Capítulo 9

Límites de la inteligencia artificial y la tecnología *big data* en el análisis de Inteligencia*

DOI: https://doi.org/10.25062/9786287602809.09

Jaime Andrés Naranjo Ardila
Jorge Luis Mejía Rosas
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: La inteligencia artificial y el *big data* proporcionan un entorno de enseñanza y aprendizaje para el proceso de información en el análisis de inteligencia. La tecnología configura nuevos escenarios en el campo geopolítico y de seguridad y defensa, con unas características que contribuyen a generar una serie de límites que serán analizados por las agencias de seguridad del Estado. En este sentido, es importante describir la evolución que ha tenido la inteligencia artificial, puesto que los avances de la ciencia y de la tecnología se encuentran progresando rápidamente. Esta tendencia es esencial para las personas que se encargan de procesar información, ya que, por su fácil acceso, es crucial para emplear lineamientos de protección legal de datos personales. En ese orden de ideas, los desafíos de la inteligencia artificial contribuyen a generar ámbitos de innovación en tendencias de protección legal de los datos personales y en el uso de aplicaciones.

Palabras clave: análisis; artificial; inteligencia; límites; tecnología.

* Este capítulo es resultado de investigación adscrito al proyecto *"Naturaleza de la guerra contemporánea. Retos y oportunidades de las Fuerzas Especiales y la Inteligencia"*, adscrito al Departamento Ejército de la Escuela Superior de Guerra, inscrito en la línea de investigación "Naturaleza de la guerra, terrorismo, nuevas amenazas", que forma parte del grupo de investigación Centro de Gravedad, con código COL0104976. Los puntos de vista pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

Jaime Andrés Naranjo Ardila
Teniente Coronel del Ejército Nacional de Colombia. Magíster en Seguridad y Defensa Nacionales, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Especialista en Conducción y Administración de Unidades Militares, y Especialista en Administración de Recursos Militares para la Defensa Nacional, Escuela de Armas y Servicios del Ejército Nacional. Diplomado en Liderazgo con Énfasis Administrativo y diplomado en Peritazgo Administrativo y Disciplinario. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia.
Contacto: **jaime.naranjoar@buzonejercito.mil.co**

Jorge Luis Mejía Rosas
Coronel (R) del Ejército Nacional de Colombia. Especialista en Inteligencia Militar, Escuela de Inteligencia y Contra Inteligencia "Brigadier General Ricardo Charry Solano". Especialista en Administración de Recursos Militares, Escuela de Armas y Servicios, y en Docencia Universitaria, Universidad Militar Nueva Granada. Profesional en Ciencias Militares y en Administración de Empresas, Escuela Militar de Cadetes "General José María Córdova", Colombia.
https://orcid.org/0000-0003-3233-4948 - Contacto: **jorge.mejia@esdeg.edu.co**

Citación APA: Naranjo Ardila, J. A., & Mejía Rosas, J. L. (2024). Límites de la inteligencia artificial y la tecnología *big data* en el análisis de Inteligencia. En L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Comandos: Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea* (pp. 209-229). Sello Editorial ESDEG. https://doi.org/10.25062/9786287602809.09

COMANDOS: RETOS DE LAS FUERZAS ESPECIALES E INTELIGENCIA EN LA GUERRA CONTEMPORÁNEA
ISBN impreso: 978-628-7602-79-3
ISBN digital: 978-628-7602-80-9
DOI: https://doi.org/10.25062/9786287602809

Colección Seguridad y Defensa
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2024

Introducción

Para nadie es un secreto que en los últimos diez años se ha producido un gran cambio tecnológico en hábitos, gustos y en cómo se adquieren las cosas o servicios. Como parte de estos avances, actualmente existen innovaciones tecnológicas que pueden ser aplicadas en el campo de la inteligencia militar, como la inteligencia artificial (IA), el internet de las cosas, la realidad virtual, la red de bloques, las app, el *e-commerce*, el *big data*, entre otras enfocadas en la necesidad de los clientes, pero que hasta ahora no se están aprovechando. En efecto, la IA optimiza los procesos de recolección de información generando un sistema integral de control de datos, el cual facilitará el desempeño organizacional y le permitirá a la Fuerza crear una serie de habilidades, acuerdos y compromisos en torno a la ciencia de la inteligencia militar.

