eventos que, sin llegar a tener la magnitud mediática de los mencionados anteriormente, merece la pena reseñarlos en este trabajo por el interés que despiertan para con la concienciación sobre ciberseguridad y la realidad tecnológica en la que vivimos actualmente.

– Interceptación de llamada telefónica a general alemán

En marzo de 2024, varios periódicos se hacían eco sobre la filtración de los servicios secretos rusos de una supuesta conversación entre altos mandos alemanes y el empleo de armamento y personal alemán en Ucrania en el contexto del conflicto con Rusia. En

[22] «Discord es un programa de comunicación gratuito que permite compartir chats de texto, voz y vídeo con amigos, comunidades de juegos y desarrolladores. Cuenta con cientos de millones de usuarios, lo que lo convierte en una de las formas más populares para conectarte con otras personas por internet. Se puede usar en la mayoría de las plataformas y los dispositivos, incluidos Windows, macOS, Linux, iOS, iPadOS, Android y navegadores web» (Pearson, 2022).

este caso, y a pesar de que el mando alemán (General del Ejército del Aire) disponía de servicio de telefonía *securizado*, la supuesta filtración se habría producido, por la conexión del dispositivo a la red Wi-Fi del hotel en Singapur, en el que se encontraba por haber asistido a una feria de armamento (Valero, 2024).

– Sospechas de espionaje en el Eurocuerpo

A finales de marzo, el general polaco Jarosaw Gromadziski fue destituido de su cargo por estar inmerso en una investigación por espionaje a favor del gobierno ruso (Efe, 2024). En este caso, los medios no mencionan la divulgación de información sensible o de acceso a sistemas, sin embargo, por la posición que ocupaba y ha ocupado el general a lo largo de su trayectoria, lo convierten en un objetivo de interés para servicios de inteligencia de potencias adversarias.

– Ciberataque a empresa de reconocimientos médicos

A mediados de abril del presente año, se conocía la noticia de que datos personales de la Guardia Civil y de personal de las FAS habían quedado expuestos por un Ciberataque contra una empresa subcontratada para la realización de reconocimientos médicos (Recio, 2024).

Hoy en día, al menos en fuentes accesibles desde Internet, se desconoce el alcance del ciberataque, sin embargo, se indica que el ataque se produjo por una evolución del Ransomware Lockbit[23] (3.0. en este caso), dejando al alcance datos sensibles como son los «número de la tarjeta de identificación personal (TIP{XE "TIP Tarjeta de Identificación Personal"}), número de teléfono móvil, fecha de nacimiento, sexo, puesto de trabajo, resultados de reconocimiento médico y certificado de aptitud» (García Méndez, 2024).

– Aumento ataques en el pasado año (2024)

Según datos del CCN-CERT, los ciberataques contra el sector público continúan en aumento, de acuerdo con distintos portales de noticias, en lo que va de año se han registrado más de 25 000 *agresiones digitales* (Di Santo, 2024).

[23] Lockbit es también es un grupo de ciberdelincuentes, con origen en Rusia, que se dedica al desarrollo y distribución de software malicioso, empleando también el concepto de *Ransomware as a service* (RaaS{XE "RaaS Ransomware as a service"}), similar al CaaS, con el que consigue atraer adeptos y expandir la esfera criminal (INCIBE, 2024).

4.4.4. Posibilidad de mitigación

Ante los ejemplos expresados en los puntos anteriores, cabría preguntarse qué consideraciones podrían tenerse en cuenta para prevenir situaciones similares o para prevenir su repetición.

En los casos de E. Snowden, Teixeira y Gromadziski (si se hubiera dado el caso), la aplicación del concepto *Zero Trust* tendría un efecto mitigador, ya que, aunque disponiendo de acceso de alto nivel (secreto o similar) no podría gestionar (ni conocer) información ajena a su campo de conocimiento. Además, el sistema de seguridad monitorizaría el uso que los analistas hacen sobre el sistema, que descargan o que imprimen en soporte físico, por lo que, en este sentido, la información, hoy en día, estaría más protegida. Por otro lado, aunque dependiente del ser humano, las barreras físicas y controles de seguridad (centinelas, vigilantes y medios de seguridad física) colaborarían tanto en la disuasión como en la perpetración de la actividad maliciosa.

En los siguientes casos, la realidad pudiera parecer más cruda, a pesar de existir una estrecha colaboración entre los organismos responsables de la ciberseguridad (y ciberdefensa) en España, una Red Nacional de Ciberseguridad y la amenaza, claramente detectada, los incidentes ocurrirán si no existe una concienciación en todos los niveles de la sociedad, especialmente en aquellos (personas e instituciones) con acceso a datos sensibles. Por suerte, como ha afirmado la Red SOC y los CERT de España, en colaboración con las agencias de los países amigos y aliados, son capaces de analizar y responder en corto espacio de tiempo, por lo que el impacto de estas situaciones se verá mitigada.

5. La inteligencia en las FAS

La instrucción 55/2021 del jefe de Estado Mayor de la Defensa (JEMAD), donde se desarrolla la estructura del EMAD, otorga al Centro de Inteligencia de las Fuerzas Armadas (CIFAS) la «responsabilidad de facilitar […] la inteligencia militar precisa para alertar sobre situaciones internacionales susceptibles de generar crisis que afecten a la Defensa Nacional, así como de prestar el apoyo necesario, en su ámbito, a las operaciones militares».

Por otro lado, la misma instrucción del JEMAD establece que el CIFAS dirigirá y coordinará los sistemas de inteligencia, vigilancia y reconocimiento (ISR) conjuntos, así como su explotación.

Para el desarrollo de la Función Conjunta Inteligencias, en marzo 2020, se desarrolla la Publicación Doctrinal Conjunta de Inteligencia (PDC{XE "PDC Publicación Doctrinal Conjunta"}-2), sirviendo de base de otras publicaciones de menor jerarquía, que contribuirán a conformar el cuerpo doctrinal de inteligencia completo.

Esta doctrina es coherente con la de la Alianza, pero teniendo muy en cuenta a las particularidades nacionales. Además de establecer doctrina, facilita las herramientas «para lograr consenso intelectual, moral y profesional entre los involucrados en la Inteligencia» y facilitar la adquisición de capacidades militares para lograr el éxito en el contexto actual de las operaciones y el adiestramiento/preparación de la fuerza.

De la misma forma, el documento establece que, en todos los escenarios, los sistemas CIS y las nuevas tecnologías serán fundamentales.

En este sentido, el aumento de las tecnologías digitales favorece la simplificación de procesos en las FAS, especialmente los relacionados con el proceso ISR, en conjunción con una adecuada infraestructura de red, formación de personal y sistemas de seguridad (Centro Conjunto de Desarrollo de Conceptos. CESEDEN, 2020b).

Para organizar las capacidades, recursos humanos, materiales y procedimentales en el cometido de obtención de información y su transformación en inteligencia (útil) para los decisores, el JEMAD emite la Directiva 02/2021, donde se desarrolla la estructura del SIFAS.

En este capítulo se expondrá la doctrina de referencia tanto nacional como la OTAN en lo que respecta a los procesos inherentes al Ciclo de Inteligencia y al Programa de Obtención (PROB{XE "PROB Programa de Obtención"}), con objeto de tratar de establecer qué fases son más susceptibles de ser explotadas por las nuevas innovaciones tecnológicas.

Adicionalmente, se tratará la organización de inteligencia de las FAS, en general y la de la Armada, en particular. El objeto será ver como deberá interconectarse la infraestructura de red, desde un punto de vista general, sin entrar en detalles técnicos.

Finalmente, se realizará una aproximación a la Armada por su especificidad, al no disponer en sus despliegues de las mismas capacidades que en TN (por ejemplo, conexión de banda ancha).

5.1. El ciclo de inteligencia. El programa de obtención

De acuerdo con lo expuesto en la PDC-2, el ciclo de inteligencia es «la secuencia de actividades en la que, tras determinar las necesidades de Inteligencia, se obtiene información, se analiza y se transforma en Inteligencia para ponerla a disposición de quien la necesite». Este ciclo, gira en torno a cuatro actividades fundamentales: dirección, obtención, análisis y difusión.

