EL USO DE LLM EN EL PROCESO DE OBTENCIÓN Y ANÁLISIS DE INTELIGENCIA

Introducción

La obtención de inteligencia y las prácticas de espionaje han ejercido un papel fundamental en la historia militar. Desde la antigüedad, la ventaja informativa ha decidido conflictos bélicos. Un ejemplo paradigmático fue la planificación de la Operación Overlord (D-Day) en 1944, en la que los aliados emplearon múltiples fuentes de inteligencia, como imágenes aéreas, redes de agentes locales, interceptación y descifrado de comunicaciones, para mapear las defensas y prever los movimientos del enemigo con el fin de decidir el momento oportuno del desembarco. Esta fusión de información permitió planificar con un alto grado de precisión la mayor operación anfibia de la historia, demostrando que el éxito operativo depende de transformar datos dispersos en conocimiento útil para el mando y la acción. Si bien los principios básicos de conocer al adversario y explotar información siguen manteniendo una naturaleza similar, el entorno actual, fuertemente influenciado por las nuevas tecnologías, presenta nuevas oportunidades y a su vez nuevos retos a los que enfrentarse. La proliferación de fuentes abiertas (medios digitales, redes sociales, bases de datos públicas) genera un volumen de datos sin precedentes, difícilmente abarcable con medios tradicionales. En paralelo, la revolución tecnológica, especialmente en inteligencia artificial (IA), ofrece herramientas potentes para procesar y analizar esa información. En los últimos años han emergido los grandes modelos de lenguaje (LLM, por sus siglas en inglés) como exponente de esta innovación, capaces de generar y comprender texto con una calidad cercana a la humana, como demuestran modelos y aplicaciones como ChatGPT, Copilot o LlaMA2. Estas capacidades sugieren un potencial transformador en el ámbito de la seguridad y defensa, donde disponer de la información correcta en el momento adecuado puede marcar la diferencia [1] [2].

Organizaciones militares y de inteligencia ya exploran el empleo de IA generativa. La OTAN, por ejemplo, ha desarrollado el proyecto AI Felix con varias aplicaciones de IA orientadas a automatizar tareas burocráticas y apoyar la toma de decisiones. Recientemente ha introducido un asistente digital de inteligencia artificial (AIDA), una aplicación basada en modelos generativos/LLM, entrenada sobre conocimiento clasificado de la Alianza para proporcionar «la información correcta, en el momento justo, a las personas adecuadas». De igual modo, estudios académicos recientes examinan cómo herramientas como ChatGPT pueden emplearse como asistentes virtuales

para analistas de inteligencia, apoyando labores de búsqueda, procesamiento de información y elaboración de informes. Se ha demostrado que los LLM poseen habilidades destacadas de procesamiento del lenguaje natural útiles en inteligencia: desde la recuperación rápida de datos pertinentes hasta la síntesis y apoyo a la toma de decisiones basadas en información. En mi Trabajo de Fin de Grado de la Universidad de Vigo, *Asistente Virtual Telegram para la interpretación de documentos*, explico cómo el uso de un LLM ajustado y entrenado puede facilitar a un analista de inteligencia para mejorar distintas facetas de su trabajo, desde la recolección y fusión de datos hasta el análisis, la elaboración de informes y el intercambio de información. Los resultados resaltan el amplio potencial de estas herramientas, evidenciando que pueden apoyar tareas complejas; sin embargo, aún carecen de pleno grado de fiabilidad y optimización, por lo que requerirán un proceso de desarrollo y adaptación para proporcionar su plena eficiencia y efectividad [1] [2] [3].

Large language models (LLM)

Los modelos de lenguaje de gran tamaño (LLM) son sistemas de inteligencia artificial entrenados sobre enormes volúmenes de texto con el objetivo de comprender, generar y manipular lenguaje natural. Su funcionamiento se basa en arquitecturas de redes neuronales profundas, particularmente los *Transformers*, que permiten procesar secuencias de palabras y predecir con alta precisión la palabra siguiente en función del contexto anterior. Estos modelos no están programados con reglas explícitas, sino que aprenden patrones lingüísticos, relaciones semánticas y estructuras gramaticales a partir de los datos [4] [5].

Los LLM actuales, como GPT-5, PaLM o LlaMA, pueden realizar tareas complejas tales como resumen de documentos, traducción, generación de informes o clasificación temática, lo que los convierte en herramientas versátiles para aplicaciones en ámbitos como la inteligencia militar, la defensa o la ciberseguridad. Además, con las herramientas adecuadas es posible entrenar, ajustar o dotar de información concreta a los modelos para adaptarlos a las necesidades específicas de la inteligencia militar [6] [7].

