"*INTELIGENCIA ARTIFICIAL EN LA SELECCIÓN DE OBJETIVOS*"

Facultad de Ciencias Jurídicas y Sociales

Universidad Rey Juan Carlos

Cátedra de Servicios de Inteligencia y Sistemas Democráticos

Luciano Blázquez Morilla

Alberto Rubiano

Adrián Varó López

Juan Tejeda Melero

16/11/2024

1. INTRODUCCIÓN

1.1 ¿Qué es la Inteligencia Artificial?

Cabe decir que la Inteligencia artificial no tiene una definición formal y universalmente aceptada.

Google define la inteligencia artificial (IA) como un conjunto de tecnologías que permiten que las computadoras realicen una variedad de funciones avanzadas, incluida la capacidad de ver, comprender y traducir lenguaje hablado y escrito, analizar datos, hacer recomendaciones…

La Comisión Europea la define como como sistemas de software (y posiblemente también de hardware) diseñados por humanos que, ante un objetivo complejo, actúan en la dimensión física o digital:

- Percibiendo su entorno, a través de la adquisición e interpretación de datos estructurados o no estructurados.
- Razonando sobre el conocimiento, procesando la información derivada de estos datos y decidiendo las mejores acciones para lograr el objetivo dado.

ChatGPT, seguramente la inteligencia artificial más conocida y una de las más avanzadas para el uso a nivel de usuario, define la IA como un campo de la informática que busca crear sistemas y programas capaces de realizar tareas que normalmente requieren inteligencia humana. Esto incluye habilidades como el razonamiento, el aprendizaje, la resolución de problemas, la comprensión del lenguaje, la percepción y la toma de decisiones.

Es la capacidad de una máquina o software para simular comportamientos inteligentes, como:

- **Aprendizaje**: Adaptarse y mejorar a partir de la experiencia (ej. aprendizaje automático o *machine learning*).

- **Razonamiento**: Tomar decisiones basadas en datos o situaciones complejas.
- **Percepción**: Interpretar información del entorno, como a través de cámaras, micrófonos o sensores.
- **Lenguaje Natural**: Comprender y generar el lenguaje hablado o escrito de manera coherente.

La IA puede ser "estrecha" (cuando se centra en realizar tareas específicas, como jugar ajedrez o reconocer imágenes) o "general" (cuando tiene la capacidad de realizar cualquier tarea cognitiva de un ser humano). La IA general aún no se ha logrado.

1.2 Tipos de Inteligencia Artificial

Existen varios tipos de inteligencia artificial (IA), y se pueden clasificar en diferentes categorías dependiendo del enfoque y los criterios que se utilicen. A continuación, te explico algunas formas comunes de clasificar la IA:

- **Clasificación por capacidad o nivel de inteligencia**
    - IA Débil (IA Específica o IA Estrecha)

      Este tipo de IA está diseñada para realizar una tarea específica y limitada. No tiene consciencia ni entendimiento más allá de su función programada. Ejemplos incluyen: Asistentes virtuales como Siri o Alexa; Sistemas de recomendación en plataformas como Netflix o Spotify; Sistemas de detección de fraude en bancos.

    - IA Fuerte (IA General o AGI, por sus siglas en inglés)

      Se refiere a una IA que tiene capacidad cognitiva similar a la de un ser humano. Puede entender, aprender, razonar y adaptarse a una variedad de tareas, no solo las que fue programada para realizar. Sin embargo, actualmente no existe una IA general.

    - IA Superinteligente (Superinteligencia)

Este concepto describe un tipo de IA hipotética que no solo emula la inteligencia humana, sino que la supera en todos los aspectos. Una IA superinteligente sería capaz de resolver problemas que están más allá de la comprensión humana, mejorando constantemente su propia inteligencia. Es un escenario futurista que aún no se ha alcanzado.

- **Clasificación por funcionalidad**
  - IA Reactiva

    Es el tipo más básico de IA. Solo responde a estímulos inmediatos y no tiene la capacidad de aprender de experiencias pasadas o de anticipar el futuro. No tiene memoria. Ejemplo: “Deep Blue”, la IA de IBM que venció al campeón mundial de ajedrez Garry Kasparov en 1997.

  - IA con Memoria Limitada

    Este tipo de IA puede utilizar experiencias pasadas para tomar decisiones futuras de manera limitada. La mayoría de las IA actuales,, como los coches autónomos, funcionan con memoria limitada, ya que toman decisiones basadas en datos de eventos recientes, pero no pueden hacer predicciones a largo plazo.

  - Teoría de la Mente

    Es una etapa futura hipotética en la que la IA no solo sería capaz de comprender y responder a su entorno, sino también de interpretar las emociones, creencias e intenciones de otros seres.

  - Autoconciencia

    Esta sería una IA que no solo entiende su entorno y las emociones de otros, sino que también tiene conciencia de sí misma. Al igual que con la "IA Fuerte" o la "Superinteligencia", es un concepto teórico.

- **Clasificación por el tipo de técnica o enfoque**

    - Sistemas Basados en Reglas

      Son programas que siguen un conjunto de reglas predefinidas para tomar decisiones. Estos sistemas fueron las primeras formas de IA, y aún se usan en aplicaciones específicas, como sistemas expertos.

    - Aprendizaje Automático (Machine Learning)

      Es una subcategoría de IA donde los sistemas aprenden de datos en lugar de seguir reglas preprogramadas. Los algoritmos de aprendizaje automático pueden clasificar, predecir y optimizar en función de los datos que reciben. Ejemplos incluyen redes neuronales, árboles de decisión y máquinas de soporte vectorial.

    - Aprendizaje Profundo (Deep Learning)

      Es una técnica avanzada de aprendizaje automático que utiliza redes neuronales artificiales profundas (varias capas de neuronas artificiales) para aprender de grandes cantidades de datos no estructurados, como imágenes, texto o sonido. Se usa en reconocimiento de imágenes, procesamiento del lenguaje natural y más.

    - Procesamiento del Lenguaje Natural (NLP/LLM)

      Un área de la IA que se centra en la interacción entre los ordenadores y el lenguaje humano, permitiendo que las máquinas entiendan, interpreten y respondan al lenguaje natural. Un ejemplo es ChatGPT.

- **Clasificación por aplicación**
    - Robótica

La IA se usa para controlar robots que pueden realizar tareas físicas. Los robots industriales y los robots autónomos son ejemplos de esta aplicación.

- Visión Artificial

  La IA aplicada en este campo permite a las máquinas ver y analizar imágenes o videos. Ejemplos incluyen reconocimiento facial, sistemas de vigilancia automatizados y conducción autónoma.

- Sistemas Expertos

  Utilizan bases de conocimiento y reglas para proporcionar asesoramiento especializado en campos como la medicina, la ley o la ingeniería.

- IA en el Procesamiento de Lenguaje Natural (NLP)

  Aquí la IA se utiliza para comprender, interpretar y generar lenguaje humano, como los asistentes de voz, chatbots o sistemas de traducción automática.

2. CONTEXTO ACTUAL: USOS QUE SE LE DA A LA IA EN LA ACTUALIDAD.

La inteligencia artificial (IA) ha avanzado significativamente en los últimos años gracias a la disponibilidad de grandes cantidades de datos, mayor potencia de procesamiento y nuevas técnicas de aprendizaje automático. En el ámbito militar, la IA se utiliza en diversas áreas como reconocimiento de objetivos, vigilancia, comunicación, logística y desarrollo de armas

A nivel terrestre, marítimo y aéreo, la IA se utiliza para coordinar sistemas autónomos que pueden realizar tareas como el seguimiento de vehículos, evitar obstáculos, o detectar minas marinas. En el ciberespacio, la IA facilita el acceso a grandes cantidades

de datos estratégicos. A pesar de sus beneficios, surgen interrogantes sobre el uso militar de la IA, especialmente respecto a la procedencia de los datos y los sesgos que puedan contener, lo que puede afectar su eficacia y objetividad.

Conceptos clave como la distinción entre civiles y combatientes, o el uso de bienes civiles con fines militares, pueden ser difíciles de interpretar para una máquina, lo que aumenta el riesgo de errores fatales. Además, si los datos iniciales están sesgados, estos sesgos se retroalimentan, ampliando su impacto.

Aspectos críticos como la identificación, la fiabilidad y la previsibilidad de los sistemas autónomos no están completamente garantizados. En un contexto militar, la identificación de objetivos y la capacidad de intervención humana son esenciales.

La IA también se utiliza para generar información falsa, que puede amplificar la propaganda y manipular la opinión pública. Los sistemas de apoyo a la toma de decisiones militares, basados en IA, deben seguir respetando los principios de proporcionalidad y buena fe, ya que una máquina no puede comprender estos principios.

