Capítulo quinto

Inteligencia artificial en apoyo a la inteligencia militar. Eje fundamental del éxito o fracaso en la competición estratégica entre grandes potencias

Juan Luis Sánchez Sánchez

Resumen

La potencia de la inteligencia artificial, IA, en los futuros desarrollos tecnológicos impactará de manera drástica en el predominio mundial y en la competición estratégica entre grandes potencias, la forma de afrontar las crisis y conflictos híbridos y la utilización multidominio de las capacidades militares y su integración con las civiles. El uso avanzado de IA aplicado a la inteligencia permitirá la mejor y más rápida comprensión del entorno estratégico y operativo para adelantar, respecto a los competidores, las soluciones ejecutivas idóneas que permitan la supervivencia del modelo social, económico y político de nuestras sociedades democráticas liberales.

Palabras clave

Inteligencia, Información, Inteligencia artificial, OSINT, Guerra cognitiva, Operaciones especiales, Disciplinas de inteligencia, Ciclo de inteligencia, IMINT, SIGINT, Competición estratégica.

Artificial intelligence in support of military intelligence. Fundamental axis of success or failure in the strategic competition between great powers

Abstract

The power of artificial intelligence, AI, in future technological developments will impact deeply in the global preeminence and in the strategic great power competition, the way of face the crisis and hybrid conflicts and the multi domain military capabilities and their integration with the civil ones. The advanced use of AI applied to intelligence will allow a better and faster understanding of the strategic and operational environment in order to anticipate, in relation to competitors, the most appropriate management solutions that will allow the survival of the social, economic and political model of our liberal democratic societies.

Keywords

Intelligence, Information, Artificial intelligence, OSINT, Cognitive warfare, Special operations, Intelligence Disciplines, Intelligence cycle, IMINT, SIGINT, Strategic competition.

1. Una película muy real

Una crisis en el país X ha provocado la escalada de tensión interracial y la explosión de violencia. La embajada española en la capital recomienda a la población residente evacuarse, acudiendo a las instalaciones de la embajada para gestionarlo. En el interregno, una organización terrorista de una de las etnias sin identificar ataca la embajada matando a su servicio de seguridad y tomando un número indeterminado de rehenes. Las peticiones del grupo terrorista son inasumibles, se prevé una intención nihilista, y que asesinen a los rehenes inmolándose. Unidades de Operaciones Especiales del MOE[1] e Inteligencia españolas son requeridas para realizar una posible liberación de rehenes, de competencia legal nacional al ser territorio consular y ciudadanos españoles; el país X solo puede apoyar.

El equipo operativo alertado para realizar la operación de rescate, de manera inmediata, comienza la recopilación de información por parte de los especialistas de inteligencia. Estos buscan y administran el acceso a todas las bases de datos de Fuerzas Armadas utilizando IA de su LLM con *prompts* ensayados en otras incidencias parecidas a la situación real. La recopilación es autónoma y sistemática, bajándose en primer lugar cartografía y fotografía aérea para los sistemas digitales de planeamiento y navegación individuales y de equipo. Simultáneamente, en fuentes abiertas, con las debidas protecciones para no alertar de las intenciones, se ponen en marcha las capacidades de búsqueda OSINT: el equipo operativo, las unidades de inteligencia del MOE (nivel táctico) y del MCOE en el nivel operacional, apoyando el resto de niveles que tienen necesidad de conocer como el RINT n.º 1[2], J2[3] del MOPS[4] en el nivel operacional coordinando con X y aliados y, por supuesto, el CIFAS en el estratégico; la unidad de conducción y planeamiento estratégica en el Estado Mayor Conjunto del Jefe de Estado Mayor de la Defensa realiza también la coordinación en STRATCOM[5].

---

1 MOE. Mando de Operaciones Especiales del Ejército de Tierra (ET).

2 RINT n.º 1. Regimiento de Inteligencia n.º 1 de Fuerza Terrestre del ET.

3 J2. Jefatura de Inteligencia a nivel conjunto. Nomenclatura OTAN.

4 MOPS. Mando de Operaciones Conjunto de la Defensa. Encargados del mando y control de las operaciones exteriores y, en caso de un conflicto o crisis, se convertiría en el Mando de nivel Operacional.

5 STRATCOM. Comunicaciones Estratégicas. Encargada de la coordinación de campañas de información y de las medidas ejecutivas para el dominio cognitivo, con operaciones psicológicas, de «influencia» y de información pública entre otras.

La IA presenta en horas lo que antes necesitaba días, toda la información disponible en las bases de datos múltiples de inteligencia básica y mediante los *prompt* adecuados lanza peticiones automatizadas de información, RFI[6], al sistema de gestión centralizado del Sistema de Inteligencia de las Fuerzas Armadas, SIFAS, y recopila con IA los requerimientos de todas las unidades implicadas en la adquisición de inteligencia actual y reparte tareas de manera automatizada a sensores, planes de vuelo de UAV, satélites de control propio y, en su caso, de aliados, barcos, submarinos o aviones de guerra electrónica e inteligencia de imágenes.

Las IA del SIFAS alerta y suministra a todos los nodos implicados, informes y productos disponibles hasta el momento sobre la crisis adaptados a sus necesidades, con dos vértices: en el equipo operativo que deberá realizar la operación, el principal; y en el nivel político-militar de decisión.

Se recopila y resume información sobre las etnias, líderes, sus perfilaciones psicológicas indirectas, intencionalidades, capacidades, tipo de armamento disponible, red de apoyo de los grupos insurgentes o terroristas; se mapean las redes sociales del país, localidad y entorno de la embajada, se recopilan videos y material multimedia de los grupos insurgentes y se separan de los mismos datos biométricos como rasgos faciales, voz, iris o tatuajes y otros atributos distintivos de identidad, para investigar quiénes pueden ser los autores. La IA separa y secuencia actores hostiles con sus rasgos físicos y los equipos OSINT[7] del CIFAS recopilan información de *Identity Intelligence*[8] de los mismos: cuentas bancarias, teléfonos, direcciones IP y detalles de ordenadores, servidores, vehículos, familiares, amigos, domicilios, costumbres como rutas frecuentadas, bares, tiendas… todo ello con la prelación automatizada con IA de importancia relativa de esos actores. Adicionalmente se recopila la información física de españoles y trabajadores que pudieran o no estar ya en la embajada. No nos olvidamos de los planos de la embajada y edificios colindantes factibles de poderse utilizar para acceder por sorpresa en el asalto que se prepara.

---

6 RFI. *Request for Information*. Petición de información.

7 OSINT. Inteligencia de fuentes abiertas.

8 *Identity Intelligence*. Departamento y actividad que aglutina todas las características de identificación biométrica de individuos, junto con el resto de rasgos que definen esa «persona» como sus cuentas bancarias, vehículos, red de amigos y familiares, costumbres, personalidad o cualquier otra vinculada.

El mapa electrónico del objetivo, y de todas las vías de aproximación, se adquiere: qué radares hostiles o amigos a los que avisar del paso de helicópteros o apoyo aéreo en tiempo y forma; qué comunicaciones y repetidores gestionan la información de la embajada, se solicita al país anfitrión la interceptación de comunicaciones radio y móvil en la embajada y proximidades, ya que pudiera haber informantes cómplices de los asaltantes fuera. Mediante IA se traducen y transcriben las comunicaciones en tiempo real, se analizan y, en caso de interés, se trasladan a los órganos de inteligencia en los diversos niveles para que aprovechen la información.

Gracias a una imagen adquirida por un equipo HUMINT[9], de un agente local encubierto colaborador que se ha acercado a la embajada, se han logrado sacar unas fotos y videos de varios terroristas y se extrae entre las máscaras una nariz y algunas orejas, formas de andar y coger las armas que, analizadas con IA, han demostrado la identidad de algunos asaltantes, pertenecientes a una de las facciones insurgentes y cuyo líder se conoce por un video de propaganda; en niveles superiores se perfila psicológicamente al líder y se analizan con IA las posibilidades conductuales del mismo. El equipo HUMINT ha conseguido colocar con micro robots cámaras de video con micrófonos desatendidas, emisores-receptores wifi; todos los sensores son controlados desde España, y recopilan el número y posición dentro de la embajada de los activistas, sus comunicaciones y rutas… y, lo más importante: dónde se encuentran los rehenes, agrupados en varias habitaciones.

El equipo operativo, con la ayuda de programas informáticos de arquitectura administrados por IA, han recreado virtualmente las instalaciones, mobiliario, posiciones de terroristas y rehenes, accesos… información que se actualiza en tiempo real al ser adquirida. El equipo comienza a ensayar los planes de rescate con equipos de realidad aumentada y armas simuladas, donde se incorporan como en un video juego el resto de componentes y apoyos. Conforme el campo de ensayo se replica en real, el equipo ya tiene memorizadas las instalaciones y entrenadas todas las incidencias posibles sobre el plan de ataque, que, una vez en físico, se optimiza con IA para reducir tiempos, optimizar lugares de acceso, armas empleadas, y, sobre todo, riesgos para

9 HUMINT. Inteligencia de fuentes humanas.

los rehenes. Prima la seguridad y rapidez de liberación de estos sobre la del equipo de intervención.

El CIFAS recopila más información y analiza con sus expertos y los externos que se adscriben del mundo académico, diplomático y empresarial y, con ayuda de sus herramientas de IA, realiza modelos predictivos de los diversos escenarios de todo nivel: político-militar, estratégico a táctico, y la incidencia de las diversas posibilidades de actuación en adversarios, aliados y neutrales. La IA pondera variables, influencia de actores, instrumentos de poder de los sistemas intervinientes, las relaciona con todo el conjunto de evidencias, productos de inteligencia relacionados, predicciones, y actualiza sus algoritmos para reducir la incertidumbre y los sesgos cognitivos, y presenta posibilidades para que finalmente el componente humano tome las decisiones finales de valoraciones y recomendaciones para los decisores.

El gobierno y el gabinete de crisis donde la ministra de Defensa, el JEMAD[10] y otros actores importantes como el Departamento de Seguridad Nacional, CNI[11], el CIFAS, Ejércitos/Armada, MCCD[12] y MOE reciben la actualización de inteligencia del CIFAS en cuanto a la opción militar a realizar; finalmente el MOE expone la acción a desarrollar y se toma la decisión ejecutiva.

El equipo operativo se ha desplazado y está próximo a intervenir en las proximidades de la embajada en el país X, y continúa recibiendo, en tiempo real, gracias a su nube de combate, toda la actualización de inteligencia, el video en directo de los UAV[13] y satélites, actualización de inhibidores de comunicaciones y la situación actualizada dentro del objetivo, la IA reconoce los patrones de importancia y presenta al equipo solo la información de interés; mediante micro UAV en enjambre, robots capaces de anticiparse y reconocer zonas no controladas, identificar y transmitir la información entre ellos y en la nube y hasta España. Cada componente del equipo recibe alertas en tiempo real en sus visores holográficos ajustados a sus cascos, mientras que las constantes vitales y circunstancias del combate como direcciones de fuego, imágenes, reconocimiento e identificación de rehenes o terroristas o apoyos de fuego sobre lugares concretos son transmitidos de la nube de combate local a los helicópteros y cazas en

10 JEMAD. Jefe de Estado Mayor de la Defensa.
11 CNI. Centro Nacional de Inteligencia.
12 MCCD. Mando Conjunto del Cíber Defensa.
13 UAV, Unmanned Aerial Vehicle. Drones voladores.

espera para dar apoyo, y recibirán los orígenes de fuego hostil y parámetros de aterrizaje en tiempo real gracias a los diversos algoritmos de IA que sugieren alternativas de actuación en relación con la información recibida por todos los sensores.

Los rehenes son rescatados y los secuestradores neutralizados, y detenidos. Parte del equipo escolta a los rehenes a sus helicópteros de evacuación, mientras que otra parte se queda en la embajada para recopilar evidencias forenses, fotos, ADN, armas, teléfonos y ordenadores para su posterior análisis; se compartirán esos indicios con aliados y el país X, con los que se cruzarán datos para resolver la implicación de algunos de los terroristas en otros atentados con IED[14]. La utilización de IA ha sido clave para buscar con ciencia de datos entre miles de pistas y cruzarlas para convertirlas en indicios relacionales para desarmar redes delictivas y terroristas en las que militaron los finados.

Pero no termina ahí la labor de inteligencia porque hay que evaluar el impacto en RRSS[15], medios de comunicación y percepción en la sociedad del país X y otros de interés, junto a España. Se detectan campañas de desinformación y de guerra híbrida conducentes a desestabilizar y sacar beneficio de criticar los éxitos, maximizar los posibles errores producidos en la operación, victimizando y engrandeciendo al grupo terrorista como luchadores por la libertad. Se trabaja en la detección de la campaña de desinformación, sus narrativas, redes de difusión, detección de robots, procedimientos y verdaderos responsables, la IA es clave para realizar el trabajo en tiempo mínimo y contribuye a relacionar vínculos ocultos. Se realizan operaciones de *hacking* y detenciones físicas de responsables de esos entes cibernéticos para saber quién está detrás y qué intencionalidades han tenido o podrían tener en el futuro.