Entre estas herramientas se encuentran las siguientes:

— *Fine-tuning* (ajuste fino): consiste en reajustar los pesos de la red neuronal que compone

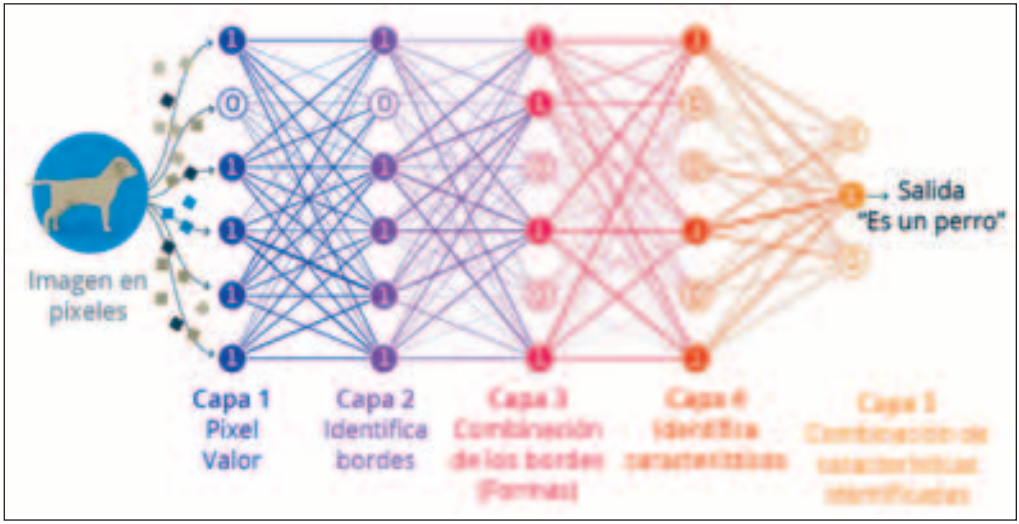

Figura 1. Ejemplo de red neuronal profunda [4]

el modelo de IA mediante el uso de un *dataset* específico proporcionado por el usuario. Este conjunto de datos puede incluir textos —manuales doctrinales, reglamentos operativos, informes de inteligencia—, imágenes u otros elementos relevantes que permitan al modelo adaptarse al contexto militar y mejorar su capacidad de interpretación e interacción [8].

— *Supervised fine-tuning* (ajuste fino supervisado): es una variante del ajuste fino en la que se expone al modelo a ejemplos concretos de tareas reales con el objetivo de que aprenda a realizarlas de forma precisa. Estas tareas pueden estar relacionadas con redacción de partes, análisis de inteligencia o aplicación de reglas de enfrentamiento, entre otras, y se orientan según los criterios definidos por un supervisor humano.

— *Reinforcement learning with human feedback* (aprendizaje por refuerzo con retroalimentación humana): este método permite refinar el comportamiento del modelo mediante un sistema de recompensas basado en la evaluación humana de sus respuestas. Es especialmente útil en entornos sensibles como la inteligencia militar, ya que permite ajustar el modelo para que responda de manera alineada con valores, normas y objetivos específicos, minimizando desviaciones o errores críticos.

— *Retrieval-augmented generation* (generación aumentada por recuperación): consiste en dotar al modelo de la capacidad de acceder dinámicamente a bases de conocimiento externas (documentos doctrinales, partes de inteligencia, bases OSINT, etc.) antes de generar

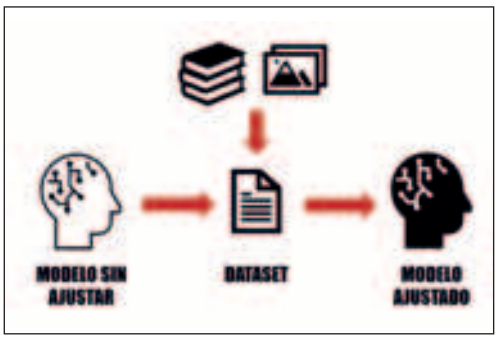

Figura 2. Proceso de *fine-tuning*. (Elaboración propia)

su respuesta. De este modo, el LLM no depende únicamente de su conocimiento entrenado, sino que combina procesamiento lingüístico con recuperación de información relevante en tiempo real. Este enfoque permite mantener la información actualizada y confiable sin necesidad de reentrenar constantemente el modelo [9].