2.1 Definiciones de Armas Automatizadas

Existen diferentes definiciones de lo que constituye un sistema de armas autónomas (AWS). El Ministerio de Defensa del Reino Unido en 2011 las definió como sistemas que comprenden intenciones y pueden tomar acciones adecuadas como un ser humano. Por otro lado, el Departamento de Defensa de EE. UU., en 2023, los definió como sistemas capaces de seleccionar y atacar objetivos sin intervención humana una vez activados. Otros organismos internacionales, como la OTAN, amplían esta noción para incluir sistemas con "conciencia" y "autodeterminación". Ejemplos incluyen defensas como la Cúpula de Hierro israelí y el MANTIS alemán, y sistemas de vigilancia como el Super aEgis II surcoreano.

El rápido desarrollo de esta tecnología podría permitir que los drones tomen decisiones instantáneas en conflictos sin intervención humana, lo que podría reducir la posibilidad de negociaciones pacíficas. Desde la Guerra de Kosovo en 1999 hasta los ataques de EE. UU. en Afganistán, el uso de drones ha evolucionado enormemente. Actualmente, drones como el Predator y el Reaper, utilizados por EE. UU. y el Reino Unido, son parte esencial de sus arsenales. Israel también ha desplegado drones en Gaza, y países como Turquía, Pakistán, y China fabrican y exportan drones a nivel global, con clientes como Arabia Saudita, Egipto y Nigeria. Incluso grupos no estatales como Hezbolá y Hamas han utilizado drones en conflictos recientes.

El uso de la IA en conflictos también está aumentando. Ucrania ha utilizado IA en drones de largo alcance para identificar objetivos rusos, mientras que Israel ha empleado su sistema de IA "Lavender" en Gaza para identificar miles de objetivos de Hamas. Aunque aún no se ha utilizado un sistema de armas totalmente autónomo (AWS) sin intervención humana significativa, el uso de IA en conflictos plantea graves preguntas éticas y legales. Un gran temor es que los drones y sistemas automatizados no puedan diferenciar adecuadamente entre combatientes y civiles, y la ausencia de leyes específicas para regular estas tecnologías aumenta los riesgos.

Grandes potencias, como Estados Unidos y China, están inmersas en una competencia por la tecnología militar. El libro blanco de defensa nacional de China de 2019 promovió la teoría de la “guerra inteligente,” en la que el uso de la IA es clave para la modernización del Ejército Popular de Liberación. Mientras tanto, Estados Unidos ha buscado limitar el acceso de China a semiconductores avanzados cruciales para los modelos de IA, temiendo el fortalecimiento de las capacidades militares chinas.

La guerra de Rusia en Ucrania ha demostrado cómo la IA está dando forma a las estrategias militares y la seguridad nacional. Calificado por la periodista Vera Bergengruen como un “laboratorio de guerra de IA,” el conflicto ha visto cómo empresas tecnológicas civiles experimentan con herramientas de IA y juegan un papel crítico en operaciones militares. Compañías privadas como Palantir y ClearviewAI se

han convertido en actores clave en el campo de batalla, proporcionando análisis de datos para ataques con drones y vigilancia.

Debido a su naturaleza general y habilitadora, la IA militar abarca una amplia gama de herramientas y aplicaciones, desde sistemas de armas autónomas letales (LAWS) y drones hasta ciberseguridad y toma de decisiones estratégicas.

La IA tiene el potencial de influir en casi todos los aspectos de la guerra, incluida la innovación en defensa, las cadenas de suministro, las relaciones cívico-militares, las estrategias militares, la gestión de batallas, los protocolos de entrenamiento, la logística y la protección de fuerzas. Por ejemplo, su papel en la ciberseguridad y en la toma de decisiones estratégicas destaca su naturaleza de doble uso, lo que complica los esfuerzos de regulación y gobernanza.

3. DETECCIÓN, IDENTIFICACIÓN Y SEGUIMIENTO DE OBJETIVOS. EMPRESAS Y SISTEMAS.

Podemos decir que los sistemas de IA “ven” de una forma diferente a los humanos. Los ojos serían los sensores, mientras que el cerebro serían los algoritmos que desarrollan las diferentes empresas. Este conjunto se completaría en un cuerpo, que son las plataformas.

3.1 Sistemas de identificación de objetivos:

- **Anduril**: Sus sistemas C-UAS, como SENTRY, emplean computación en el borde (edge computing) y algoritmos avanzados de inteligencia artificial. Utilizan múltiples sensores y radares para identificar, detectar y rastrear de manera autónoma objetos relevantes, garantizando la seguridad de fronteras, bases militares, oleoductos, gasoductos y otras infraestructuras clave.

- **Palantir:** La unidad TITAN fusiona sensores, redes y automatización para acelerar el tiempo entre la detección de un objetivo y la acción. Mediante el uso

de IA y aprendizaje automático, proporciona datos procesados para decisiones tácticas rápidas en el campo.

- **Sensores TK (Overwatch)**: Estos sistemas de sensores multiespectrales capturan imágenes de alta precisión, ideales para inteligencia y mapeo de grandes extensiones de terreno.

- **Shield AI**: Su dron V-BAT, con capacidad de despegue y aterrizaje vertical (VTOL), soporta diversas cargas útiles y sensores intercambiables, como cámaras EO/IR, sistemas AIS, y soluciones de búsqueda en amplias áreas basadas en inteligencia artificial.

- **2ACI**: Integrado en el sistema de combate Scorpion, este sistema permite detectar, identificar y clasificar vehículos, ya sean estáticos o en movimiento, utilizando tecnología de imágenes infrarrojas.

- **STORE**: Combina sensores optrónicos con análisis impulsado por inteligencia artificial para aumentar la percepción de las tropas en el terreno. Mejora la conciencia situacional táctica, acelera las decisiones y refuerza la supervivencia en escenarios complejos.

- **Hensoldt**: Esta empresa aprovecha la innovación del sector de vehículos autónomos y automotriz para desarrollar sensores que vigilan grandes áreas y detectan o predicen anomalías rápidamente. Sus sistemas abarcan radares SAR aéreos, inteligencia de señales, y sensores EO/IR multiespectrales, con aplicaciones potenciales en proyectos europeos como el MGCS y el FCAS.

- **Preligens**: Ofrece soluciones automatizadas de análisis geoespacial (GEOINT), combinando aprendizaje automático y visión por computadora. Su tecnología integra datos de inteligencia múltiple (IMINT, ELINT, OSINT) para mejorar la comprensión operativa. Desarrolla algoritmos para analizar imágenes satelitales,

identificar objetos y detectar comportamientos inusuales, como vehículos en movimiento o la llegada de aviones. Su software maneja grandes volúmenes de imágenes, generando alertas basadas en patrones anormales y construyendo perfiles geoespaciales detallados.

- **HABSORA o GOSPEL BATTELFIELD MANAGMENT SYSTEM**: Software avanzado que se encarga de procesar grandes bases de datos de inteligencia. Entre estas fuentes destacan fotografías, grabaciones de audio, videos, publicaciones en los medios de comunicación y redes sociales…así como otras muchas fuentes que, a través de un algoritmo avanzado, asesora y propone posibles objetivos a neutralizar.

- **SMART SHOOTER**: Se trata de un software combinado con un hardware de fácil instalación cuyo objetivo es asistir al soldado a la hora de seleccionar y neutralizar un objetivo. Existen diferentes variantes del software que se pueden instalar tanto en armas de infantería como el Smash 2000, Smash X4, en armas de infantería montadas en estructuras fijas como el Smash Hopper, o en drones con armamento como el Smash Dragon.

4. TIPOS DE PLATAFORMAS

4.1 Plataformas terrestres:

Vehículos terrestres no tripulados (UGV): Utilizados para misiones de desactivación de explosivos, logística y, más recientemente, combate en entornos urbanos. Estos vehículos pueden operar de forma autónoma en terrenos difíciles y bajo fuego enemigo.

Sistemas como el C-RAM (Counter Rocket, Artillery, and Mortar) son una herramienta vital para defenderse de amenazas indirectas en conflictos modernos, mejorando significativamente la seguridad de personal e infraestructuras.

Iron Dome: Israel utiliza IA para identificar, rastrear y destruir amenazas aéreas como misiles, cohetes y drones entrantes. La IA mejora la velocidad de respuesta y la precisión de estos sistemas, identificando el tamaño, velocidad y modelo del proyectil, así como la zona de impacto y los posibles daños que causaría en caso de alcanzar el objetivo. Una vez analizadas todas las variables, el operador del sistema de armas, dispone de un minuto para decidir si se debe neutralizar el objetivo.