El presente capítulo tiene el objetivo de analizar el empleo de la inteligencia artificial (IA) y la tecnología *big data* en la Inteligencia militar para el planeamiento en Operaciones Especiales (OO. EE.). En primer lugar, se examina el desarrollo tecnológico que afecta la Inteligencia militar y las Fuerzas Especiales (FF. EE.), teniendo en cuenta que la innovación facilita la recolección de datos de forma segura mediante un código criptográfico que hasta el día de hoy no ha podido ser vulnerado. En este sentido, el capítulo propone que es necesario definir un planeamiento que facilite la adopción de medidas prospectivas para no improvisar frente a una amenaza de alto riesgo. De esta manera, se considera que el uso del *big data* y la inteligencia artificial contribuye a prevenir, controlar y mitigar los impactos y también el respeto por la anonimización de los datos personales.

Este proceso debe incorporar "la minería de datos y la *big data*", pues si no se tienen en cuenta las variables y las expectativas de todas las partes interesadas con las que interactúa la organización, no podrá cumplir sus objetivos ni metas, de

allí que en esta fase sea muy importante realizar control y seguimiento para garantizar que el plan sea realista.

En segundo lugar, se relaciona la inteligencia artificial y la tecnológica del *big data* para la inteligencia humana en las OO. EE. Con base en el análisis, se sugiere que es necesario implementar procesos y procedimientos que ayuden a la organización a posicionarse de la mejor forma. Para cumplir este objetivo, la inteligencia artificial resulta una opción viable, ya que permite encadenar todos los procesos que son realizados de forma automatizada, establecer un modelo que genere resultados eficientes y, por lo tanto, mejorar el proceso de recolección de información. Esto permite identificar las características, costumbres, preferencias, procedimientos, comportamiento y desarrollo de las personas y las organizaciones.

Finalmente, se analiza el papel de la tecnología de *big data* para el mejoramiento continuo como tendencia de un entorno globalizado, para lo cual se sugiere analizar todo tipo de buenas prácticas gerenciales.

Antecedentes

Las primeras aplicaciones móviles datan de finales de los años 90, cuando ya estaban implícitas en los computadores. Un ejemplo claro fue la agenda en *Windows 95,* que empezó como una aplicación que enviaba señales de alerta, o los *arcade games* ("juegos de celular"), que fueron tendencia en esa época, cuyos productores encontraron un nicho de mercado (Bonami et al., 2020).

De acuerdo con Ahedo y Danvila (2014), la evolución de las aplicaciones continuó con los editores de *ringtone* ("tono de celular"), que efectuaban funciones muy básicas y su diseño era suficientemente escueto. A partir de este punto, el desarrollo de las apps se aceleró gracias a las innovaciones en tecnología, lo cual estuvo soportado por los grandes avances de los celulares, pues las compañías que los producían generaron prácticas de ventaja competitiva.

De hecho, comienza una revolución en la creación de las apps, los juegos, las noticias, el diseño, el arte, la fotografía y la medicina, todo en las manos de los usuarios gracias a los procesos acelerados de innovación de las aplicaciones móviles (Fernández, 2020). Simultáneamente, el internet creaba un sinnúmero de herramientas de muy alta calidad dirigidas hacia la innovación con el uso de las Tecnologías de la Información y las Comunicaciones (TIC), mediante las cuales garantizaba el acceso personalizado a los datos y, de esta manera, brindó al ciudadano la posibilidad de identificar las debilidades y las fortalezas de la gestión pública.