— *Prompt engineering* y plantillas de instrucciones: diseñar cuidadosamente las instrucciones o *prompts* que se proporcionan al modelo es esencial para controlar el tipo, tono y estructura de la respuesta. En el ámbito militar, esto puede incluir plantillas específicas para partes SITREP (*Situation Report*), informes INTSUM (*Intelligence Summary*) o cualquier estructura similar.

Figura 3. Ciclo de la inteligencia. (Elaboración propia)

Para poder integrar estas herramientas correctamente, se debería realizar una implementación segura en un entorno cerrado, es decir, el modelo debería ser construido y ejecutado en entornos de red cerrados, aislados de internet y con capacidad de auditoría [10] [11].

Aplicaciones de los LLM en la inteligencia

El proceso de obtención y análisis de inteligencia se estructura en torno a un ciclo continuo y dinámico que garantiza la transformación de información dispersa en conocimiento útil para la toma de decisiones. Tradicionalmente, este ciclo consta de cinco fases interdependientes: planificación, obtención de datos, procesamiento, análisis, difusión y evaluación del ciclo (figura 3). En la fase de planeamiento, se definen los requerimientos de inteligencia y se priorizan los objetivos de recolección. A continuación, en la fase de obtención, se recogen datos provenientes de las diversas fuentes de obtención. Posteriormente, estos datos son procesados para facilitar su análisis, lo que implica su depuración, estructuración y codificación. La fase de análisis consiste en evaluar, interpretar y fusionar la información disponible para generar inteligencia valorada. A continuación, la fase de difusión garantiza que el producto resultante llegue oportunamente a los niveles operativos o estratégicos que lo requieran. Finalmente, se evalúa el ciclo para detectar los errores cometidos y optimizar el proceso. Este modelo, recogido doctrinalmente en la *Allied Joint Doctrine for Intelligence Procedures* (AJP-2.0) de la OTAN, constituye la base estructural de los sistemas de inteligencia modernos. La incorporación de tecnologías como los modelos de lenguaje y la inteligencia artificial está comenzando a transformar cada una de estas etapas, mejorando su eficiencia, alcance y capacidad de respuesta [12].

Como se puede observar en la figura 4, la obtención de inteligencia se nutre de diversas fuentes clasificadas tradicionalmente en disciplinas como HUMINT (inteligencia humana), SIGINT (inteligencia de señales), IMINT (inteligencia de imágenes), MASINT (medición y firmas), TECHINT (inteligencia técnica) y OSINT (inteligencia de fuentes abiertas). Cada una aporta perspectivas únicas sobre las capacidades, intenciones o actividades de actores adversarios o aliados. En este contexto, la inteligencia de fuentes abiertas ha cobrado un papel creciente debido al volumen y accesibilidad de la información disponible en internet, redes sociales y medios digitales, donde los modelos de lenguaje de gran tamaño (LLM) y la inteligencia artificial están demostrando una utilidad operativa creciente [14].

La inteligencia de fuentes abiertas (OSINT, *Open Source Intelligence*) se define clásicamente como la inteligencia obtenida a partir de información disponible públicamente. En la legislación de Estados Unidos (Ley Pública 109-163) se describe OSINT como «aquella inteligencia producida a partir de información disponible públicamente que se recopila, explota y difunde de manera oportuna a una audiencia apropiada con el propósito de atender un requisito de inteligencia específico». Asimismo, la doctrina aliada la define como «aquella inteligencia derivada de información disponible públicamente, así como de otra información no clasificada que tiene una distribución o acceso público limitado». En otras palabras, OSINT abarca todo conocimiento útil obtenido de fuentes abiertas o accesibles: medios de comunicación, redes sociales, sitios web, registros públicos, imágenes satelitales comerciales, entre otros. Se distingue de otras disciplinas de obtención (HUMINT, SIGINT, IMINT, etc.) en que la información origen no es secreta ni clasificada, aunque su recopilación y análisis sistemáticos pueden revelar inteligencia valiosa [14].