Armas de infantería: con la simple instalación de un visor especial con un software integrado (Smart shooter) un rifle de infantería se convierte en un arma que dispara automáticamente a un objetivo. Simplemente debes mantener el gatillo apretado y buscar tu objetivo. El análisis de tus movimientos y otras condiciones procesadas por la IA, hará que el rifle dispare automáticamente cuando tenga las mayores posibilidades de acertar.

Lobos robot de combate: dron terrestre que funciona a través de una tecnología autónoma desarrollada por la Corporación del Grupo de Industrias del Sur de China (CSGC). Estos robots cuadrúpedos, diseñados para misiones de combate y reconocimiento, han captado la atención de expertos por su capacidad de operar en conjunto, imitando el comportamiento de una manada de lobos.

4.2 Plataformas aéreas:

Drones aéreos (UAV): Los drones son una de las plataformas más comunes donde se aplica la IA. Estos vehículos no tripulados son capaces de realizar tareas de reconocimiento, vigilancia y ataques aéreos sin intervención humana constante. La IA les permite operar de forma autónoma en zonas hostiles, buscar objetivos, evitar defensas enemigas y decidir cuándo y cómo atacar.

Dron kamikaze *Kagem*: Desarrollado por Baykar, la empresa responsable de los drones Bayraktar TB2, es una avanzada munición de merodeo diseñada para operaciones a larga distancia, con un alcance de comunicación superior a 50 kilómetros. Este dron kamikaze está preparado para operar de manera integrada con los sistemas de combate aéreo no tripulado (UCAV) como el Akinci, el Bayraktar TB2 y el Bayraktar TB3. Lanzado desde estos UCAV, el Kagem amplía su alcance y su versatilidad en misiones de ataque a larga distancia.

El *Kagem* incorpora un sistema de inteligencia artificial en su piloto automático, lo que mejora su precisión y eficiencia al impactar contra objetivos enemigos, consolidándose como una herramienta revolucionaria en el ámbito de la guerra contemporánea. Este dron kamikaze alcanza una altitud operativa máxima de 18,000 pies y es capaz de descender en picado hacia su objetivo a una velocidad máxima de Mach 0,7, mientras que su velocidad de crucero se mantiene en Mach 0,3 durante el vuelo.

Dron de ataque *Saker Scout*: son capaces de identificar y atacar, a una distancia de 12 kilómetros, hasta 64 tipos de 'objetivos militares' de forma independiente. Desarrollado por la empresa ucraniana Saker UAV, utiliza software de inteligencia artificial que es capaz de fijar y atacar objetivos sin supervisión humana. Capaces de cargar hasta 3kg de explosivos, que normalmente son granadas de RPG adosadas al cuerpo del dron.

Dron de reconocimiento Rooster (*Hybrid Reconnaissance Aerial & Ground Robot*) Se trata de un dron fabricado por la empresa israelí *ROBOTICAN*. Es un dron especializado en reconocimiento subterráneo. Cuenta con una protección en forma de jaula que le permite recorrer diversos tipos de túneles. Está equipado con unos sensores LIDAR, que junto con la IA crean un mapa en 3D. Estos drones cuentan con software de reconocimiento facial que se conectan directamente con bases de datos para ayudar y seleccionar objetivos dentro de lugares remotos

Caza de combate F16: A través del programa ACE (Air Combat Evolution) se han llevado a cabo pruebas en las que el avión ha sido pilotado única y exclusivamente por IA. Se llevó a cabo una simulación de combate, denominada *dogfighting*, entre un avión pilotado por humanos y otro pilotado por IA.

4.3 Plataformas marinas:

La Unidad de Innovación de Defensa (DIU) del Pentágono, una oficina dedicada a integrar tecnología comercial en el ámbito militar, ha permitido reducir a la mitad el tiempo necesario para inspeccionar el fondo marino en busca de minas, según Alex Campbell, líder del proyecto para la Marina. Actualmente, se están firmando nuevos contratos de producción para ampliar la implementación de esta tecnología en drones submarinos y explorar su aplicación en la detección de amenazas como barcos y aviones enemigos.

Los algoritmos de aprendizaje automático utilizan sensores de sonar para identificar formas submarinas y navegar por el lecho oceánico. Las imágenes recolectadas por los drones son revisadas por marineros para asegurar la seguridad de rutas comerciales o áreas en conflicto. Estas herramientas de IA han optimizado las operaciones, permitiendo usar 10 marineros menos y reducir la duración de las misiones en dos días.

Un avance clave ha sido la capacidad de actualizar los modelos de IA de manera remota cuando los drones emergen, eliminando la necesidad de retirarlos del agua. Este proceso, que anteriormente tomaba seis meses, ahora se realiza en menos de una semana. Los modelos se reentrenan rápidamente para adaptarse a diversos entornos, ya que los lechos oceánicos pueden variar significativamente en textura y composición. Los drones ya operan en la región del Indo-Pacífico y han sido utilizados en ejercicios militares.

El proyecto, respaldado por empresas tecnológicas como Arize AI, Domino Data Lab, Fiddler AI, Latent AI y Weights & Biases, tiene contratos valorados en hasta 7,5 millones de dólares.

5. CONTRAMEDIDAS

La inteligencia artificial (IA) ha tenido un impacto transformador en el campo de la defensa y la seguridad. Su capacidad para procesar grandes volúmenes de datos, tomar decisiones rápidas y ejecutar tareas autónomas la convierte en una herramienta poderosa en escenarios de conflicto. Uno de los campos en los que ha tenido un efecto significativo es en las **contramedidas militares**, donde su papel ha evolucionado rápidamente para abordar amenazas complejas y dinámicas. Las contramedidas son tecnologías y tácticas diseñadas para neutralizar o mitigar los ataques enemigos, ya sean físicos, electrónicos o cibernéticos.

5.1 La IA en las contramedidas militares: visión general

En el contexto militar, las contramedidas se pueden dividir principalmente en varios tipos: **cinemáticas**, **electrónicas** y **cibernéticas**. Tradicionalmente, estas han sido gestionadas por operadores humanos, pero la creciente complejidad de los entornos de combate, la rapidez de las amenazas y la evolución de las tecnologías adversarias, han hecho que la IA sea una herramienta indispensable en estos sistemas.

La IA ha permitido a los sistemas de contramedidas ejecutar **análisis en tiempo real** de datos provenientes de múltiples fuentes, como sensores de radar, cámaras y comunicaciones. Al analizar estos datos de manera autónoma, la IA es capaz de identificar amenazas, predecir patrones de ataque y formular respuestas, todo en fracciones de segundo, lo que le da a las fuerzas defensoras una ventaja crucial.

- **Ejemplos de usos específicos de la IA en contramedidas.**

Contramedidas electrónicas

Un área clave donde la IA ha encontrado un amplio uso es en las **contramedidas electrónicas** (ECM). Estas buscan deshabilitar o neutralizar los sistemas de radar y comunicación del enemigo mediante el bloqueo o la manipulación de señales. Antes de

la IA, estas acciones eran controladas manualmente, lo que no siempre permitía una respuesta eficiente en situaciones dinámicas. La IA puede ahora analizar el espectro electromagnético en tiempo real y aplicar estrategias de interferencia de forma autónoma, maximizando la efectividad de las contramedidas electrónicas.

Ejemplo: Interferencia inteligente

En el caso de un ataque aéreo, la IA puede coordinar diferentes fuentes de interferencia para que actúen de manera más eficiente. Por ejemplo, un avión equipado con IA puede detectar múltiples radares enemigos y priorizar la interferencia de aquellos que representan un mayor riesgo, mientras minimiza las emisiones electromagnéticas para evitar ser detectado. Esto es algo que ya se está utilizando en aviones de combate avanzados como el **F-35**, que emplea IA para gestionar sus sistemas de contramedidas electrónicas.

Otros ejemplos:

Sistemas de Guerra Electrónica en Vehículos Terrestres: Equipos de guerra electrónica en vehículos terrestres usan IA para identificar y bloquear señales de comunicación enemigas en áreas de combate urbano. Al detectar frecuencias de radio críticas, la IA puede determinar el origen y bloquearlas de inmediato, dificultando la comunicación del enemigo.

Defensas Contra Jamming (interferencias): En situaciones donde el enemigo utiliza interferencias para bloquear los sistemas de comunicación, la IA puede reajustar frecuencias automáticamente, asegurando una comunicación continua sin intervención humana directa.

5.2 Contramedidas en sistemas de defensa antimisiles

Las **defensas antimisiles** son otro campo donde la IA ha demostrado ser esencial. Los sistemas como el **Iron Dome** de Israel o el **Aegis** de EE. UU. integran IA para interceptar y destruir misiles antes de que alcancen sus objetivos. La IA se utiliza para

calcular las trayectorias, evaluar el tipo de amenaza, y decidir el método más adecuado para interceptarla, todo en tiempo real.