Para todo lo anterior, el MCCD y especialistas DOMEX[16] del MOE, RINT y CIFAS realizan la extracción de información de esos terminales informáticos, para lo que se rompen los códigos de encriptación y se analizan sus ficheros remotamente para encontrar instigadores y redes clandestinas en la *dark web* dedicadas a la financiación con criptomonedas, recluta, propaganda y adiestramiento de terroristas y grupos de crimen organizado relacionados

[14] IED, artefacto explosivo improvisado.

[15] RRSS, Redes sociales.

[16] DOMEX. Extracción de datos e información de documentación y medios informáticos/electrónicos capturados.

entre ellos. Y con J9/10 Influencia[17] y EMACON en su unidad de Comunicación Estratégica STRATCOM suministrar la información pertinente para desarrollar la contra campaña de infoxicación y desinformación con medidas dinámicas. Finalmente, gracias a las labores de inteligencia después de una operación, se detectan y previenen acciones hostiles futuras contra los intereses de España y sus aliados.

2. Una introducción

Con este relato, parecido al de un guion de película que bien pudiera ser real, hemos repasado de manera general los grandes efectos multiplicadores actuales de la IA en una operación militar de rescate de rehenes, quizás una de las más difíciles; y las intersecciones con la inteligencia como disciplina, responsable del éxito de las operaciones.

Efectivamente, la importancia creciente de la inteligencia en las crisis de todo tipo es incuestionable desde que se popularizó el paradigma *Intelligence leads operations*[18], aplastante corriente con la doctrina de contrainsurgencia (Kilcullen, 2010) tras la segunda guerra del Golfo y reflejo de la importancia de la inteligencia en las operaciones «quirúrgicas» tipo de las operaciones especiales y fuerzas de seguridad policiales, con sus *Intelligence Lead Policy* (ILP), en las que el detalle y contrastabilidad de la inteligencia condiciona y autoriza todas las operaciones[19] (Burcher y Whelan, 2018), todas ellas con supervisión legal final tras el proceso de recopilación de evidencias de inteligencia.

Si hay algo que caracteriza a esas operaciones quirúrgicas antedichas es la necesidad ingente de información e inteligencia, su proceso y análisis. Con la irrupción de la IA, somos capaces de abarcar más, con menos esfuerzo, de mejor manera, menos personal y más rápido.

---

17 Secciones del Estado Mayor J9 Información y J10 Influencia.

18 «La inteligencia lidera las operaciones». La traducción puede llevar a engaño, pues el verbo lead significa según el diccionario Cambridge: dirigir, liderar, ir ganando, conducir, llevar, conducir, llevar, … Su sentido invierte el paradigma de las fuerzas armadas burocratizadas de paz, acostumbradas a los ejercicios en el que el papel todo lo aguanta, que no han participado en situaciones bélicas de máximo esfuerzo y bajas; en estas últimas las Operaciones lideran y justifican todo el resto de las facetas de las funciones organizativas de Estado Mayor, incluida la Inteligencia.

19 *Intelligence-led policing* (ILP). Modelo para fuerzas de seguridad del estado policiales que busca colocar la inteligencia sobre el crimen al frente de las decisiones o las operaciones. Concepto manejado por los países anglosajones.

La utilización de la IA para la resolución de problemas de inteligencia está en relación con los desarrollos tecnológicos y a la revolución en los mismos, experimentada, sobre todo, en este primer cuarto de siglo XXI. En otros capítulos de este trabajo se expone la historia reciente de la IA, pero recordemos que el desarrollo de los ordenadores y los primeros algoritmos complejos nacieron de las necesidades bélicas durante la Segunda Guerra Mundial, en particular, de la inteligencia militar en descifrar los mensajes codificados por la herramienta analógica y mecánica Enigma; gracias a lo cual y a la interceptación de las comunicaciones, lo que llamamos SIGINT[20], los aliados consiguieron una ventaja estratégica, que favoreció su triunfo. En la actualidad, el visor de prospectiva de la IA en apoyo de las operaciones militares en su conjunto, y en particular de la Inteligencia, está sobre Ucrania, que se analiza expresamente en otro apartado del presente trabajo.

3. La IA como eje en la competición estratégica actual

Los EE. UU., desde la Segunda Guerra Mundial, han liderado todo lo concerniente a la innovación militar y, en particular, la IA no podía mantenerse ajena a la misma, si bien el entorno global de seguridad emplaza la competición estratégica entre EE. UU. y China. Podemos considerar que Rusia pasaría más a aliado del nuevo pretendiente a «hegemon» en el balance geopolítico mundial, aunque mantenga ese peso estratégico que le da el poder nuclear y no tanto el militar convencional y de desarrollo tecnológico, como se está constatando en su agresión a Ucrania.

China, a nivel económico, ya está a nivel de equilibrio, lo que le permite pasar a la última fase en su estrategia enunciada por Pillsbury del «Maratón de los 100 años»: la supremacía militar; y esta estará basada en encontrar su *Assessin's Mace*, el arma definitiva de su imaginario ancestral, que le dé el éxito frente a sus enemigos más poderosos (Pillsbury, 2016). Esas armas, estrategias (Aranda, 2023) o tecnologías disruptivas con las que China pretende superar a EE. UU., el actual hégemon, y sus aliados tienen como finalidad impedir que este y sus aliados le rodeen,

[20] SIGINT. Inteligencia de señales, dividida en las relativas a comunicaciones COMINT y firmas electrónicas ELINT.

como en el wo[21], y estrangulen la economía y salida estratégica de China con su superioridad aeronaval y espacial.

Para ello, en la búsqueda del arma definitiva, están creando una serie de sistemas de armas con una carga importante de IA en su desarrollo, diseño y C4I[22]. Tenemos ejemplos como los submarinos, las armas hipersónicas, los misiles anti satélites, los medios de interceptación y armas cíber, el *hacking* y todo lo concerniente a la guerra cognitiva. Todo ello fue introducido por los trabajos conceptuales chinos (Liang y Xiangsui, 1999), que probablemente inspiraron a Al Qaida y resto de las estrategias asimétricas que hoy llamamos de zona gris o guerra híbrida[23] (Pillsbury, 2016).

Pero, para el predominio tecnológico de China, uno de los ejes fundamentales ha sido el desarrollo de sus capacidades de copia y robo de tecnología utilizando sus importantes capacidades de espionaje, esto es inteligencia (Pérez, 2023), con infiltración tanto humana como tecnológica, con el uso extendido de las capacidades cíber para incluso acceder a información personal de gran parte de la población de EE. UU. (Clarín, 2020).

El nexo común que interrelaciona todas esas necesidades y capacidades está siendo el desarrollo de la IA, en el que se presume será el verdadero cemento de su pretendida supremacía mundial futura, que le ayudará a desarrollar su *Assessin's Mace*, junto con el conocimiento profundo e influencia en los sistemas de gobernanza mundiales, con superioridad en la prospectiva estratégica y el conocimiento gracias a la inteligencia y su gestión mediante IA, que pretende liderar para el 2030 (Knight, 2017).

Pero antes de continuar, aclaremos algunos términos.

4. Conceptos básicos: tipos de IA y de inteligencia

Entendemos como IA al proceso llevado a cabo por una máquina que puede analizar, organizar y convertir información en conocimiento

[21] Wo, juego ancestral chino, preferido al ajedrez, y en el que las piedras rodeadas del adversario son eliminadas; hay que rodear sin ser rodeado. En la educación china «Las 36 estratagemas» (Aranda, A. 2023) y las historias ancestrales de las luchas de los reinos chinos en guerra antes de la unificación, son la base de la estructura mental y cultural.

[22] C4I. Mando, Control, Comunicaciones, Computadoras e Inteligencia.

[23] La estrategia de la guerra irrestricta fue primeramente abrazada por Al Qaida, según múltiples analistas, ya que ejemplos de acciones descritas en este ensayo fueron realizadas muy poco después de su publicación, como el ataque a las Torres Gemelas el 11S, o atentados en África, además de existir constancias de asesores chinos en el Afganistán de los Talibanes y son previas a la famosa formulación de la guerra híbrida de Gerasimov.

(Jiménez, 2021). Estas IA utilizan programas, que son una representación de un algoritmo en un lenguaje de programación que puede ser interpretado y ejecutado por un ordenador. Y los algoritmos son la descripción del método mediante el cual se realiza una tarea; una secuencia de instrucciones que, ejecutadas correctamente, dan lugar al resultado que se busca. Los diseños de algoritmos están basados en procesos matemáticos que pueden ser trasladados a un ordenador, luego son computables e incluidos en la teoría de la computabilidad (Abellanas y Lodares, 1990).

4.1. Tipos de IA

Los tipos de campos de la IA, sin profundizar, los recordamos en las siguientes ramas de la IA, haciendo referencia al desarrollo de la aplicación de la materia o al campo de investigación de esta.

Estos campos de investigación de la IA son diversos (Russell y Norvig, 2004) en referencia al *test* de Turing en:

- Machine Learning (ML). Toman decisiones futuras utilizando la experiencia pasada.
- Procesamiento del lenguaje natural (PLN).
- Sistemas expertos. Proporcionarían una solución de un determinado problema.
- Visión artificial.
- Lógica difusa. Creando aproximaciones matemáticas para la resolución de problemas se producen resultados exactos mediante información imprecisa.
- Agentes inteligentes. Utilizando su propio conocimiento, ajustándose a los cambios del entorno, son capaces de realizar operaciones que satisfacen lo solicitado por un usuario.
- Deep Learning. Redes neuronales artificiales.
- Robótica.
- Algoritmos genéticos. Son aquellos inspirados en los procesos de la evolución genética y la supervivencia de las soluciones mejor adaptadas al medio.

Todos estos campos de la IA son de diversa aplicación a las actividades de inteligencia, como vamos a desarrollar a continuación.

4.2. Tipos de inteligencia

Los avances que en los últimos años se han producido en los campos de la IA son extraordinarios y tienen aplicación cada vez

mayor en la inteligencia. De una manera inmediata en lo que llamamos la inteligencia actual[24], gracias a la velocidad y automatismo de sus procesos, que permiten aproximar al tiempo real el que trascurre desde la captura de la información por el sensor al aprovechamiento de esta gracias a los mecanismos también autónomos en el procesado y preparación de los datos para transformarlos en inteligencia.

Pero para esa transformación final de la inteligencia se requiere una compilación de la información actual con la preexistente en forma de inteligencia básica. Hasta tiempo muy reciente, el uso de cierta IA se implementaba en los procesos de gestión y almacenamiento en bases de datos. Con la irrupción de la IA y técnicas tan específicas como el *Machine, el Deep Learning*, y el procesamiento del lenguaje natural (PNL), es posible el uso intensivo en cualquier base de datos de procesos estadísticos avanzados que permiten sacar segundos provechos de los datos almacenados.

Antes de la irrupción de la IA, era limitada la utilización masiva de datos y la mecanización con cómputo de tareas arduas y muy exigentes en cuanto a precisión; trabajo óptimo para robots. A lo anterior, unimos, desde hace poco más de un año, con la aparición de los LLM[25] o los grandes modelos de lenguaje natural como ChatGPT y su revolución conceptual y técnica global, que muchos han comparado con la invención de la rueda o internet (Leonhard, 2023), y, como no, también en el de la inteligencia como actividad genérica.

Vamos a analizar la situación actual y de desarrollo futuro, desde la perspectiva de la inteligencia, sus fases y disciplinas, y cómo la IA interviene o puede afectarles.

5. La IA en el ciclo de inteligencia

Pasemos ahora a revisar los procesos generales de inteligencia, en los cuales destaca el omnipresente ciclo de inteligencia, pero, de los diversos tipos existentes, cogeremos como referencia el de la doctrina OTAN y española: dirección, obtención, análisis y difusión.

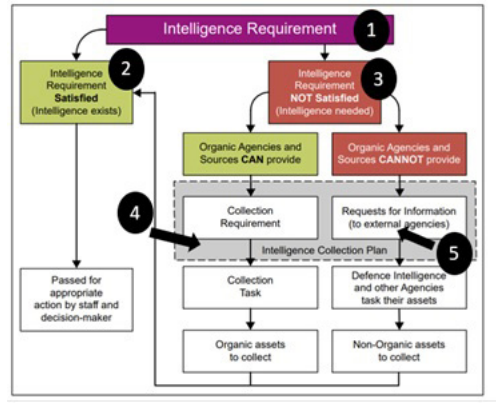
[24] Inteligencia actual. La del momento, muy vinculada a plazos inferiores a las 24 horas y cómo no la de tiempo próximo al real, gracias a la sensorización e intervención de IA en los procesos JISR.

[25] LLM. *Large Language Models*. En los que se inspiran los revolucionarios desarrollos de Open IA (ChatGPT) y del resto de gigantes tecnológicos en sus respectivos desarrollos todavía no tan avanzados.

5.1. Dirección

Esta fase de los procesos de inteligencia ha sido tradicionalmente la más reticente a la intervención robótica de la IA en los aspectos de decisión volitiva de los jefes. Pero la situación está cambiando por la irrupción de campos de la IA como el «Razonamiento Aproximado», la automatización de procesos que ya eran mecánicos en su realización humana, como gran parte de los que están bajo el paraguas conceptual de JISR[26] (Scott y Michell, 2022) y sus subprocesos de IRM[27], de gestión de las necesidades de inteligencia y CM, gestión de los medios de obtención. Interesante nueva aportación con un peso importante de IA es el centrado en la inteligencia, información, cíber, guerra electrónica y capacidades espaciales, I2CEWS[28] (Borne, 2019).