Esto fue resulta evidente en el manejo de la pandemia por coronavirus (Fernández, 2020), cuando se discutió públicamente que estas innovaciones podrían llegar a vulnerar las normas en materia del derecho al *habeas data*, ya que recolectan y centralizan la información de los usuarios por medio de la ubicación de sus datos personales. Aunque son utilizados con fines netamente estadísticos de salud, estos datos se encuentran centralizados para informar a las demás personas (Navarro, 2014).

Por lo tanto, si bien esta información puede ser empleada para verificarla con las centrales de información, también pueden servir para localizar a la persona en tiempo real con fines delictivos. Por lo tanto, como señala Daza (2020),

> es muy importante no simplificar, polarizar ni reducir la cuestión a una renuncia a la privacidad para mantener la vida o la salud, o para evitar los confinamientos y otras restricciones de nuestras libertades. Las lesiones de la privacidad, como el coronavirus, no se ven ni se sienten hasta que ya es tarde. Por ello, si se plantea el debate en estos términos maximalistas, nadie apostaría por la privacidad. (p. 12)

El aprendizaje es otro campo en el que la IA adquiere sentido, ya que en la actualidad existen aplicaciones que, por ejemplo, convierten los mapas en escenarios de tres dimensiones (3D) cuando se mira con un dispositivo móvil o una cámara web. Aunque estas aplicaciones responden a la necesidad de averiguar el estado de salud de las personas, identificar riesgos e incluir alarmas o estados de alerta, es claro que estos avances tecnológicos conducen a un escenario que trasciende el nivel de información, por cuanto despliegan funcionalidades con características invasivas (Orozco, 2003).

Evolución en la concepción y el planeamiento de escenarios de guerra o confrontaciones híbridas contemporáneas

Actualmente, la evolución de las confrontaciones en el sistema internacional ha hecho invisible al adversario debido al uso de las tecnologías, lo cual implica todo tipo de retos para las sociedades modernas. Esto resulta muy notorio en lo que se refiere al establecimiento de mecanismos de seguridad y defensa, así como de políticas públicas que puedan cumplir con los intereses nacionales, ya que ahora

existe una serie de riesgos a la tranquilidad y la convivencia armónica de los pueblos. La importancia de este tema resulta evidente cuando se tiene en cuenta la llegada de nuevos actores con capacidad para desestabilizar las instituciones con el ánimo de lograr sus intereses, amparados en el marco de la economía ilegal y por encima de los objetivos de un Estado (Valencia et al., 2019).

En ese contexto, la evolución de la tecnología ha permitido el avance de la IA, la cual ha obtenido resultados en diferentes campos de acción de la sociedad, pues ha incrementado la capacidad para tomar decisiones ante sucesos inesperados gracias a la información que consiguen y procesan las máquinas. Esto crea escenarios con alto riesgo para la existencia de la humanidad, pues países como Estados Unidos, Rusia y China han revolucionado su estrategia de seguridad nacional con los recursos que les brinda la IA para proteger sus intereses nacionales en tiempos de conflictos armados o tareas de mantenimiento de la paz.

Históricamente, los fenómenos de globalización fueron cambiando progresivamente los métodos para definir una estrategia de seguridad nacional, de manera que se apostó por instaurar áreas de crisis, normalización y estabilización, todas ellas con el propósito de contribuir con el establecimiento de la paz. En este contexto, la seguridad de los Estados fue evolucionando con el paso de los años y tuvo un gran salto con los atentados del 11 de septiembre de 2001 a las Torres Gemelas en Nueva York, pues este suceso evidenció que habían emergido nuevas amenazas a la seguridad global, las cuales tenían diferentes técnicas de actuar y atacar. Como resultado, las agencias de Inteligencia de los Estados cambiaron y se prepararon empleando la tecnología como medio para obtener sus resultados.