Ejemplo: Sistema Iron Dome

El **Iron Dome**, desarrollado por Israel, utiliza IA para determinar si un proyectil enemigo aterrizará en una zona poblada o deshabitada, permitiendo así economizar municiones y evitar pérdidas humanas innecesarias. La IA también optimiza el lanzamiento de misiles interceptores, decidiendo el momento y lugar exacto para garantizar una intercepción exitosa. La eficiencia de este sistema se debe, en gran parte, a su capacidad para tomar decisiones autónomas basadas en datos en tiempo real

Otros ejemplos son también:

IA para Misiles Autoguiados: Los sistemas de defensa antimisiles utilizan IA para redirigir misiles interceptores en tiempo real, permitiéndoles ajustar su trayectoria en respuesta a los movimientos de un misil enemigo, aumentando la probabilidad de intercepción.

Protección de Activos Móviles: IA aplicada en vehículos de defensa móvil (como barcos y submarinos) permite reaccionar automáticamente ante amenazas múltiples, gestionando las defensas antimisiles según el tipo de objetivo, y optimizando la asignación de interceptores.

5.3 Contramedidas cibernéticas

En el ámbito de la **ciberseguridad militar**, la IA juega un rol crucial en la detección y neutralización de amenazas. Las redes militares son objetivos prioritarios en cualquier conflicto moderno, y la IA ha revolucionado la manera en que se defienden. Los sistemas de contramedidas cibernéticas basados en IA pueden identificar patrones de ataque y responder antes de que el daño se extienda.

Ejemplo: Defensa de redes militares

Los sistemas de IA pueden analizar patrones de tráfico en las redes y detectar anomalías que podrían indicar un ataque inminente. Por ejemplo, si se detecta un aumento inusual en las solicitudes de acceso desde una ubicación sospechosa, el sistema puede activar automáticamente protocolos de seguridad, como el aislamiento de la red o la limitación de accesos a servidores críticos.

Sistemas de IA para Defensa contra Ataques Zero-Day: La IA detecta patrones de comportamiento sospechosos que podrían ser indicativos de un ataque de día cero. Al reconocer y analizar las anomalías, el sistema puede bloquear el acceso a segmentos sensibles de la red.

Contrainteligencia Automatizada: Los sistemas de IA pueden identificar, monitorizar y desactivar bots de espionaje y malware en las redes internas de defensa. Utilizan algoritmos para aprender de cada intento de infiltración, mejorando continuamente su capacidad de detección.

Estos ejemplos ilustran cómo la IA se emplea en diferentes capas de defensa, permitiendo una respuesta rápida y autónoma ante diversas amenazas.

5.4 Comparación de contramedidas tradicionales y actuales con IA

Contramedidas tradicionales: antes de la implementación masiva de la IA, las contramedidas militares dependían casi exclusivamente de la intervención humana.

En el caso de las **contramedidas electrónicas**, los operadores manualmente ajustaban los sistemas de interferencia basados en sus percepciones y análisis del campo de batalla. Los sistemas de defensa antimisiles, aunque efectivos, también dependían en gran medida de la supervisión humana para decidir cuándo y cómo interceptar las amenazas.

Contramedidas con IA: la integración de IA ha reducido significativamente la dependencia de operadores humanos, lo que permite respuestas más rápidas y precisas.

En las **contramedidas electrónicas**, la IA puede analizar grandes volúmenes de señales electromagnéticas simultáneamente, priorizando las amenazas de manera automática. En

los sistemas antimisiles, la IA optimiza tanto el tiempo como la precisión en la interceptación de proyectiles. En el ámbito cibernético, la IA se ha convertido en una herramienta esencial para la detección temprana de ciberataques y la implementación de contramedidas automatizadas.

5.5 Perspectiva futura del uso de la IA en contramedidas

Sistemas autónomos de defensa : en el futuro, se espera que la IA juegue un papel aún más importante en las **contramedidas autónomas**. Los drones y robots autónomos podrían desplegarse para ejecutar misiones de defensa y ataque sin intervención humana directa. Por ejemplo, se están desarrollando drones equipados con IA capaces de desactivar otros drones enemigos de forma autónoma o de llevar a cabo misiones de reconocimiento en áreas de alto riesgo.

Defensa cibernética con IA avanzada: la evolución de la IA permitirá a los sistemas de defensa cibernética predecir y bloquear amenazas antes de que estas puedan materializarse. A medida que los ataques cibernéticos se vuelven más sofisticados, los algoritmos de IA podrán adaptarse rápidamente a nuevas formas de ataque, incluso diseñando y desplegando contramedidas automáticas en tiempo real.

Interoperabilidad y colaboración hombre-máquina: en el futuro cercano, la **colaboración hombre-máquina** será clave en las operaciones de contramedidas. Si bien la IA puede ejecutar una gran cantidad de funciones de forma autónoma, los humanos seguirán desempeñando un papel crucial en la toma de decisiones estratégicas. Los sistemas avanzados de IA podrán trabajar en estrecha colaboración con los comandantes, brindando recomendaciones basadas en el análisis de datos en tiempo real, mientras los humanos conservan el control sobre las decisiones finales.

Desafíos éticos y legales: el uso de IA en las contramedidas plantea **desafíos éticos** significativos. La posibilidad de que la IA actúe de forma completamente autónoma en el campo de batalla genera preocupaciones sobre la falta de supervisión humana y la posibilidad de errores catastróficos. Organismos internacionales, como las Naciones

Unidas, están comenzando a desarrollar marcos legales para regular el uso de sistemas autónomos en conflictos militares, asegurando que siempre haya algún grado de control humano en el proceso de toma de decisiones.

6. LEGISLACIÓN Y ÉTICA

La IA aporta indudables ventajas en la recopilación de información, la toma de decisiones y la autonomía de sistemas, pero supone grandes **desafíos éticos y legales.**

La toma de decisiones autónomas por parte de sistemas de IA plantea interrogantes sobre la responsabilidad y la rendición de cuentas en caso de incidentes. Además, la posibilidad de que la IA pueda ser utilizada en operaciones ofensivas ha suscitado discusiones sobre la necesidad de regulaciones internacionales que controlen su desarrollo y uso.

6.1 Comité Internacional de la Cruz Roja - CICR

- **Protocolo I adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales, 1977. Artículo 36 - Armas nuevas**

Cuando una Alta Parte contratante estudie, desarrolle, adquiera o adopte una nueva arma, o nuevos medios o métodos de guerra, tendrá la obligación de determinar si su empleo, en ciertas condiciones o en todas las circunstancias, estaría prohibido por el presente Protocolo o por cualquier otra norma de derecho internacional aplicable a esa Alta Parte contratante.

6.2 Unión Europea

- **Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia**

de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).

El Reglamento de Inteligencia Artificial de la UE es la **primera ley integral en materia de inteligencia artificial del mundo.** Su objetivo es tratar los riesgos para la salud, la seguridad y los **derechos fundamentales**. El Reglamento también protege la democracia, el Estado de Derecho y el medio ambiente.

Hay casos en los que las características específicas de determinados sistemas de inteligencia artificial pueden dar lugar a nuevos riesgos relacionados con la seguridad, incluso física, y los derechos fundamentales.

Esto da lugar a **inseguridad jurídica** y a una aceptación potencialmente más lenta de las tecnologías de inteligencia artificial por parte de las autoridades públicas, las empresas y los ciudadanos, debido a la falta de confianza.

El Reglamento sobre Inteligencia Artificial (la Ley de IA), "promueve **usos de la IA que sean éticos y respeten los derechos fundamentales**, pero discretamente menciona en su introducción y en su artículo 2.3 que **los usos militares de la IA no entran en su ámbito de aplicación**"[1]. Así,

- En caso de que, y en la medida en que, los sistemas de IA se introduzcan en el mercado, se pongan en servicio o se utilicen, con o sin modificación, **con fines militares, de defensa o de seguridad nacional, deben excluirse del ámbito de aplicación del presente Reglamento, independientemente del tipo de entidad que lleve a cabo esas actividades**, por ejemplo, **con independencia de que se trate de una entidad pública o de una entidad privada**.

- Por lo que respecta a los **fines militares y de defensa**, dicha exclusión está justificada tanto por el **artículo 4, apartado 2, del TUE** como por las

especificidades de la **política de defensa de los Estados miembros y de la política común de defensa de la Unión a que se refiere el título V, capítulo 2, del TUE**, que están sujetas al Derecho internacional público que, por lo tanto, es el marco jurídico más adecuado para la regulación de los sistemas de IA en el contexto del uso de la fuerza letal y de otros sistemas de IA en el contexto de las actividades militares y de defensa.