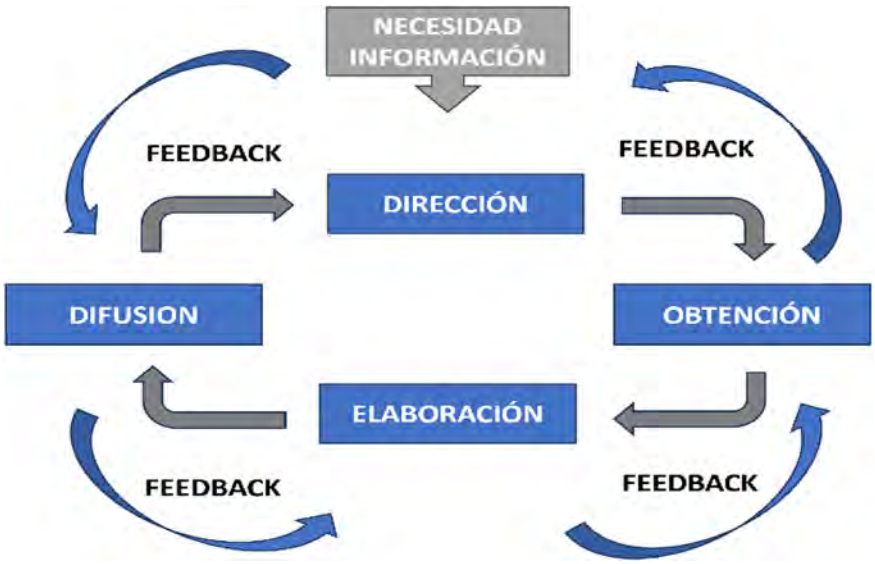

Figura 5. Ciclo de inteligencia. Aunque el ciclo de inteligencia se representa de forma «circular y cíclica», no es una herramienta lineal, sino que se trata de un conjunto de tareas que se superponen y se ejecutan simultáneamente, operando en distintos niveles y a distintas velocidades. Fuente: elaboración propia, en base a la Publicación Conjunta Inteligencia (PDC-2)

La función del ciclo es permitir que el proceso de producción de inteligencia este en permanente revisión, de forma que pueda llegar a los decisores en el momento oportuno. El ciclo, en opiniones de algunos expertos (Greciano, 2016), adolece de problemas, principalmente por basarse en «solucionar problemas de forma lineal», por el hecho de tomar el ciclo como un proceso secuencial y ordenado, desde la que se crea la necesidad (en la dirección) hasta su difusión.

En este sentido, Greciano (2016) asocia el fallo a considerar los procesos cognitivos de la mente humana. Destaca que la mente humana salta de una fase a la otra del ciclo, por lo que realmente no se trata de un proceso lineal.

Sin embargo, tanto la OTAN como la PDC-2, reseñan que no se trata de un proceso simple, sino que más bien se trata de un conjunto de tareas que se ejecutan simultáneamente y que a menudo de superponen, todas operando en distintos niveles y a distintas velocidades.

5.1.1. Procesos del ciclo de inteligencia

Teniendo en cuenta las distintas fases del ciclo, y sin entrar en consideraciones sobre cuál de ellas es la más importante, es en la fase de dirección donde se establecen las prioridades hacia las que orientar el esfuerzo de inteligencia, estableciendo los objetivos de interés de inteligencia. A su vez, se definirán las áreas y temas de interés de inteligencia, estableciendo las necesidades prioritarias de inteligencia (NPI o PIR), entre otras.

Una vez obtenidas las NPI, estas servirán de base para la confección del PROB.

– PROB, NPI, SIR y EEI

El PROB es un documento de trabajo de los órganos de inteligencia donde se plasma, de forma esquemática las necesidades de información y la forma en las que se van a acometer.

Las NPI son, de manera general, preguntas clave formuladas por el comandante con apoyo del personal de inteligencia e irán dirigidas a tomar una decisión que contribuya al éxito de la misión. Deben estar coordinadas, ser coherentes y complementarias con

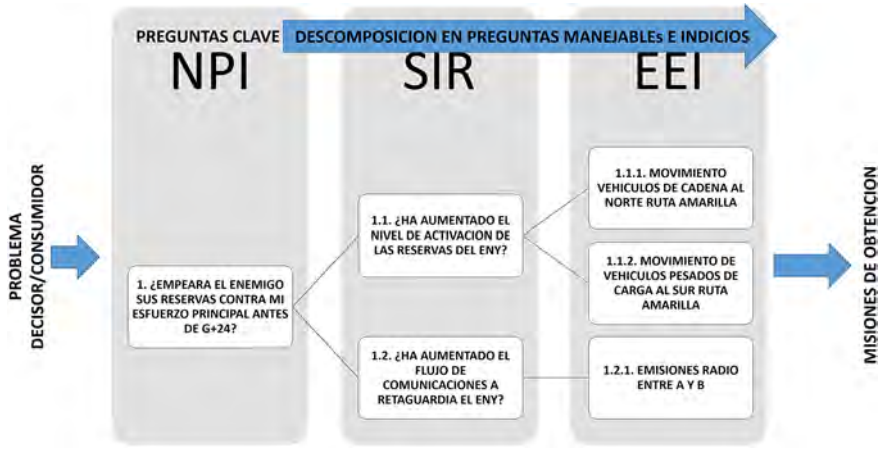

Figura 6. Generalidades PROB. Fuente: elaboración propia

las de los escalones superiores e inferiores, además de no ser excesivas en número.

Las NPI, debido a su complejidad, se desglosarán en Necesidades Específicas de Inteligencia (SIR{XE "SIR Necesidades Específicas de Inteligencia"}) y estas a su vez en Elementos Esenciales de Información (EEI{XE "EEI Elementos Esenciales de Información"}). Unas para orientar el esfuerzo de obtención y las otras, más específicas, para crear los cometidos de obtención, el medio y realizar las coordinaciones necesarias.

– Subproceso IRM (Intelligence Requirements Management)

El ciclo de inteligencia podría desgranarse en varios procesos en los que se observarían distintos flujos de información, cumpliéndose igualmente lo expuesto para el ciclo como un «conjunto de tareas que se ejecutan simultáneamente y que a menudo de superponen, todas operando en distintos niveles y a distintas velocidades».

En este subproceso se resolverían las necesidades de inteligencia a través de la consulta en bases de datos propias o de unidades adyacentes/superiores.

– Subproceso CM-CRM (Collection Management)

Cuando la IR (Intelligence Requeriments) no se puede responder con la información disponible, ya sea en base de datos propia o en la de otras unidades, se procede a gestionar, mediante otros medios/disciplinas, su obtención. Para la necesidad de gestionar la obtención, hay que comprender que los medios que se emplean para ella, normalmente, son también requeridos para actividades operativas, por lo que sea necesario priorizar, coordinar y *deconflictar* en muchos de los casos.

– Subproceso JISR (Inteligencia, Vigilancia y Reconocimiento Conjunto)

El proceso JISR busca dar respuesta a todas las necesidades de inteligencia, tanto en el planeamiento como en la conducción de operaciones. De la misma forma, alimenta las bases de datos continuamente, siendo lo suficientemente flexible como para actuar en todo el espectro del conflicto.

Como parte de su proceso, se lleva a cabo la explotación primaria de los datos recogidos por los sensores en tiempo real, proporcionando apoyo a las operaciones o a la toma de decisiones. Esto

le confiere la capacidad de explotar información de oportunidad, poniéndolas inmediatamente a disposición de los decisores.

Idealmente, este proceso busca la máxima eficiencia de medios, pero la realidad es que, en cualquier situación, especialmente en conflictos armados, los medios son finitos y, generalmente, escasos, necesitándose tanto de coordinación como de priorización, llegando a quedar, en algunos casos, necesidades sin cubrir.

5.2. Organización de la inteligencia en las FAS. SIFAS

El primer precepto que hay que tener en cuenta cuando se habla de inteligencia en las Fuerzas Armadas es que la inteligencia es única, tanto en el planeamiento como en la ejecución y en todos los niveles de las operaciones: el estratégico el operacional y en el táctico.

En España, el JEMAD regula en su Directiva 02/21, que será el SIFAS quien ejecutará lo especificado en el párrafo anterior.