En las últimas décadas, la importancia de la OSINT ha crecido exponencialmente impulsada por el avance de la era digital. Hoy la información pública relevante abunda en internet, desde foros y redes sociales hasta bases de datos académicas o comerciales que pueden

Figura 4. Principales fuentes de inteligencia. (Elaboración propia)

resultar muy útiles para analizar actividades de adversarios, detectar cambios en el entorno operativo o determinar la opinión pública sobre cualquier materia. Tal y como cita el exdirector del NATO International Military Staff, sir Christopher Parker, la OSINT es ahora «más importante y más poderoso que nunca», aunque reconoce también que su potencial aún no se explota plenamente por falta de inversión y por una cultura tradicional que favorece las fuentes clasificadas. Sin embargo, es un hecho que la inteligencia artificial se vislumbra como el habilitador clave para cribar esta masa de información abierta: la OTAN ha instado a sus miembros a superar barreras y adoptar OSINT potenciado por IA como complemento del ciclo de inteligencia convencional. Integrada adecuadamente, la OSINT automatizada puede proveer a los analistas militares una comprensión rápida y actualizada de su entorno operacional, respondiendo a preguntas del tipo quién hace qué, cuándo y dónde con la inmediatez que el ritmo de las crisis actuales exige.

La automatización de OSINT mediante LLM permitiría manejar volúmenes masivos de datos abiertos de forma eficiente. Un modelo de lenguaje puede, por ejemplo, monitorear miles de fuentes en tiempo real, filtrando las relevantes y descartando ruido, algo inviable para un equipo humano. Asimismo, los LLM pueden resumir rápidamente documentos extensos, noticias o informes, extrayendo las claves para que el analista humano focalice su atención. Otra capacidad importante podría ser la identificación de menciones y referencias específicas en el torrente informativo: un LLM entrenado en el dominio de defensa puede reconocer con alta precisión términos militares, nombres de unidades, sistemas de armamento o lugares estratégicos dentro de un texto [14].

Por su naturaleza accesible, la OSINT desempeña un papel fundamental en las fases iniciales del ciclo de inteligencia, especialmente en las de obtención y procesamiento, aunque su valor se extiende también al análisis, al complementar productos derivados de fuentes clasificadas. Un ejemplo actual de aplicación de OSINT potenciada por inteligencia artificial es la plataforma Horizon, desarrollada por la empresa británica Logically. Esta herramienta permite rastrear, analizar y visualizar campañas de desinformación, actividad coordinada y narrativas emergentes en redes sociales, medios digitales y foros, combinando técnicas de análisis de redes, *machine learning* y modelos de lenguaje. Utilizada por organismos gubernamentales y unidades de defensa, ha demostrado su eficacia en conflictos recientes, como la guerra de Ucrania, proporcionando análisis situacional en tiempo real y contribuyendo a la alerta temprana frente a amenazas informativas. Este tipo de capacidades, integradas en arquitecturas de inteligencia híbrida, permiten prever y neutralizar amenazas antes de que se materialicen. De hecho, algunas personas apuntan que integrando la OSINT en el ciclo más amplio de inteligencia y potenciándola con IA se pueden «prever, disuadir y derrotar esfuerzos adversarios» antes de que representen un peligro tangible. El analista aumenta su capacidad de alerta temprana, ya que, además de comprender lo ocurrido, puede vislumbrar lo que el adversario podría estar planeando hacer con semanas o meses de antelación. Todo ello se consigue liberando al analista humano de la tarea de cribar manualmente montañas de publicaciones, permitiéndole enfocarse en la interpretación y juicio, que siguen siendo insustituibles [15].

Además de su uso consolidado en OSINT, los modelos de lenguaje de gran tamaño (LLM) están ganando posición como herramientas de apoyo en otras disciplinas de inteligencia. En el ámbito de la inteligencia de señales (SIGINT), los LLM ofrecen capacidades notables para analizar grandes volúmenes de comunicaciones interceptadas, especialmente cuando éstas incluyen lenguaje natural no estructurado, como mensajes de texto, correos electrónicos, chats o transcripciones de voz. Pueden emplearse para realizar traducciones automáticas en múltiples idiomas, clasificar conversaciones por tema o nivel de riesgo y detectar patrones lingüísticos o semánticos indicativos de actividad sospechosa. Investigaciones recientes han explorado incluso su uso en la identificación de técnicas de cifrado y en el análisis de vulnerabilidades criptográficas. La ventaja clave radica en su capacidad para realizar un preprocesamiento inteligente que priorice los flujos de información más relevantes para el analista, aliviando la sobrecarga cognitiva que caracteriza a entornos con alta densidad de datos SIGINT [16] [17].

