https://doi.org/10.58752/1HNRLXNA

Desafíos de la inteligencia estratégica ante los avances de la inteligencia artificial*

Challenges of strategic intelligence in the face of artificial intelligence advances

Diana C. Salazar Vega** / **Elkin Figueroa Medina*****

Recibido: 29/4/2023 • Aceptado: 6/5/2023 • Publicado: 4/8/2023

Palabras clave: inteligencia artificial – inteligencia estratégica – seguridad y defensa – agencia de inteligencia

Resumen

El presente artículo tiene como objetivo analizar la relación entre la inteligencia estratégica y la inteligencia artificial (IA). La adopción de la tecnología de la IA no es opcional para la inteligencia estratégica, sino que su implementación es imperativa para todos los servicios, pues de lo contrario quedarán obsoletos en el nuevo mundo que esta plantea y no serán capaces de proporcionar información útil para la toma de decisiones estratégicas que permitan proteger los intereses del Estado y promover sus objetivos a largo plazo. La implementación de la IA en la inteligencia estratégica mejorará cada una de las etapas del ciclo de inteligencia y otorgará nuevas capacidades a las naciones en diferentes áreas relevantes para la defensa del Estado y la toma de decisiones estratégicas en diversos ámbitos, como la política, la economía, la seguridad, la tecnología, entre otros. Sin embargo, es necesario establecer una regulación para su implementación por parte del Estado con el fin de garantizar que esta tecnología se use de forma ética y transparente.

Key words: artificial intelligence – strategic intelligence – security and defense – intelligence agency

Abstract

This article aims at analyzing the relationship between strategic intelligence and artificial intelligence (AI). The adoption of AI technology is not optional for strategic intelligence, but rather its implementation is imperative for all services. Otherwise, they will become obsolete in the new world that it presents and will not be able to provide useful information for making strategic decisions that allow to protect the interests of the Nation and promote its long-term objectives. The implementation of AI in strategic intelligence will improve each stage of the intelligence cycle and grant new capabilities to nations in various areas relevant to national defense and strategic decision-making in various fields, such as politics, economy, security, technology, among others. However, it is necessary to establish regulation for its implementation by the State to ensure that this technology is used in an ethical and transparent manner.

* Las opiniones aquí expresadas son responsabilidad de los autores y, por lo tanto, no deben ser interpretadas como propias de las instituciones en que desempeñan sus labores profesionales.

** Economista en Finanzas y Comercio Internacional y docente (Escuela Nacional de Inteligencia "Jorge Luis Yance Navarro").

*** Ingeniero industrial e investigador en ciberdefensa (Escuela Nacional de Inteligencia "Jorge Luis Yance Navarro").

1. Introducción

La inteligencia artificial (IA) ha avanzado de manera significativa en las últimas décadas y ha llegado para transformar muchas áreas del mundo tal como las conocemos, incluyendo la de la inteligencia estratégica. A lo largo de la historia moderna, los Estados han utilizado diferentes técnicas y tecnologías para obtener información y proteger sus intereses nacionales. La IA representa una nueva era en el campo de la inteligencia y ofrece una gran cantidad de herramientas para mejorar la capacidad de recopilación y análisis de gran cantidad de información.

En este artículo se explorará la relación entre la IA y la inteligencia estratégica, examinando cómo las capacidades de la IA pueden ser utilizadas para mejorar la producción de inteligencia estratégica y con ello los insumos con los que se toman decisiones estratégicas que permitan proteger los intereses del Estado y promover sus objetivos a largo plazo.

Como conclusión del artículo, se plantea que los servicios de inteligencia estratégica deben adoptar la IA en todas las etapas de su ciclo para no quedar obsoletos en el nuevo mundo que esta tecnología plantea. Se exhorta a la reflexión sobre hasta qué punto los servicios de inteligencia y el Estado están dispuestos a depender de la IA para producir la información más importante en la toma de decisiones estratégicas, teniendo en cuenta la incertidumbre sobre la precisión de los resultados generados por la IA.

La organización del artículo está planteada del siguiente modo: en la segunda sección, se examinará el estado actual de la IA y de los países que están liderando su desarrollo, investigación e implementación. En el tercer apartado, se abordará el tema de la inteligencia estratégica y se detallará paso a paso el ciclo de inteligencia. En cuarto lugar, se desarrollará la relación entre la IA y la inteligencia estratégica, explorando los retos y desafíos que ello genera, y los riesgos que se presentan al adoptar su implementación. Por último, en la quinta sección se hará referencia a las conclusiones que se plantean en el artículo.

En resumen, este artículo examinará la creciente relación entre la IA y la inteligencia estratégica, analizando tanto sus beneficios como sus riesgos y desafíos. Al hacerlo, esperamos proporcionar una visión más completa y crítica del papel de la IA en producción de información para la toma de decisiones estratégicas y fomentar un debate informado y reflexivo sobre el futuro de la inteligencia estratégica.

2. Inteligencia artificial

En una revisión de la literatura académica sobre la IA, se define a esta inteligencia como el comportamiento inteligente de artefactos, lo cual implica percepción, razonamiento, aprendizaje, comunicación y actuación en entornos complejos (Nilsson, 1998).

Revista de la Escuela Nacional de Inteligencia · Número 2 · Enero a junio de 2023 · pp. 151-171
ISSN 2953-4623 (en línea) y 0327-6961

Estas tareas, hasta hoy, se creían exclusivas de los seres humanos; sin embargo, la IA ha mostrado que el desarrollo tecnológico conlleva a que estas actividades pueden llegar a ser realizadas por las mentes digitales con una mayor eficiencia y productividad, creando la expectativa de que este tipo de tecnología supere en el futuro el poder cognitivo de los seres humanos. En otras palabras, la IA puede definirse como cualquier sistema artificial que tiene la capacidad de planear y gestionar diferentes acciones sin la supervisión humana, bajo condiciones que no son predecibles y que han sido aprendidas por la máquina a partir de los datos.

Uno de los líderes más importantes en materia de tecnología, Bill Gates, afirmó que

> el desarrollo de la IA es tan fundamental como la creación del microprocesador, el computador personal, internet y el móvil. Cambiará la forma en que las personas trabajan, aprenden, viajan, reciben atención médica y se comunican entre sí. Industrias completas se reorientarán en torno a ella. Las empresas se distinguirán por cuán bien la utilizan. (Gates, 2023)[1]

La IA es uno de los principales avances tecnológicos que ha despertado el interés de las grandes potencias mundiales, quienes la consideran como un pilar fundamental para su posición en el futuro cercano. En este sentido, en el año 2017, el presidente de Rusia, Vladímir Putin, durante una presentación en una clase magistral sobre IA en su país, dejó clara la importancia de la IA para la supremacía mundial, al afirmar que "quien sea el líder en IA también será el dirigente del mundo" (CNN, 2017). Este interés en la IA ha dado lugar a una competencia tecnológica entre las grandes potencias para lograr la supremacía en este ámbito. Dicha competencia se ha traducido en diversas iniciativas tanto a nivel político como de programas tecnológicos, con el fin de influir, dominar o beneficiarse del ciberespacio para potenciar los intereses de su nación y reducir los riesgos. Así, la carrera por la IA es una muestra de cómo la tecnología ha dejado de ser una herramienta y se ha convertido en un objetivo estratégico de la geopolítica global, donde la capacidad de los Estados para desarrollar y utilizar la IA determinará su posición en el mundo.