- Por lo que respecta a los fines de **seguridad nacional**, la exclusión está justificada tanto por el hecho de que **la seguridad nacional sigue siendo responsabilidad exclusiva de los Estados miembros de conformidad con el artículo 4, apartado 2, del TUE**, como por la naturaleza específica y las necesidades operativas de las actividades de seguridad nacional y por las normas nacionales específicas aplicables a dichas actividades.

- No obstante, si un sistema de IA desarrollado, introducido en el mercado, puesto en servicio o utilizado con fines militares, de defensa o de seguridad nacional **se utilizara temporal o permanentemente fuera de estos ámbitos con otros fines** (por ejemplo, con fines civiles o humanitarios, de garantía del cumplimiento del Derecho o de seguridad pública), **dicho sistema entraría en el ámbito de aplicación del presente Reglamento.**

En tal caso, la entidad que utilice el sistema de IA con fines que no sean militares, de defensa o de seguridad nacional debe garantizar que el sistema de IA cumple lo dispuesto en el presente Reglamento, a menos que el sistema ya lo haga.

- Los sistemas de IA introducidos en el mercado o puestos en servicio para un fin excluido, a saber, militar, de defensa o de seguridad nacional, y uno o varios fines no excluidos, como fines civiles o de garantía del cumplimiento del Derecho, entran en el ámbito de aplicación del presente Reglamento y los proveedores de dichos sistemas deben garantizar el cumplimiento del presente Reglamento.

En esos casos, el hecho de que un sistema de IA pueda entrar en el ámbito de aplicación del presente Reglamento no debe afectar a la posibilidad de que las entidades que llevan a cabo actividades militares, de defensa y de seguridad nacional, independientemente del tipo de entidad que lleve a cabo estas actividades, utilicen sistemas de IA con fines de seguridad nacional, militares y de defensa, cuyo uso está excluido del ámbito de aplicación del presente Reglamento.

- Un sistema de IA introducido en el mercado con fines civiles o de garantía del cumplimiento del Derecho que se utilice, con o sin modificaciones, con fines militares, de defensa o de seguridad nacional no debe entrar en el ámbito de aplicación del presente Reglamento, independientemente del tipo de entidad que lleve a cabo esas actividades.

❖ **Tratado de la Unión Europea, artículo 4, apartado 2.**

- "La Unión respetará la igualdad de los Estados miembros ante los Tratados, así como su identidad nacional, inherente a las estructuras fundamentales políticas y constitucionales de éstos, también en lo referente a la autonomía local y reg*ional. **Respetará las funciones esenciales del Estado, especialmente las que tienen por objeto garantizar su integridad territorial, mantener el orden público y salvaguardar la seguridad nacional.** En particular, la seguridad nacional seguirá siendo responsabilidad exclusiva de cada Estado miembro*."

  Esto deja a los Estados miembros un amplio margen de maniobra para regular el uso de la IA en la guerra. Dada la inversión de la Unión en IA y otras tecnologías avanzadas que alcanzará el valor de casi 8.000 millones de euros entre 2021-2027, podría ser preocupante. Esto es posible gracias al **Fondo Europeo de Defensa y a que la UE no prohíbe el uso de armas autónomas**, a pesar de las resoluciones aprobadas por el Parlamento Europeo en 2014, 2018 y 2021.

  A pesar de la exclusión de la inteligencia artificial militar, el Reglamento de IA tendrá un impacto considerable en la seguridad europea. Esto se debe a que **muchos sistemas de IA tienen una naturaleza de doble uso, lo que implica que pueden aplicarse tanto en contextos civiles como militares**[2].

En casos de doble uso como estos, la Ley de IA sería aplicable, ya que exige que los sistemas cumplan con sus regulaciones en lo que respecta a la IA de alto riesgo. No obstante, la implementación de estos requisitos regulatorios puede resultar problemática para sistemas que funcionan de manera autónoma o en entornos clasificados. Además, la mayoría de las organizaciones de defensa no siguen de cerca los desarrollos en política digital civil, lo que podría dejarlas poco preparadas para cumplir con la Ley de IA una vez que entre en vigor.

Esta exclusión, que ha sido polémica, en cuanto supone la **ausencia de regulación** de un tema capital en la primera norma de rango legal que realiza un esfuerzo por dotar de un régimen jurídico coherente e integral al fenómeno que está llamado a configurar el futuro inmediato de nuestras sociedades, no significa que los usos militares se hayan situado automáticamente al margen del derecho y que todo esté permitido en este campo.

A nivel político, los gobiernos se están implicando cada vez más en las cuestiones regulatorias en torno a la IA militar[3]. **No existe un marco legal y ético a escala de la UE** para los usos militares de la IA. En consecuencia, los Estados miembros pueden adoptar enfoques diferentes, lo que provocará lagunas en la regulación y la supervisión.

Por lo tanto, l**a Unión Europea debería asumir un papel proactivo y establecer un marco que abarque tanto las aplicaciones de doble uso como las aplicaciones militares de la inteligencia artificial.** Esto se llevaría a cabo a través de una estrategia europea destinada a fomentar la utilización responsable de la inteligencia artificial en defensa, fundamentada en la categorización de riesgos conforme a la Ley de IA. Dicho enfoque proporcionaría orientación a las instituciones de defensa y a la industria en la promoción del desarrollo, adquisición y uso responsables de la inteligencia artificial, respaldados por valores compartidos

6.3 España

- **Resolución 11197/2023 del Ministerio de Defensa.**

- Mediante esta Resolución el Ministerio de Defensa aprueba la "Estrategia de desarrollo, implantación y uso de la Inteligencia Artificial en el Ministerio de Defensa"[4].

  En ella se proclama "el uso de datos e información, herramientas y aplicaciones habilitadas para la IA para mejorar el entendimiento y capacidades de las personas, no con el objetivo de reemplazarlas, sino de complementarlas y facilitar que aporten mayor valor a sus actividades, alineándose además con los principios éticos que sean de aplicación".

  Por otro lado, destaca especialmente el **principio de "responsabilidad humana y rendición de cuentas"**. Se garantiza por escrito que "cualquier desarrollo de inteligencia artificial, así como su utilización, deberá permitir una clara supervisión humana con el fin de garantizar la debida rendición de cuentas y la atribución de responsabilidades".

  El uso de la inteligencia artificial "estará siempre **de acuerdo con la legislación nacional e internacional, los principios de uso ético** de la IA y dirigida a su área de aplicabilidad".

- Se fijan una serie de "principios de desarrollo, implantación y uso responsable de la Inteligencia Artificial en la Defensa".

  El primero de ellos es la **legalidad**. Las aplicaciones de la inteligencia artificial en su ámbito "se desarrollarán y emplearán **de acuerdo con el derecho nacional e internacional** que sea de aplicación, incluida la Declaración Universal de Derechos Humanos y el Derecho Internacional Humanitario". Otro principio hace alusión a la responsabilidad humana y rendición de cuentas.

- La inteligencia artificial ha añadido nuevos elementos a un debate que se arrastra desde hace años, de hasta qué punto se pueden incorporar elementos automáticos en los sistemas de armas, por ejemplo, en drones aéreos y en vehículos terrestres o marinos no tripulados, en vez de tener un control directo por parte de una persona.

  La estrategia del Ministerio contempla este tipo de desafíos, y de hecho un punto del documento está dedicado a la resolución de conflictos éticos relacionados con la inteligencia artificial: Defensa ordena a todos los órganos de la estructura del ministerio que "**la utilización de IA en sistemas de armas estará condicionada a la clara e inequívoca posibilidad de identificar a la persona responsable de su empleo directo y de la decisión de uso"**.

- Se citan algunas capacidades y operaciones militares en las que se contempla introducir el uso de inteligencia artificial, en una lista que se podrá ir ampliando, destacando la autonomía en el comportamiento de sistemas no tripulados. Desarrollo de funciones autónomas no letales en sistemas no tripulados terrestres, navales y aeroespaciales.

- El Ministerio de Defensa sugiere que se podrán utilizar tecnologías basadas en inteligencia artificial en **sistemas no tripulados**, pero establece una condición: que sean **funciones "no letales"[5]**.

❖ **Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.**

- El Código Penal español, hasta el momento, **no recoge ninguna prohibición alguna sobre el uso de la IA** en cualquiera de sus vertientes.

- Si que prohíbe la fabricación, comercialización o el establecimiento de depósitos de armas o municiones no autorizados por las leyes, variando la pena aplicada en función de si se trata de armas o municiones de guerra o de armas químicas, biológicas, nucleares o radiológicas o de minas antipersonas o municiones en racimo o de si se trata de trata de armas de fuego reglamentadas o municiones para las mismas.