En estos procesos IRM se comparan los requerimientos e información necesarios para la elaboración de un producto de inteligencia y la IA puede cotejar de manera autónoma cuáles ya están en las bases de datos de inteligencia básica y, para los que no están, pasarlos a la siguiente estructura doctrinal, la gestión de la obtención CM, donde se dividen y preparan las necesidades de información para la elaboración de órdenes de obtención a los propios sensores y unidades o, en su defecto, solicitar esa información mediante peticiones de información a las unidades o entes de igual o superior nivel, con las RFI[29], según cuadro que se anexa y orden de procesos del uno al cinco.



Tareas y procesos para requerimientos de obtención. Collection Management (DCDC, 2011)

[26] JISR. *Joint Intelligence, Survaillance and Reconnaissance*. Inteligencia, vigilancia y reconocimiento conjuntos (cualquier dominio).

[27] IRM. *Intelligence Requirement Management.* CM, *Collection Managements.*

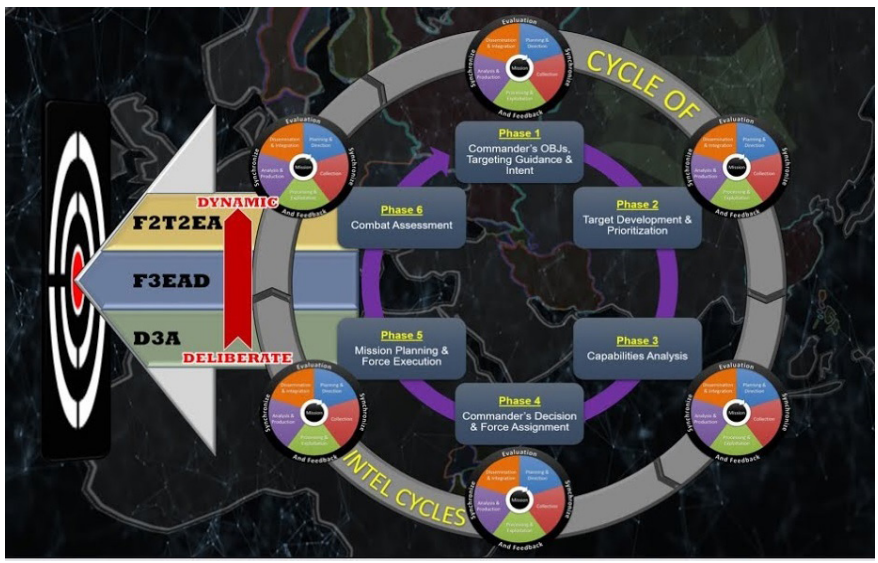
[28] I2CEWS. Concepto nuevo en implantación en EE. UU. *Intelligence, Information, Cyberspace, Electronic Warfare, and Space*

[29] RFI. *Request for Information.* Petición de información, con un formato determinado y estandarizado de circulación y uso común en todos los ejércitos y servicios occidentales. Ver en bibliografía presentación de la ONU.

La asignación automatizada con IA de misiones a sensores cada vez se puede realizar en tiempo próximo al real y el *dynamic re-tasking* (Saling, 1999) de los medios de obtención, esa reasignación de misiones una vez lanzados en ejecución, es más sencilla y está haciendo replantearse los plazos de petición y planeamiento de las mismas. De manera concurrente, la extensiva ocupación y sensorización del campo de batalla no continuo hace que la reasignación de misiones dinámica ya no sea excepcional, gracias a la intervención de la IA en la gestión administrativa y operativa necesaria para variar órdenes, rutas aéreas, sobrevuelos anunciados normalizados y gestiones de los espacios de batalla aeroterrestres y marítimos.

La IA aumenta la seguridad en esas reasignaciones dinámicas para evitar conflictos o colisiones. Algoritmos que soslayan los fallos humanos y aumentan la velocidad necesaria de trasvase de informaciones y cálculos de interés compartido complementario entre diversas plataformas/sensores u organizaciones; todas esas decisiones y gestiones necesitan la automatización para disminuir el tiempo de todos los procesos a tiempos inasumibles por el hombre.

Los plazos se minimizan gracias a la IA para solicitar y planear misiones para entrar en el ATO[30] de un determinado día.



Representación del ciclo conjunto de Targeting de la doctrina de EE. UU.

[30] ATO, *Air Tasking Order.* La publicación de las misiones aéreas con sus rutas, horarios y ocupación del espacio aéreo.

Esos ciclos de planeamiento se dinamizan y aceleran, debiendo imponerse a los del adversario, ya que son importantes para la coordinación del resto de ciclos como el de *targeting* (ATP 3-60) y JISR, y para la priorización de misiones, la asignación de sensores y medios para cada obtención. Estos procesos pueden ser también automatizados con IA.

De hecho, el modelo de la asignación de medios y misiones en los campos de la inteligencia y las operaciones enmarcados por el *targeting* moderno (Kyle, 1999) implica una automatización con IA para los TST[31], esos blancos de oportunidad típicamente desarrollados en las operaciones contra terroristas o insurgentes, como excepciones en las largas listas de objetivos, y que paraban todos los planes en marcha para reorientarlos a ese blanco sumamente importante que debía ser alcanzado lo antes posible cuando quiera que fuera localizado.

Otros campos de empleo de la IA pueden tener aplicación a esta fase, facilitando que no haya esa distinción de fases, sea todo fluido con el mérito de la rapidez y fiabilidad de la IA que nos permita desdibujar cuándo estamos en una u otra fase.

De esta manera, se pueden interconectar simultánea o secuencialmente una combinación de las diversas Necesidades de Información, NI, que se complementan y retroalimentan en tiempo próximo al real conforme se dan las condiciones y desarrollando nuevas NI, y adaptaciones de las Necesidades Críticas de Información del comandante, CCIR, que podrán ser más dinámicas conforme se sincronizan los ciclos de inteligencia, *targeting* (EE. UU. Joint Targeting School Guide, 2017) y operaciones: los ciclos de decisión, inteligencia, control y comunicaciones, C4ISR, se aceleran también por la IA para colapsar los ciclos del adversario.

¿Qué campos específicos de IA son de aplicación para este conjunto de actividades tan variopintas? Entre otros, los algoritmos adaptados a la resolución de decisiones complejas, problemas de decisiones secuenciales[32], sean estas parcialmente observables

[31] TST, *Time Sensitive Targets*. Objetivos de oportunidad de suma importancia.

[32] Richard Bellman, trabajando en la RAND Corporation desarrolló el concepto en 1949. *Dynamic Programming* (1957) para la resolución de problemas de horizonte infinito. Problemas de decisión secuencial en entornos inciertos, llamados, en inglés, por el acrónimo MDP, *Markov Decision Processes*, proceso que especifica los resultados probabilísticos de acciones y la función de premio que puntúa el mismo para cada caso.

o no[33]; también las redes dinámicas de decisión para adaptarse en sus estados de conocimiento conforme se recibe nueva información que complete la percepción de la realidad, para en último término inferir acciones posibles futuras; y, por último, también los conceptos adaptados de la teoría de juegos[34], entre otros.

Las necesidades específicas de inteligencia[35] (SIR), los elementos esenciales de información (EEI) e incluso las necesidades críticas de información del comandate (CCIR) se descomponen en variables y algoritmos de búsqueda de las que las necesidades prioritarias de inteligencia (PIR), se concretan en indicadores de escenarios; todos son indicadores (KPI) de diversos niveles de detalle que pueden ser relacionados como variables cualitativas transformables a cuantitativas y accionables con IA.

En definitiva, los sistemas de alerta de inteligencia necesitan la mecanización que permita monitorizar en tiempo real los cambios en las condiciones y, con sistemas de apoyo a la toma de decisiones (DSS), disminuir los tiempos de reacción de los decisores humanos. Estos procesos se aplican a cualquier actividad de respuesta a emergencias o civil, con la nomenclatura OTAN según las funciones que incluya (Delgado, 2020).

En este sentido, las Fuerzas Armadas españolas están implantando un sistema integral, el Sistema de Mando y Control Nacional, SC2N, (Ruiz, 2023) dentro del cual existe un subsistema dedicado a las labores de inteligencia, donde encontramos integradas las actividades del ciclo de inteligencia e interrelacionadas con el resto de sistemas como el de *targeting* u operaciones entre otros.

5.2. Obtención

En esta fase se explotan las fuentes, los sensores humanos o técnicos, y, por tanto, intervenidos en mayor o menor medida con IA, todos medios de obtención. También tenemos en esta fase los mecanismos para la entrega de la información obtenida a los

[33] POMDP. Acrónimo inglés referido a *Partial Observable* MDP, Problemas de decisión secuencial parcialmente observables.

[34] En la teoría de juegos se busca el equilibrio de Nash en el que no hay incentivos para las decisiones que se desvíen de una estrategia definida por humanos, y, por tanto, transformable en algoritmia controlada por humanos.

[35] SIR, *Special Intelligence Requirements;* EEI, *Essential Elements of Information*; CCIR, *Commander Critical Information Requirements*; PIR, *Priority Intelligence Requirements*; KPI, *Key Performance Indicator.*

órganos de análisis de la siguiente fase del ciclo de inteligencia, pero incluyendo un primer análisis eminentemente técnico del propio órgano recolector.

Esos sensores de los que hablamos son los medios JISR, en su mayor parte, que en la doctrina OTAN ha cobrado tal importancia como para fundamentar procesos específicos y la integración con los de mando control, comunicaciones, el conocido como JC4ISR, que vertebra esa sensorización masiva del campo de batalla, y que requiere de una gestión en la que la IA pasa de simple ayuda a ser protagonista imprescindible en ese *big data* autónomo.

Las creaciones conceptuales de la futura nube de combate de comunicaciones tipo 5G y 6G están haciendo que grandes empresas como Telefónica y GMV exploren soluciones para exportar el mundo tecnológico de la conectividad permanente a áreas remotas o denegadas por acciones hostiles y sacar ventaja de la superioridad tecnológica en los futuros conflictos.

Aquí vamos a dividir esa captura de información no elaborada en las disciplinas, campos y técnicas de explotación de inteligencia principales (no todas) que permiten dividir las facetas en las que la realidad puede ser diseccionada para su mejor asimilación.

5.2.1. OSINT. Inteligencia de fuentes abiertas

Empezamos por la disciplina que más ha crecido en su relación con la IA gracias a la digitalización con internet en la práctica totalidad de las actividades humanas.

Como ya avanzara Alvin Toffler en algunos de sus premonitorios libros de los noventa del siglo pasado, entre ellos *El cambio de poder* o *Las Guerras del Futuro*, la digitalización permitiría el paso de una sociedad de la segunda ola[36] a la tercera en la que el conocimiento, y por extensión la inteligencia, son las claves para el éxito y catalogación como sociedades avanzadas. En estas, su valor añadido lo da la calidad de la población fundamentalmente con el acceso a la educación avanzada para transformar por la tecnología la sociedad misma. Digamos que esta última reflexión casa muy bien con el efecto transformador de la IA en nuestra

[36] Teoría de las olas de Toffler de desarrollo de las sociedades. 1.ª ola con la revolución agraria, 2.ª ola con la revolución industrial y la 3.ª actual en la que la globalización y el cambio a sociedades del conocimiento con la irrupción de las tecnologías de la información.

sociedad actual, y que algunos teóricos ya catalogan como la 4.ª Revolución Industrial (Pérez y Sánchez, 2019).

La importancia actual del OSINT viene dado por el uso global de las fuentes abiertas, el *Open Source*, y la democratización de la tecnología que muchos teóricos iniciales de la IA preconizaban. Podemos decir que en el cajón de herramientas de un analista OSINT las que tienen un carácter de acceso abierto son preponderantes.

Prácticamente ningún servicio de inteligencia es capaz de competir con el *Open Source* mundial en el que individuos no adscritos a organización alguna y unidos por un sentido tribal de pertenencia a ese mundo de compartición avanzan sin restricciones. En él, los retos, trasvase de innovación y soluciones entre la comunidad de interés y hasta la compartición de código entre la colectividad OSINT hace que en cuestión de meses las herramientas que eran una solución factible se queden obsoletas o sean bloqueadas por sus desarrolladores para monetizarlas, pero son sustituidas inmediatamente por otras con el mismo carácter inicial llamémosle *Open Source*.

La unión tecnológica de las capacidades y necesidades del mundo cíber y del mundo OSINT es un hecho, y analistas o equipos OSINT integran capacidades de ingenieros y desarrolladores informáticos, así como diversos perfiles de científicos de datos y estadísticos. La necesidad de código específico y de *hacking* ético aúna los mundos que hasta hace poco estaban distantes. Así, cada vez se requieren más analistas de inteligencia, ya especializados en seguridad, ciencias políticas y relaciones internacionales, pero añadiendo conocimientos profundos informáticos y de cíber seguridad. Con este tipo de profesionales, el salto a la utilización de IA, ya sea propia o adaptada, potencia las capacidades OSINT a unos niveles de autosuficiencia técnica y de importancia capital para los servicios de inteligencia.

Ese hecho se constata por la mayor importancia de una disciplina que reivindica su papel clave para el resto, no solo para fundamentar el conocimiento de partida para otras disciplinas como el HUMINT, IMINT o el SIGINT, sino como fuente del conocimiento único sobre la mayoría de necesidades de inteligencia, ya sea por ser capaces de recopilar el conjunto disponible de información sobre las mismas, como por no haber otras disciplinas que tengan acceso al nicho donde se encuentra la información disponible.