La IA se puede dividir en dos categorías: la débil y la fuerte (Abraham y Grosan, 2011). La IA débil hace referencia a los sistemas diseñados para realizar tareas específicas sin tener capacidad de aprendizaje; ejemplos de ello son el reconocimiento de voz y el análisis de datos. Por otra parte, la IA fuerte se refiere a sistemas que tienen la capacidad de aprender, adaptarse a nuevas situaciones y resolver problemas de manera similar a como lo haría un ser humano. Para algunas de las aplicaciones de la IA se necesitan datos reales y requisitos para entrenar al sistema (por ejemplo, por aprendizaje supervisado o por refuerzo) con el fin de probarla y garantizar su efectividad antes de su despliegue.

[1] Traducción propia.

Los avances tecnológicos de la IA como el del procesamiento del lenguaje natural y la comprensión del habla han facilitado la comunicación e interacción entre los seres humanos y las máquinas, llegando a un punto de cambio para la humanidad y para el modo en que esta se relaciona con las máquinas. A continuación, se listan las capacidades más representativas asociadas a la IA, basadas en el aprendizaje automático (algoritmos que permiten que las máquinas aprendan de los datos y mejoren su rendimiento sin ser programadas explícitamente para hacerlo) y en la automatización de procesos (tareas realizadas de manera autónoma y sin intervención humana):

- Razonamiento y toma de decisiones: es la capacidad de las máquinas para tomar decisiones lógicas basadas en datos y modelos de aprendizaje automático (Abraham y Grosan, 2011). Esto hace que puedan recomendar productos, servicios o contenido personalizado basados en el comportamiento del usuario y preferencias, así como también optimizar el uso de recursos (como la energía, el agua o el combustible) para maximizar la eficiencia y minimizar costos.
- Planificación y programación: es la capacidad de las máquinas para planificar y programar tareas y procesos (Norvig y Russell, 2010).
- Análisis de datos: es la capacidad de las máquinas para analizar grandes cantidades de datos y extraer información valiosa de ellos, detectar patrones anormales o inusuales en los datos y alertar a los humanos para que investiguen más a fondo; y para detectar y mitigar amenazas de seguridad (como el fraude o los ataques cibernéticos). Además, permite predecir eventos futuros basados en patrones y datos históricos (por ejemplo, pueden recopilar y analizar datos meteorológicos para predecir el clima futuro o pueden analizar los datos de los pacientes y los registros médicos para ayudar en el diagnóstico y tratamiento de enfermedades) (Abraham y Grosan, 2011).
- Reconocimiento de voz: es la capacidad de las máquinas para reconocer y entender el habla humana (Norvig y Russell, 2010).
- Robótica: es la capacidad de las máquinas para moverse físicamente y realizar tareas en el mundo real (Norvig y Russell, 2010), como por ejemplo conducir vehículos sin intervención humana.
- Visión por computadora: es la capacidad de las máquinas para analizar imágenes y videos y comprender lo que están viendo (Marr, 2019). Esto permite el reconocimiento de objetos o personas (mediante el reconocimiento facial).
- Procesamiento del lenguaje natural: es la capacidad de las máquinas para entender el lenguaje humano y comunicarse con los seres humanos de manera efectiva. Además, incluye la capacidad de traducir el lenguaje hablado o escrito de un idioma a otro de manera efectiva (Abraham y Grosan, 2011).
- Detección de emociones: es la capacidad de las máquinas para detectar emociones humanas y actitudes expresadas en los textos, imágenes y videos, y responder en consecuencia (Hao *et al.*, 2021).

Revista de la Escuela Nacional de Inteligencia · Número 2 · Enero a junio de 2023 · pp. 151-171
ISSN 2953-4623 (en línea) y 0327-6961

- Interacción social: es la capacidad de las máquinas para interactuar con las personas de manera socialmente inteligente y comprensiva de forma verbal o escrita (por ejemplo, cuando pueden responder a las preguntas y preocupaciones de los clientes de manera efectiva y personalizada) (Hao *et al.*, 2021).
- Creatividad: es la capacidad de las máquinas para generar soluciones creativas a problemas complejos (Rico Sesé, 2019).
- Generación de contenidos: es la capacidad de las máquinas para generar contenido de manera autónoma, como texto, música o imágenes (Torres, 2017). Además, tienen la capacidad de crear imágenes y videos que parecen reales, incluso si no existen efectivamente.
- Adaptabilidad: es la capacidad de las máquinas para adaptarse a nuevos entornos y situaciones, así como detectar y corregir errores o defectos en la producción o el rendimiento de los sistemas (Norvig y Russell, 2010).

Hoy en día, la IA se ha convertido en un "trofeo" que todos los laboratorios de diferentes países quieren alcanzar, lo cual genera una carrera fuera de control para desarrollar máquinas cada vez más poderosas que no se puedan predecir, ni siquiera por quienes las están desarrollando. El último avance representativo en este plano tuvo lugar el 30 de noviembre de 2022 y corresponde al lanzamiento de un prototipo de *chatbot* desarrollado por OpenAI conocido como ChatGPT. Durante su lanzamiento, se realizó una demostración que exhibe cómo esta tecnología tiene la capacidad de redactar demandas, aprobar exámenes estandarizados (como lo fue el examen de posgrado de la Escuela de Negocios Wharton de la Universidad de Pensilvania [Gallegos, 2023]) y crear sitios web funcionales a partir de bocetos dibujados a mano (Murphy Kelly, 2023). Además, este chat cuenta con la capacidad de entender imágenes y extraer información a partir de ellas.

A futuro, se espera que la IA sea más avanzada y compleja, tenga la capacidad de aprender de forma más eficiente y autónoma, y pueda tomar sus propias decisiones y realizar tareas complejas sin intervención humana, lo cual podría ser particularmente útil en áreas como la robótica, donde los robots de IA podrían ser utilizados para realizar tareas peligrosas o difíciles para los humanos, como la exploración de zonas de alto riesgo. También se espera que la IA esté más integrada con nuestra vida cotidiana a través de la utilización de dispositivos inteligentes y sistemas de automatización en el hogar, las oficinas, los gobiernos y las empresas. Además, la implementación de la IA traerá consecuencias en la estructura y gestión del trabajo, lo que obligará a adaptarse a su uso. Esto podría implicar la supresión de algunos trabajos y la creación de otros nuevos, o la necesidad, por ejemplo, de ajustar las políticas de contratación y beneficios de las empresas.

El hecho de que se estén dando avances tan importantes en el campo de la IA conlleva a que las personas reflexionen sobre el avance de esta tecnología y planteen los peligros que esta puede implicar para la humanidad. En este sentido, Elon Musk,

junto con profesores, investigadores y líderes tecnológicos, firmó una carta publicada por Future of Life Institute (organización sin fines de lucro respaldada por Musk) en la que se solicita a los laboratorios detener el entrenamiento de los sistemas de IA por al menos seis meses, debido a los riesgos que, a su juicio, ello genera para la sociedad y la humanidad.