Su principal misión será:

> «Satisfacer de forma oportuna las necesidades de información e inteligencia militar de las Autoridades Militares, con objeto de contribuir eficazmente al planeamiento de la Defensa, la preparación de la Fuerza, el planeamiento y la conducción de las operaciones y ejercicios, la valoración de las amenazas presentes y emergentes, así como la toma de decisiones en el ámbito de las FAS, tanto en tiempo de paz como en crisis o conflicto».

Teniendo en cuenta lo anterior. Es necesario disponer de un conjunto de medios, personas y procedimientos, para regular y emplear la capacidad de inteligencia las FAS, así como colaborar con otros organismos y agencias.

Dispondrá de un órgano de dirección que será el CIFAS, disponiendo de todos los recursos y subdirecciones del propio CIFAS en el nivel superior de ejecución.

El escalón intermedio estará compuesto por los Ejércitos y la Armada, además de los Mandos Conjuntos, el Mando de Operaciones Especiales, el Mando Conjunto de Ciberespacio, así como los subsistemas específicos asignados para sus misiones.

En el nivel básico, se dispone de los órganos de inteligencia y CI de los EEMM y Planas de las Grandes Unidades o Fuerzas Conjuntas,

además de los recursos que aporten las unidades orgánicas en el desempeño de sus misiones en el nivel ejecución.

Todo este sistema deberá disponer del *software* y *hardware* adecuado que facilite su función desde el punto de vista de las comunicaciones (CIS) y la gestión de la información obtenida.

5.2.1. I3D y sistemas C2 nacional

En el 2019, el JEMAD expresó la necesidad de que se dispusiera de un sistema CIS para ejercer el Mando y Control resiliente y seguro. Hasta entonces, los distintos actores del SIFAS disponían de distintas redes clasificadas sin integrar, lo que aumentaba la dificultad en la ejecución en la transmisión de la información (CESTIC, 2022).

De esta forma, se trabajó en la nueva Infraestructura integral de la Información para la Defensa (I3D{XE "I3D Infraestructura integral de la Información para la Defensa"}) y en el Sistema de Mando y Control Nacional (SC2N{XE "SC2N Sistema de Mando y Control Nacional"}), un sistema que permitiría realizar el planeamiento y la conducción de operaciones de la Fuerza Conjunta (FC{XE "FC Fuerza Conjunta"}). Además, permitiría la transmisión de información y la coordinación, en todas las situaciones, con otras organizaciones tanto nacionales como internacionales, incluyendo los ámbitos del ciberespacio y la inteligencia militar. (Pita da Veiga Subirats, 2021).

El JEMAD, en 2022, comunicó Capacidad Operativa Inicial (IOC{XE "IOC Capacidad Operativa Inicial"}) de la SC2N (figura 18), consistiendo en la validación de *hardware*, *software*, personal y procedimientos, participando de ello tanto las FAS como el CESTIC (CESTIC, 2022).

Finalmente, tras llevar a cabo el proceso de certificación, en julio de 2023, la secretaria de Estado de Defensa certificó que la I3D había alcanzado la IOC. La I3D está prevista que continúe su evolución, adaptándose a los Objetivos de Capacidades Militares (OCM{XE "OCM Objetivos de Capacidades Militares"}) para 2024-2029 y futuro, asegurando la evolución tecnológica. (CESTIC, 2023)

El SC2N, como parte del proceso de Transformación Digital, constituye el núcleo protegido de la I3D, incorpora tecnologías de nube privada y dispone de medidas de ciberseguridad para gestionar información clasificada (CESTIC, 2022).

En los ámbitos de mejora de esta red, se incluye el lanzamiento de dos satélites, de tecnología dual, que amplificaran la capacidad de banda ancha de las comunicaciones militares (Banda X y Ka), siendo una novedad y un salto cualitativo la posibilidad de emplear UHF. (Dubois, 2023). Este conjunto de satélites, mejorarán tanto la cobertura como la capacidad de transmisión en despliegues. Estas transmisiones, aunque aumentadas, es necesario relativizarlas con las posibilidades que ofrecen las redes en TN (Ministerio de Hacienda, 2019).

5.2.2. Gestión de la inteligencia

La transformación digital también alcanza a la gestión de inteligencia que se realiza a través de todos los órganos del SIFAS, empleando para ello todas las disciplinas de obtención de inteligencia.

En los últimos años, se han producido avances en la adquisición de equipos y *software* para la mejora de la función de inteligencia, así, por ejemplo: en lo referente a SIGINT (Inteligencia de Señales), Defensa invertirá más de 300 millones de euros para la actualización del Sistema Santiago. El objetivo de este sistema es obtener información en las áreas de interés estratégica de España, mediante el empleo de plataformas de los Ejércitos y la Armada capaces de obtener señales de comunicaciones y electrónica (InfoDefensa, 2024). Por otro lado, busca potenciar la independencia tecnológica nacional, lo que se encuentra en línea con las principales estrategias citadas en el primer capítulo.

En lo referido a ACINT (Inteligencia Acústica), la nueva clase de submarinos S-80+ mejorarán las capacidades que ofrecían la clase S-70.

No obstante, a pesar de las mejoras de las disciplinas, la PDC-2 remarca que es combinando la información de diversas disciplinas, integrándola y analizándola en conjunto (concepto de multisensor), cuando el analista obtiene un producto más completo y fiable.

Sobre el OSINT (Inteligencia de fuentes abiertas), la inmensidad de datos disponibles en la red, el acceso a satélites comerciales y la posibilidad de acceso a la red de forma discreta hacen de esta disciplina clásica una fuente imprescindible para la conducción de las operaciones militares en cualquiera de sus niveles (político, estratégico, operacional y táctico) (NATO, 2023b). En cualquiera

de los conflictos actuales se ha podido observar cómo gobiernos y particulares emplean esta disciplina para anticiparse, para confirmar, desmentir o atribuir ataques (Hockenhull, 2022).

A pesar de todas las innovaciones tecnológicas, es importante señalar que la información obtenida por fuentes humanas o personas (HUMINT) continúa siendo muy valorada y, por ello, siempre dispone de una protección especial.

Un ser humano capta detalles, emociones y sensaciones que un sensor o IA es incapaz de captar (hoy en día), pero también las fuentes humanas son susceptibles a sus propios sesgos o a la influencia externa, razón por la cual debe ser evaluada por un operador cualificado (Valero, 2016).

En cuanto a la integración, la evolución tecnológica ha permitido adquirir herramientas para la integración de inteligencia de múltiples fuentes y sensores, así como para realizar un análisis casi inmediato.

En actual campo de batalla *saturado de datos*, las capacidades de los analistas se pueden ver superadas, necesitándose formación en nuevas herramientas y metodologías para manejar esas grandes cantidades de información.

El 16 de octubre 2023 se publicó en el BOD la adquisición del *software* Palanthir Gothan, como sistema de fusión de inteligencia para el CIFAS. Este sistema permite acelerar los procesos de análisis de inteligencia y de toma de decisiones, basados en un complejo sistema de análisis de bases de datos (Ministerio de Hacienda, 2023a). El empleo de datos e información fiable son fundamentales para el correcto funcionamiento del *software*.

En el campo del adiestramiento y formación, se resalta la importancia urgente y crucial de potenciar la inteligencia, en todos los niveles, con la posibilidad de la creación de un cuerpo único que atienda las necesidades conjuntas (Sanchez de Toca Alameda *et al*., 2023). En otro sentido, se reconoce la necesidad de potenciar la capacidad de inteligencia en las estructuras orgánicas, mejorando de esta forma la inteligencia de preparación (Albadalejo López, 2023).

6. Conclusiones

El mundo avanza a pasos agigantados hacia un entorno tecnológico complejo, en el que es necesario mantenerse actuali-

zado, llevando a cabo una inversión cada vez más acentuada en tecnología.

En lo que respecta al plano militar, no mantenerse actualizado tecnológicamente, puede significar no solo caer en la irrelevancia, sino también poner en peligro la seguridad nacional. De los documentos estratégicos expuestos, se podría afirmar que, *sí existe una necesidad de continuar y potenciar con la inversión en innovaciones* aplicadas a defensa.