En efecto, se encuentra que los principales desarrollos de la IA se producen en los Estados que son potencias mundiales, tanto en sus políticas de seguridad y defensa, como en la materialización de sus planes estratégicos. No obstante, el hecho de que esta tecnología se emplee en escenarios muy diversos crea la posibilidad de que surjan serias amenazas, algunas de carácter tecnológico y otras de origen humano. Según los expertos, una de estas amenazas es que la IA se convierta en autosuficiente o superinteligente, de manera que supere las capacidades de los seres humanos, y la otra es que sea empleada con fines letales o perversos contra otros Estados o actores no estatales.

La autosuficiencia de la IA, es decir, cuando supera al hombre en todos sus aspectos inteligibles, ya ha sido contemplada por la ciencia y se ha denominado "la gran singularidad". Esta postura fue argumentada por Stephen Hawking, quien manifestó abiertamente que este tipo de tecnologías podría significar el fin de la

humanidad. Por su parte, Nick Bostrom (2016), catedrático de la Universidad de Oxford, considera que la IA puede reemplazar en cierta forma el trabajo intelectual de los seres humanos, por ejemplo, realizando mejores análisis. Por eso afirma que este tipo de tecnología debe tener valores humanos y actuar de forma coordinada con todos los actores de la sociedad para lograr buenos resultados; de lo contario, advierte Bostrom (2016), el escenario sería catastrófico e irreversible para la humanidad.

Desde una visión más moderada, el Dr. Ramón López, director de IA en España, manifiesta que una súper IA todavía se encuentra lejos de la realidad y, por lo tanto, la idea de que este tipo de tecnología podría dominar el mundo carece de fundamento científico, ya que para materializar la gran singularidad es necesario que se produzca la evolución tecnológica correspondiente (Pérez, 2023). Otros expertos señalan que si existiera una IA con mejor nivel intelectual, nunca podrá ser superior al del ser humano, pues no tiene una interacción similar con el entorno. No obstante, estas reflexiones hacen evidente que se debe analizar a fondo todo tipo de dilemas éticos, fundamentalmente respecto al uso de las armas autónomas (Valls, 2018).

Ahora bien, respecto a la IA utilizada para actividades criminales, Sonia Pacheco (citada por Rubio, 2018), directora del Business World Congress, señala que puede generar gran afectación por los riesgos a las seguridad y defensa de un Estado. En ese sentido, considera que se debe distinguir entre el mal uso de la IA "no intencionado" y el mal uso "con intencionalidad", como la utilización de drones con objetivos terroristas o manipular las contiendas electorales usando cuentas con algoritmos en redes sociales que facilitan la automatización de mensajes, denominadas *bots,* que realizan tareas repetitivas las 24 horas del día. Un ejemplo de este uso malintencionado de la IA es el ataque a bases militares en Siria por actores no estatales o la invención de armas autónomas que son letales (Rubio, 2018).

La inteligencia artificial, componente estratégico de defensa de un Estado

La IA es una tecnología que se puede considerar bien como un componente desequilibrante en el uso de las Fuerzas Militares, o bien como un instrumento disruptivo en todos los campos de acción de la sociedad, económico, industrial o social. La capacidad de carácter geoeconómico y geopolítico que genera esta tecnología afecta directamente el contexto estratégico internacional porque facilita la toma de

decisiones y la construcción de la estrategia de seguridad nacional, pues permite ponderar el mejor curso de acción mediante la evaluación de las variables más críticas. Aunque su empleo depende de las capacidades que tengan los Estados, actualmente es un mecanismo que han integrado grandes potencias como Estados Unidos, Rusia, entre otros.

Por lo tanto, la evolución de la IA es un componente vital en la seguridad nacional, el cual contribuye a generar políticas internas que tienen amplia relación con las consideraciones expuestas por la comunidad internacional. Esta tecnología goza de gran aceptación, a tal punto que en 2017 China estableció una política de Estado bastante ambiciosa con un programa tecnológico prospectivo (2030) para posicionarse como líder mundial en este campo, para lo cual orientó sus esfuerzos en las aplicaciones de IA. De esta manera, comenzó una carrera global por tener la hegemonía en este ámbito tecnológico, según señala un informe del Foro Económico Mundial publicado en 2018, el cual proyectó que la inversión en IA alcanzará los 127 mil millones de dólares en el año 2025.