2.1 Países líderes

De acuerdo con el Artificial Intelligence Index Report 2023 publicado por la Universidad de Stanford, la inversión privada en IA para el año 2022 está liderada por los Estados Unidos[2] con una inversión de 47,36 miles de millones de dólares, seguido por China con una inversión privada de 13,41 miles de millones de dólares. Los demás países están lejos de estas cifras, con menos de 4,5 miles de millones de dólares. Es de destacar que el único país de Latinoamérica que aparece dentro de este índice es la Argentina, con una inversión privada de 1,52 miles de millones de dólares.

En este sentido, los Estados Unidos son considerados líderes mundiales en IA. Cuentan con importantes centros de investigación en universidades como Stanford, Carnegie Mellon y el Instituto de Tecnología de Massachusetts (MIT, por su sigla en inglés), que están produciendo constantemente innovaciones en este campo.

Por su parte, China ha establecido una estrategia nacional para el desarrollo de la IA y ha invertido miles de millones de dólares en la creación de centros de investigación y empresas tecnológicas dedicadas a ella. En 2017, el gobierno chino publicó un plan para convertirse en líder mundial en IA para 2030, y desde entonces ha estado trabajando en su implementación.

Con respecto a los países latinoamericanos, gran parte del camino del desarrollo de la IA aún está por recorrerse. Colombia busca ser líder en IA en América Latina, como queda evidenciado en el hecho de que, de acuerdo con el más reciente Global AI Index (Tortoise Media, 2021) elaborado por Tortoise Intelligence, en el tema de *estrategia gubernamental* (profundidad del compromiso del gobierno nacional con la IA e investigación de los compromisos de gasto y las estrategias nacionales), Colombia ocupa el primer puesto en Latinoamérica y el noveno puesto a nivel mundial en este asunto. Asimismo, los países latinoamericanos que se destacan en los demás temas del índice son: Brasil, líder regional en talento (personal capacitado para provisión de soluciones en IA), infraestructura (confiabilidad y escala de la infraestructura de acceso) y desarrollo (de plataformas y algoritmos de base para proyectos innovadores en IA); México, líder regional en investigación (cantidad de publicaciones y citas en revistas académicas de

[2] La inversión pública en IA no es factible de calcular con un alto grado de exactitud debido a que la información relacionada con la inversión de las agencias de inteligencia y del sector Defensa son de carácter confidencial.

Revista de la Escuela Nacional de Inteligencia · Número 2 · Enero a junio de 2023 · pp. 151-171
ISSN 2953-4623 (en línea) y 0327-6961

renombre); Chile, líder regional en comercio (nivel de actividad de las *startups*, inversiones e iniciativas empresariales basadas en IA); y la Argentina, líder regional en entorno operativo (contexto regulatorio y opinión pública en torno a IA).

3. Inteligencia estratégica

La inteligencia estratégica es la disciplina que se enfoca en la identificación, análisis y evaluación de información para apoyar la toma de decisiones trascendentales que permitan proteger los intereses del Estado y promover sus objetivos a largo plazo en temas como política exterior, seguridad y economía, entre otros ámbitos estratégicos. Según Sherman Kent (1949), la inteligencia estratégica es un conocimiento vital para la supervivencia nacional y la toma de decisiones estratégicas.

La inteligencia estratégica del Estado responde al gobierno y su objetivo principal es recopilar información para producir conocimiento que proteja los intereses del Estado a largo plazo y garantice los derechos humanos. Busca información sobre planes y acciones de otros Estados, grupos terroristas, organizaciones criminales, empresas y otros actores que amenacen al Estado. Además, identifica oportunidades y riesgos, evaluando la estabilidad de otros Estados, el desarrollo tecnológico y científico en otros países, el comercio internacional y otros factores que afecten los intereses nacionales.

La inteligencia estratégica utiliza el ciclo de inteligencia, que consta de fases interrelacionadas: planeación, recolección, procesamiento y análisis, y difusión de información. Según Harris y Markowitz (2016), este ciclo es un proceso sistemático y repetitivo que asegura la obtención de información útil para la toma de decisiones importantes.

La planeación es fundamental, pues es donde se establecen los objetivos de inteligencia y el plan para alcanzarlos. Dichos objetivos deben ser claros, específicos, relevantes y pertinentes para obtener la información necesaria para la toma decisiones (Bernhardt, 2003). Se debe identificar fuentes de información y desarrollar un plan para recolección y análisis. Requiere asignación de recursos, identificación de prioridades en términos de objetivos de inteligencia y una línea de tiempo clara para llevar a cabo un proceso eficiente.

La recolección de información busca obtener y reunir datos relevantes, oportunos, pertinentes y fiables para su posterior análisis. Es importante identificar las fuentes relevantes y confiables en función de su credibilidad y acceso para que la información sea precisa y confiable. Se basa en fuentes humanas y fuentes técnicas. Las fuentes humanas incluyen a las personas que tienen acceso a información relevante para la producción de inteligencia, como por ejemplo informantes, diplomáticos o incluso agentes de inteligencia de otras agencias de interés. Las fuentes técnicas abarcan el uso de equipos y tecnologías de recolección de información, como satélites, sistemas de radar, cámaras y tecnología informática. Sin embargo, es importante aclarar que los dispositivos técnicos, como los

Revista de la Escuela Nacional de Inteligencia · Número 2 · Enero a junio de 2023 · pp. 151-171
ISSN 2953-4623 (en línea) y 0327-6961

drones, no son propiamente fuentes técnicas en sí mismos, sino más bien dispositivos o herramientas técnicas utilizadas para la obtención de información.

Las fuentes humanas son especialmente importantes en la recolección de información sobre objetivos estratégicos, ya que pueden proporcionar información detallada y valiosa sobre las actividades y planes del objetivo. Además, pueden proporcionar información sobre intenciones, motivaciones y relaciones entre individuos y organizaciones. Sin embargo, las fuentes humanas también son costosas, requieren tiempo y esfuerzo de los agentes de inteligencia y pueden ser peligrosas para los individuos involucrados.

Las fuentes técnicas pueden proporcionar información detallada y en tiempo real sin arriesgar la vida de los analistas de inteligencia. Los sistemas de radar, los satélites y las cámaras pueden brindar información detallada sobre la actividad en la superficie terrestre, el mar y el aire. La tecnología informática puede utilizar *software* para monitorear comunicaciones electrónicas y recopilar información de fuentes abiertas. Y herramientas, como los drones, pueden proporcionar información sobre áreas de difícil acceso y permitir la recolección de información en tiempo real.

Durante la recolección, es importante considerar la ética y la legalidad. Según Ross Bellaby (2012), las regulaciones aplicables a la recolección de información deben ser consideradas y respetadas para garantizar que tanto las acciones de inteligencia utilizadas como la información recolectada sean legales y éticas.

El procesamiento y análisis de información se basa en la revisión y evaluación de datos y materiales recolectados, proceso que incluye la organización y clasificación de la información recopilada, la eliminación de datos irrelevantes y la identificación de patrones y tendencias. Inicialmente, los analistas deben asegurarse que la información recopilada sea precisa, relevante y completa. La información que no cumple con estos criterios debe ser descartada o verificada antes de su inclusión en el proceso de análisis. Además, deben considerar el contexto de la información y cómo se relaciona con otros datos recopilados. Posteriormente, los analistas deben procesar la información (organizarla, eliminar información redundante o no esencial e identificar patrones y tendencias). Este análisis debe inclinarse a la objetividad, lo cual es difícil para un analista a quien le interesa sobremanera el resultado de su trabajo, por lo que se le dificulta aislar sus expectativas y emociones respecto al problema (Clark, 2004).