Los informes de única disciplina, los OSINTREP, ya no son considerados un informe menor, sin distinción ni valor añadido en comparación a las otras disciplinas diferentes del OSINT, que suelen ser exclusivas de las capacidades militares y de servicios de Estado, estos son los que pueden pagar los medios y sensores tan caros que los soportan, como por ejemplo satélites, drones o pods de SIGINT, o la posibilidad de reclutamiento y adiestramiento de agentes HUMINT, los James Bond de nuestro imaginario cinematográfico colectivo.

Es extensiva la utilización por los investigadores periodísticos, o el mundo OSINT, de los informantes ocasionales que cuelgan en las diversas redes sociales sus videos y fotos, sus valoraciones o comentarios. Estas redes sociales, se sitúan en la web profunda, la *deep web*, aquella en la que la información no está indexada, no buscada ni catalogada por buscadores tipo google, yahoo: la *surface web* y que explotan solo del 4-8 % de toda la información que circula por internet. La inmediatez que posibilita tener testigos improvisados allá donde se da la noticia o evento de importancia, trasciende a nivel mundial gracias a la posibilidad de compartición de esa experiencia a nivel global. El que haya plataformas comerciales como las de empresas como Dataminr que hayan llegado a explotar esas capacidades con el uso intensivo de IA para extraer la información, verificar la veracidad de esta, contrastarla con otras fuentes disponibles, y todo en tiempo próximo al real, está posibilitando la irrupción de la empresa privada en el uso de estas tecnologías de conocimiento al servicio, antes exclusivo, de grandes corporaciones y Estados.

El que esas herramientas desarrolladas por empresas especializadas en inteligencia OSINT puedan ser adaptadas a las necesidades y preferencias de cada usuario las hace muy atrayentes para otras empresas en las que el uso de la información es vital para su negocio en campos tan dispares como el análisis de riesgos, el planeamiento estratégico de actividad, el marketing, o el impacto de la situación social, cognitiva, o política en sus actividades de negocio en determinados espacios geográficos o de modo global.

La revolución tecnológica actual hace que las capacidades que antes estaban solo al alcance de entidades oficiales y empresas poderosas, se extienda con la inteligencia económica y la irrupción de las necesidades de inteligencia en empresas para alerta temprana, evaluación del riesgo de sus inversiones en

lugares comprometidos y la seguridad del personal destacado. El OSINT es la disciplina que se ha extendido y está al alcance de cualquier empresa, ya sea de manera orgánica y permanente, o como servicio externo con asesorías de seguridad e inteligencia. Estamos ante tecnologías de doble uso: civil y militar (Toffler, 2001).

Portales como *Github, Google Colab* u otros de compartición o colaboración hacen que esa cesión de código en diferentes lenguajes minimice los esfuerzos de desarrollo de soluciones singulares y únicas adaptadas a las necesidades no solo de las organizaciones, sino de los equipos de analistas. Las capacidades de los mismos en OSINT se multiplica gracias a la implementación de soluciones *ad hoc* de IA para resolver problemas muy específicos.

Empleos efectivos del OSINT son cada vez más concluyentes e interesantes y la guerra en Ucrania está siendo un visor mundial del auge de la disciplina. El valor agregado de su democratización y las posibilidades que permite el acceso generalizado de la población con sus aplicaciones en *smartphones* y teléfonos a redes sociales por las que se difunden fotos, videos y comentarios directos, convierte a simples ciudadanos espectadores en agentes improvisados o testigos de primer orden, que rayan el «ciber HUMINT».

5.2.2. HUMINT. Inteligencia humana

Es la inteligencia de la información recolectada por operadores humanos del entorno físico y humano, de fuentes humanas.

Podríamos pensar que son actividades fuera de la cobertura de la IA, pero estos operadores humanos presentan limitaciones, prejuicios y sesgos cognitivos (Heuer, 1999), no controlan todos los idiomas de teatro en los que se pueden desplegar y a la hora de las entrevistas o interrogatorios, la ayuda de IA permitirá la interpretación de dialectos, lenguaje no verbal, detección de la mentira, entre otras necesidades, todas ellas en tiempo real.

Uno de sus cometidos son las misiones de reconocimiento, que perfectamente se pueden hacer a la vieja usanza con unos prismáticos o cámara y anotando incidencias, vehículos, personas… o bien expandiendo los usos de la IA con cámaras vinculadas en nube con algoritmos de reconocimiento y detección como si en

un circuito cerrado de televisión, CCTV, se tratara, pero pudiendo expandir las capacidades de imágenes visibles a infrarrojas o térmicas, reconocimiento automatizado de actores o vehículos, o implementando nuevas tecnologías de interpretación de señales wifi en el objetivo, cerca de él o por el propio equipo usando cámaras RGB, LiDAR, y radares portátiles o no para detectar movimientos y personas detrás de paredes (Newcomb, 2023) y en el que se utilizan algoritmos DensePose[37].

5.2.3. IMINT. Inteligencia de imágenes (De la Fuente *et al.*, 2022)

Es la inteligencia derivada de la adquisición de imágenes desde diferentes sensores y plataformas, ya sean basadas en tierra, aire o espacio. La adquisición de las citadas imágenes se puede realizar en el espectro visible, infrarrojo, multiespectrales, de detección de radiación electromagnética o en las imágenes obtenidas mediante señales radar.

El campo específico de la IA (Lauroba, 2021) que se ocupa de las imágenes está desarrollándose extensamente con set de datos de imágenes desde las diversas plataformas y ángulos de toma para detectar por ejemplo los expuestos por el INTA[38]:

– Detección de cambios

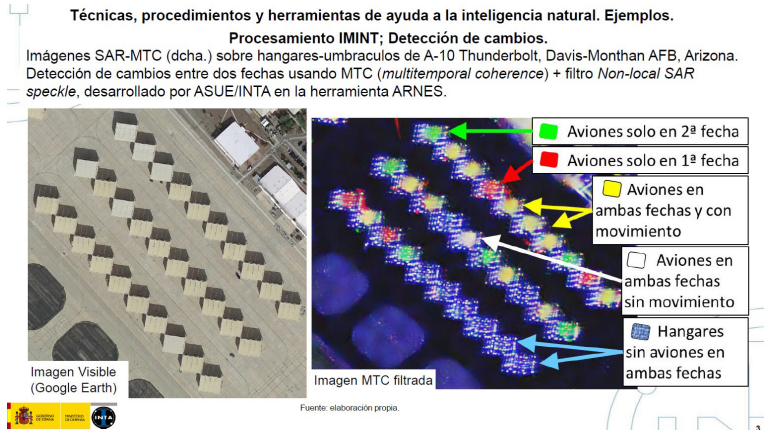


Figura 3

[37] Disponible en: densepose.org. Es parte de COCO and Mapillary Joint Recognition Challenge Workshop en ICCV 2019.

[38] INTA. Instituto Nacional de Técnica Aeroespacial.

Figura 4

– Detección de radares activos

Figura 5

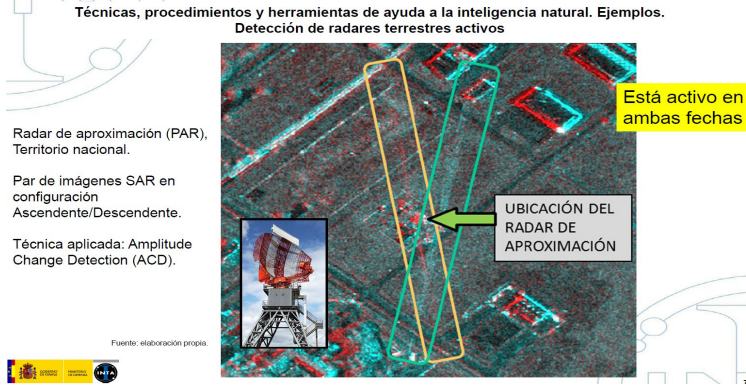


Figura 6

– Detección de movimiento

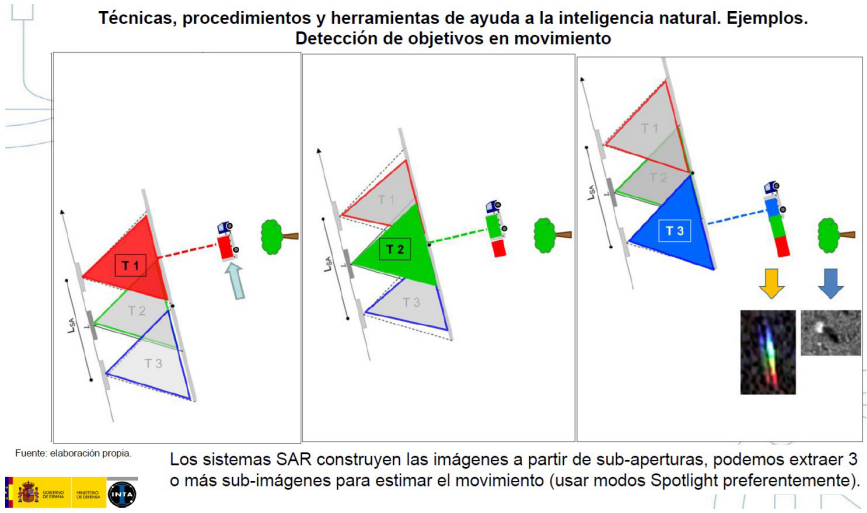


Figura 7

Y, por supuesto, todo el reconocimiento de objetos usando set de datos y fundamentalmente diversas técnicas de *Deep Learning* con redes neuronales combolucionales, con todo tipo de construcciones, aeronaves, etc.

La visión computerizada o artificial está en pleno desarrollo, pudiendo comprender su entorno, contribuyendo a la autonomía de los sistemas y aplicable a todo tipo de drones y es el nexo entre la disciplina IMINT clásica, que se circunscribía a imágenes aéreas, a poder integrar las de cualquier sensor terrestre y marítimos también, con lo que el campo de batalla envuelto en la nube[39] de combate, gracias a la computación en el borde[40] y en la niebla[41].

El procesamiento de imágenes incorpora potentes tarjetas gráficas que aportan potencia de cálculo para imágenes electroópticas e infrarrojas, con módulos de radio definidas por *software* (SDR) y PNT de posición, navegación y tiempo, que permiten la

[39] Servicios de computación en la red, internet u otra red propia.

[40] Estrategia de computacón distribuida que acerca la computación y almacenamiento de los datos a la ubicación donde se toman los datos y se necesita el cálculo, para reducir la latencia y el ancho de banda de comunicaciones requerido.

[41] Infraestructura descentralizada de computación en las que los ordenadores, datos y aplicaciones se sitúan entre la fuente de los datos y la nube.

comunicación e interacción de los sensores y sistemas entre sí para garantiza referencias únicas con el estándar de vetrónica de la OTAN. Todo ello permitirá la interactuación de sistemas de inteligencia con el FCAS, del Futuro Sistema Aéreo de Combate, y los enjambres de drones como fundamentales para los futuros campos de batalla.

El desarrollo de los sistemas espaciales está suponiendo un incremento de las funciones de ISR y su importancia para todos los dominios y sistemas autónomos, utilizando nuevas constelaciones de microsatélites.

Los satélites y plataformas espaciales de órbita intermedia (MEO) y sensores espaciales de órbita baja (LEO) con mayor intensidad de la señal y seguridad que mejorarán los sistemas de posicionamiento como el GPS, Galileo o el GNSS[42] y también mediante sensores inerciales, odómetros, cámaras, giroscopios. Todas estas mejoras implican computación a bordo e IA para fusionar datos con preprocesamiento de datos, reduciendo datos de comunicación con base, y autonomía ante procesos de navegación y superación de averías; pero con grandes limitaciones de espacio y energía necesaria, entretanto no lleguen los ordenadores cuánticos.

Las posibles supervisiones de robots o drones, mediante realidad virtual, aumentada o extendida, permitirán esa interactuación hombre-máquina que será la clave en la presentación de información e inteligencia accionable de manera inmediata a todos los niveles a todos los combatientes cualquiera que sea su función: de mando, asesoramiento, ejecutiva.

5.2.4. SIGINT. Inteligencia de señales

Es la inteligencia obtenida de las emisiones electromagnéticas. Su campo de actuación se divide en dos:

- Inteligencia de Comunicaciones (COMINT), cuando interviene la voz transmitida por cualquier medio electromagnético.
- Inteligencia Electrónica (ELINT), propia de las emisiones electromagnéticas que no pertenecen a la anterior.

Las posibilidades que da la IA de analizar, eliminar distorsiones, y comparar dichas señales, cualquiera que sea el tipo, asociando con análisis de redes actores y relaciones aumenta los éxitos ya

[42] GNSS: *Global Navigation Satellite System.*

cosechados en misiones contra insurgencia y contra terroristas, como en Iraq contra Al Qaida. En la actualidad, en Ucrania se ha hecho un uso combinado de esa localización, cíber jacking, extracción ISR de contenido de móviles, contactos, multimedia y la gestión de la información a unidades de operaciones psicológicas, de inteligencia y de SIGINT, artillería y planificadores. Esa información ha permitido desarrollar unas TTP por Rusia con la preparación de operaciones ofensivas sobre unidades previamente desmoralizadas y preocupadas por decepción masiva de sus combatientes, sus familias/amigos, noticias y fotos manipuladas para conseguir el efecto e inquietud justo antes del ataque convencional tradicional.