Otro campo de aplicación relevante lo encontramos en la guerra electrónica, concretamente en la detección temprana de sistemas aéreos no tripulados (RPAS). Un modelo de lenguaje adecuadamente configurado y entrenado puede analizar los parámetros electromagnéticos captados por receptores de señales, como frecuencia, modulación o firma espectral, y asociarlos a perfiles conocidos de drones. A partir de esta correlación, el sistema puede generar una estimación probabilística sobre el tipo de RPAS detectado, asignando además un nivel de amenaza en función de su comportamiento, procedencia o capacidades conocidas

Figura 5. Operador usando IA para alerta temprana de RPAS. (Imagen elaborada con IA)

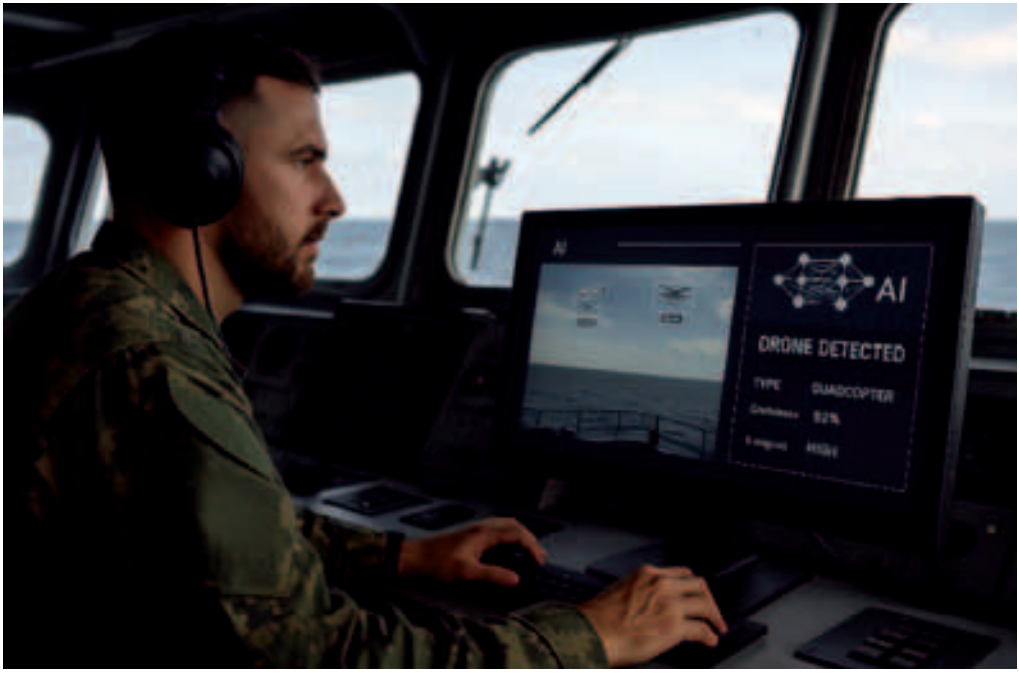

Figura 6. Operador usando IA en una obtención de HUMINT. (Imagen elaborada con IA)

(figura 5). Esta integración permite acelerar la clasificación de amenazas emergentes en escenarios donde el tiempo de reacción es crítico.

En lo que respecta a la inteligencia humana (HUMINT), los LLM pueden actuar como asistentes en el análisis de testimonios, entrevistas operativas o informes de contacto, ayudando a extraer entidades clave, detectar cambios de tono o contradicciones sutiles e incluso generar resúmenes sintéticos orientados al tipo de operación (figura 6). Asimismo, pueden ser entrenados para respetar los protocolos doctrinales en la elaboración de informes de primera mano (como los SALUTE o los partes de contacto). En el ámbito de la inteligencia de imágenes (IMINT), aunque los modelos visuales son los protagonistas en la detección automática de objetos o cambios geoespaciales, los LLM pueden integrarse como parte de sistemas multimodales, encargándose de transformar los hallazgos visuales en descripciones textuales útiles para el mando o para otros analistas. Esta combinación ha sido objeto de estudio en programas piloto liderados por agencias de defensa de Estados Unidos y de la OTAN con el objetivo de fusionar datos SIGINT, IMINT y OSINT mediante modelos lingüísticos centralizados que generen productos analíticos coherentes, contextualizados y en tiempo real. Así, los LLM no sólo mejoran la eficiencia de las tareas específicas, sino que contribuyen a la interoperabilidad y a la síntesis entre distintas disciplinas de inteligencia [18] [19].