Se observa a la función inteligencia como un conjunto de procesos, destacando su propio ciclo, gobierna y engloba a los demás. Las innovaciones tecnológicas tienen cabida en estos procesos facilitando el acceso, gestión y difusión de la información. Sin embargo, ni en las estrategias ni en los documentos consultados se observa la necesidad de un cambio doctrinal.

Al entender el ciclo de inteligencia como un marco conceptual, las tecnologías de gestión de datos por IA, sistemas de fusión de inteligencia y comunicaciones de banda ancha acelerarán el ciclo donde, en algunos casos, se superpondrán sus fases y en otros se realizarán de una manera más o menos ágil, pero en el fondo no cambiarán la doctrina. Según lo expuesto a lo que se tiende con la tecnología, es acelerar los procesos y facilitar el trabajo a los analistas, en ningún caso a sustituirlos totalmente.

Por otro lado, si se observa que las tecnologías pueden provocar cambios en la gestión de procesos en inteligencia, al tener la capacidad de ofrecer mayor conectividad, velocidad y acceso a respuestas automatizadas.

Del PROB se observa que sus elementos (IR) se asemejan a *prompts* que una IA, con la programación y adiestramiento adecuado, podría estar en condiciones de responder de forma automática, bien a través de la búsqueda de información en BB. DD. existentes o, si se desconoce, emitiendo IR o generando necesidades de obtención de forma autónoma.

Resulta interesante añadir que la saturación de elementos inteligentes en el campo de batalla (IoMTs), no específicos de inteligencia, supondrán un valor añadido para la respuesta automática al PROB y dotando de mayor SA a los comandantes. Tal será la cantidad de datos aportados, que un analista humano sería incapaz de procesarlos sin la asistencia de la tecnología apropiada.

De esta forma, el PROB parece que no cambiará en el fondo, pero sí se facilitarán sus procesos internos, mejorará el asesoramiento

o se automatizará en ciertos aspectos. Por lo tanto, *se producirá un cambio en la forma de gestionar la inteligencia* debido a la innovación, como los siguientes:

- Será necesario tener en cuenta todos los sensores desplegados, así como efectuar las preguntas (*prompt*) concretas a la IA para responder las necesidades de información.
- Será necesario disponer de personal con el conocimiento adecuado para elaborar los *prompt* y corroborar las respuestas.
- Será necesario llevar a cabo una adecuada gestión del dato para obtener una mayor fiabilidad de las respuestas de la IA.
- Será necesario haber llevado a cabo un aprendizaje de la IA para minimizar las respuestas erróneas o sesgadas.
- Será necesario mantener la supervisión final humana, realizando los procesos finales del análisis y valoración, tratando de identificar respuestas erróneas o sesgadas de la IA y dándole la correspondiente retroalimentación. Al fin y al cabo, la tecnología seguirá teniendo *corazón y mente humana.*

En cualquier caso, estos procesos tendrán que adaptarse a las capacidades tecnológicas que se dispongan y al momento de la operación.

Aunque la tecnología puede que sea el eje central de la recopilación de la información, disciplinas clásicas como *HUMINT* no podrán ser sustituidas por elementos tecnológicos, ya que sus operadores son capaces de detectar, analizar o, incluso, intuir sentimientos, palpitaciones y otros patrones de conducta típicamente humanos que una máquina, aún, no puede apreciar.

Sobre la disciplina OSINT, y debido a la capacidad de acceso a datos de todo tipo, será necesario dedicar recursos a detectar la información maliciosa o *fake* procedente de fuentes no seguras, así como pensar el nivel de automatismo que se quiera delegar en sus herramientas.

Por lo anterior, estas disciplinas clásicas *no solo no desaparecerán, sino que se verán potenciadas, no solo por* valerse de sí mismas para acceder a información sino también por servir para verificar/apoyar otras fuentes tecnológicas.

De forma general, pero especialmente en las FAS, las organizaciones de ciberseguridad *tendrán que potenciar personal y medios*. El aumento de la superficie de exposición, redes 5G, IoMTs, servidores y demás tecnología de la comunicación supone un aumento del riesgo.

Por otro lado, año tras año se constata el aumento de los ciberataques contra las instituciones públicas y particulares relacionados con ellas, por lo que no solo se debe de aumentar las plantillas y presupuestos si no también *mejorar en la coordinación ante la respuesta a los ciberincidentes.*

Dada la evolución al alza de los ciberataques y la transposición a la NIS2, pudiera ser de interés llevar a cabo la revisión del actual modelo de cibergobernanza hacia un modelo más centralizado, con *objeto de ser más rápidos, ágiles y eficaces.* En este sentido, disponer de una red nacional de SOC de gestión centralizada sería esencial en el contexto actual de la ciberseguridad. Esta centralización permitiría una respuesta rápida, eficaz y coordinada ante amenazas cibernéticas, así como una mayor eficiencia en la detección y mitigación de incidentes.

Además, es muy necesario emplear métodos de cifras eficientes y con alto grado de soberanía digital para garantizar la seguridad y privacidad de la información en un entorno cada vez más digitalizado.

Finalmente, y aun contando con la mejor de las tecnologías, deberá realizarse un *mayor esfuerzo en concienciación y adiestramiento,* especialmente en aquellas organizaciones con información y sistemas críticos o sensibles.

En esta línea, la *aplicación correcta del concepto Zero Trust* será de gran utilidad, aunque ello suponga una incomodidad necesaria, asumiendo que ningún usuario puede ser confiable por defecto y obligando a validar continuamente la autenticidad y autorización. Este enfoque proactivo, basado en la segmentación y el cifrado de extremo a extremo, es fundamental para prevenir fugas de información, ya sea por métodos ajenos o a través de *insiders*.

En este sentido, la IA mejorará la supervisión de los patrones inusuales del personal conectado a la red, generando avisos a los supervisores del sistema o simplemente cortando el acceso ante acciones de dudosa reputación.

Sobre asumir el *cambio tecnológico*, aun existiendo *cierta resistencia al cambio*, se considera que *será irrelevante,* por dos motivos principales: primero, el impulso a la tecnología viene desde los más altos escalones del liderazgo tanto civil como militar y, segundo, el cambio generacional natural hace que se vaya imponiendo más tarde o más temprano.

Aun así, de acuerdo con el modelo de Rogers, existe el riesgo de que, en escalones intermedios, la diferencia generacional genere interferencias importantes en el proceso de TD en las FAS.

Así, algunas de las estrategias para disminuir este riesgo serán:

- El conocimiento, explicar adecuadamente la necesidad fundamental de la organización. La enseñanza formaría parte de esta estrategia, por lo que expandir la TD a la enseñanza militar y la capacitación en tecnologías digitales facilitaría la tarea.
- El liderazgo, solo a través del impulso de la cadena alta del escalafón se podrá cambiar la percepción en el grueso de la curva de Gauss, acercando el punto de cambio hacia los *early adopters*.

Avanzando en la propia tecnología, también se podrá reducir esa caja negra hasta llegar a un modelo de inteligencia artificial explicable donde se pueda entender la forma de procesar.

En definitiva, en lo concerniente a la toma de decisiones y asesoramiento, la tecnología se encuentra *desarrollada a un nivel que puede acelerar multitud de procesos relacionados con la toma de decisiones y el apoyo a la inteligencia, por lo que sí es (y será) una herramienta fundamental del apoyo al mando*, sin embargo, sobre la toma de *decisiones autónoma***,** es muy probable que *NO se implemente la capacidad,* al menos, en la mayoría de las naciones occidentales. En esta línea, la decisión adoptada es apostar por *una IA ética, transparente y supervisada*, en mayor o menor medida, por operadores humanos, una vez más *la tecnología deberá tener corazón y mente humana.*

Bibliografía

Alarcón, N. (2024). La Comisión Europea pide reforzar el control de inversiones extranjeras en sectores críticos [en línea]. El Confidencial. [Consulta: 20 febrero 2024]. Disponible en: https://www.elconfidencial.com/economia/2024-01-24/bruselas-inversiones-extranjeras-sectores-criticos-control_3817029/

Albadalejo López, J. (2023). Inteligencia de preparación: realismo y responsabilidad. Cuadernos de Inteligencia. Madrid, Ministerio de Defensa, CESEDEN, pp. 27-37.