También prohíbe el tráfico, el desarrollo o la no destrucción cuando proceda de armas o municiones de guerra o de defensa, o de armas químicas, biológicas, nucleares o radiológicas o de minas antipersonas o municiones en racimo[6].

- Asimismo, define el concepto de depósito de armas de guerra, químicas, biológicas, nucleares o radiológicas, de minas antipersonas o de municiones en racimo como la mera fabricación, comercialización, tenencia[7].

- En caso de conflicto armado castiga el empleo de métodos o medios de combate prohibidos o destinados a causar sufrimientos innecesarios, y la realización u dar órdenes para realizar cualquier infracción contraria a los tratados internacionales en los que España fuere parte y relativos a la conducción de las hostilidades, regulación de los medios y métodos de combate, …[8]

❖ **Estrategia de Inteligencia Artificial 2024 (AESIA). Ministerio para la Transformación Digital y de la Función Pública**

- Esta Estrategia **clasifica los sistemas de IA según su riesgo**, prohibiendo el uso de sistemas relacionados con la explotación de las vulnerabilidades de personas, la manipulación cognitivo-conductual, la extracción no selectiva de imágenes faciales de Internet para crear o ampliar bases de datos de reconocimiento facial, el reconocimiento de emociones en el lugar del trabajo y en las instituciones educativas y algunos casos de vigilancia policial predictiva para las personas.

- Hay que reseñar que está prohibido en la UE el uso de sistemas de IA que supongan una amenaza para la seguridad, los derechos o los medios de subsistencia de las personas, **pero la Estrategia no indica nada sobre uso para fines militares.**

- Con la creación de la AESIA, España se convierte en el primer país europeo en tener una institución de estas características, anticipándose a la entrada en vigor del Reglamento Europeo de Inteligencia Artificial, asegurando que el desarrollo

y la aplicación de la IA sean responsables y beneficiosos para la sociedad en su conjunto.

- Por tanto, debe desarrollar la capacidad de supervisión de los sistemas de IA de alto riesgo para garantizar el cumplimiento, y más concretamente, la supervisión y, en su caso, sanción, de acuerdo con lo estipulado en la normativa europea.

6.4 Organización del Tratado del Atlántico Norte - OTAN

❖ **Reunión de Ministros de Defensa de 22 de octubre de 2021**

- El primer paso para regular el uso de la IA con fines militares o de defensa lo dio la OTAN que, en la reunión de Ministros de Defensa en fecha 22/10/2021, aprobando una Estrategia de Inteligencia Artificial que junto a importantes medidas de investigación y fomento de esta tecnología e incorporando una regulación del uso militar de la IA mediante su sometimiento a seis principios generales: **legalidad, responsabilidad y rendición de cuentas, inteligibilidad y trazabilidad, fiabilidad, gobernabilidad y mitigación del sesgo.**

❖ **Creación de la Junta de Revisión de Datos e Inteligencia Artificial (DARB)**

- Para asegurar la implementación correcta de los anteriores principios por los Estados miembros se ha creado un órgano específico: la **Junta de Revisión de Datos e Inteligencia Artificial (DARB)** integrada por un equipo multidisciplinar con representantes de todos los estados y que supervisa los usos de la IA y elaborará normas de certificación para facilitar que la industria militar y los ejércitos elaboren e implementen sistemas acordes con los citados principios.

- El DARB se establece con los siguientes objetivos:

Generar confianza, con el público, los innovadores y los usuarios finales operativos, así como con la comunidad internacional para dirigir los esfuerzos responsables de innovación en defensa de acuerdo con nuestros valores, normas y derecho internacional;

Guiar la adopción de la IA responsable (RAI), traduciendo las PRU en normas RAI fáciles de usar y mejores prácticas que ofrezcan a la empresa de la OTAN y a sus aliados una línea de base común para ayudar a **crear controles de calidad, mitigar riesgos y adoptar sistemas de IA fiables e interoperables**.

Actuar como un foro para que los Aliados y la empresa de la OTAN compartan las mejores prácticas e intercambien puntos de vista.

- El DARB debe asegurarse de que sus resultados no levanten barreras innecesarias para la adopción de la IA a la velocidad de la relevancia. A través del DARB, los Aliados y la OTAN perfeccionarán las prácticas de RAI que ofrezcan sistemas más fiables, interoperables y seguros, lo que ayudará a obtener una ventaja cualitativa en relación con los competidores estratégicos y los adversarios potenciales.

6.5 Organización de las Naciones Unidas – ONU

❖ **Resolución de fecha 21.03.24**

- Es la primera vez que la Asamblea adopta una resolución para regular este campo emergente. La resolución pide a los Estados que se **abstengan de utilizar sistemas de inteligencia artificial que no puedan funcionar de conformidad con las normas internacionales de derechos humanos o los pongan en riesgo.**

Al adoptar sin votación un proyecto de resolución liderado por Estados Unidos, la Asamblea también destacó el respeto, la protección y la promoción de los derechos humanos en el diseño, el desarrollo, el despliegue y el uso de la IA.

La Asamblea pidió a todos los Estados miembros y partes interesadas que “se abstengan de utilizar sistemas de inteligencia artificial que no puedan funcionar de conformidad con las normas internacionales de derechos humanos o que planteen riesgos indebidos para el disfrute de los derechos humanos".

6.6 Estados Unidos

- **Declaración Política sobre el Uso Responsable de la Inteligencia Artificial y la Autonomía en el Ámbito Militar. Departamento de Estado de los Estados Unidos**

La Declaración Política sobre el Uso Responsable de la Inteligencia Artificial y la Autonomía en el Ámbito Militar proporciona un marco normativo que aborda el uso de estas capacidades en el ámbito militar. Lanzada en febrero de 2023 en la Cumbre sobre IA responsable en el Ámbito Militar (REAIM 2023) en La Haya, la Declaración tiene como objetivo construir un consenso internacional en torno al comportamiento responsable y guiar el desarrollo, el despliegue y el uso de la IA militar por parte de los Estados. La Declaración proporciona una base para el intercambio de mejores prácticas y el desarrollo de capacidades de los Estados, lo que permitirá a los Estados que la respaldan compartir experiencias e ideas.

El objetivo de la Declaración es crear un consenso internacional sobre cómo los ejércitos pueden incorporar de manera responsable la IA y la autonomía en sus operaciones, y ayudar a guiar el desarrollo, el despliegue y el uso de esta tecnología por parte de los Estados con fines de defensa para garantizar que promueva el respeto por el derecho internacional, la seguridad y la estabilidad. El Departamento de Estado describe su Declaración como "una serie de **directrices no vinculantes desde el punto de vista jurídico** que describen las mejores prácticas para el uso responsable de la IA en un contexto de defensa".

6.7 Reino Unido

❖ ESTRATEGIA DE INTELIGENCIA ARTIFICIAL EN DEFENSA

- La Estrategia de Ciencia y Tecnología del Ministerio de Defensa (2020) destaca la importancia de la "formulación de políticas anticipatorias", es decir, la resolución de problemas políticos antes del punto de maduración de la tecnología, para la adopción exitosa de nuevas capacidades.

  La Unidad de IA y Autonomía de Defensa (DAU) se creó en 2018 para ayudar al departamento a adoptar estas tecnologías a buen ritmo.

- La adopción efectiva de la IA también depende de las preguntas sobre la legislación existente relacionada con la inteligencia y los permisos para compartir información; y la planificación y realización de operaciones militares que impliquen capacidad habilitada por la IA estarán determinadas por las políticas que rigen factores como la delegación de mando y control.

- Se deben acelerar los esfuerzos para garantizar que las políticas, procesos y enfoques de la legislación permitan, en lugar de limitar.

6.8 China

❖ 8.1 CONFERENCIA DE PRENSA DEL MINISTERIO DE DEFENSA NACIONAL.

- En fecha 30.11.2023, el Ministerio de Defensa Nacional chino celebró una conferencia de prensa, en la que el Coronel Wu Qian, director de la Oficina de Información del Ministerio de Defensa Nacional y portavoz del Ministerio de Defensa Nacional informó de que en los últimos años, China **ha presentado documentos de posición a la plataforma de las Naciones Unidas sobre la regulación de la aplicación militar de la IA y el fortalecimiento de la gobernanza ética de la IA, y se ha comprometido a participar de manera constructiva en la gobernanza mundial de la IA**.

6.9 Rusia

- En diciembre del año pasado, el gobierno presentó a la Duma Estatal un **proyecto de ley** que obliga a los desarrolladores de IA que operan en un régimen legal experimental a asegurar la responsabilidad por posibles daños a la vida, la salud o la propiedad al usar la tecnología. Una innovación significativa de esta iniciativa es la propuesta de reducir el tiempo de tramitación de las solicitudes de participación en la RAP. Todavía no está claro qué camino de regulación tomará la legislación rusa.