Este ejemplo expuesto denota el hecho de la tendencia en la convergencia de la ciberdefensa y la guerra electrónica en lo que llaman ciberelectromagnéticas (Porche *et al.,* 2013).

En España la ciberdefensa depende del MCCD[43] en todos sus aspectos, ofensivos, defensivos y de reconocimiento electrónico de sistemas, sin embargo, las intencionalidades de actores y su prospectiva en conjunción con el resto de disciplinas de inteligencia reside en los órganos del sistema de inteligencia, si son amenazas de entes designados como tales al más alto nivel: el JEMAD.

Por otro lado, la guerra electrónica (EW, por sus siglas en inglés) en cuanto a actividad de inteligencia SIGINT en sus dos subdivisiones tiene una responsabilidad máxima en los órganos de inteligencia nacionales en los diversos niveles con la cúspide en el CIFAS, pero la parte de acción ofensiva y defensiva de contramedidas, etc. depende de los mandos operativos en sí y de las unidades de EW con sus vehículos, drones y antenas especializadas que necesitarán mayores procesos de IA para su protección automática ya sea de ataques cíber, medidas o contramedidas electrónicas como chafs, etc. contra misiles o ataques de armas contra radiación. También cambiando las señales de perturbación adaptados a las amenazas de manera automatizada con IA.

La sucesiva presencia de la IA junto con sistemas de análisis de redes y grafos, entidades, acciones, etc. supone el descubrimiento e interconexión efectiva de masivas cantidades de datos, trazas electromagnéticas características, números de teléfono, repetidores, etc.

[43] MCCD. Mando Conjunto de Cíber Defensa.

5.2.5. ACINT. Inteligencia acústica

Es aquella que describe la inteligencia obtenida de señales acústicas emitidas, siendo siempre asociada al movimiento. Para el uso de esta disciplina de obtención hacen falta; grandes avances tecnológicos, como puede ser el sonar de última generación; sofisticados algoritmos de IA para el procesamiento y análisis de las señales adquiridas, la actualización de las BBDD correspondientes con la clasificación pertinente de lo encontrado; y, por último, una alta cualificación y entrenamiento de los operadores acústicos.

5.2.6. MASINT. Inteligencia de medidas y firmas

Es aquella derivada de análisis técnico de la información obtenida por instrumentos de detección y que finalmente asociaran a diversas fuentes emisoras. Toda la inteligencia obtenida se refiere a comparaciones con las dispuestas en una BBDD con información técnica conocida.

5.3. Elaboración

De manera general, el aprendizaje supervisado de ML, con sus algoritmos de regresión, produciendo valores medibles numéricos, y de clasificación, en los que se consiguen etiquetas dentro de un conjunto finito de posibles resultados, se pueden elegir alternativas cuando estén definidas; así, las incertidumbres puedan ser valoradas y cuantificadas. Además, se pueden hacer predicciones cuando se conocen las probabilidades de los efectos, dadas las causas, o al contario, conocer la probabilidad de las causas dados los efectos (algoritmos basados en la teoría de Bayes), simulando condiciones de incertidumbre y contrafactuales cuando no se sabe si la hipótesis enunciada es verdadera o falsa.

De otro lado, en la fase de elaboración, y en todos sus subprocesos, es donde tienen cabida los algoritmos de agrupación y de reducción de dimensionalidad del aprendizaje no supervisado de ML, enfrentándose al caos y encontrando patrones en grandes BBDD con todo tipo de información.

En esta fase, la información obtenida es transformada en inteligencia con los subprocesos siguientes que, con las nuevas tecnologías, no suponen que hayan de ser secuenciales necesariamente:

5.3.1. Compilación

De la información obtenida. Si cuando hablábamos de OSINT ya considerábamos la IA como solución para la «infosicación», la intoxicación provocada al producir y adquirir más datos de los que éramos capaces de asimilar, en esta etapa replicamos las soluciones habladas y con el uso de IA, agregamos toda la información necesaria referente a un evento, persona, lugar, investigación u objeto, en el sentido informático del término, que pueda dar sentido global e integrador de lo percibido en la realidad por nuestros sensores varios.

5.3.2. Evaluación

De la información y sus fuentes. Esta etapa cada vez más se realiza por cada disciplina de obtención si tiene entidad y capacidades para la misma, y forma parte del primer análisis de disciplina única por los especialistas y técnicos que están en contacto directo con la realidad. Aquí la toma en consideración de evaluaciones anteriores de las fuentes, pueden ser objeto de investigación dedicada para el resto de disciplinas, como pueda ser, por ejemplo, la categorización de una fuente HUMINT, reuniendo información por SIGINT y OSINT para verificar su veracidad, valía de las informaciones a las que tiene acceso, carácter personal o fracturas de seguridad de la misma como agente infiltrado o doble. Para todo ello el contar con extensos datos bien categorizados de las diversas fuentes, gracias a IA con técnicas de refuerzo profundo puede comprobar la veracidad a lo largo del tiempo de las informaciones recibidas. Así, de nuevo estamos hablando de un *big data* y la gestión del mismo para esta finalidad. Las informaciones sacadas de nuestras bases de datos dan la ventaja competitiva y la importancia de mimar la inteligencia básica de la organización.

5.3.3. Análisis de la información

En todas las fases del ciclo de inteligencia tenemos analistas en sus diversas funciones y grados de especialización, pero en esta parte del ciclo es donde se requieren capacidades analíticas más refinadas. El trabajo del analista consiste en encontrar las relaciones causa y efecto entre diferentes hechos, circunstancias, actores y situaciones, todo ello para tener un conocimiento de la situación y poder realizar sus predicciones a futuro (Heuer, 1999). Y en todos los procesos en los que intervienen humanos,

con su experiencia anterior, se producen errores motivados por estrategias simplificadas utilizadas por la mente de las personas para el procesamiento de información a los que se les denomina sesgos cognitivos (Heuer, 1999).

Podíamos hablar hace pocos años, cuando la palabra de moda en estos tipos de tecnología era el *big data*, que los procesos de inteligencia raramente incorporaban la IA a los razonamientos y procesos de análisis estructurado que desde la guerra de Iraq se han generalizado en los servicios de inteligencia.

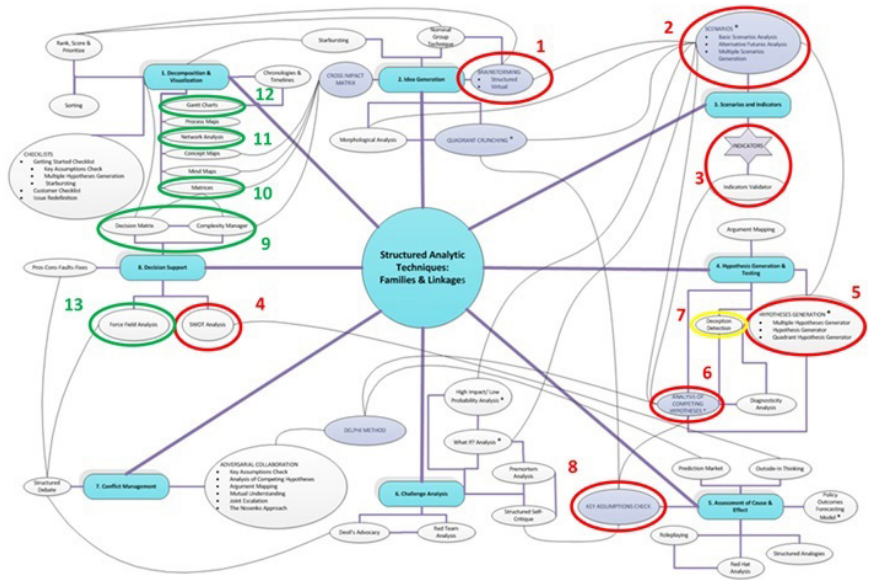
Estas técnicas estructuradas permiten la reducción de sesgos y la implantación de procesos de pensamiento y análisis científicos modulares y perfeccionables por equipos de analistas, utilizando las capacidades racionales y lógicas, su conocimiento de la realidad como expertos de un área, actividad o actor. Todo ese análisis estructurado da un valor añadido tendente a hacer una prospectiva, como producto final.

La irrupción de la estadística como campo en las ciencias sociales y políticas ha sido clave para trasladar el razonamiento científico y matemático a esferas colonizadas anteriormente por la intuición: ese olfato que daba la experiencia de esos asesores de inteligencia especializados.

El uso de la IA está posibilitando ir un punto más allá de las técnicas puramente estadísticas y gracias al M/DL poder sacar provecho de grandes cantidades de datos existentes o adquiribles por la sensorización del mundo y del campo de batalla para utilizar los set de datos en el entrenamiento de algoritmos de predicción, de inferencia que ayuden a los analistas y luego a los asesores a discernir las posibilidades de futuro y, por tanto, poder adelantar acciones correctoras al mismo mediante tareas ejecutivas en la organización. La IA no reemplaza a los analistas humanos, sino que ya los está empoderando.

Si tenemos en cuenta las técnicas de análisis estructurado podríamos dividir las que son más de razonamiento directo humano, que simplistamente podríamos catalogar de «analógicas», de las que permiten una digitalización y automatización mediante IA que potencia los resultados limitando el tiempo de análisis y mejorando la capacidad de asimilación de datos y variables en los procesos. Recordemos que uno de los inconvenientes de las técnicas de análisis estructurado es el tiempo necesario, su carácter predominante cualitativo frente al cuantitativo, ideal para medir con precisión los parámetros.

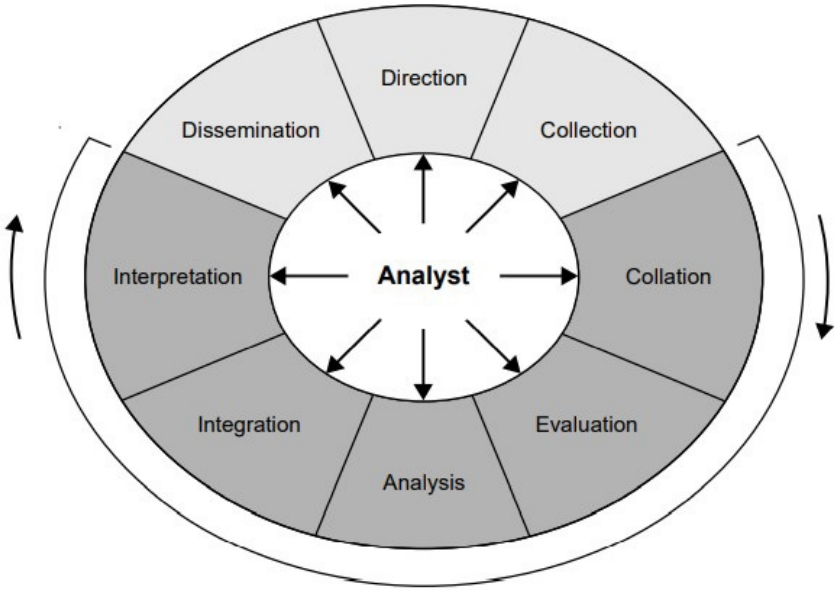
En el siguiente cuadro señalamos cuáles de las técnicas de la recopilación de técnicas de análisis estructurado (Heuer y Pearson, 2015) son más factibles de poder adaptarse a procesos con IA en contraposición a las técnicas más «analógicas» humanas, si bien todas las técnicas, de una manera u otra, podrían ser ayudadas con IA.



Técnicas de análisis estructurado factibles de automatizar con IA en verde y menos en rojo (Heuer y Pearson, 2015)

La incorporación de la IA en los procesos de análisis, y en sus subfases en los lugares adecuados, pueden ayudar a reducir esos sesgos cognitivos, ya que los procesos matemáticos y estadísticos informados en tiempo real por procesos de DSS e IA tienen la objetividad y prontitud de reducir la incertidumbre y presentar la realidad de una manera uniformada y similar en todas las ocasiones, o modificada para evitar errores anteriores de apreciación, evaluación o sesgo. En este campo los LLM modernos y los sistemas con algoritmos entrenados de manera autónoma o supervisada por humanos expertos en esas evaluaciones, son los de mayor avance, desarrollo y aplicación.

Existe un punto de inflexión en la historia de la inteligencia como actividad que fue la guerra del Golfo y los fallos achacados a la inteligencia en la justificación de la guerra sobre la existencia de armas de destrucción masiva, sin entrar en si fueran fallos



Fase de elaboración (DCDC, 2011)

reales en sí o manipulaciones para seguir un procedimiento[44] en la democracia americana de tergiversación o manipulación de sociedades democráticas para adherirse a medidas necesarias para una élite política, pero impopulares hasta ese momento, como era empezar una guerra.

Si bien en servicios de inteligencia tan dimensionados como el americano, no era nueva la aproximación a las ciencias sociales y a la aplicación de la ciencia para la resolución de problemas de prospectiva de inteligencia, sí fue el detonante para que a nivel mundial se abrazaran las técnicas de análisis estructurado como caja de herramientas a disposición de los analistas para justificar y modularizar sus análisis de modo lógico y secuencial para que la intervención de los decisores ya no dejase de atribuirse solo los logros exonerándose de los fracasos en una falta o fallo de inteligencia, un clásico.