Álvarez, S. (2022). Nube de combate o nube táctica, el futuro de la defensa ya está aquí [en línea]. Grupo Oesía. [Consulta:

1 abril 2024]. Disponible en: https://es.linkedin.com/pulse/nube-de-combate-o-t%C3%A1ctica-el-futuro-la-defensa-ya-est%C3%A1-aqu%C3%AD-oesia

Antebi, L. (2021). Artificial Intelligence and National Security in Israel [en línea]. Memorandum. The Institute for National Security Studies. [Consulta: 15 febrero 2024]. Disponible en: https://www.inss.org.il/publication/artificial-intelligence-and-national-security-in-israel/

ARMYSOS. (s. f.). Defense Mapping Software [en línea]. [Consulta: 3 mayo 2024]. Disponible en: https://armysos.com.ua/defense-mapping-software/

Baños Abril, D. (2023). La máquina universal de Turing [en línea]. La Máquina Oráculo. [Consulta: 8 abril 2024]. Disponible en: https://lamaquinaoraculo.com/ciencias-computacion/la-maquina-de-turing/

Bellione, A. (2023). The Heart of decission Superiority. Evolve or Lose – Why Your Next War May Be Won or Lost in Seconds. *The Journal of the Joint Air Power Competence Centre* (JAPCC). 36, pp. 60-69.

Candau, J. y Loste, M. (2023). Conferencia magistral Actividad [en línea]. [Consulta: 27 diciembre 2023]. Disponible en: https://www.youtube.com/watch?app=desktop&v=ZdCvYXhKqi0&list=PLIZWmGs0YDodhOA5p2VFgJiUh-X5jLkQc&index=2

Carl, N. (2023). Iran Update Special Edition [en línea]. Institute for the Estudy of War. [Consulta: 2025]. Disponible en: https://www.understandingwar.org/backgrounder/iran-update-special-edition-october-7-2023

Catalá Lloret, J. (2022). Retos de la Inteligencia Artificial aplicada a la Defensa. DGAM [en línea]. Ministerio de Defensa, Dirección General de Armamento y Material. [Consulta: 20 diciembre 2023]. Disponible en: https://blogs.upm.es/wp-content/uploads/sites/580/2022/07/CV2022.S03P01.Catala.pdf

Centro Conjunto de Desarrollo de Conceptos (CESEDEN). (2020a). *Nota Conceptual "Opearciones Multidominio"*. Madrid, Ministerio de Defensa.

Centro Conjunto de Desarrollo de Conceptos (CESEDEN). (2020b). *Usos Militares de la Inteligencia Artificial, la automatización y la robótica*. Madrid, Ministerio de Defensa.

Centro Criptológico Nacional. (2023a). *Aproximación a la inteligencia Artificial y a la Ciberseguridad. Informe de Buenas*

Prácticas. Ministerio de Defensa, Centro Criptológico Nacional. [Consulta: 14 abril 2024]. Disponible en: https://ens.ccn.cni.es/es/

Centro Criptológico Nacional. (2023b). *Ciber_Amenazas y Tendencias. IA-35/23* [en línea]. Ministerio de Defensa, Centro Criptológico Nacional. [Consulta: 2 febrero 2024]. Disponible en: https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7188-ccn-cert-ia-35-23-ciberamenazas-y-tendencias-edicion-2023/file.html

CESEDEN. (2022). Entorno Operativo 2035. Primera Revisión [en línea]. Ministerio de Defensa, Secretaría General Técnica. [Consulta: 2025]. Disponible en: https://publicaciones.defensa.gob.es/entorno-operativo-2035-primera-revision-libros-papel.html

CESTIC. (2022). *Declaración de la capacidad operativa inicial del sistema de mando y control nacional* [en línea]. Ministerio de Defensa, CESTIC. [Consulta: 15 diciembre 2023]. Disponible en: https://www.defensa.gob.es/cestic/noticias/2022/listado/noticia12.html

CESTIC. (2023). Un hito más: La I3D, operativa [en línea]. Ministerio de Defensa, CESTIC. [Consulta: 15 diciembre 2023]. Disponible en: https://www.defensa.gob.es/cestic/noticias/2023/listado/noticia1.html

Chudleigh, S. (2023). ¿Qué es la IA conversacional? Una inmersión profunda en el futuro de la comunicación [en línea]. *Botpress*. [Consulta: 10 abril 2024]. Disponible en: https://botpress.com/es/blog/what-is-conversational-ai-a-deep-dive-into-the-future-of-communication

CNN. (2023). *Bienvenida a las XVII Jornadas STIC CCN-CERT | V Jornadas de CIberdefensa ESPDEF-CERT*. [Consulta: 20 febrero 2024]. Disponible en: https://www.youtube.com/watch?v=SFF6wmXpMgA

Colom Piella, G., 2021. El planeamiento de la defensa en España. Navegando hacia el horizonte 2035 con una pesada mochila. *Documento de Opinión*. Ministerio de Defensa, Instituto Español de Estudios Estratégicos. 121. [Consulta: 31 enero 2024]. Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2021/DIEEEO121_2021_GUICOL_Planeamiento.pdf

Consejo de la Unión Europea. (2023). Reglamento de Inteligencia Artificial: el Consejo y el Parlamento alcanzan un acuerdo so-

bre las primeras normas del mundo en materia de inteligencia artificial [en línea]. Consejo Europeo. [Consulta: 20 diciembre 2023]. Disponible en: https://www.consilium.europa.eu/es/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/

Dagan, A. (2022). *The IDF's New Information and AI Strategy* [en línea]. [Consulta: 15 febrero 2024]. Disponible en: https://www.youtube.com/watch?v=THNvQgQh9v4

DARPA. (2021). XAI: Explainable Artificial Intelligence [en línea]. *DARPA*. [Consulta: 10 abril 2024]. Disponible en: https://www.darpa.mil/program/explainable-artificial-intelligence

De Spiegeleire, S., Maas, M. y Sweijs, T. (2017). *Artificial Intelligence and the Future of Defense. Strategic Implications for Small –And Medium–Sized Force Providers* [en línea]. The Hague Centre for Strategic Studies. [Consulta: 15 febrero 2024]. Disponible en: https://hcss.nl/wp-content/uploads/attachments/Artificial%20Intelligence%20and%20the%20Future%20of%20Defense-7.pdf

Departamento de Seguridad Nacional. (2019). Estrategia de Ciberseguridad Nacional [en línea]. Gobierno de España, DSN. [Consulta: 2025]. Disponible en: https://www.dsn.gob.es/

Departamento de Seguridad Nacional. (2021). Estrategia de Seguridad Nacional 2021 [en línea]. Gobierno de España, DSN. [Consulta: 2025]. Disponible en: https://www.dsn.gob.es/es/publicaciones/estrategia-de-seguridad-nacional

Department of Defense. (2023). *Data, Analytic, and Artificial Intelligence Adoption Strategy. Acelerating Decision Advantage* [en línea]. Department of Defense, Office of Prepublication and Security Review. [Consulta: 2 mayo 2024]. Disponible en: https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF

Di Santo, A. (2024). Aumentan en un 190 % los ciberataques al sector público español en 2024 [en línea]. *Escudo Digital*. [Consulta: 2 mayo 2024]. Disponible en: https://www.escudodigital.com/ciberseguridad/aumentan-en-190-ciberataques-sector-publico-espanol-en-2024_58476_102.html

Díaz-Caneja Greciano, J. M. (2016). Campos de actuación de la inteligencia. En: Instituto Español de Estudios Estratégicos (ed.). *Inteligencia. Un enfoque integral*. Madrid, Ministerio de Defensa, pp. 77-109.