En ese sentido, es importante analizar el concepto estratégico de la IA y el fundamento por el cual los Estados invierten grandes sumas de dinero. Específicamente, el contexto es que el mundo actual se encuentra en constante evolución, las grandes potencias quieren alcanzar el liderazgo tecnológico y militar, compitiendo por la jerarquización internacional y por proteger sus intereses nacionales.

En efecto, es importante para los Estados que emplean la IA conformar una política exterior multilateral debido a las diferentes amenazas que se ciernen en el entorno global, como son: el impacto que genera el cambio climático, las armas de destrucción masiva, las crisis financieras, las pandemias, entre otros. Como se observa, es evidente la necesidad de crear e implementar mecanismos de cooperación que puedan unir esfuerzos de manera multidimensional.

Del mismo modo, el uso de la IA resulta significativo para, por ejemplo, combatir las pandemias y la pobreza multidimensional, o consolidar los compromisos internacionales orientados a mejorar su infraestructura de transporte. Cuanto más desarrollo económico y social haya, aumentan la calidad de vida de las personas y la demanda por mejorar la protección ambiental, de manera que potencie su participación dentro de las dinámicas del comercio global.

En este contexto cabe señalar que la cadena de bloques optimiza los procesos de IA en la seguridad y defensa de un Estado, pues facilita un mayor manejo de la información en pro de los intereses nacionales. Además, contribuye a emplear metodologías contables en el desempeño organizacional que le permite generar

una serie de habilidades, acuerdos y compromisos en el uso de estos ámbitos tecnológicos, aunque siempre con limitaciones a la protección de datos, la reserva y la confidencialidad (Martínez, 2019).

A su vez, esta tendencia de la cadena de bloques facilita el almacenamiento de datos de forma segura mediante un código criptográfico que hasta el día de hoy no ha podido ser vulnerado. Los mecanismos para controlar dicha información está creciendo bajo un marco de globalización y de evolución tecnológica en torno a la aldea global, lo cual evidencia que las empresas enfrentan ciertos riesgos que pueden afectar su sostenibilidad y rentabilidad.

Medios empleados en el planeamiento y la ejecución de escenarios de guerra o confrontaciones híbridas contemporáneas

En el planeamiento se realizan todo tipo de metodologías que comprenden procedimientos sistemáticos, un paso a paso que lleva a tomar una serie de decisiones que pueden generar un resultado en el campo militar. Específicamente, los estados finales deseados se definen por medio de un estudio del ambiente operacional, de manera que están conexos entre sí para emplear las capacidades de las unidades militares, entre las cuales se encuentra la optimización de la IA para tomar una posición de ventaja relativa sobre el adversario y otras amenazas. Esas tareas se encuentran desde la acción decisiva y promueven unas maniobras ofensivas (Bonami & Dala, 2020).

Teniendo en cuenta los nuevos desafíos en seguridad y defensa existentes, la Fuerza Conjunta está llamada a realizar todo tipo de actividades mediante el empleo de la inteligencia artificial, en asociación con el desarrollo de operaciones militares, para crear una ventaja y una capacidad estratégica que le permita ser más eficaz frente a las amenazas actuales y las tendencias en seguridad global (Hueso, 2019).

Por lo tanto, el uso de tecnologías de IA no solo es importante para tener movimiento y maniobra, pues potencian la integración de la seguridad y defensa del país con la finalidad de lograr un solo esfuerzo en la consolidación de los territorios, sino también en las operaciones militares, las cuales buscan obtener una posición de ventaja relativa frente alguna amenaza que atente contra la vida y la dignidad de los colombianos (Bravo, 2010).