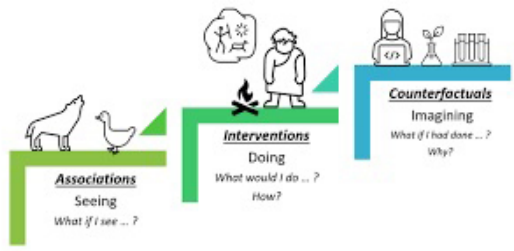
Así, esa modularidad permitía presentar las decisiones como un proceso en el que si el decisor, normalmente de especialidad de

[44] Hechos contrastados de ese tipo fueron la explosión fortuita o interesada del Maine que comenzó la campaña de prensa antiespañola y justificó la guerra de Cuba de 1898, o el análisis pretendidamente erróneo y ocultación de indicios e informes que alertaban de un ataque japonés a Pearl Harbour que justificaron y cambiaron el sentimiento popular americano para la entrada en la II Guerra Mundial.

operaciones o Estado Mayor, sin entender el porqué del análisis final se le exponían los pasos intermedios y la metodología científica empleada, si no estaba de acuerdo podía modificar y bajar al detalle de qué parte del proceso veía errónea, para rehacerla, insertarla de nuevo en el proceso general y dar un resultado analítico final, muchas veces igual al inicial, pero que ya daba confianza al decisor por su intervención directa.

Evidentemente en estos procesos modulares y técnicas diferenciadas, la aplicación de la IA es más que factible y con el paso de los años y el desarrollo de campos más ambiciosos de la IA, entre los que está la IA generativa y los modelos de LLM[45] que hacen obsoleto al cuadro de identificación de técnicas factibles de mecanizar (en verde) del imprescindible libro recopilatorio de Heuer y McPherson, en cuanto a técnicas eminentemente cualitativas y analógicas de intervención de expertos, equipos de trabajo multidisciplinar, mentes blancas, etc. de las que son factibles de transformar en cuantitativas y, por tanto, modelizables con algoritmia e intervención dinámica de la IA, con ciclos de análisis y reevaluación de parámetros más necesarios en tiempo próximo al real.

Por tanto, la incorporación de la IA a las técnicas de análisis, entre las que los profesionales de la inteligencia prefieren en gran medida las estructuradas, con la irrupción de las técnicas de análisis de la ciencia sociológica, política y estadística avanzada con ciencia de datos que va a revolucionar en muchas facetas la disciplina por cuanto reducirá los plazos de planeamiento, el esfuerzo y tiempo dedicado a análisis puntuales de materias, efectos, decisiones, escenarios prospectivos. Los análisis de amplio espectro de ambición estratégica pueden tener aprovechamiento, ya no operacional, sino táctico, en cuanto que la actualización de los mismos va a la par del ritmo y tempo de las operaciones a nivel táctico, más inmediato.



Representación de la escalera causal (Pearl y Mackenzie, 2018)

[45] LLM, *Large Lenguage Models.*

Punto que necesitaría un artículo aparte es la incorporación al mundo de la inteligencia de la llamada «revolución causal» (Pearl, 1981). La incorporación conceptual de la escalera causal a los niveles de interiorización y conocimiento profundo de la materia, lugar, personaje o circunstancia objeto de un análisis es para algunos profesionales de la inteligencia de muy correcta y necesaria implantación. Brevemente diríamos que esa escalera establece los límites en los que la mente humana establece el conocimiento de cualquier materia, siempre basado en procesos de causa y efecto, de experimentación y retroalimentación.

Primero tendríamos el primer escalón básico que Pearl llama de asociación (Pearl, 2009), en el que, mediante la observación de la realidad, con nuestros sensores intentamos hacernos una idea los más correcta posible de la realidad. Son hechos, eventos y evidencias que reuniríamos en nuestros mapas de situación, SITMAP, perfeccionando la alerta situacional del término *Situational Awareness* [46] y que la IA está revolucionando con la posibilidad de visualizar en una única pantalla los diversos sensores, cómo y dónde está el enemigo y las tropas propias, qué hacen… y somos capaces de ver lo que ocurre si uno de nuestros sensores localiza un fogonazo en una posición por un tipo de arma que impacta a los pocos segundos en otra localización y con un efecto, por ejemplo una batería artillera enemiga.

En definitiva, somos capaces de establecer variables y ver cómo se relacionan. En este peldaño se necesitan predicciones que se basan en observaciones pasivas (Pearl y Mackenzie, 2018), y cuya base matemática y estadística es la probabilidad condicional, la correlación y regresión para asociar efectos, variables y actores. Aquí necesitamos datos, cuantos más mejor, y, por tanto, la gestión de los mismos requiere la intervención de la IA, en definitiva.

En el segundo escalón causal, de intervención, hacemos una experimentación que demuestra cómo se comporta la realidad, resolvemos y somos capaces de conocer los procesos que dan lugar a ciertos resultados y, por tanto, seríamos capaces de diseccionar el conjunto de soluciones posibles y con metodología bayesiana podemos inferir qué efecto produciría en otro blanco si el disparo realizado por esa pieza de artillería, que hemos

[46] *Situational Awareness.* Conciencia situacional, término extendido en OTAN para denominar el conocimiento de la realidad que incluiríamos en nuestro concepto de inteligencia actual.

previamente visualizado en el primer escalón, le impactara. En este nivel no nos conformamos con ver, sino que modificamos lo que existe, alteramos el entorno. Aquí entran operadores estadísticos modernos como el *do* para probabilidades (P(destrucción de mi unidad | do (batería enemiga dispara)) que se adaptan a este tipo de condicionantes.

Por último, tenemos el tercer escalón causal, el de aplicación de contrafactuales, en el que utilizamos la capacidad humana única de imaginar, de comprender profundamente los procesos y somos capaces de enlazar los mismos para darnos cuenta de que la clave para minimizar el impacto de esa batería de artillería de nuestro ejemplo, ya que nos preguntamos ¿y si la batería no hubiera recibido información de cálculo de tiro o situación de nuestra posición?, ¿y si la información es errónea porque le damos un señuelo a los sensores del enemigo?, ¿qué pasaría si el camión o la cadena logística no le da los proyectiles que necesita a esa batería?, ¿y si el camino de acceso a la posición artillera se bloquea por unas minas lanzadas, qué ocurriría? Como vemos, integramos muchos tipos de conocimiento, además del balístico, para comprender profundamente las capacidades e incluso intencionalidades del problema, en este caso del enemigo. Aquí entran las matemáticas y una vez que entran estas, el paso a la algoritmia computacional es inmediato.

Los tres escalones causales son inteligencia pero la verdaderamente prospectiva, anticipatoria y eficaz implica un conocimiento de los contrafactuales que nos permiten establecer escenarios futuribles con base en indicios y KPI[47] comunes en el mundo de la inteligencia de negocios, BI, el *big data*, la toma de decisiones automatizada o ayudada por algoritmia, los paneles de mando interactivos informados, la utilización de *data warehouse* dedicados a una determinada temática, y, en definitiva, el empleo masivo de la IA.

5.3.4. Integración de la información

La utilización de las posibilidades que nos da el análisis de redes, el *link analysis*, y la utilización de las matemáticas matriciales y la teoría de grafos han permitido expandir la IA a campos en los que la integración de la información está disponible en diversas bases de datos, estructuradas o no. La utilización de

[47] KPI. *Key Performance Indicators*

herramientas o robots de búsqueda de conexiones de manera autónoma, buceando en nuestro *data lake*[48] también ha superado los límites de nuestros procesos de integración de información y aprovechamiento de la misma.

Ese *data lake*, en su terminología inglesa más aceptada, se refiere a la base de datos general en la que todos los datos y metadatos se encuentran disponibles para esos robots, esos algoritmos de IA que buscan lo que nosotros les digamos de una manera más eficiente, rápida y con menos errores, ya que permiten autónomamente recatalogar, renombrar, reorganizar la información a formatos entendibles por el metabuscador, siendo capaces de reducir drásticamente ese 70 % de tiempo que el científico de datos empleaba hasta ahora en la organización, reparación y preparo de los datos, de manera manual antes de aplicarles ciencia de datos, *Machine o Deep learning*, según la finalidad que buscase, tomemos por caso. La gestión de las diversas bases de datos y cubos OLAP/ROLAP son de las más solventes para la aplicación de las nuevas tecnologías (Jiménez, 2023; JFD, 2017; Gómez, 2021).

Volvamos a la importancia del análisis de redes sociales y la expansión de las herramientas iniciales en servicio de los analistas de inteligencia que buscaban entender, estructurar, visualizarlas de una manera coherente para con los principios de las matemáticas de grafos buscar la topofrafía, la cohesión y agrupamiento (*clustering*), los vínculos entre los nodos, su poder, centralidad y otros tantos conceptos que empezaron a analizarse con programas como UCINET, Netdraw, Pajek y ORA (Everton, 2012)[49], y, por supuesto, el *software* tan extendido entre servicios de policía, inteligencia y OTAN, casi estándar podríamos decir: Analyst Notebook, ANB, de i2 que ahora se han diversificado a librerías de IA en lenguaje javascript, R o Python, códigos democratizados en el mundo del *Open Source*, como expusimos en el apartado de OSINT.

Con la eclosión de la IA, las capacidades para extraer entidades, nexos, pesos de los mismos, acciones, sentimientos… posibilita la transformación automatizada masiva de informes al formato CSV y ANB, que en Afganistán necesitaba naves enteras de analistas junior 24/7, extrayendo y preparando esos grafos y tablas, que una vez relacionados por el programa posibilitaba a los analistas

48 *Data Lake*. Lago de datos.

49 ORA. *Organizational Risk Analyzer.*

de alto nivel hacerse una imagen espacial de las redes y sus interconexiones.

Es nuclear contar con sistemas informáticos que sean capaces de extraer datos de diversos tipos de bases de datos, materia en la que fueron pioneros la empresa americana de Palo Alto, Palantir, que desde hace tiempo buscó mecanizar el acceso a esas bases de datos que no se hablaban aunque físicamente tuvieran oficiales de enlace cada uno con su sistema en los centros de fusión de inteligencia, las *Intelligence Fusion Center*, que el general McCrystal plantó en Bagdad cuando el Surge del 2007, y que para muchos de nosotros fue una nueva revolución en la inteligencia y en la manera en la que se integraba la misma para aumentar el tempo y ritmo en las operaciones especiales para ser capaces de ganar colapsando a una guerrilla insurgente con el uso intensivo de nuevas aproximaciones y usos conjuntos e integrados de la inteligencia.

5.3.5. Interpretación

Esta puede que sea la subfase más humana e implica una experiencia, y, por qué no decirlo, arte, olfato de analista, para ver e intuir lo que no es a veces tan aparente, eso sí ayudado por las técnicas y el conocimiento científico que hay detrás de tantos procesos como los descritos.

5.4. Difusión

La entrega oportuna de los productos de inteligencia por los medios adecuados a los clientes que la requirieron o le pueda interesar. El factor tiempo es fundamental y la clasificación de seguridad adecuada. Muchas veces los productos son repetitivos y estandarizados, lo que permite la mecanización y el relleno de formatos, con la presentación de productos anteriores para dar un contexto y una sugerencia por IA de los eventos o puntos a incluir en informes descriptivos, por ejemplo.

La integración de los productos de inteligencia con los sistemas DSS será en las células de fusión de inteligencia, IFC, que preparan, dirigen y recopilan todas las misiones informativas y de elaboración conformadas en el ciclo de inteligencia para, posteriormente, integrarlas con el ciclo de operaciones y sus centros de operaciones conjuntos, JOC, donde, mediante sistemas informáticos, se pueden seguir y coordinar en los COP, *Common Operational Picture,* esos SITMAP enriquecidos, suministrando

acceso rápido a imágenes e inteligencia (JFD, 2017), donde se fusionan también los sistemas de alerta temprana, conocimiento de la situación de inteligencia (SA), con mapas de la situación para dar sentido al conjunto.

Todo ello, que es un EIS, se puede potenciar con IA para relacionar variables e indicadores, sean críticos o no, con procesos solo visibles bajo parámetros fijados por los usuarios, pero que detrás realizan multitud de procesos de manera automatizada y en tiempo real (Jiménez, 2021; DCDC, 2011).

6. Contrainteligencia y seguridad

En la OTAN está extendida la nomenclatura de J2X para unificar estas labores de inteligencia que tienen los mismos procedimientos y herramientas ya relatados, pero que tienen su foco mirando hacia el interior de nuestros países y organizaciones, en evitar las fugas de información hacia servicios externos, sean potencialmente hostiles o amigos, porque en la búsqueda de información todos buscamos de todo y de todos (Herraiz, 2023).

La interrelación de ciertos departamentos de seguridad para proteger la seguridad física de instalaciones, personas, documentación, etc. se complementa con la propiamente cíber de los sistemas informáticos, comprobando y certificando sistemas de seguridad y anti intrusión. No cabe duda de que la aplicación de sistemas de IA para la comprobación rutinaria de claves, vulneraciones de seguridad y automatización en las respuestas ya protocoladas, dará supervivencia y mantendrá nuestros secretos y datos a buen recaudo de espías externos.