Dubois, G. (2023). España comenzó a construir su próxima generación de satélites de comunicaciones seguras Spainsat NG [en línea]. *AviacionLine*. [Consulta:18 diciembre 2023]. Disponible en: https://www.aviacionline.com/espana-comenzo-a-construir-su-proxima-generacion-de-satelites-de-comunicaciones-seguras-spainsat-ng

EC/Agencias. (2021). Una vuelta de tuerca al caso de espionaje de EE. UU. a Merkel implica a Dinamarca [en línea]. *El Confidencial*. [Consulta: 21 febrero 2024]. Disponible en: https://www.elconfidencial.com/mundo/europa/2021-05-31/una-vuelta-de-tuerca-de-al-caso-de-espionaje-de-eeuu-a-alemania-implica-a-dinamarca_3108303/

Efe (2024). Destituido e investigado por espionaje el general polaco al mando del Eurocuerpo [en línea]. *El Mundo*. [Consulta: 2 mayo 2024]. Disponible en: https://www.elmundo.es/internacional/2024/03/27/6604576fe9cf4a82378b4583.html

Ejército de Tierra. (2018). Un nuevo concepto de mando y control [en línea]. Ministerio de Defensa, Ejército de Tierra. [Consulta: 1 abril 2024]. Disponible en: https://ejercito.defensa.gob.es/reportajes/2018/70_briex2035.html

El-Hadi, M. (2022). Artificial Intelligence vs. Machine Learning vs. Deep learning. What is the Difference? [en línea]. JSTC Journal. 29(29), pp. 82-84. [Consulta: 2 mayo 2024]. Disponible en: https://jstc.journals.ekb.eg/article_274483_a5ef67646456c9d9ddd5a7bd37c18990.pdf

Esquema Nacional de Seguridad (ENS) [en línea]. (s. f.). Ministerio de Defensa, CCN. [Consulta: 17 abril 2024]. Disponible en: https://ens.ccn.cni.es/es/

Estado Mayor de la Defensa (EMAD). 2024. El jefe de Estado Mayor de la Defensa firma un convenio de colaboración entre el EMAD y telefónica [en línea]. Ministerio de Defensa, EMAD. [Consulta: 20 febrero 2024]. Disponible en: https://emad.defensa.gob.es/prensa/noticias/2024/02/Listado/240213-ni-firma-convenio-telefonica.html

Estado Mayor de la Defensa (EMAD). 2024. Mando conjunto del ciberespacio (MCCE) [en línea]. Ministerio de Defensa, Estado Mayor de la Defensa. [Consulta: 25 febero 2024]. Disponible en: https://emad.defensa.gob.es/unidades/mcce/

Esteller, R. (2024). La UE impone un escudo económico para defenderse de China y Rusia [en línea]. *El Economista*. [Consulta: 20 febrero 2024]. Disponible en: https://www.eleconomista.

es/economia/noticias/12637822/01/24/la-ue-impone-un-escudo-economico-para-defenderse-de-china-y-rusia.html

Faba de la Encarnación, E. y Simón Canal, T. (s. f.). Soberania Digital, ¿un problema normativo o un problema geopolítico? [en línea]. Ministerio de Industria y Turismo. [Consulta: 20 febrero 2024]. Disponible en: https://www.mintur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/427/ELENA%20FABA%20Y%20TOMAS%20SIMON.pdf

Fernandez, O. (2023). Data Lake: Definición y Tecnologías [en línea]. *Aprender Big Data*. [Consulta: 5 febrero 2024]. Disponible en: https://aprenderbigdata.com/data-lake/

García Méndez, A. (2024). Una brecha de seguridad pone en peligro los datos de personal de las Fuerzas Armadas [en línea]. *ADSL Zone*. [Consulta: 2 mayo 2024]. Disponible en: https://www.adslzone.net/noticias/seguridad/brecha-seguridad-datos-fuerzas-armadas/

Garrido García, F. J. (2023). 5G: Aplicacion de las comunicaciones móviles en el ámbito de la Defensa [en línea]. Ministerio de Defensa, Armada. [Consulta: 1 abril 2024]. Disponible en: https://armada.defensa.gob.es/archivo/rgm/2023/01-02/rgmenefeb2023_Parte07.pdf

Gil Clemente, J. (2022). Efectos de la transformación digital en la Armada. [en línea]. Ministerio de Defensa, Armada. [Consulta: 20 marzo 2024]. Disponible en: https://armada.defensa.gob.es/archivo/rgm/2022/07/rgmjul2022cap09.pdf

GMV. (2024). Suite de herramientas JISR SAPIIEM. GMV innovating solutions. [Consulta: 20 marzo 2024]. Disponible en: https://www.gmv.com/es-es/productos/defensa-y-seguridad/sapiiem-jisr-suite#suite-de-herramientas-jisr-sapiiem

Gobierno de España. (2022). Publicada la Directiva NIS2 relativa a medidas de ciberseguridad [en línea]. Portal Administración Electrónica. [Consulta: 26 febrero 2024]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2023/Enero/Noticia-2023-01-09-Publicada-la-Directiva-NIS2-relativa-a-medidas-de-ciberseguridad.html

Gobierno de España. (2023). Quantum Spain: el primer ordenador cuántico del sur de Europa [en línea]. Plan de Recuperacion, Transformacion y Resiliencia. [Consulta: 25 febrero 2024]. Disponible en: https://planderecuperacion.gob.es/no-

ticias/quantum-spain-el-primer-ordenador-cuantico-del-sur-de-europa

Goldfarb, A. y Lindsay, J. R. (2022). Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War. *International Security*. 46(3), pp. 7-50.

Gómez, E. (2022). Diferencia entre machine learning y deep learning [en línea]. *Tecnología ++*. Universitat Oberta de Catalunya. [Consulta: 9 abril 2024]. Disponible en: https://blogs.uoc.edu/informatica/es/machine-learning-vs-deep-learning-diferencias/

Greenwood, F. (2023). The Drone War in Ukraine Is Cheap, Deadly, and Made in China [en línea]. Foreign Policy Magazine. [Consulta: 3 mayo 2024]. Disponible en: https://foreignpolicy.com/2023/02/16/ukraine-russia-war-drone-warfare-china/

Hindlekar, S. (2024). Understanding AI prompts: A comprehensive guide [en línea]. [Consulta: 3 mayo 2024]. Disponible en: https://www.promptworld.in/post/understanding-ai-prompts-a-comprehensive-guide

Hockenhull, J. (2022). How open-source intelligence has shaped the Russia-Ukraine war [en línea]. GOV.UK. [Consulta: 3 mayo 2024]. Disponible en: https://www.gov.uk/government/speeches/how-open-source-intelligence-has-shaped-the-russia-ukraine-war

IBM. (2023). AI vs. Machine Learning vs. Deep Learning vs. Neural Networks: What's the difference? [en línea]. *IBM*. [Consulta: 2 mayo 2024]. Disponible en: https://www.ibm.com/blog/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks/

IBM. (s. f.) ¿Qué son las redes neuronales? [en línea]. *IBM*. [Consulta: 2 mayo 2024]. Disponible en: https://www.ibm.com/es-es/topics/neural-networks

IDF. (2023a). A glimpse of IDF's target factory that operates around the clock [en línea]. *IDF*. [Consulta: 3 mayo 2024]. Disponible en: https://www.idf.il/

IDF. (2023b). Dozens of ADANIM are operational for the first time [en línea]. *IDF*. [Consulta: 13 noviembre 2023]. Disponible en: https://www.idf.il/en/mini-sites/idf-press-releases-israel-at-war/november-23-pr/providing-intelligence-to-forces-operating-in-gaza-dozens-of-adanim-are-now-operational/

INCIBE. (2023). Metodología Zero Trust: fundamentos y beneficios [en línea]. Instituto Nacional de Ciberseguridad. [Consul-

ta: 25 febrero 2024]. Disponible en: https://www.incibe.es/incibe-cert/blog/metodologia-zero-trust-fundamentos-y-beneficios

INCIBE. (2024). LockBit: acciones de respuesta y recuperación [en línea]. Instituto Nacional de Ciberseguridad. [Consulta: 2 mayo 2024]. Disponible en: https://www.incibe.es/incibe-cert/blog/lockbit-acciones-de-respuesta-y-recuperacion

InfoDefensa. (2023). Epicom se hace con un contrato de 29 millones para blindar las comunicaciones de Defensa [en línea]. InfoDefensa.com. [Consulta: 28 diciembre 2023]. Disponible en: https://www.infodefensa.com/texto-diario/mostrar/4222225/epicom-hace-contrato-29-millones-blindar-comunicaciones-defensa

InfoDefensa. (2024). Defensa Relanza el programa de Inteligencia Santiago con una inyección de 300 millones [en línea]. InfoDefensa.com. [Consulta: 8 enero 2024]. Disponible en: https://www.infodefensa.com/texto-diario/mostrar/4290776/defensa-relanza-programa-inteligencia-santiago-inyeccion-300-millones

Jones, S. G., McCabe, R. y Palmer, A. (2023). Ukrainian Innovation in a War of Attrition [en línea]. Center for Strategic International Studies (CSIS). [Consulta: 3 mayo 2024]. Disponible en: https://www.csis.org/analysis/ukrainian-innovation-war-attrition

Krelina, M. y Dúbravčík, D. (2023). Quantum Technology for Defence. What to Expect for the Air and Space Domains [en línea]. *The Journal of the JAPCC*. [Consulta: 25 febrero 2024]. Disponible en: https://www.japcc.org/articles/quantum-technology-for-defence/

Lavigne, P. (2024). Mando Aliado de Transformación. *Revista Española de Defensa*. 37(412), pp. 54-57.