De esta manera, además, el empleo de la IA permite neutralizar las principales estructuras de los Grupos Armados Organizados (GAO) mediante reconocimientos aéreos para identificar las posiciones de las columnas móviles y con labores de Inteligencia (humanas y técnicas) sobre el enemigo. Esto hizo posible que entre 2018 y 2022 el Gobierno fuera efectivo en la disminución de actividades como el secuestro, los homicidios y todo tipo de hechos ilícitos. Esta política de Estado, como se convirtió, muestra la importancia de que las instituciones "ocupen" todas las regiones nacionales y contribuye al desempeño de la sociedad para erradicar las desigualdades sociales que enfrenta el país (Galindo, 2005).

En efecto, el planeamiento es la combinación continua y simultánea de las actividades de las Fuerzas Militares y en la doctrina constituye uno de los primeros componentes fundamentales de las capacidades. Esto simboliza la conversión de las nuevas estructuras organizacionales de la institución en procura de ejercer estrategias de transformación y renovación, la nueva visión, el despertar y la transformación prospectiva en el entrenamiento y fortalecimiento de las capacidades. En este sentido, las Operaciones Terrestres Unificadas (OTU) permiten obtener la iniciativa y una posición de ventaja frente a los múltiples generadores de violencia, con una serie de operaciones ofensivas y defensivas, así como trabajando la conjuntez desde un enfoque interinstitucional o internacional.

Los profesionales militares aplican el arte del movimiento y la maniobra mediante el entrenamiento y la táctica, contenidos en la intención del comandante, por medio de la elección entre opciones conectadas:

- Tipos de tareas ofensivas o defensivas que describen las maniobras y tareas tácticas de misión.
- Organización para el combate de fuerzas disponibles, para incluir la distribución de recursos limitados.
- Elección fundamental de las medidas de control.
- Tiempo (antes, durante y después) de la operación.
- Desafíos y retos que el comandante está dispuesto a asumir (Vigevano, 2021).

Este elemento es de vital importancia para fortalecer la cooperación entre Colombia y sus aliados, teniendo en cuenta que la Inteligencia estratégica y la Contrainteligencia de Estado son factores de vital importancia para la toma de decisiones. Además, se debe considerar que existen elementos externos que influyen directamente en la política exterior colombiana, por lo cual este factor contribuirá para el cumplimiento de los fines esenciales del Estado:

- Desde el carácter estratégico, se pueden fortalecer las relaciones de las agencias de Inteligencia de Colombia con sus aliados, desarrollando actividades de inteligencia estratégica y contrainteligencia para proteger los intereses nacionales, con el fin de generar mayor control frente a los crímenes transnacionales.
- Desde el carácter operacional, la inteligencia militar se puede fortalecer en sus capacidades y medios con el principal propósito de poder generar operaciones coordinadas que afecten directamente a las organizaciones armadas ilegales que delinquen en las zonas de frontera.

En ese orden de ideas, el ciclo de Inteligencia dentro de un contexto de guerra híbrida debe ser definido como el conjunto de habilidades y destrezas que, por medio del empleo de la IA, permiten estudiar los factores económicos, políticos y sociales. Estos componentes, que actúan de forma integral, potencian el poder de combate con la finalidad de obtener una ventaja militar e iniciativa para contrarrestar todo tipo de amenazas que atenten la soberanía de una política del Estado. Actualmente, la aplicación de todas las intervenciones se basa en una gestión de programas sensibles a los conflictos y con un enfoque transversal con los temas de equidad, además se presta especial atención a la creación de soluciones sostenibles y formas de intervención, una de las cuales es la Inteligencia militar involucrando la mayor participación posible.

Escenarios de confrontación híbrida aplicados a Colombia en el contexto de una confrontación hegemónica y regional

Actualmente, existe una carrera armamentística para obtener la hegemonía mundial, donde los protagonistas son Estados Unidos, China y Rusia. Estos Estados conocen la importancia que tiene mejorar sus sistemas de IA para materializar sus intereses nacionales, lo cual ha sido denominado por la comunidad académica como la *guerra fría de la inteligencia artificial.* Un ejemplo claro es China, que ha establecido dentro de sus planes de desarrollo una fuerte inversión de aproximadamente 150 mil millones de dólares en tecnología, de tal forma que realizan estrategias prospectivas que les permitan, en un futuro no lejano, ser líderes mundiales en IA y constituirse como el centro de la innovación global.