Un campo que se toca con todas las relaciones forenses y de gran aplicación de los avances de IA, es todo lo que implica la subdisciplina de la inteligencia de personalidades e identidades, la *Identity Intelligence*, que ya explicamos anteriormente y que tiene grandes aplicaciones para la contra inteligencia y la seguridad. Solo subrayar un hecho, es en J2X donde existe un mayor nexo con otros servicios de inteligencia civiles y policiales con organismos internacionales como Interpol y Europol para la compartición de información y en donde la información biométrica, por ejemplo, no está clasificada y permite el intercambio ágil de esos datos técnicos, «ceros y unos», en los que se representan a las personnas; sin intervención ni ralentización judicial ni vulneración de derechos fundamentales.

7. Conclusiones

Empezamos este capítulo con el relato de una operación especial exponiendo la exorbitante cantidad de inteligencia que se maneja para el desarrollo y ejecución de ese ejemplo de misión y sus derivadas. Para terminar con las conclusiones, pongamos en esas unidades de operaciones especiales el devenir que se nos presenta de manera inquietante, en conflictos de alta intensidad dentro de la «competición estratégica entre grandes poderes por el dominio mundial» en la que nos vemos ya inmersos.

- PRIMERA. Cambio de paradigma para ampliar el foco de las amenazas a afrontar de las organizaciones no estatales insurgentes/terroristas a adversarios convencionales con estructura, medios y orden de batalla, doctrina y reglas de enfrentamiento de un Estado; esto es: una fuerza militar reconocible.
  Todo ello implica cambiar el tipo y metodología del sistema de *targeting*, obtención de inteligencia, reporte y asesoramiento a los decisores. La intensidad y ritmo de todos los procesos será la clave del éxito en todos los dominios. La IA permitirá automatizar procesos para acortar los ciclos de decisión, inteligencia y planeamiento respecto al competidor (Brown, 2022).
  Mantenemos la idea de ampliar el foco en tanto que no han desaparecido aquellas organizaciones insurgentes islamistas, u otras nuevas pueden continuar o aprovecharse como *proxies* de potencias Estado. En nuestro caso tendremos que operar en esa Zona Gris (Nieto, 2021), promoviendo resistencias armadas aliadas o como contrainsurgencias en nuestro terreno y todas ellas necesitarán fuerzas de inteligencia y operaciones especiales, entre otras, que sean capaces de operar en la zona gris.
  Allí, la superioridad de la información y comprensión de lo que implica la competición estratégica será facilitada por la IA en todos los aspectos: político, militar, económicos, social, de información y de infraestructura (PMESII), junto al diplomático, cultural y legal que necesita el acceso al máximo de conocimiento profundo de la realidad por los niveles más bajos tácticos: ese cabo estratégico (Krulak, 1999) o los guerreros autónomos del futuro (Toffler, 1991) como silogismo de los soldados de operaciones especiales e inteligencia con capacitación equivalente a la de diplomáticos con grados en economía, política, *marketing*/propaganda, psicología, sociología, medicina… y letales soldados; capaces de resolver situaciones al máximo nivel sin instrucciones.

- SEGUNDA. Lucha por todos los dominios: cognitivo, moral, físicos (tierra, mar, aire/espacial). La lucha por la narrativa y la legitimidad, así como la competición en la zona gris, será facilitada por la masiva irrupción de la IA en la coordinación de las acciones multidominio. Especial importancia por su desarrollo con las nuevas tecnologías es el cognitivo, con el impacto de las redes sociales y los enlaces e información residentes en la Deep y Dark web y la utilización de técnicas de ingeniería social ofensivas y defensivas para influir en las percepciones, sentimientos y actitudes de la población y entes políticos, mediante operaciones psicológicas y de información para modificar la moral, fundamental para la victoria. El empleo creciente de la IA para analizar el entorno de la información mediante OSINT será fundamental para prevalecer y adelantar escenarios de inteligencia para el posterior empleo defensivo/ofensivo que asegure los dominios cognitivo y de moral con la utilización de campañas, creación y manipulación de noticias, desinformación con las las fake news, deep fakes, si necesario para controlar finalmente los dominios cíber y físicos (tierra, mar, aire).
- TERCERA. Interconexión de sistemas y digitalización de manera automatizada con IA. Tecnología que pueda adquirir y fusionar información de esos sistemas en cualquier dominio[50] (Kyle, 2019) y nivel de conducción (estratégica, operacional o táctica) con acceso a sensores[51] para asegurar la aplicación de la medida, letal o no letal, más apropiada, una vez se ha seguido, identificado y adquirido el posible blanco. Como corolario, la hiper sensorización, informatización y análisis con IA de todos los entornos, principalmente urbanos, hace más complicadas la infiltración de agentes, y requieren de capacidades adicionales cíber para ser capaces de engañar o enmascarar perfiles y firmas físicas a esos sensores o sistemas, utilizando sistemas alternativos como OSINT e IMINT.
- CUARTA. Mayor letalidad por el uso de armas inteligentes y autónomas, cada vez más robotizadas y sin decisión final humana a la hora de la elección de misiones o blancos con ayuda de IA, con efectos letales o no. La guerra sin contacto directo[52] (Brown, 2022) en los diversos niveles desde drones a misiles hipersónicos, sistemas de armas integradas, que

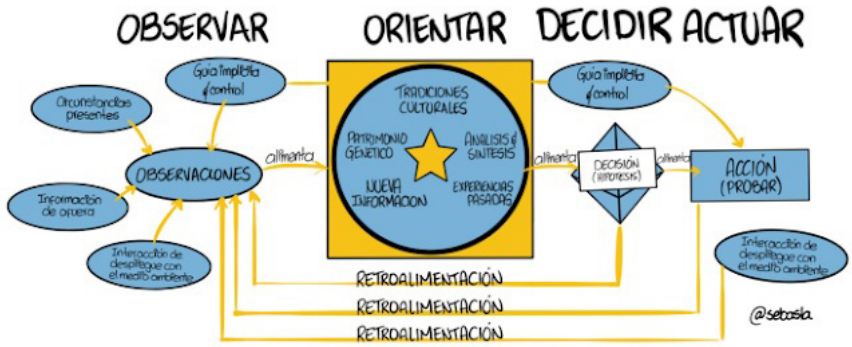
[50] *Joint All Domain Operations,* JADO.

[51] Concepto de *Internet of things* aplicado a las nubes de comunicación tácticas en zonas de operaciones donde se proyectan acciones militares de inteligencia.

[52] Concepto de *Contactless war.*

componen la adquisición y análisis autónomo con sensores de información útil para su operación en tiempo real, con cada vez menos necesidad de intervención humana desde su base por la intervención de IA en las diversas fases.

– QUINTA. Incremento de la velocidad y el tempo en las operaciones y crisis con la intervención de la IA en todo el proceso de orientación y toma de decisiones «OODA loop» (Boyd, 1987) en el que básicamente realizamos análisis causales encadenados en los que observamos, orientamos, decidimos y actuamos/ejecutamos y en los que los dos primeros son eminentemente responsabilidad del ciclo de inteligencia.



El OODA loop de Boyd. Observación, orientación, decisión y ejecución. Del original The Essence of Winning and Losing. Fuente: foto Sebasla Blog

La IA supondrá llevar al extremo la guerra de mando y control para colapsar la correspondiente capacidad del adversario. Si a esto unimos las hiperbólicas capacidades que darán los computadores y tecnologías cuánticas a lo que ahora conocemos, podemos inferir que la proyección a futuro de la aplicación automatizada de IA no ha de tener límites técnicos, sino éticos.

Fuel	Analytic Type	Observe	Orient	Decide	Act
Data Assets/Sensor Data ->	Descriptive - What happened?	X			
	Diagnostic - Why did it happen?	X	X		
	Predictive - What will happen?	X	X		
	Prescriptive - What should I do?	X	X	X	
	AI - Automation	X	X	X	X

Influencia del análisis de datos con IA en el ciclo de decisión OODA y su impacto causal

– SEXTA. Opinamos que no hay que tener miedo de la transformación que va a suponer IA en todos los ámbitos de la sociedad, también en el militar, pues permitirá un salto tecnológico y de capacidades que es difícil de valorar. Algunos analistas sostienen que el salto será equiparable a la invención de la rueda en la antigüedad, y sabemos qué pasó con las civilizaciones que no la aprovecharon.
  La híper regulación de la UE en muchos ámbitos, entre los que se encuentra la referente a la IA, puede constreñir la capacidad europea y occidental en la competición mundial por el desarrollo y aplicación de la IA, por loable que sea esta primera iniciativa de regulación en el mundo; algunas prácticas y usos de la IA estarán totalmente prohibidos, como la manipulación cognitiva conductual y el uso de sistemas de reconocimiento facial indiscriminado (Política Exterior 1358, 2024).
  El reglamento no se aplicará a ámbitos fuera del de aplicación del Derecho de la UE y no afectará a las competencias de los Estados miembros en materia de seguridad nacional. Tampoco se aplicará a los sistemas utilizados exclusivamente con fines militares o de Defensa, entre los que están las actividades de inteligencia; así como a los empleados con fines de investigación e innovación (Representación en España de la Comisión Europea, artículo 25/1/2024).
  Otros factores que habrá que evaluar son los que suponen la intervención humana en procesos de IA: *human OUT of the loop*, de autonomía total; *human ON the loop*, capacidad del operador de monitorizar y parar procesos; y *human IN the loop,* con control completo del operador humano. Para las labores de inteligencia, el riesgo de fatalidades es menor por ser labores no letales, y, por tanto, permiten el primer tipo, de máximo de desarrollo de la IA autónomamente.
– SEPTIMA. La IA tendrá un impacto significativo en los interfaces hombre-máquina y en el análisis de big data para aumentar la alerta situacional[53], reduciendo la carga cognitiva y aumentando los procesos de toma de decisiones asistidos a todos los niveles. Un buen ejemplo es el concepto Hyper-Enabled Operator (HEO), desarrollado por el USSOCOM[54], como un sistema innovador electrónico en el que se incluyen sensores, procesadores, realidad aumentada y enlace todo tiempo en la nube y con las bases donde radicarán las capacidades de cóm-

[53] *Situational Awareness,* SA*,* término de uso extendido en la jerga de OTAN.
[54] USSOCOM. Mando Conjunto de Operaciones Especiales de EE. UU.

puto y bases de datos para el procesamiento computerizado distribuido (MacCalman et al., 2019).

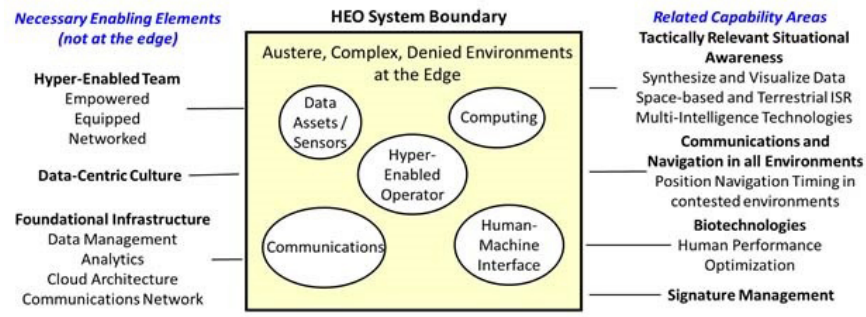


Diagrama del sistema de operadores hipercapaces (Hyper-Enabled Operators, HEO)

Su objetivo será proveer de la correcta información a cada combatiente, analista y decisor de manera oportuna sin saturarlo, enlazando todos los niveles de aprovechamiento (táctico a estratégico) de la inteligencia que es única para que cada eslabón humano realice las actividades con valor añadido y creativo que le son propias y diferenciadoras con la IA que le ayuda en el resto.

– OCTAVA. De forma global, la aplicación de la IA al ciclo de inteligencia posibilita mejores resultados.
  Tanto la IA por síntesis, que procesa grandes cantidades de datos para extraer información, como la IA lógica inductiva, que busca patrones en la información extraída, produciendo inteligencia dentro de los sistemas de apoyo de una forma concreta, benefician a los órganos decisores que utilizan el ciclo de inteligencia complejo. La intervención temprana de la IA en todas las fases permite el procesamiento acelerado para permitir su difusión inmediata.

Bibliografía

Abellanas, M. y Lodares, D. (1990). *Análisis de Algoritmos y Teoría de Grafos.* Ra-Ma.

Aranda Vasserot, A. (2023). *Las 36 estratagemas chinas. Manual Secreto del Arte de la Guerra*. Ariel.

Arévalo, A. (2018). *Inteligencia artificial, prioridad en la estrategia de defensa de EE. UU.* [Consulta: 2024]. Disponible en:_ http://hdl.handle.net/10654/21066.

Army Pubs. (2023). ATP 3-60 – Targeting, enlace doctrinal de EE. UU. En su versión para fuerzas terrestres. [Consulta: 5 de febrero de 2024]. Disponible en: https://www.armypubs.org/atp-3-60-targeting/.

Borne, K. D. (2019). Targeting in Multidomain Operations*. Military Review*. [Consulta: 5 de febrero de 2024]. Disponible en: https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2019/Borne-Targeting-Multi-domain/.