López, A. (2024). Todo sobre criptografía: Algoritmos de clave simétrica y asimétrica [en línea]. *Redes Zone*. [Consulta: 22 febrero 2024]. Disponible en: https://www.redeszone.net/tutoriales/seguridad/criptografia-algoritmos-clave-simetrica-asimetrica/

López, M. (2021). Roba ahora, descifra después: los atacantes que roban datos cifrados los almacenan a la espera de poder acceder a ellos con ordenadores cuánticos [en línea]. *Ataka*. [Consulta: 29 febrero 2024]. Disponible en: https://www.xataka.com/ordenadores/roba-ahora-descifra-despues-ata-

cantes-que-roban-datos-cifrados-almacenan-a-espera-poder-acceder-a-ellos-ordenadores-cuanticos

Martínez Millán, J. M. (2023). La tecnología debe tener corazón humano [Entrevista].

Martorell, A. (2022). *Líneas Generales de la Armada*.

Microsoft Threat Intelligence. (2022). An overview of Russia's cyberattack activity in Ukraine [en línea]. Microsoft. [Consulta: 3 mayo 2024]. Disponible en: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/special-report-ukraine

Mimran, T., Pacholska, M., Dahan, G. y Trabu, L. (2024). Israel – Hamas 2024 Symposium – Beyond the Headlines: Combat Deployment of Military AI-Based Systems by the IDF [en línea]. *Articles of War*. Lieber Institute. [Consulta: 3 mayo 2024]. Disponible en: https://lieber.westpoint.edu/beyond-headlines-combat-deployment-military-ai-based-systems-idf/

Ministerio de Defensa. (2024). Transformación Digital de las FAS para el combate multidominio. Madrid, Ministerio de Defensa. [Consulta: 1 abril 2024]. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/t/r/transformacion_digital_de_las_fas.pdf

Ministerio de Hacienda. (2019). SATCOM SPAINSAT NG renovación de la capacidad de comunicaciones por satélite de la actual constelación de satélites SAPINSAT y XTAR-EUR [en línea]. Ministerio de Hacienda, Plataforma Contratación del Estado. [Consulta: 28 diciembre 2023]. Disponible en: https://contrataciondelestado.es/wps/portal/!ut/p/b0/04_Sj9CPykssy0xPLMnMz0vMAfIjU1JTC3Iy87KtUlJLEnNyUuNzMpMzSxKTgQr0w_Wj9KMyU1zLcvQjgwxNzPyDfSvKnQtzC40MSysykhLDAm1t9Qtycx0BXiF6hA!!/

Ministerio de Hacienda. (2023a). Contratación sistema Fusión de Inteligencia [en línea]. Ministerio de Hacienda, Plataforma Contratación del Estado. [Consulta: 28 diciembre 2023]. Disponible en: https://contrataciondelestado.es/wps/portal/!ut/p/b0/04_Sj9CPykssy0xPLMnMz0vMAfIjU1JTC3Iy87KtUlJLEnNyUuNzMpMzSxKTgQr0w_Wj9KMyU1zLcvQjk4JK05LMMirygwyqspwzyk2qVA0iysptbfULcnMdASc0JyI!/

Ministerio de Hacienda. (2023b). Suministro de una red AD-HOC de alta capacidad aérea y nube táctica distribuida [en línea]. Ministerio de Hacienda. [Consulta: 28 diciembre 2024]. Dis-

ponible en: https://contrataciondelestado.es/wps/portal/!ut/p/b0/DcqxCoAgEADQT7rNIXBwkMCCoKHSJQ6VODrNQoT-vsY-HDxxs4DI2OrDSIZF_2xBjYcpnF2JF5rgzearo_wArOHAUd-GOwxty9EEWPw0TaPMt88_UqKaGkpD4OUGil/

Mishra, S. (2023). Zero Trust vs Full Trust [en línea]. [Consulta: 25 febrero 2024]. Disponible en: https://www.linkedin.com/pulse/zero-trust-vs-full-sourabh-mishra

Morales Trueba, A. (2023). La OTAN, la UE y la cooperación en el Desarrollo de Capacidades [en línea]. *Documento de Opinión*. Ministerio de Defensa, Instituto Español de Estudios Estratégicos. 21. [Consulta: 12 febrero 2024]. Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEEO21_2023_ADOMOR_Capacidades.pdf

National Security Agency/Central Security Service. (s. f.). Quantum Key Distribution (QKD) and Quantum Cryptography (QC) [en línea]. NSA. [Consulta: 26 diciembre 2023]. Disponible en: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

NATO. (2020). *Allied Joint Doctrine for Intelligence, Counter-Intelligence And Security. AJP-2 (Edition B, Version 1)*. NATO Standarization Office.

NATO. (2021). *Summary of the NATO Artificial Intelligence Strategy* [en línea]. [Consulta: 22 diciembre 2023]. Disponible en: https://www.nato.int/cps/en/natohq/official_texts_187617.htm

NATO. (2022). *NATO Strategic Concept* [en línea]. NATO. [Consulta: 12 febrero 2024]. Disponible en: https://www.nato.int/cps/en/natohq/topics_210907.htm

NATO. (2023a). *Empowering NATO's Multi-Domain Operations Through Digital Transformation* [en línea]. NATO, Allied Command Transformation. [Consulta: 25 noviembre 2023]. Disponible en: https://www.act.nato.int/article/empowering-nato-mdo-through-digital-transformation/

NATO. (2023b). *Russian War against Ukraine. Lesson learned Curriculum guide* [en línea]. NATO. [Consulta: 3 mayo 2024]. Disponible en: https://www.nato.int/cps/en/natohq/official_texts_187617.htm

NATO. (2023c). *Science & Technology Trends 2023-2043*. Volume 1: Overview [en línea]. NATO, Science & Technology Organization. [Consulta: 10 febrero 2024]. Disponible en: http:\www.sto.nato.int

NATO. (2023d). *Science & Technology Trends 2023-2043*. Volume 2: Analysis [en línea]. NATO, Science & Technology Organization. [Consulta: 10 febrero 2024]. Disponible en: http:\ www.sto.nato.int

NATO. (2024). DIANA. [Consulta: 13 febrero 2024]. Disponible en: https://diana.nato.int/index.html

Oficina C. (2022). España en un ecosistema tecnológico y social en constante evolución [en línea]. Oficina C. [Consulta: 26 febrero 2024]. Disponible en: https://www.oficinac.es/es/informes-c/ciberseguridad

Parker, J. (2024). Operación Singapur: cómo unos espías lograron interceptar las comunicaciones secretas del ejército alemán que publicaron medios estatales rusos [en línea]. *BBC News*. [Consulta: 2 mayo 2024]. Disponible en: https://www.bbc.com/mundo/articles/c2jx4p80rl8o

Parra, S. (2023). ¿Qué es el Domo de Hierro de Israel y cómo funciona? [en línea]. *National Geographic*. [Consulta: 3 mayo 2024]. Disponible en: https://www.nationalgeographic.com.es/mundo-ng/que-es-domo-hierro-israel-como-funciona_20842

Patel, S. (s. f.). What Is Deep Learning? [en línea]. MathWorks. [Consulta: 9 abril 2024]. Disponible en: https://www.mathworks.com/videos/introduction-to-deep-learning-what-is-deep-learning--1489502328819.html

Pearson, C. (2022). ¿Qué es Discord y para qué se usa? [en línea]. Epic Games Store. [Consulta: 26 febrero 2024]. Disponible en: https://store.epicgames.com/es-ES/news/what-is-discord-and-what-is-it-used-for

Pereda, C. F. (2013). EE. UU. admite que recoge información en el exterior, como todos los países [en línea]. *El País*. [Consulta: 20 febrero 2024]. Disponible en: https://elpais.com/internacional/2013/10/24/actualidad/1382638660_405667.html

Peréz y Peréz, M. A. (2022). La guerra ya no es lo que era. *Global Strategy Report*. 13.