Sin duda, frente a las anteriores revoluciones económicas y sociales, el desarrollo de la IA, además de dinámica, es universal, en la medida en que garantiza conexiones simultáneas y permanentes que son la base de la llamada globalización, pues incide a escala global en las actividades económicas, comerciales, políticas y sociales, la acumulación de capital, la generación y la transmisión del conocimiento y la gestión de la información.

Del mismo modo, después de la Revolución Industrial y con la llegada de la producción en masa, la automatización y la robótica, la "industria 4.0" ya es considerada como la "Cuarta Revolución Industrial", debido a su potencial y beneficios relacionados con la integración, la innovación y la autonomía de los procesos. Los conceptos de industria 4.0 y manufactura inteligente son relativamente nuevos y contemplan la introducción de las tecnologías digitales en la industria de la fabricación. Es decir, la incorporación al ambiente de manufactura de tecnologías como el internet de las cosas, el cómputo móvil, la nube, el *big data*, las redes de sensores inalámbricos, los sistemas embebidos, los dispositivos móviles, entre otros (Valencia et al., 2019).

Sin embargo, existen objetivos que ayudan a mejorar los procesos de información con el empleo de las fuentes abiertas. Un claro ejemplo es que estas tecnologías propician situaciones en las que los individuos pueden desplegar su capacidad de colaboración, integrarse a grupos y hallar el espíritu de equipo para obtener un método de recolección de información valiosa dentro de grandes flujos de información. Como se evidencia, estas características tecnológicas permiten educar a largo plazo.

En este sentido, para que el proceso de la información en la IA sea integral se requiere una serie de especialidades –perfilamiento de identidades, análisis situacional sistémico, prospectiva, entre otras– muy particulares que ayudan a determinar una representación propia del ser humano, en la medida en que determinan características de unificación, consolidación, comunicación y actividades decisivas para que la conjunción entre la IA y la inteligencia se lleve a cabo de manera controlada. En este aspecto es en el cual la cadena de bloques contribuye a que la información digital sea distribuida, pero no copiada, lo cual se puede explicar con un ejemplo claro: una hoja de cálculo que está duplicada miles de veces a través de una red de computadoras. Luego esa misma red está diseñada para actualizar regularmente esta hoja de cálculo y con ello se produce la cadena de bloques (Palomo-Zurdo, 2018, pp. 11-23).

Actualmente, en el entorno cibernético existe una gran variedad de programas de recolección de información, no solo académica sino también de datos precisos en la función pública de un Estado. Por consiguiente, hay programas que se basan en organizar la información de personas según la empresa en donde trabajan, la ubicación de su domicilio, la afinidad en los intereses o gustos, entre otros aspectos relevantes para recoger datos importantes (Navarro, 2014). Algunos de los programas de fuentes abiertas más utilizados son:

- *Shodan:* un investigador que localiza computadoras, webcams, impresoras y distintos dispositivos electrónicos.
- *Namechk:* demuestra si un nombre de usuario está disponible en más de 150 servicios *online*.
- *Tineye*: es un explorador que parte de una fotografía y muestra en qué sitios web se encuentra (Navarro, 2014).
- *Pipl:* explorador de personas que las relaciona con distintas redes sociales y vínculos en internet.
- *Domaintools:* es un servicio que permite identificar, monitorear, buscar y analizar un nombre de dominio.
- *Tagboard:* permite analizar distintos *hashtags* o etiquetas de Twitter (ahora X).
- *Twopcharts:* es un instrumento que analiza todo lo que se publica en Twitter, admite conocer los *likes,* el cronograma e historial de publicaciones, listas y contenido relevante.
- *Foca:* es un programa que permite extraer y analizar los metadatos a distintos tipos de documentos (Arcos, 2015). Al conocer los metadatos, se puede saber quién los creó o modificó, el tipo de software que lo generó y la distinta información relacionada con un archivo (Rosales, 2005).
- *Metapicz:* permite extraer los metadatos a fotografías y con esto conocer distinto tipo de información, como qué cámara, software, fechas y teléfono fueron utilizados.