Dentro de las herramientas y técnicas analíticas para analizar la información e identificar riesgos, amenazas y oportunidades se encuentran las siguientes: *software* de análisis de datos para procesar grandes cantidades de información y extraer patrones y tendencias; herramientas de minería de datos (que aplican algoritmos de aprendizaje automático) para descubrir patrones y relaciones en grandes conjuntos de datos; herramientas de visualización de datos para crear gráficos que permitan entender la información de manera clara y rápida; y *software* de procesamiento de lenguaje natural para extraer información de grandes cantidades de texto.

Revista de la Escuela Nacional de Inteligencia · Número 2 · Enero a junio de 2023 · pp. 151-171
ISSN 2953-4623 (en línea) y 0327-6961

La difusión de información tiene un papel fundamental, ya que el éxito del proceso de inteligencia depende de cómo se comparta la información, de cómo se utilice para la toma de decisiones y de que llegue a los tomadores de decisión adecuados en el momento oportuno. La difusión puede llevarse a cabo a través de diferentes medios, como informes de inteligencia, presentaciones orales, *briefings* y documentos oficiales. Las presentaciones orales y los *briefings* pueden ser utilizados para proporcionar información de manera más rápida y efectiva, mientras que los documentos oficiales y los informes de inteligencia se pueden emplear para comunicar la información de manera más detallada y formal.

Es responsabilidad de los agentes de inteligencia involucrados en esta fase, así como de los tomadores de decisión, asegurarse de que la información se difunda solo a las personas que tienen la autoridad legal para recibirla y que, además, se utilice de manera responsable y ética. La difusión indebida de información sensible puede tener consecuencias graves y comprometer los intereses estratégicos del Estado. Como señala Clark (2004), la difusión de información clasificada está restringida por regulaciones y políticas que protegen la información sensible de ser compartida con aquellos que no tienen el derecho legal de conocerla.

Es importante destacar los principios éticos que deben guiar la actividad de inteligencia en materia de producción de información enfocada a dar herramientas para la toma de decisiones estratégicas del Estado. De acuerdo con Miller (2021), la actividad de inteligencia debe estar sujeta a principios de no discriminación, necesidad, proporcionalidad y reciprocidad para garantizar que las acciones de inteligencia sean éticas y respeten los derechos y las libertades civiles de las personas.

En esta misma línea ética, cabe mencionar el planteamiento de Lilian Coutinho (2020), quien establece la importancia para los servicios de inteligencia de mantener un equilibrio entre el procesamiento y la protección de los datos personales enfocado a proteger tanto los derechos y garantías fundamentales de las personas como del agente de inteligencia y de la actividad misma. En caso de perder este equilibrio, puede haber manipulación, discriminación, pérdida de seguridad o de confidencialidad, chantaje, reducción de la confianza en el Estado y cambios de comportamiento.

4. La inteligencia artificial en la inteligencia estratégica

Actualmente, muchas de las agencias de inteligencia utilizan principalmente la IA débil, explotando su capacidad para recolectar información mediante extracción de datos web en fuentes abiertas, así como para analizar grandes cantidades de datos y proporcionar información relevante y procesable —y, con ello, alcanzando una velocidad mucho mayor a la que sería posible para un ser humano—. De esta manera, la IA débil ayuda a identificar patrones y relaciones que pueden no ser evidentes para un analista humano.

Revista de la Escuela Nacional de Inteligencia · Número 2 · Enero a junio de 2023 · pp. 151-171
ISSN 2953-4623 (en línea) y 0327-6961

Respecto a la IA fuerte, existen agencias de inteligencia que están a la vanguardia en su implementación y están cambiando el paradigma que limita a los espías a ser seres humanos, para incluir como principal componente del espionaje máquinas inteligentes capaces de ser invisibles ante los sistemas.

Tal es el caso de la Agencia Central de Inteligencia de los Estados Unidos (CIA), que está fuertemente comprometida en la implementación de tecnologías avanzadas en sus actividades de inteligencia. En este sentido, la IA es una herramienta clave para ellos. De acuerdo con Dawn Meyerriecks, directora de la Dirección de Ciencia y Tecnología, la CIA está trabajando en la implementación de la IA y del aprendizaje automático para descubrir patrones y conexiones en grandes cantidades de datos, lo que les permitiría identificar amenazas terroristas y prevenir ataques cibernéticos (CNN, 2018). Otro de los actuales usos es la implementación de la IA para mejorar sus capacidades de reconocimiento facial y de identificación de personas sospechosas.

Según Meyerriecks, la vigilancia digital (incluida la televisión de circuito cerrado y la infraestructura inalámbrica) está funcionando en alrededor de treinta países, lo que hace que el seguimiento físico pueda ser reemplazado por la IA (CNN, 2018). No obstante, esta autora considera que la IA no reemplaza la inteligencia humana, pues los seres humanos son capaces de diferenciar la intención real a partir de lo que una persona dice, lo cual muestra que existe una gran diferencia en términos de evaluar y separar la retórica de la intención real, lo que aún no es posible con las máquinas (The New York Times, 2021).

Además, la CIA tiene alianzas estratégicas con diferentes organizaciones y empresas tecnológicas, lo que le permite estar en constante actualización y desarrollo de nuevas tecnologías para mejorar sus capacidades de inteligencia y mantenerse actualizada en un entorno en constante evolución. Algunas de estas organizaciones son In-Q-Tel, una organización sin fines de lucro que busca tecnologías emergentes para la CIA y otras agencias de inteligencia estadounidenses; DARPA (Defense Advanced Research Projects Agency), una agencia del Departamento de Defensa de los Estados Unidos que se enfoca en el desarrollo de tecnología avanzada para uso militar; e IARPA (Intelligence Advanced Research Projects Activity), una organización de investigación en ciencias sociales y conductuales para el desarrollo de tecnología de inteligencia. Además, la CIA también tiene alianzas con empresas tecnológicas líderes en el mercado, como Amazon Web Services (AWS) y Google. En 2019, la CIA otorgó un contrato multimillonario a AWS para desarrollar una nube privada para el almacenamiento de datos de la agencia (The New York Times, 2021). También se sabe que la CIA ha trabajado con Google en el pasado en proyectos de tecnología de inteligencia.

La agencia de inteligencia de la República Popular China también ha mostrado avances en su aplicación en la IA. Algunas de las aplicaciones de la IA utilizadas por el servicio de inteligencia chino incluyen la vigilancia, el reconocimiento facial y el análisis de datos.

Revista de la Escuela Nacional de Inteligencia · Número 2 · Enero a junio de 2023 · pp. 151-171
ISSN 2953-4623 (en línea) y 0327-6961

El Ministerio de Seguridad del Estado (MSS), la principal agencia de inteligencia de la República Popular China, ha utilizado la IA en diversas áreas para mejorar su capacidad de recopilación y análisis de información y de toma de decisiones estratégicas. El gobierno chino ha estado utilizando la IA para crear una base de datos de reconocimiento facial que se utiliza para identificar a las personas en las calles y en lugares públicos, así como para realizar vigilancia de video y monitoreo de las redes sociales (Das *et al.*, 2018). Esta gran cantidad de datos recolectados probablemente pueda proporcionar alertas tempranas sobre posibles amenazas a la estabilidad y el bienestar del país y sus ciudadanos, y a los intereses estratégicos del Estado.