Desafíos y consideraciones éticas-operativas en el uso de LLM

A pesar de sus ventajas, la incorporación de LLM e IA en el proceso de inteligencia conlleva una serie de desafíos y consideraciones que es imprescindible abordar. Entre los principales puntos de atención, conforme a la doctrina OTAN y la experiencia de diversas organizaciones de defensa, encontramos los siguientes:

— *Fiabilidad de la información y sesgos algorítmicos*: los grandes modelos del lenguaje pueden cometer errores o generar contenido incorrecto (alucinaciones) con convicción aparente, y es un hecho que en inteligencia basarse en un análisis erróneo puede ser desastroso. Además, los modelos aprenden de datos abiertos que conllevan sesgos (culturales, ideológicos, doctrinales) que podrían trasladarse a sus salidas. Es crucial por tanto implementar métodos de validación y verificación de los resultados proporcionados por la IA y aplicar mecanismos de mitigación de sesgos. La OTAN ha establecido explícitamente la mitigación de posibles sesgos como uno de los seis principios rectores para un uso responsable de la IA en defensa. Se deben tomar medidas proactivas para minimizar sesgos no deseados en los algoritmos y en los datos con que se entrenan, asegurando que las conclusiones del LLM no estén contaminadas por prejuicios sistemáticos. Igualmente, la explicabilidad es importante, ya que los analistas requieren comprender, aunque sea de forma básica, por qué la IA sugiere una determinada conclusión, a fin de confiar en ella. Por ello, la OTAN aboga por la trazabilidad y transparencia de las aplicaciones de IA, incluyendo mecanismos de auditoría de los modelos [2] [18] [19].

— *Barreras organizativas y culturales*: la adopción de IA en comunidades de inteligencia tradicionales enfrenta inercias y desconfianza. Un estudio del Royal United Services Institute identificó que, junto a retos técnicos, existe un importante obstáculo cultural, pues muchos analistas y decisores tienden a otorgar mayor confianza a la información clasificada y a las fuentes secretas que a la inteligencia abierta asistida por IA. Esta reticencia en confiar en herramientas algorítmicas puede limitar su aprovechamiento. De hecho, se ha observado en la OTAN que persiste un escepticismo hacia la información de fuentes abiertas, percibida como de menor valor. Superar este sesgo requerirá capacitación, casos de éxito y, sobre todo, establecer claramente el rol de la IA como apoyo (y no sustituto) del analista. Es vital definir nuevos procedimientos que integren las salidas de IA en el ciclo analítico y ajustar la doctrina y entrenamiento en consecuencia. Asimismo, la implementación de LLM en inteligencia requiere afrontar desafíos como la inversión en infraestructuras seguras, el acceso a extensos conjuntos de datos de entrenamiento y la capacitación de personal experto en ciencia de datos [11] [17].

— *Seguridad de la información y adversarios en la era de la IA*: al emplear modelos de lenguaje se deben extremar las precauciones de ciberseguridad y protección de la información sensible. Un riesgo latente es la filtración de datos clasificados si, por ejemplo, los analistas introducen en un LLM público, como ChatGPT, fragmentos de informes confidenciales buscando su resumen. Esto podría exponer secretos a sistemas fuera del control militar. Varias organizaciones han prohibido el uso de *chatbots* públicos en entornos gubernamentales precisamente por este motivo. La solución pasa por utilizar modelos cerrados y controlados, instalados en redes clasificadas

o con blindaje de datos. Para ello, sería necesario que las Fuerzas Armadas cuenten con su propio modelo entrenado o ajustado (*fine-tuned*) sobre bases doctrinales y datos internos validados, ejecutado en infraestructuras seguras, aisladas de internet, y sometido a auditorías regulares. Esta implementación debe ir acompañada de políticas de control de acceso, cifrado robusto, procesos de revisión humana y formación especializada del personal en ciencia de datos y manejo ético de la IA.

Por otra parte, la irrupción de la IA en inteligencia es un arma de doble filo, ya que el «adversario» también puede utilizarla. Se vislumbra una carrera armamentística algorítmica en la que cada bando intenta aprovechar la IA para superar al otro. Esta dinámica obliga a estar un paso adelante en la adopción de IA, pero con prudencia, ya que cualquier herramienta puede volverse en contra si el enemigo logra infiltrarla o engañarla. Un ejemplo de debilidad clara es la posible manipulación de datos de entrenamiento o de los insumos que consume la IA, por ejemplo, inundando las redes sociales con desinformación específica para sesgar el análisis automatizado. Mitigar esto requiere robustecer los modelos contra ataques adversarios, diversificar fuentes para corroborar la información y mantener siempre al mando el juicio humano ante posibles anomalías [19]:

— *Consideraciones éticas y legales*: el empleo de IA en operaciones militares debe regirse por los mismos valores y marcos legales que cualquier otra capacidad. La OTAN, en su estrategia de IA, ha definido principios de legalidad, responsabilidad, gobernanza, fiabilidad, trazabilidad y mitigación de sesgos para guiar el desarrollo y uso de estas tecnologías. Un debate ético recurrente es el grado de autonomía que se otorga a la IA en la toma de decisiones. En el contexto de inteligencia, podría plantearse si un LLM debiera, por ejemplo, determinar automáticamente que cierto individuo es una amenaza y elevarlo a una lista de objetivos. La doctrina mayoritaria sostiene que decisiones de ese calibre no pueden delegarse completamente en máquinas. Autores españoles de la Universidad de Navarra argumentan que no se debe permitir que sistemas autónomos seleccionen y ataquen objetivos por su cuenta, dada su falta de empatía y de capacidad para discernir matices legales y morales. La decisión de clasificar a una entidad u objetivo como amenaza o de actuar contra ella debe recaer en un humano responsable, que sopese contexto, fiabilidad y consecuencias. En línea con ello, la OTAN enfatiza la responsabilidad de los operadores, considerando que deberían rendir cuentas del uso de IA igual que de cualquier arma o medio. Por último, la integración de LLM debe hacerse asegurando en la medida de lo posible el cumplimiento legal (leyes nacionales, derecho internacional humanitario, derechos humanos), la protección de la privacidad, los derechos civiles (especialmente cuando se analiza *big data* que pudiera incluir datos personales de ciudadanos) y la transparencia hacia la sociedad. Además, es imprescindible respetar los términos de uso y políticas de las plataformas cuyas fuentes se exploten. Redes sociales como Facebook prohíben expresamente el uso de sus servicios con fines bélicos, y cualquier tratamiento de datos debe ajustarse a las condiciones de uso y a la normativa de protección de datos aplicable. Ignorar estas restricciones puede no sólo vulnerar derechos fundamentales, sino comprometer la legitimidad y legalidad de toda operación de obtención y análisis de inteligencia [20] [21].

Teniendo en cuenta todo lo anterior, lo implementación exitosa de los LLM en inteligencia demandará avances técnicos y también ajustes doctrinales, normativos y culturales. El desarrollo e implementación de las nuevas tecnologías requerirá un enfoque de *human-machine teaming*, en el que las fortalezas de la IA complementen a las del analista humano en un marco de confianza y control apropiado. La formación del personal será igualmente clave: los futuros analistas de inteligencia deberán ser tan competentes en análisis estratégico como en entender y manejar herramientas de IA. Sólo así se podrá aprovechar el potencial de estos sistemas de forma segura y ética [22] [23].

Conclusiones

La irrupción de los modelos de lenguaje de gran tamaño en la inteligencia militar no supone únicamente un cambio tecnológico, sino un replanteamiento fundamental sobre cómo desarrollamos, gestionamos y explotamos el conocimiento estratégico. Este nuevo contexto no ofrece respuestas fáciles ni soluciones automáticas, ya que presenta desafíos que trascienden la técnica y alcanzan lo ético, lo doctrinal y lo organizativo. La evolución futura dependerá críticamente de nuestra capacidad para integrar la tecnología de manera consciente y responsable, reconociendo tanto su poder transformador como sus limitaciones inherentes. En última instancia, serán las decisiones humanas, respaldadas pero no reemplazadas por la IA, las que determinen el éxito operativo y estratégico.

El camino hacia la inteligencia militar del futuro está marcado por la necesidad de una adaptación constante y una vigilancia permanente. Sólo mediante el entendimiento profundo de estas tecnologías y una actitud proactiva ante sus desafíos podremos mantener la ventaja estratégica en un entorno de seguridad global cada vez más complejo. La tecnología ha abierto la puerta a nuevas posibilidades; ahora corresponde a la comunidad de defensa garantizar que estas capacidades se aprovechen plenamente, siempre bajo el mando firme del criterio humano.

Es innegable que la IA está aquí para quedarse, y su lugar en la historia de la inteligencia militar dependerá enteramente de nuestra habilidad para comprenderla, controlarla y aplicarla con sabiduría.

BIBLIOGRAFÍA

[1] NATO (2024a): AI Felix & AIDA: Asistentes digitales para la toma de decisiones militares. Presentaciones internas de la Alianza, 2024.