- En Rusia, aún **no existe un marco regulatorio** sistemático para regular la IA, solo se está preparando. Desde el año pasado, Rusia ha estado trabajando en un proyecto de ley que está diseñado para **determinar la responsabilidad de los desarrolladores** y excluir los casos de uso de inteligencia artificial con fines fraudulentos.

- El servicio de prensa de Yandex señala que en la regulación legislativa de la IA es importante "no adelantarse a la realidad" y responder a riesgos reales, pero no fobias, apoyándose en la práctica del uso de la tecnología, que apenas comienza a acumularse".

En cuanto al intento de regular la IA en Rusia, al igual que en China, no se hace alusión a su uso militar.

6.10 Israel

- **Ensayo[9] de fecha 20.04.24 publicado en la página web "OPINIOJURIS" del Dr. Tal Mimram[10] y de Gal Dahan[11]**

- Los Estados están obligados, en virtud del artículo 36 del Primer Protocolo Adicional a los Convenios de Ginebra (AP I), a evaluar las nuevas armas, medios o métodos de guerra antes de su despliegue en la práctica.

  "Medios de guerra" es un término amplio que se extiende a equipos militares, sistemas, plataformas y otros dispositivos asociados utilizados para facilitar operaciones militares. Las herramientas desplegadas para acciones ofensivas por Israel constituyen un nuevo medio de guerra que debería estar sujeto a una revisión legal bajo el Artículo 36.

  Es importante determinar si el uso de un determinado medio de guerra está prohibido o restringido por un tratado o por el derecho internacional consuetudinario. En cuanto a las herramientas militares de IA, **el Estado de Israel no ha ratificado un tratado que prohíba específicamente el uso de la tecnología de IA en general o en aplicaciones militares, ya que no existe ninguno en la etapa actual.** Además, parece que actualmente no existe una prohibición consuetudinaria sobre el despliegue de la IA en contextos militares.

7. ÉTICA

Evidentemente, aunque la implementación de la IA para uso militar ofrece ventajas estratégicas potenciales, también genera preocupaciones éticas.

Uno de los **principales problemas** es el de la **delegación de funciones a un algoritmo**. Existen muchas dudas respecto a la selección y ataque a objetivos, y la utilización en este cometido por sistemas autónomos, argumentándose que **no se puede dejar la responsabilidad de esa decisión en máquinas o robots por su falta de empatía** si llegan a tener «la capacidad de seleccionar a los objetivos y atacar a estos por su cuenta»[12].

Se justifica la crítica en que los sistemas autónomos y la IA que los dirige son **incapaces de comprender las complejas situaciones que se pueden producir en el campo de**

batalla, como la posibilidad de que determinados objetivos hayan perdido su valor militar, o discernir si un objetivo pretende atacar o rendirse[13].

A pesar de que la IA busca mejorar el rendimiento humano y reducir sus limitaciones, las máquinas carecen de una inteligencia similar a la humana ni nuestra habilidad para interactuar socialmente que nos permite reconocer e interpretar la conducta social compleja apoyados en diferentes códigos de signos y señales, y medida por pautas culturales y también por complejas circunstancias morales, como las que se producen en el campo de batalla.

Por lo tanto, diversas iniciativas han expresado su inquietud por el uso inapropiado, prematuro o malintencionado de las tecnologías emergentes, señalando la **necesidad de códigos de comportamiento éticos** que promuevan un uso apropiado de la inteligencia artificial. Entre ellas 'Stop Killer Robots', lanzada en 2013 por el premio Nobel Jody Williams para promover la prohibición de lo que llama «robots asesinos», sistemas que ya tienen la **habilidad de seleccionar y disparar sobre objetivos sin ninguna intervención humana.**

Es incuestionable que la ética y el sistema jurídico han progresado en función de las necesidades humanas, y no con el objetivo de tratar asuntos relacionados con las máquinas. Por lo tanto, **aparecen objeciones a la hora de otorgar personalidad jurídica a los robots,** lo que implicaría la capacidad de asignarles responsabilidad por sus acciones o las consecuencias de estas. En consecuencia, "son los científicos que programan algoritmos y desarrollan la IA, y en todo caso los Estados, los que no pueden desechar su responsabilidad y deben regular el uso de estos sistemas, especialmente en su utilización militar. **Son investigadores y Estados los que deben mantener en su actuación los principios éticos y hacerse responsables legales al determinar su empleo y utilización**".

Es crucial tener en cuenta éticamente la autonomía de los sistemas y el control que el ser humano tiene sobre ellos, que no puede eludir la responsabilidad en relación con los efectos de las acciones realizadas con armas que pueden resultar letales.

Así que es necesario hacerse estas preguntas: **¿Cómo se pueden responsabilizar a las armas autónomas? ¿Quién tiene la culpa de que una máquina cometa crímenes de guerra? ¿Quién sería llevado a juicio? ¿El arma? ¿El soldado? ¿Los superiores del soldado? ¿La empresa que fabricó el arma?**

Las ONG y los expertos en derecho internacional manifiestan inquietud ante el peligro de que las armas autónomas provoquen una notable falta de transparencia en la responsabilidad. Frente a posibles errores en el funcionamiento y elecciones realizadas por sistemas automatizados, se plantea la **necesidad ética de mantener un nivel de control humano constante**, asegurando que siempre exista una persona responsable y que la rendición de cuentas por sus acciones y decisiones sea comprobable.

Los diseñadores deben estar al tanto de los riesgos inherentes, como los **prejuicios y los sesgos**. Esto no significa que sugerimos atribuir la responsabilidad penal a los diseñadores, ya que el responsable último de la toma de decisiones es el mando militar, cuanto más comprendan los diseñadores la forma en que las limitaciones del sistema podrían inhibir su funcionamiento, mejor podrán manejar con las preocupaciones previas y, también mitigarlas. También es clave la **formación de los operadores del sistema, y de quienes dependen de él**, y debe incluir aspectos técnicos, éticos y jurídicos.

Recientemente, la **Comisión** ha implementado una consulta sobre un **Código de Buenas Prácticas** para los proveedores de modelos de inteligencia artificial de uso general. Este Código, previsto por el Reglamento de Inteligencia Artificial, abordará ámbitos críticos como la transparencia, las normas relacionadas con los derechos de autor y la gestión de riesgos. Se solicita a los proveedores de los modelos de inteligencia artificial de uso general que operan en la UE, a las empresas, a los representantes de la sociedad civil, a los titulares de derechos y a los expertos académicos a que presenten sus puntos de vista y conclusiones, que se incorporarán al próximo proyecto de Código de Buenas Prácticas de la Comisión sobre modelos de inteligencia artificial de uso general.

La Comisión espera finalizar el Código de Buenas Prácticas a más tardar en abril de 2025. Además, las observaciones de la consulta también servirán de base para el trabajo

de la Oficina Europea de Inteligencia Artificial, que supervisará la aplicación y el cumplimiento de las normas del Reglamento de Inteligencia Artificial relativas a los modelos de inteligencia artificial de uso general.

La exclusión del uso militar de la IA del Reglamento europeo plantea desafíos éticos y jurídicos significativos. Aunque la regulación basada en principios, como la adoptada por la OTAN y España, ofrece un marco orientador, carece de la precisión que podría proporcionar una regulación más específica y detallada. Esta ambigüedad puede llevar a interpretaciones dispares y a una falta de coherencia en la aplicación de la normativa, lo que podría resultar en riesgos no deseados o en el uso indebido de tecnologías de IA en el ámbito militar.

En definitiva, mientras que la Unión Europea ha hecho un esfuerzo significativo por regular el uso civil de la IA, **su decisión de excluir los usos militares de esta normativa deja un vacío regulatorio que plantea desafíos éticos y de seguridad.**

---

[1] [1] Fanni, Rossana. (28 de junio de 2023). “La UE debe abordar los riesgos que plantea la IA militar”. Política Exterior.

[2] Por ejemplo, un algoritmo de detección de patrones puede desarrollarse para identificar células cancerosas o para seleccionar objetivos en operaciones militares.

[3] El gobierno holandés y el surcoreano organizaron conjuntamente una cumbre sobre la IA responsable en el ámbito militar (REAIM) en febrero de 2023, que reunió a más de 50 representantes gubernamentales para respaldar un llamamiento conjunto a la acción, con el objetivo de situar “el uso responsable de la IA en un lugar más destacado de la agenda política”

[4] Ruiz Enebral, Aurelio (14 de julio de 2023). “Defensa garantiza que el uso militar de la inteligencia artificial tendrá siempre un control humano”. Confidencial Digital.

https://www.elconfidencialdigital.com/articulo/defensa/defensa-garantiza-que-uso-militar-inteligencia-artificial-tendra-siempre-control-humano/20230712171647607253.html

[5] Es decir, por ejemplo en ningún caso se permitiría que un dron disparara un misil contra un objetivo sin que detrás haya una persona, un militar tomando esa decisión. De ahí que sólo se permita en “funciones autónomas no letales”.