De acuerdo con la información conocida en temas de IA, China tiene el mejor sistema de reconocimiento visual, está investigando en diferentes tipos de vehículos no tripulados de aire, tierra y agua, y está desarrollando un portafolio de herramientas para operaciones en el ciberespacio (Sayler, 2020).

Sin embargo, el uso de la IA por parte del gobierno chino ha generado preocupaciones sobre la privacidad y la ética. La recopilación y el uso de datos personales y de reconocimiento facial pueden violar los derechos de privacidad y libertad individual. Para abordar estas preocupaciones, China ha implementado medidas de protección de la privacidad, como la Especificación de seguridad de la información personal. Sin embargo, la Especificación es voluntaria y tiene lagunas significativas, por lo que el problema ético relacionado con la privacidad aún no está resuelto (Cowls *et al.*, 2021).

Los avances de la IA que han venido surgiendo en el mundo generan la necesidad de que todas las agencias de inteligencia estén a la vanguardia de la tecnología y la innovación y no se queden rezagadas. Si bien lo ideal sería que cada una de las agencias tuviera su propia investigación, de no ser posible es necesario buscar otros mecanismos para adoptar los avances de la IA en el logro de su misión, en el marco ético de su implementación y del respeto por los derechos humanos.

Se identifican varios aspectos importantes en los que la IA puede ser beneficiosa para la inteligencia estratégica, en línea con el ciclo de inteligencia, los cuales se presentan a continuación.

Planeación

La IA puede ser utilizada para predecir y prevenir amenazas futuras mediante el análisis de datos históricos y en tiempo real. Además, es útil para modelar escenarios futuros y evaluar su probabilidad de ocurrencia y sus consecuencias con el fin de tomar decisiones estratégicas. Esto ayuda a que las agencias de inteligencia estratégica tomen medidas preventivas para minimizar el riesgo de posibles amenazas.

En este mismo sentido, la IA puede ser utilizada para identificar enemigos potenciales y amenazas para los intereses del Estado o de la nación que no estén siendo

Revista de la Escuela Nacional de Inteligencia · Número 2 · Enero a junio de 2023 · pp. 151-171
ISSN 2953-4623 (en línea) y 0327-6961

considerados dentro de los objetivos actualmente planteados para proteger los intereses del Estado y promover sus objetivos a largo plazo.

Recolección

La IA puede, en materia de planeación, contribuir a:

- Automatizar recolección de información: se pueden establecer algoritmos que sean entrenados para recolectar información de fuentes abiertas con el fin de identificar patrones específicos de datos, palabras clave y tendencias en el contenido en línea, y así automatizar la recolección de información en una escala masiva en diferentes idiomas. Estos algoritmos pueden ser programados para filtrar y verificar automáticamente la precisión y la confiabilidad de los datos recopilados, eliminando así información redundante o falsa, o que no sea relevante para la investigación.
- Análisis de audio y video: la IA puede realizar análisis de grandes volúmenes de audio y video para identificar personas, objetos, acciones o palabras clave relevantes, así como relaciones con fenómenos de interés para la inteligencia estratégica. Esto puede incluir la detección automática de armas, explosivos y otras amenazas.
- Vigilancia electrónica y física: la IA puede ser utilizada en la vigilancia electrónica para monitorear comunicaciones y el comportamiento en línea de personas y grupos. También puede ser utilizada para monitorear el tráfico web en busca de determinadas actividades terroristas o de extremismo violento. Además, respecto a la vigilancia física, la IA puede utilizarse para el reconocimiento facial las veinticuatro horas, lo que podría permitir la identificación de personas en lugares públicos y la recopilación de información de ellas, así como la detección de comportamientos sospechosos. Los drones equipados con cámaras y sensores pueden recopilar información de personas o comportamientos sobre actividades en áreas remotas o inaccesibles.
- Ciberinteligencia: la IA puede ser utilizada para identificar campañas de desinformación (difusión de información falsa), reclutar fuentes humanas a través de internet y crear perfiles y comunidades falsas.[3] Además, puede utilizarse para crear rápidamente páginas web que soporten las coberturas de los agentes de

[3] Estas capacidades de la IA se plantean por el hecho de que dicha tecnología tiene la posibilidad de realizar estos procesos, dejando de lado el debate ético existente alrededor del tema como lo es el cuestionamiento existente sobre las garantías de un orden democrático o en la injerencia en procesos de otros países. Por ejemplo, si se utiliza la desinformación para influir en una elección, se estaría socavando el derecho de los ciudadanos a tomar decisiones informadas y participar en un proceso electoral justo y transparente. De igual manera, si se utilizan estas técnicas para influir en procesos políticos de otros países, se estaría violando la soberanía y autonomía de esos Estados.

Revista de la Escuela Nacional de Inteligencia · Número 2 · Enero a junio de 2023 · pp. 151-171
ISSN 2953-4623 (en línea) y 0327-6961

inteligencia. También puede utilizarse para monitorear redes y sistemas; analizar patrones de tráfico y de comportamiento; hacer seguimiento de la actividad en el ciberespacio de los grupos de amenazas conocidos; y recolectar información de fuentes abiertas (como redes sociales y foros en línea).

- Monitoreo de la *dark web*: la IA tiene la capacidad de analizar grandes volúmenes de datos de la *dark web*, lo que permite identificar patrones y tendencias. Esto es particularmente útil para detectar actividades ilegales (como la venta de drogas, armas y servicios de *hacking*), así como amenazas a la seguridad (como la planificación de ataques terroristas o ciberataques). Otra aplicación de la IA en la monitorización de la *dark web* es la identificación de personas y organizaciones que están involucradas en actividades ilegales o que representen una amenaza para la seguridad mediante el análisis de grandes cantidades de datos de la *dark web* para identificar patrones de comportamiento, conexiones y actividades sospechosas. Esto puede ayudar a las agencias de inteligencia a desarticular organizaciones criminales e identificar individuos que representen una amenaza para la estabilidad y el bienestar del país y sus ciudadanos, y a los intereses estratégicos de un Estado.

Procesamiento y análisis

Las tecnologías de aprendizaje automático y procesamiento de lenguaje natural pueden analizar y clasificar grandes conjuntos de datos estructurados y no estructurados, que incluyen datos de redes sociales, de satélites, financieros, de tráfico de internet, de comunicaciones electrónicas y de telecomunicaciones, como llamadas telefónicas y correos electrónicos, entre otros. Son capaces, además, de realizar análisis predictivos y de tendencias, identificar patrones y relaciones en los datos y detectar anomalías o comportamientos sospechosos. También pueden identificar patrones y tendencias a largo plazo que les permitan a los gobiernos tomar decisiones informadas sobre política exterior o seguridad internacional, o monitorear el comportamiento de adversarios potenciales de un país.

La IA puede ser utilizada para examinar informes que han elaborado los analistas de inteligencia, y así detectar patrones y relaciones objetivas en los datos que indiquen la presencia de una amenaza o un posible ataque. De igual forma, la IA puede contribuir a disminuir la subjetividad del analista en la elaboración de los análisis de inteligencia.