Pinedo Lapeña, A. (2022). Ciberseguridad, geopolítica y energía. En: Instituto Español de Estudios Estratégicos (ed.). *Energía y Geoestrategia 2022*. Madrid, Ministerio de Defensa, pp. 159-196.

Piñeiro Sánchez, A. (2022). Concepto de Transformación Digital en la Armada. Madrid, Secretaría General del EMA, Sección GIC.

Piñeiro Sánchez, A. (2022-2025). Plan de Transformación Digital en la Armada. Madrid, Secretaría General del EMA, Sección GIC.

Pita da Veiga Subirats, J. (2021). Evolución y futuro del próximo sistema de Mando y Control nacional (SC2N). En: Ministerio de Defensa, Armada Española (eds.). *Revista General de Marina*. Madrid, Ministerio de Defensa. 281, pp. 773-785.

Pontijas Calderón, J. L., 2023. Unión Europea: ciberseguridad y ciberdefensa [en línea]. *Documento Análisis*. Ministerio de Defensa, Instituto Español de Estudios Estratégicos. 4. [Consulta: 19 febrero 2024]. Disponible en: https://www.ieee.es/Galerias/fichero/docs_analisis/2023/DIEEEA04_2023_JOSPON_Europa.pdf

Recio, E. (2024). Un ciberataque deja expuestos los datos personales de toda la Guardia Civil y el Ejército [en línea]. *The Objetive*. [Consulta: 2 mayo 2024]. Disponible en: https://theobjective.com/espana/2024-04-15/ciberataque-expuestos-datos-personales-guardia-civil/

Reese, H. (2017). Understanding the differences between AI, machine learning, and deep learning [en línea]. *Tech Republic*. [Consulta: 23 mayo 2024]. Disponible en: https://www.techrepublic.com/article/understanding-the-differences-between-ai-machine-learning-and-deep-learning/

Rodríguez Abril, R. (s. f.). Neuronas de McCulloch y Pitts [en línea]. *La Máquina Oráculo*. [Consulta: 8 abril 2024]. Disponible en: https://lamaquinaoraculo.com/deep-learning/el-modelo-neuronal-de-mcculloch-y-pitts/

Rodriguez Collantes, D. y Sanchez Piedra, M. Á. (2023). Las aplicaciones actuales y futuras de la investigación espacial [en línea]. En: Ministerio de Defensa, Armada Española (eds.). *Revista General de Marina*. Madrid, Ministerio de Defensa. 285, pp. 367-380. [Consulta: 2 abril 2024]. Disponible en: https://armada.defensa.gob.es/archivo/rgm/2023/08-09/RGMAgoSep2023Parte8.pdf

Rühlig, T. (2023). La estrategia tecnológica de Xi [en línea]. *Le Grand Continent*. Groupe d'Études Géopolitiques. [Consulta: 15 febrero 2024]. Disponible en: https://legrandcontinent.eu/es/2023/04/05/la-estrategia-tecnologica-de-xi/

Sánchez de Toca Alameda, M., Díaz Muriana, J., Martín Martín, R. y Muñoz Galdeano, A., 2023. El subsistema de inteligencia del Ejército de Tierra: presente y retos de futuro. En: Ministerio

de Defensa (ed.). *Cuadernos de Inteligencia*. Madrid, Ministerio de Defensa. 1, pp. 15-25.

Sanz Romero, M. (2020). El gato de Schrödinger, mucho más que una simple paradoja [en línea]. *Computer Hoy*. [Consulta: 25 febrero 2024]. Disponible en: https://computerhoy.com/noticias/tecnologia/gato-shrodinger-paradoja-736517

Secretaría de Estado de Defensa, 2020. Estrategia de Tecnología e Innovación para la Defensa ETID-2020 [en línea]. Ministerio de Defensa, Dirección General de Armamento y Material. [Consulta: 2025]. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/e/t/etid_estrategia_de_tecnolog_a_e_innovaci_n_para_la_defensa_2020.pdf

Servimedia. (2024). Pablo Casado lanza un fondo de inversión en pymes de defensa, sector aeroespacial e Inteligencia Artificial [en línea]. *El Mundo*. [Consulta: 20 febrero 2024]. Disponible en: https://www.elmundo.es/economia/empresas/2024/01/22/65aeaba0e4d4d8322c8b458b.html

Sierra, G. (2023). Cómo utiliza Israel la Inteligencia Artificial para combatir en Gaza [en línea]. *Infobae*. [Consulta: 3 mayo 2024]. Disponible en: https://www.infobae.com/america/mundo/2023/12/09/como-utiliza-israel-la-inteligencia-artificial-para-combatir-en-gaza/

Snowden, E. (2019). *Vigilancia Permanente*. Barcelona, Editorial Planeta.

Suárez Sánchez-Ocaña, A. (2015). *El quinto elemento*. Deusto.

The Inspector General of the Department of the Air Force. (2023). *Report of Investigation (S9691). Unauthorized Disclosure of National Security Information* [en línea]. United States of America, Department of the Air Force. [Consulta: 2025]. Disponible en: https://media.npr.org/assets/pdf/2023/12/UD-ROI-11Dec23.pdf

The Institute for National Security Studies [en línea]. (2023). Tel Aviv University. [Consulta: 2025]. Disponible en: Inss.org.il

Toffler, A. (1993). *La tercera ola*. Barcelona, Plaza & Janés.

Tushkanov, V., Sergeev, V., Ochepovsky, A. y Schlychkova, Y. (2023). Story of the year: the impact of AI on cybersecurity [en línea]. *SecureList*. Kapersky. [Consulta: 15 diciembre 2023]. Disponible en: https://securelist.com/story-of-the-year-2023-ai-impact-on-cybersecurity/111341/

UK Ministry of Defense. (2023). *Joint Doctrine Note 1/23. Intelligence, Surveillance and Reconnaissance* [en línea]. GOV.

UK. [Consulta: 1 abril 2024]. Disponible en: https://www.gov.uk/government/groups/development-concepts-and-doctrine-centre

Underwood, K. (2023). Data Remains Key to Military Artificial Intelligence Strategy [en línea]. *Signal*. AFCEA International. [Consulta: 14 febrero 2024]. Disponible en: https://www.afcea.org/signal-media/defense-operations/data-remains-key-military-artificial-intelligence-strategy

Unión Europea. (2022). A Strategic Compass For Security and Defense. [En línea]. The Diplomatic Service of the European Union. [Consulta: 10 febrero 2024]. Disponible en: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en

Valero, C. (2024). Rusia intercepta y difunde una conversación de altos mandos militares alemanes sobre Ucrania que pone a Scholz en aprietos [en línea]. El Mundo. [Consulta: 2 mayo 2024]. Disponible en: https://www.elmundo.es/internacional/2024/03/02/65e33306e85ece9f4c8b4593.html

Valero, V. M. (2016). Beneficios de la inteligencia en apoyo de la política estrategia de una organización. En: Instituto Español de Estudios Estratégicos (ed.). *Inteligencia. Un enfoque integral*. Madrid, Ministerio de Defensa, pp. 141-180.

Victoria. (2018). ¿Cómo será la tecnópolis militar rusa Era? [en línea]. [Consulta: 15 febrero 2024]. Disponible en: https://geoestrategia.eu/20540-icomo-sera-la-tecnopolis-militar-rusa-era

Watling, J. (2023). Supporting Command and Control for Land Forces on a Data-Rich Battlefield. *Rusi*. Londres, Royal United Services Institute.

Xin, Y. *et al*. (2018). Machine Learning and Deep Learning Methods for Cybersecurity [en línea]. *IEEE Access*. 6, pp. 35365-35381. [Consulta: 2 mayo 2024]. DOI: 10.1109/ACCESS.2018.2836950

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Nueva York, Public Affairs.