Boussad, A., Kodjabachian, J. y Meyer, C. (s.f.). *CIA evasion attacks transferability between machine learning models.* [Consulta: 5 de febrero de 2024]. Disponible en:_ https://www.cesar-conference.org/wp-content/uploads/2018/11/articles/C&ESAR_2018_J1-08_B-ADDAD_CIA_evasion_attacks_transferability_between_ML_models.pdf

Boyd, J. R. (1995). La guerra de mando y control y la teoría del OODA Loop. *Dialnet.* [Consulta: 2024]. Disponible en:_ https://dialnet.unirioja.es>descarga>articulo https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiX-Ozw8bmEAxU1gv0HHbA0DiQQFnoECDIQAQ&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F4604097.pdf&usg=AOvVaw2z_dQaNnMqiwSTcu8tOkyg&opi=89978449.

Bringas, A. (2019). The Influence of Big Data in the Intelligence Cycle. *The Security Distillery.* [Consulta: 2024]. Disponible en:_ https://thesecuritydistillery.org/all-articles/the-influence-of-big-data-in-the-intelligence-cycle.

Brown, A. L. (ed.) *et al*. (2022). *A Perilous Future: High-Intensity Conflict and the Implications for SOF. Special Operations Forces and Great Power Competition.* CANSOFCOM Education&Research Centre. Canadian Special Forces Command. [Consulta: 2024]. Disponible en: https://jsou.edu/Press/PublicationDashboard/218.

Burcher, M. y Whelan, C. (2018). Intelligence-Led Policing in Practice: Reflections From Intelligence Analysts. *Police Quarterly*. Vol. 22. [Consulta: 4 de febrero de 2024]. Disponible en: https://www.researchgate.net/publication/327294043_Intelligence-Led_Policing_in_Practice_Reflections_From_Intelligence_Analysts. DOI: 10.1177/1098611118796890.

Clarín. (2020). EE. UU. acusó a cuatro militares chinos por el robo de datos de 145 millones de personas. [Consulta: 5 de

febrero de 2024]. Disponible en: https://www.clarin.com/mundo/ee-uu-acuso-militares-chinos-robo-datos-145-millones-personas_0_xjx5F8J7.html.

De la Fuente Chacón, J. C. *et al.* (2022). *Sistemas autónomos y robótica inteligente en Defensa*. Academia de las Ciencias y las Artes Militares. EEC.

Delgado Gamella, J. L. (2020). *Sistemas de Mando y Control y su función en la ayuda humanitaria.* GMV. [Consulta: 5 de febrero de 2024]. Disponible en:_ http://www.gmv.com/media/blog/defensa-y-seguridad/sistemas-de-mando-y-control-y-su-funcion-en-la-ayuda-humanitaria.

Dhamija, P. y Bag, S. (2020). Role of artificial intelligence in operations environment: a review and bibliometric analysis. *The TQM Journal*. ISSN: 1754-2731. [Consulta: 4 de febrero de 2024]. Disponible en: https://www.emerald.com/insight/content/doi/10.1108/TQM-10-2019-0243/full/html. DOI:10.1108/TQM-10-2019-0243.

EE. UU. Joint Targeting School Student Guide. (2017). [Consulta: 5 de febrero de 2024]. Disponible en: https://www.jcs.mil/Portals/36/Documents/Doctrine/training/jts/jts_studentguide.pdf?ver=2017-12-29-171316-067

Everton, S. F. (2012). *DIFUSIÓN disrupting Dark Networks.* Cambridge University Press.

Gómez de Ágreda, Á. *et al.* (2019). *Usos militares de la inteligencia artificial, la automatización y la robótica (IAA&R).* Vol. 04/2019.

Gómez González, Á. S. (2021). Tendencias de evolución de la inteligencia militar. *Documento de Opinión IEEE 35/2021.* [Consulta: 5 de febrero de 2024]. Disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2021/DIEEEO35_2021_ANGGOM_Inteligencia.pdf.

Heuer, R. J. (1999). *Psychology of Intelligence Analysis.* Central Intelligence Agency.

Heuer, R. J. y Pherson, R. H. (2015). *Técnicas analíticas estructuradas para el análisis de inteligencia*. Madrid, Plaza y Valdés, S. L.

Herraiz, P. (2023a). ¿Por qué filtraron secretos a EE. UU. los agentes del CNI? *El Mundo*. [Consulta:_ 3 de febrero de 2024]. Disponible en: https://www.elmundo.es/espana/2023/12/05/656e2433fc6c8367208b45b3.html.

Jiménez, Á. (2021). *Inteligencia Artificial y Machine Learning al servicio de la Inteligencia* [trabajo de fin de máster]. Universidad Nebrija y ESFAS.

Joint Force Development. (2017). *Joint and National Intelligence Support to Military Operations US Joint Publication 2-01.* Vol. 297.

Kilcullen, D. (2010). *Counterinsurgency*. Oxford University Press.

Knight, W. (2017). China planea utilizar la inteligencia artificial para obtener el dominio económico mundial en 2030. *MIT Technology Review.* [Consulta: 5 de febrero de 2024]. Disponible en: https://www.technologyreview.es/s/8475/china-planea-utilizar-la-inteligencia-artificial-para-obtener-el-dominio-economico-mundial-en.

Krulak, C. C. (1999). The Strategic Corporal: Leadership in the Three Block War. *Marines Magazine.* Air University. [Consulta: 23 de noviembre de 2023]. Disponible en: https://www.mca-marines.org/wp-content/uploads/1999-Jan-The-strategic-corporal-Leadership-in-the-three-block-war.pdf.

Lauroba, E. (2021). La importancia del IMINT. *Code Space*. [Consulta: 5 de febrero de 2024]. Disponible en: https://codespaceacademy.com/importancia-imint-ciberinteligencia/.

León, G. (2020). *Repercusiones estratégicas del desarrollo tecnológico. Impacto de las tecnologías emergentes en el posicionamiento estratégico de los países.* Madrid, Ministerio de Defensa.

Leonhard, G. (2023). *Revolución: el ChatGPT y su impacto similar a la invención de Internet*. [Consulta: 5 de febrero de 2024]. Disponible en: https://www.mdzol.com/mundo/2023/5/10/revolucion-el-chatgpt-su-impacto-similar-la-invencion-de-internet-336595.html.

Liang, Q. y Xiangsui, W. (1999). *Unrestricted Warfare: China's Master Plan to Destroy America*. Natraj Publishers. New Delhi.

MacCalman, A. *et al*. (2019). The Hyper-enabled Operator. *Small Wars Journal Online.* [Consulta: 5 de febrero de 2024]. Disponible en: https://smallwarsjournal.com/jrnl/art/hyper-enabled-operator.

Martínez, L. (2016). *El Ciclo de Inteligencia Complejo: una ágil herramienta para operar en red*. Instituto Español de Estudios Estratégicos, pp. 1-15.

National Defense Strategy. (2018). *Summary of the 2018 National Defense Strategy of The United States of America.*

[Consulta: 2024]. Disponible en: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

Newcomb, T. (2023). Scientists Can Now Use WiFi to see Through People's Walls. *Popular Mechanics*. [Consulta: 5 de febrero de 2024]. Disponible en: https://www.popularmechanics.com/technology/security/a42575068/scientists-use-wifi-to-see-though-walls/.

Nieto, I. (2021). El papel de las Fuerzas Armadas en la zona gris. *Global Strategy Report*. N.º 41/2021. [Consulta: 5 de febrero de 2024]. Disponible en: https://global-strategy.org/el-papel-de-las-fuerzas-armadas-en-la-zona-gris/.

Parlamento Europeo. (2023). *Ley de IA de la UE: primera normativa sobre inteligencia artificial.* Temas. [Consulta: 5 de febrero de 2024]. Disponible en: https://www.europarl.europa.eu/topics/es/article/20230601STO93804/ley-de-ia-de-la-ue-primera-normativa-sobre-inteligencia-artificial.

Pearl, J. (2009). *Causality: Models, Reasoning, and Inference*. Cambridge University Press, Nueva York.

Pearl, J. y Mackenzie, D. (2018). *El libro del porqué. La nueva ciencia de la causa y el efecto*. Editorial Pasado&Presente, p. 39.

Pérez Triana, J. M. (2023). *¿Libertad para innovar en una autocracia? Duelo por la hegemonía tecnológica militar: China copia, roba y desarrolla, ¿pero podrá innovar?* [Consulta: 5 de febrero de 2024]. Disponible en: https://www.elconfidencial.com/tecnologia/2023-03-02/hegemonia-tecnologia-militar-eeuu-china-innovacion_3585169/.

Pérez González, N. y Sánchez, M. (2019). *Inteligencia Artificial: la cuarta Revolución Industrial.* [Consulta: 5 de febrero de 2024]. Disponible en: https://www.ayming.es/insights-y-noticias/noticias/inteligencia-artificial-la-cuarta-revolucion-industrial/.

Pillsbury, M. (2015). The *Hundred-Year Marathon. China's Secret Strategy to Replace America as the Global Superpower.* Henry Holt and Company. New York. Reedición con St. Martin's Griffin. 2016.

Política Exterior. (2024). Europa se abre paso en materia de IA. N.º 1358. [Consulta: 18 de febrero de 2024]. Disponible en: https://www.politicaexterior.com/articulo-completo/europa-se-abre-paso-en-materia-de-ia-342290/

Porche, I. R. *et al.* (2013). *Redefining Information Warfare Boundaries for an Army in a Wireless World*. Santa Monica, CA:

RAND Corporation. [Consulta: 5 de febrero de 2024]. Disponible en: https://www.rand.org/pubs/monographs/MG1113.html.

Rainer Granados, J. J. *et al*. (2019). *La inteligencia artificial aplicada a la defense.* Documentos de Seguridad y Defensa 79. Madrid, Ministerio de Defensa.

Representación en España de la Comisión Europea. (2024). *Las Claves de la nueva ley de Inteligencia Artificial*. Comisión Europea. Grupo independiente de expertos de alto nivel sobre Inteligencia Artificial. [Consulta: 4 de febrero de 2024]. Disponible en: https://spain.representation.ec.europa.eu/noticias-eventos/noticias-0/las-claves-de-la-nueva-ley-de-inteligencia-artificial-2024-01-25_es.

Request for information Management. (s.f.). [Consulta: 5 de febrero de 2024]. Disponible en: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiox63giZeEAxX_g_0HHZ2gDBEQFnoECBAQAQ&url=https%3A%2F%2Fresourcehub01.blob.core.windows.net%2Ftraining-files%2FTraining%2520Materials%2F042%2520PKISR%2520RTP%2F042-011%2520PKISR%2520RTP%2520Lesson%25203.4%2520RFI%2520Management.pdf&usg=AOvVaw0DO5ill-4zkGVFb0jcnBRW&opi=89978449.

Roldán, F. S. (2012). Opinión e Inteligencia. *Documento de opinión IEEE 1-4*. [Consulta: 2024]. Disponible en: http://www.ieee.es/contenido/noticias/2012/06/DIEEEO45-2012.html.

Roldán, J. M. *et al.* (2018). *La inteligencia artificial aplicada a la defensa*. Madrid.

Rosales, I. A. *et al*. (2005). *El papel de la inteligencia ante los retos de la seguridad y la defensa internacional.* Madrid, Ministerio de Defensa.

Rouhiainen, L. (2018). *Inteligencia Artificial: 101 cosas que debes saber hoy sobre nuestro futuro inteligencia artificial.* Barcelona, Editorial Planeta, S. A.

Ruiz Enebral, A. (2023). Defensa instala terminales del nuevo sistema de gestión de información clasificada [en línea]. *El Confidencial Digital.* [Consulta: 5 de febrero de 2024]. Disponible en: https://www.elconfidencialdigital.com/articulo/defensa/defensa-instala-terminales-nuevo-sistema-gestion-informacion-clasificada/20231218000000688906.html#emstrongrenovacion-tecnologica-strong-em.

Russell, S. y Norvig. P. (2004). *Inteligencia Artificial, Un enfoque moderno*. Madrid, PEARSON Prentice Hall. [Consulta: 2024].

Disponible en: Tendencias de evolución de la inteligencia militar (ieee.es).

Ruvalcaba, E. (2004). Sistemas de soporte a la decisión o DSS. *Gestiopolis*. [Consulta: 2024]. Disponible en: https://www.gestiopolis.com/sistemas-soporte-decision-dss/.

Saling, J. M. (1999). *Dynamic Re-Tasking: The JFACC and the Airborne Strike Package*. Defense Technical Information Center. [Consulta: 5 de febrero de 2024]. Disponible en: https://apps.dtic.mil/sti/citations/ADA398855.

Scott, B. y Michell, A. (2022). Enhancing Situational Understanding through Integration of Artificial Intelligence in Tactical Headquarters. *Army University Press.* [Consulta: 4 de febrero de 2024]. Disponible en: https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/November-December-2022/Scott/

Tariq, M. U., Poulin, M. y Abonamah, A. A. (2021). Achieving Operational Excellence Through Artificial Intelligence: Driving Forces and Barriers. *Frontiers in psychology*. Vol.º 12, p. 686624. [Consulta: 4 de febrero de 2024]. DOI: https://doi.org/10.3389/fpsyg.2021.686624. Disponible en: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8295597/.

UK Ministry of Defence (2011). *DCDC. Understanding and Intelligence Support to Joint Operations (JDP 2-00).*

Urquizu, P. (2009). ¿Qué es un DSS? [en línea]. *Business Intelligence.* [Consulta: 4 de febrero de 2024]. Disponible en: https://www.businessintelligence.info/dss/dss-apoyo-decisiones.html.