Además, la IA puede usarse para identificar potenciales vulnerabilidades en sistemas críticos como infraestructura de transporte y redes eléctricas, haciéndolo de una manera preventiva para proteger a los ciudadanos.

Revista de la Escuela Nacional de Inteligencia · Número 2 · Enero a junio de 2023 · pp. 151-171
ISSN 2953-4623 (en línea) y 0327-6961

Difusión

La inteligencia artificial (IA) puede ofrecer un importante beneficio en esta etapa del ciclo al ayudar a identificar nuevos posibles destinatarios de productos de inteligencia y contrainteligencia, siempre respetando los límites legales establecidos. De igual forma, podría contribuir a decidir qué parte de la información sería conveniente ponerla en conocimiento exclusivo de determinado tomador de decisiones manteniendo la confidencialidad. Esto permite ampliar el impacto potencial de los productos de inteligencia tanto en el sector público como en el privado de cada país, los cuales pueden tener un carácter orientador en la toma de decisiones, dentro de la órbita funcional de los nuevos destinatarios. Es decir, la IA puede ayudar a generar alertas o sugerencias de posibles receptores (legalmente autorizados) a quienes de una u otra forma les puede resultar de utilidad determinada información para una mejor toma de decisiones en su campo concerniente, evitando los inconvenientes que pueden derivar del sesgo o error humanos.

Actividades transversales al ciclo

En general, la IA puede ser utilizada para automatizar tareas repetitivas (que tengan lineamientos establecidos implícita o explícitamente) como la clasificación de documentos, la identificación de información relevante en grandes conjuntos de datos, la gestión documental, la elaboración y el reporte de indicadores de gestión, el pago de nómina, el control de inventario y la localización de todos los activos, entre otras.

Sin embargo, en nuestra opinión, el mayor impacto de la IA en las actividades transversales al ciclo tendrá lugar en el campo de la ciberseguridad. La IA podrá ser utilizada para detectar y prevenir ataques cibernéticos a infraestructura crítica, sistemas, redes de información u otros sistemas sensibles en tiempo real; y en caso de que ocurran los ataques, puede contribuir a hacer un diagnóstico preventivo y subsanar lo que haya sido afectado lo más rápido posible. También sería útil para identificar patrones y comportamientos anómalos en los datos de redes y sistemas, lo que puede permitir detectar intrusiones y ataques cibernéticos y generar una respuesta rápida y efectiva ante estos.

En este sentido, la IA mejorará aspectos como la gestión de intrusiones; la protección *antimalware*; la gestión de fraude; la gestión de identidades y de acceso; la prevención de correos maliciosos, entre otros.

Además, la IA podrá aumentar la capacidad de reacción y efectividad de los incidentes de ciberseguridad, ya que las máquinas serán capaces de aprender del entorno, identificar patrones dentro de las amenazas y tomar decisiones críticas en tiempo real ante ataques cibernéticos, donde la intervención humana será relevante para tomar decisiones finales y determinar que las acciones apropiadas sean coherentes con las políticas de seguridad y las regulaciones gubernamentales. De igual forma, la IA podrá

Revista de la Escuela Nacional de Inteligencia · Número 2 · Enero a junio de 2023 · pp. 151-171
ISSN 2953-4623 (en línea) y 0327-6961

predecir posibles ataques (mejorando de esta forma las defensas y minimizando los riesgos basados en datos, contexto y experiencia) y priorizará la gestión de ataques sobre las posibles falsas amenazas, lo que conllevará a aumentar la eficiencia de los sistemas.

Finalmente, la implementación de IA en las estructuras cibernéticas del Estado también puede ser vista como parte de la capacidad de disuasión contra los ciberdelincuentes.

4.1 Retos y desafíos

El principal reto para la inteligencia estratégica es no quedarse rezagada con respecto a la tecnología de IA. Si el Estado no se apropia de esta tecnología antes que los criminales, podría verse en la misma situación de alguien que intenta apagar un incendio forestal con un balde de agua.

Un desafío en la implementación de la IA en la inteligencia estratégica es que existe una separación con la industria que desarrolla la tecnología, por lo que los datos, al ser clasificados, no pueden ser compartidos con destinatarios no autorizados. Esto implica garantizar que los datos generados en inteligencia estratégica no sean utilizados por las compañías de IA para entrenar sus modelos de lenguaje.[4] Por lo tanto, se hace necesario crear una estrategia de cooperación entre las agencias de inteligencia con la industria de desarrollo tecnológico, especialmente con los laboratorios de IA, sin poner en riesgo los intereses estratégicos de la nación, para entrenar sistemas de información enfocados a mejorar la inteligencia estratégica.

El último reto —y, desde nuestra perspectiva, el más importante— al que se deben enfrentar las agencias de inteligencia y los Estados es determinar hasta qué punto están dispuestos a confiar la producción de información utilizada para la toma de decisiones de los asuntos más relevantes del Estado a la IA, teniendo en cuenta las ventajas y desventajas que ello representa. Es decir, esto aumenta la necesidad de aplicar un enfoque crítico y cuidadoso en la adopción de esta tecnología por parte de los servicios de inteligencia, puesto que, por una parte, su implementación es necesaria para no quedar obsoletos en un mundo cada vez más tecnológico y así poder proteger y promover los intereses del Estado; y por otra parte, se debe tener en cuenta la incertidumbre sobre la precisión de los resultados generados por la IA, así como la posibilidad de que durante su uso pueda llegar a tener filtraciones por parte de enemigos internos o externos que conlleve a tomar decisiones erróneas que afecten los intereses de la nación. Dichas filtraciones hacen referencia a tres escenarios. El primero es aquel en el que los adversarios del Estado logran manipular, mediante un acceso no autorizado, los datos utilizados para entrenar la IA y, en

[4] Los modelos de lenguaje empleados por las compañías de IA son entrenados a partir de inmensas cantidades de texto y datos en general, y algunas compañías, como OpenIA, pueden utilizar los resultados de la interacción generada por los usuarios para entrenar modelos posteriores.

Revista de la Escuela Nacional de Inteligencia · Número 2 · Enero a junio de 2023 · pp. 151-171
ISSN 2953-4623 (en línea) y 0327-6961

consecuencia, generar resultados incorrectos. El segundo escenario refiere a la inserción de información falsa o engañosa en los sistemas de IA de una agencia de inteligencia específica, lo cual afectaría la precisión de los productos de inteligencia generados. Por último, el tercer escenario implica que la propia IA adopte posturas específicas en determinados temas, lo que podría influir en los resultados para que se tomen decisiones que la IA desea, lo cual la convertiría en un enemigo silencioso del Estado.

4.2 Nuevos delitos que surgen a partir de la IA

El desarrollo de la IA ha creado nuevas posibilidades para delitos que antes no existían relacionados con la inteligencia estratégica. Uno de los mayores retos que deberán enfrentar las agencias de inteligencia es la rápida implementación de la IA por parte de los delincuentes y ciberdelincuentes, quienes emplean soluciones cada vez más precisas y complejas para realizar sus actividades. Ejemplo de ello son los ataques cibernéticos más avanzados. Los delincuentes pueden utilizar la IA para realizar ataques cibernéticos más sofisticados y efectivos, como el *phishing* de voz (en donde los ciberdelincuentes pueden utilizar la IA para personalizar los mensajes de *phishing* y hacer que parezcan más auténticos y convincentes). De igual forma, los atacantes pueden utilizar la IA para realizar ataques de *ransomware* más sofisticados, que pueden propagarse de manera más efectiva y ser más difíciles de detectar.