[6] Artículo 566.

1. Los que fabriquen, comercialicen o establezcan depósitos de armas o municiones no autorizados por las leyes o la autoridad competente serán castigados:

1.º Si se trata de armas o municiones de guerra o de armas químicas, biológicas, nucleares o radiológicas o de minas antipersonas o municiones en racimo, con la pena de prisión de cinco a diez años los promotores y organizadores, y con la de prisión de tres a cinco años los que hayan cooperado a su formación.

2.º Si se trata de armas de fuego reglamentadas o municiones para las mismas, con la pena de prisión de dos a cuatro años los promotores y organizadores, y con la de prisión de seis meses a dos años los que hayan cooperado a su formación.

3.º Con las mismas penas será castigado, en sus respectivos casos, el tráfico de armas o municiones de guerra o de defensa, o de armas químicas, biológicas, nucleares o radiológicas o de minas antipersonas o municiones en racimo.

2. Las penas contempladas en el punto 1.º del apartado anterior se impondrán a los que desarrollen o empleen armas químicas, biológicas, nucleares o radiológicas o minas antipersonas o municiones en racimo, o inicien preparativos militares para su empleo o no las destruyan con infracción de los tratados o convenios internacionales en los que España sea parte.

[7] Artículo 567.

1. Se considera depósito de armas de guerra la fabricación, la comercialización o la tenencia de cualquiera de dichas armas, con independencia de su modelo o clase, aun cuando se hallen en piezas desmontadas. Se considera depósito de armas químicas, biológicas, nucleares o radiológicas o de minas antipersonas o de municiones en racimo la fabricación, la comercialización o la tenencia de las mismas. El depósito de armas, en su vertiente de comercialización, comprende tanto la adquisición como la enajenación.

2. Se consideran armas de guerra las determinadas como tales en las disposiciones reguladoras de la defensa nacional. Se consideran armas químicas, biológicas, nucleares o radiológicas, minas antipersonas o municiones en racimo las determinadas como tales en los tratados o convenios internacionales en los que España sea parte. Se entiende por desarrollo de armas químicas, biológicas, nucleares o radiológicas, minas antipersonas o municiones en racimo cualquier actividad consistente en la investigación o estudio de carácter científico o técnico encaminada a la creación de una nueva arma química, biológica, nuclear o radiológica, o mina antipersona o munición en racimo o la modificación de una preexistente.

3. Se considera depósito de armas de fuego reglamentadas la fabricación, comercialización o reunión de cinco o más de dichas armas, aun cuando se hallen en piezas desmontadas.

4. Respecto de las municiones, los Jueces y Tribunales, teniendo en cuenta la cantidad y clase de las mismas, declararán si constituyen depósito a los efectos de este capítulo.

[8] Artículo 610.

El que, con ocasión de un conflicto armado, emplee u ordene emplear métodos o medios de combate prohibidos o destinados a causar sufrimientos innecesarios o males superfluos, así como aquéllos concebidos para causar o de los que fundamentalmente quepa prever que causen daños extensos, duraderos y graves al medio ambiente natural, comprometiendo la salud o la supervivencia de la

población, u ordene no dar cuartel, será castigado con la pena de prisión de 10 a 15 años, sin perjuicio de la pena que corresponda por los resultados producidos.

Artículo 614.

El que, con ocasión de un conflicto armado, realice u ordene realizar cualesquiera otras infracciones o actos contrarios a las prescripciones de los tratados internacionales en los que España fuere parte y relativos a la conducción de las hostilidades, regulación de los medios y métodos de combate, protección de los heridos, enfermos y náufragos, trato debido a los prisioneros de guerra, protección de las personas civiles y protección de los bienes culturales en caso de conflicto armado, será castigado con la pena de prisión de seis meses a dos años.

[9] Inteligencia Artificial en el Campo de Batalla: Una Perspectiva desde Israel - Opinio Juris

[10] Dr. Tal Mimran es profesor asociado en el Colegio Académico Zefat y coordinador académico del Foro de Derecho Internacional de la Universidad Hebrea. También es miembro del Centro de Investigación de Seguridad Cibernética Federmann en la Facultad de Derecho de la Universidad Hebrea, y director de un programa de investigación sobre derechos humanos digitales en el Instituto Tachlith.

[11] Gal Dahan es investigador del Centro de Políticas Tachilit. También es coeditor de 'Hukim' Law Review en la Universidad Hebrea de Jerusalén. Gal también se desempeña como entrenadora del equipo israelí que participa en la Competencia Jessup International Law Moot Court 2024.]

[12] IEEE (2018). “La inteligencia artificial aplicada a la defensa”. Documentos de seguridad y defensa 79. Instituto Español de Estudios Estratégicos.

https://publicaciones.defensa.gob.es/la-inteligencia-artificial-aplicada-a-la-defensa-n-79-libros-pdf.html

[13] Por ejemplo, «evaluar si un tanque es un objetivo militar o si el sistema de armas letal autónomo aceptaría su rendición no solo es cuestión de tener algoritmos inteligentes con altas capacidades de discernimiento

8. FUENTES

¿Qué es la inteligencia artificial o IA? | Google Cloud. (s. f.). Google Cloud. https://cloud.google.com/learn/what-is-artificial-intelligence?hl=es-419#types-of-artificial-intelligence

Qué es la Inteligencia Artificial. (s. f.). Plan de Recuperación, Transformación y Resiliencia Gobierno de España. https://planderecuperacion.gob.es/noticias/que-es-inteligencia-artificial-ia-prtr

El reto de la inteligencia artificial para la seguridad y defensa. Global Affairs. Universidad de Navarra

El Reglamento de Inteligencia Artificial entra en vigor: - Comisión Europea

La seguridad del Estado en un mundo cambiante y complejo | Global Strategy

Gobernanza de la IA en los proyectos de seguridad y defensa - Noticias Defensa defensa.com noticias industria defensa

La inteligencia artificial militar ha sido excluida del Reglamento europeo de IA, pero la OTAN y la normativa española han abordado estos usos | Garrigues Digital

NATO - Official text: NATO's Data and Artificial Intelligence Review Board, 13-Oct.-2022

https://publicaciones.defensa.gob.es/la-inteligencia-artificial-aplicada-a-la-defensa-n-79-libros-pdf.html

La Comisión pone en marcha una consulta sobre el Código de buenas prácticas para la inteligencia artificial de uso general | Configurar el futuro digital de Europa

Ética de la IA autónoma: Decisiones éticas en manos de algoritmos

La inteligencia artificial militar ha sido excluida del Reglamento europeo de IA, pero la OTAN y la normativa española han abordado estos usos | Garrigues Digital

Ley de IA de la UE: primera normativa sobre inteligencia artificial | Temas | Parlamento Europeo

Defence_In_a_Competitive_Age_CP_411_Mar_21_-_SPANISH.pdf

Artificial Intelligence in the Battlefield: A Perspective from Israel - Opinio Juris

https://www.defensa.com/espana/baterias-estructurales-inteligencia-artificial-defensa-antiaerea

https://www.unav.edu/web/global-affairs/el-reto-de-la-inteligencia-artificial-para-la-seguridad-y-defensa

https://www.infobae.com/wapo/2024/06/21/drones-submarinos-equipados-con-inteligencia-artificial-ayudan-a-la-marina-de-eeuu-a-buscar-amenazas/

https://www.politicaexterior.com/inteligencia-artificial-militar-union-europea/

https://www.youtube.com/watch?v=HXYcHCSY7nE

https://carnegieendowment.org/research/2024/07/governing-military-ai-amid-a-geopolitical-minefield?lang=en

https://gjia.georgetown.edu/2024/07/12/war-artificial-intelligence-and-the-future-of-conflict/
https://www.wsj.com/tech/drone-swarms-are-about-to-change-the-balance-of-military-power-e091aa6f?st=xbnzh243w8iw8a5

https://larepublica.pe/mundo/2024/11/12/asi-son-los-lobos-robot-los-futuros-soldados-de-china-tienen-una-gran-movilidad-y-se-adaptan-a-terrenos-complejos-200412

https://carnegieendowment.org/research/2024/07/governing-military-ai-amid-a-geopolitical-minefield?lang=en

https://arbor.revistas.csic.es/index.php/arbor/article/view/2417/3638