[2] NATO (2024b): «Summary of the NATO Artificial Intelligence (AI) Strategy», 10 julio [*online*]. Disponible: *https://www.nato.int/cps/en/natohq/official_texts_227237.htm*

[3] Fernández Conde, G. (2025): *Asistente virtual Telegram para la interpretación de documentos*. Trabajo Fin de Grado. Universidad de Vigo. Escuela de Ingenieros de la Armada.

[4] Wolchover, N.: «New theory cracks open the black box of deep learning». *Quanta Magazine*, 21 septiembre 2017 [*online*]. Disponible: *https://www.quantamagazine.org/new-theory-cracks-open-the-black-box-of-deep-learning-20170921/*

[5] Vaswani, A., *et al.*: «Attention is All You Need». *Advances in Neural Information Processing Systems (NeurIPS)*, vol. 30, 2017 [*online*]. Disponible: *https://proceedings.neurips.cc/paper_files/paper/2017/file/3f5ee243547dee91fbd053c1c4a845aa-Paper.pdf*

[6] Narang, S.; Chowdhery, A.: «PaLM: Scaling Language Modeling with Pathways». Google AI Blog, 2022 [*online*]. Disponible: *https://ai.googleblog.com/2022/04/pathways-language-model-palm-scaling-to.html*

[7] «GPT-4 Technical Report», 2023. *OpenAI* [*online*]. Disponible: *https://openai.com/research/gpt-4*

[8] «Fine-tuning pretrained models. Transformers Documentation». *Hugging Face* [*online*]. Disponible: *https://huggingface.co/docs/transformers/training*

[9] Lewis, P., *et al.*: «Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks». NeurIPS 2020 [*online*]. Disponible: *https://arxiv.org/abs/2005.11401*

[10] OTAN, Science & Technology Trends 2023-2043. NATO STO, 2023 [*online*]. Disponible: *https://www.nato.int/science/technology-trends*

[11] ENISA (European Union Agency for Cybersecurity). Artificial Intelligence Threat Landscape, 2023 [*online*]. Disponible: *https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025%20Booklet.pdf*

[12] *AJP-2.0 Allied Joint Intelligence Doctrine*. NATO Standardization Office, 2001.

[13] «Generative AI in the Defense Sector». *Arize*, 2024 [*online*]. Disponible: *https://arize.com/resource/generative-ai-in-the-defense-sector*

[14] Harper, C., & Bassett Cross, R.: «NATO must recognize the potential of open-source intelligence». *Atlantic Council-New Atlanticist*, 2024 [*online*]. Disponible: *https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-must-recognize-the-potential-of-open-source-intelligence/*

[15] «ShadowDragon Releases. The OSINT Platform, Horizon». *Business Wire*, 13 abril 2024 [*online*]. Disponible: *https://www.businesswire.com/news/home/20240413210644/en/ShadowDragon-Releases-The-OSINT-Platform-Horizon*

[16] Kim, B. D., Vasudevan, V. A., D'Oliveira, R. G. L., Cohen, A., Stahlbuhk, T., & Médard, M.: «Cryptanalysis via Machine Learning Based Information Theoretic Metrics». arXiv preprint, 2025 [online]. Disponible: https://arxiv.org/abs/2501.15076

[17] O'Toole, B.: «Using ChatGPT to Break Encryption LinkedIn», 2023 [*online*]. Disponible: *https://www.linkedin.com/pulse/using-chatgpt-break-encryption-brian-o-toole*

[18] Nitzl, C., *et al.*: «The Use of Artificial Intelligence in Military Intelligence». Munich: Bundeswehr University Munich, 2024 [*online*]. Disponible: *https://arxiv.org/abs/2412.03610*

[19] Moret, V.: «Estrategia OTAN sobre Inteligencia Artificial». ACAMI, 2021 [*online*]. Disponible: *https://www.acami.es/noticia/estrategia-otan-sobre-inteligencia-artificial/*

[20] Las Heras, P.: «El reto de la inteligencia artificial para la seguridad y defensa», 2023 [*online*]. Disponible: *https://www.unav.edu/web/global-affairs/el-reto-de-la-inteligencia-artificial-para-la-seguridad-y-defensa*

[21] Meta Platforms, Inc., Terms of Service, consultados en junio 2025 [*online*]. https://www.facebook.com/terms/

[22] Goecks, V. G., & Waytowich, N.: «COA-GPT: Generative Pre-trained Transformers for Accelerated Course of Action Development in Military Operations». US Army Research Lab., 2024.

[23] «What ChatGPT Can and Can't Do for Intelligence», marzo 2023. *Lawfare Blog* [*online*]. Disponible: *https://www.lawfareblog.com*