También se espera que los ciberdelincuentes utilicen *malwares* inteligentes, que aprenden de las vulnerabilidades del sistema para saber cómo evitar las protecciones existentes en los sistemas y atacar cuando encuentren el momento más propicio, o cuando logren conocer a los usuarios a tal punto que sepan cómo convencerlos para que accedan a recursos maliciosos con los que serán infectados. Esto muestra la necesidad de que las empresas refuercen sus sistemas de seguridad de modo tal que la ciberseguridad sea más inteligente que los ataques cibernéticos que reciba.

Otros delitos que se espera que aparezcan o se fortalezcan son:

- Robo de datos personales: los algoritmos de IA pueden ser utilizados para extraer información personal de grandes bases de datos de forma más eficiente y con mayor precisión que los métodos tradicionales de recopilación de datos.
- Robo de propiedad intelectual: los delincuentes pueden utilizar la IA para robar propiedad intelectual y secretos comerciales, lo que puede tener graves consecuencias para las empresas afectadas.
- Fraude de identidad con IA: los delincuentes pueden utilizar la IA para generar imágenes y videos falsos que parezcan auténticos, lo que puede ser utilizado para cometer fraudes de identidad y engañar a las personas.
- Fraude financiero: la IA puede ser utilizada para generar contenido falso o engañoso, como noticias o informes financieros, para manipular los mercados y

Revista de la Escuela Nacional de Inteligencia · Número 2 · Enero a junio de 2023 · pp. 151-171
ISSN 2953-4623 (en línea) y 0327-6961

realizar operaciones fraudulentas. Además, mediante imágenes y videos falsos pueden suplantar personas para acceder a sus datos bancarios.

- Ataques a sistemas autónomos: los sistemas autónomos, como los drones y los vehículos autónomos, pueden ser atacados por *hackers* que aprovechen las debilidades de los algoritmos de IA que los controlan.

4.3 Riesgos

La implementación de la IA en la inteligencia estratégica del Estado puede ser una herramienta valiosa para el análisis y evaluación de información crítica en la toma de decisiones. Sin embargo, también presenta riesgos significativos.

El principal riesgo para los servicios de inteligencia es la posibilidad de que la IA genere y difunda información errónea; y el riesgo que esto implica (sin saberlo) a la hora de crear informes de inteligencia que pueden ser usados para tomar decisiones estratégicas para una nación.

De igual forma, si los datos con los cuales es entrenado el sistema tienen algún tipo de sesgo, esto podría conllevar a que reproduzca y profundice la discriminación a determinados grupos de la población; y que estos sean marginados o señalados como amenaza.

En esta misma línea, si un adversario logra modificar o corromper los datos con los cuales es entrenado el sistema de IA (utilizado en el proceso de producción de inteligencia estratégica), podría tener resultados desastrosos, puesto que esos datos conllevarían a realizar análisis erróneos y estos, a su vez, a tomar decisiones erróneas que incluso podrían llegar a perjudicar los intereses del Estado y de sus ciudadanos.

La implementación de la IA en la toma de decisiones requiere precaución para que no haya respuestas sesgadas o discriminación. Se debe evitar la recopilación de información por género, raza u otros factores que puedan influir en la toma de decisiones. Es crucial garantizar la precisión y confiabilidad de los sistemas de IA mediante el entrenamiento adecuado y la verificación constante de los algoritmos de aprendizaje automático. Si se entrenan con datos sesgados, pueden producir resultados inexactos o erróneos, profundizar el sesgo inicial de los datos e incluso exacerbar los prejuicios y la discriminación existentes, lo que puede tener graves consecuencias para la formulación de políticas públicas y los intereses estratégicos de la nación, e incluso puede llegar a erosionar la confianza en el Gobierno.

Asimismo, es de vital importancia reflexionar sobre cómo la inteligencia estratégica debe adaptarse a los avances que se realicen en la IA. Esto implica plantearse preguntas sobre cómo van a mutar las profesiones sobre la estructura jerárquica que se maneja en la inteligencia; y también revisar el ciclo de inteligencia que se aplica. Además, los

Revista de la Escuela Nacional de Inteligencia · Número 2 · Enero a junio de 2023 · pp. 151-171
ISSN 2953-4623 (en línea) y 0327-6961

avances en IA ofrecen la posibilidad de suplir la necesidad continua de los servicios de inteligencia de tener personal, lo que puede implicar una reducción en los costos de contratación y de formación de nuevos agentes.

Otro de los riesgos es romper el equilibrio entre el procesamiento y la protección que debe regular el tratamiento de los datos personales realizado para fines exclusivos de seguridad del Estado. Este equilibrio puede verse amenazado por la IA, la cual, con su autonomía, puede llegar a violentar la privacidad de las personas para alcanzar los objetivos que le sean trazados.

En este mismo sentido, si la IA alcanza niveles excesivos de recolección de datos personales e información en el ciberespacio, se puede crear un Estado de vigilancia, lo que puede erosionar la confianza de la población en las instituciones democráticas y crear un ambiente de miedo y desconfianza. Por ello, es necesario revisar el impacto en la privacidad de las personas y la ética en el uso de la IA.

En general, es importante regular y supervisar el uso de la IA en el mundo para garantizar que se respete la privacidad de las personas, la libertad de expresión y el tratamiento de los datos personales. La IA debe ser vista como un apoyo a la toma de decisiones humanas, con el fin de no dejar el control y garantizar que el criterio ético en la recolección y el análisis de información sea cumplido a cabalidad.

5. Conclusiones

La adopción de la tecnología de la IA no es opcional para la inteligencia estratégica, sino que su implementación es imperativa para todos los servicios, pues de lo contrario quedarán obsoletos en el nuevo mundo que esta plantea y no serán capaces de proteger los intereses de su nación. La pregunta, entonces, que deben formularse las agencias de inteligencia es cuándo, cómo y qué tan rápida será su implementación, y hasta qué punto se permitirá que esta tecnología participe en la producción de la información más importante de los Estados utilizada para la toma de decisiones estratégicas. Esto, teniendo en cuenta la incertidumbre sobre la precisión de los resultados generados por la IA y la posibilidad no descartada de que esta tecnología sea vulnerada, comprometida o manipulada por adversarios de la nación.

La IA aporta grandes beneficios y será determinante para el éxito de la inteligencia estratégica, ya que otorgará nuevas capacidades en diferentes áreas relevantes para la defensa y seguridad de la nación. Estos beneficios se verán reflejados en todas las fases del ciclo de inteligencia y mejorarán de forma significativa la planeación, la recolección, el procesamiento y análisis, y la difusión de inteligencia estratégica.

Además, la IA permitirá responder con éxito a ataques hostiles (físicos o en ciberespacio) mediante acciones autónomas con poca o ninguna supervisión humana, a la

Revista de la Escuela Nacional de Inteligencia · Número 2 · Enero a junio de 2023 · pp. 151-171
ISSN 2953-4623 (en línea) y 0327-6961

vez que puede proporcionar una ventaja crucial en la identificación de amenazas y en la toma de decisiones.

La colaboración entre humanos y máquinas seguirá siendo una máxima para el éxito de la inteligencia estratégica. La intervención humana garantiza que se tengan en cuenta las consideraciones éticas y de privacidad, ya que las máquinas probablemente no alcanzarán las habilidades de juicio al ser estas muy difíciles de replicar.

En cuanto al desarrollo, investigación e implementación de IA en Latinoamérica, es claro que existe un rezago frente a países líderes en el tema como los Estados Unidos y la República Popular China. En este sentido, se hace un llamado a la comunidad de inteligencia de los países latinoamericanos para que procuren generar alianzas que permitan que los servicios de inteligencia no se queden rezagados de esta nueva tecnología determinante para el éxito de sus labores.

En el futuro, se espera que la IA siga siendo una herramienta crítica para la inteligencia estratégica del Estado. La cantidad de datos que los países recopilan y analizan seguirá aumentando, y la IA será esencial para manejar esta creciente cantidad de información. Además, se espera que la IA se convierta en una herramienta aún más sofisticada y precisa para la identificación de patrones y tendencias. En esta línea, probablemente será utilizada también para la toma de decisiones en tiempo real, lo que puede ser crucial en situaciones de crisis.

Finalmente, es importante que se establezcan normas y regulaciones claras para el uso de la IA en la inteligencia estratégica del Estado. Esto incluye la necesidad de garantizar que el uso de la IA sea ético y transparente, y que se respeten los derechos humanos y la privacidad de las personas.

Bibliografía

Abraham, A. y Grosan, C. (2011). *Intelligent Systems: A Modern Approach (17)*.

Bellaby, R. (2012). What's the Harm? The Ethics of Intelligence Collection. *Intelligence and National Security, 27*(1), 93-117.

Bernhardt, D. (2003). *Competitive Intelligence. How to acquire and use corporate intelligence and counter-intelligence*. Pearson Education.

Brynjolfsson, E., Clark, J., Etchemendy, J., Fattorini, L., Ligett, K., Lyons, T., Manyika, J., Maslej, N., Niebles, J., Ngo, H., Parli, V., Perrault, R., Shoham, Y. y Wald, R. (2023). *The AI Index 2023 Annual Report*. Stanford University.

Clark, R. M. (2004). *Intelligence Analysis: A Target-Centric Approach*. CQ Press.

CNN. (2 septiembre de 2017). Este es el país que dominará al mundo, según Vladimir Putin. https://cnnespanol.cnn.com/2017/09/02/este-es-el-pais-que-dominara-al-mundo-segun-vladimir-putin/

CNN. (22 de abril de 2018). CIA agents in 'about 30 countries' being tracked by technology, top official says. https://edition.cnn.com/2018/04/22/politics/cia-technology-tracking/index.html

Coutinho, L. (2020). LGPD e inteligência: os limites no tratamento de dados pessoais coletados em fontes abertas. *Revista Brasileira de Inteligência*, (15). https://doi.org/10.58960/rbi.2020.15.183

Cowls, J., Floridi, L., Morley, J., Roberts, H., Taddeo, M. y Wang, V. (2021). El enfoque chino de la inteligencia artificial: un análisis de la política, la ética y la regulación. En L. Floridi (Ed.), *Ética, Gobernanza y Políticas en Inteligencia Artificial. Serie de estudios filosóficos, 144*.

Das, V., Hussain, M., Kostyuk, N. y Liang, F. (2018). Constructing a data driven society: China's social credit system as a state surveillance infrastructure. *Policy & Internet, 10*(4), 415-453.

Gallegos, C. (23 de enero de 2023). Alerta universitaria: ChatGPT aprueba un examen de maestría de una prestigiosa escuela de negocios. *El Economista*. https://www.eleconomista.es/tecnologia/noticias/12119475/01/23/Alerta-universitaria-ChatGPT-aprueba-un-examen-de-maestria-de-una-prestigiosa-escuela-de-negocios.html

Gates, Bill. (21 de marzo de 2023). The age of AI has begun. *Gates Notes*. www.gatesnotes.com/The-Age-of-AI-Has-Begun/

Hao, Y., Ihalage, A. A., Khan, A. N., Liu, B., Liu, Y. y Ma, Y. (2021). Deep learning framework for subject-independent emotion detection using wireless signals. *Plos One, 16*(2). https://doi.org/10.1371/journal.pone.0242946

Harris, D. y Markowitz, S. (2016). *Intelligence Analysis: A Target-Centric Approach* (5.a ed.). CQ Press.

Kent, S. (1949). *Strategic Intelligence for American World Policy*. Princeton University Press.

Marr, B. (8 de abril de 2019). 7 Amazing Examples Of Computer And Machine Vision In Practice. *Forbes*. https://www.forbes.com/sites/bernardmarr/2019/04/08/7-amazing-examples-of-computer-and-machine-vision-in-practice/?sh=3e4d8c041018

Miller, S. R. M. (2021). Truth-seeking and the principles of discrimination, necessity, proportionality and reciprocity in national security intelligence activity. En S. Miller, M. Regan y P. F. Walsh (Eds.), *National Security Intelligence and Ethics*. Taylor and Francis.

Murphy Kelly, S. (16 de marzo de 2023). 5 cosas asombrosas que GPT-4 puede hacer que ChatGPT no pudo. *CNN en Español*. https://cnnespanol.cnn.com/2023/03/16/5-cosas-que-hace-gpt4-chatgpt-no-pudo-trax/

Nilsson, N. (1998). *Artificial intelligence: A new synthesis*. Morgan Kaufmann Publishers.

Norvig, P. y Russell, S. (2010). *Artificial intelligence: A modern approach*. Pearson Education.

Rico Sesé, J. (13-14 de noviembre de 2019). *La inteligencia artificial y la creatividad* [Ponencia]. Conference Proceedings CIVAE 2019. 1st Interdisciplinary and Virtual Conference on Arts in Education, pp. 68-71. Disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=8091364

Romero, S. (2020). Inteligencia artificial como herramienta de estrategia y seguridad para defensa de los Estados. *Revista de la Escuela Superior de Guerra Naval, 16*(1), 51-70.

Sayler, K. M. (10 de noviembre de 2020). Artificial Intelligence and National Security. *Congressional Research Service Report*. https://crsreports.congress.gov/product/pdf/R/R45178/10

The New York Times. (26 de abril de 2021). The C.I.A.'s top technologist is uncomfortable with Facebook. Dawn Meyerriecks talks spy gear and why Hollywood and Silicon Valley play a critical role in national security. https://www.nytimes.com/2021/04/26/opinion/sway-kara-swisher-dawn-meyerriecks.html

Torres, L. C. (2017). Creatividad artificial. *Revista de Tecnología, 16*(2), 18-26.

Tortoise Media. (2021). The Global AI Index 2021. https://www.tortoisemedia.com/intelligence/global-ai/

Ying, S. (2020). Study on the Application of Artificial Intelligence Technology in the Public Security Field. IOP Conference Series: Earth and Environmental Science, 608.

Cómo citar este artículo
Salazar Vega, D. C. y Figueroa Medina, E. (2023). Desafíos de la inteligencia estratégica ante los avances de la inteligencia artificial. *Revista de la Escuela Nacional de Inteligencia*, (2), 151-171. https://doi.org/10.58752/1HNRLXNA.