En ese sentido, la realidad es que las organizaciones no pueden permitirse esperar tanto tiempo en una era donde las intrusiones de ciberseguridad ocurren en instantes, pues la seguridad de una organización depende de una rápida identificación y acciones de respuesta. Por ello se plantea este interrogante: ¿Cómo puede un país como Inglaterra, con procesos sólidos de seguridad de la información, mejorar las capacidades para identificar "adversarios avanzados" en los sistemas y

red? La respuesta se evidencia en que, últimamente, las organizaciones han intentado generar todo tipo de procesos de forma proactiva, y a la vez, han optimizado sus estructuras e instituciones cíber y de IA. (Chipuxi & Paucar, 2020).

El papel de las Fuerzas Especiales con el uso de la inteligencia artificial como herramienta de estrategia

El proceso de automatización y monitoreo por medio de sensores tiene una función muy significativa y necesaria para el soldado de las FF. EE. en el ambiente operacional actual. La IA cada vez toma más fuerza para extraer todo tipo de información meteorológica, sobre el estado físico y de salud del personal, así como de las capacidades de un soldado en tiempo real para tomar las mejores decisiones. Además, con respecto al adversario, permite conocer su armamento, identificar sus estrategias y analizar sus cursos de acción para atacar o defender con base en una serie de patrones suministrados por los grandes servidores, entre otros aspectos de suma relevancia.

Por lo tanto, para desarrollar el máximo potencial de la IA es fundamental la interconexión, es decir, el intercambio de información constante entre varios sistemas para que cada uno pueda reaccionar ante una posible amenaza. Sin embargo, para eso es evidente que los protocolos de acceso a este tipo de datos deben ser robustos, de forma que no exista ningún tipo de pérdida y para evitar intromisiones enemigas.

A su vez, la IA facilita la toma de decisiones gracias a que hace posible ponerle sensores al soldado para conocer su estado físico y emocional, a los vehículos y a los sistemas, tomar aerofotografías, así como tener audio y video del ambiente operacional, lo cual proporciona una gran cantidad de información valiosa. Generalmente, el noventa por ciento de las operaciones especiales (OO. EE.) consiste en planear y establecer las estrategias, los puntos de control, la ubicación del enemigo, entre otros aspectos de suma importancia. De acuerdo con el General Clarke, Comandante del Comando de Operaciones Especiales de los Estados Unidos, la mayoría de los líderes militares, específicamente los que agrupan las FF. EE., concentran la mayor parte de su tiempo en el planeamiento (Barceló, 2001).

Por ende, los ejércitos modernos con FF. EE. deben instalar nuevas estructuras organizacionales que contengan tecnología IA para escanear todo tipo de

computadoras y teléfonos celulares; recopilar y contrarrestar los mensajes que deja el adversario en las redes sociales y sus tendencias; analizar de forma detallada la situación y los intereses u objetivos del enemigo, y brindar un centro de operaciones para contrarrestar todo tipo de fanatismo y extremismo violento que quiera desestabilizar los entes gubernamentales (Palomo-Zurdo, 2018).

A su vez, la IA debe ayudar a detectar las amenazas electromagnéticas. Por ejemplo, los drones diseñados con esta tecnología y aprendizaje autónomo tienen la posibilidad de seleccionar los objetivos y realizar una acción directa de fuego. Estas operaciones deben estar bajo la supervisión de un asesor jurídico operacional para tomar la mejor decisión en ámbitos legales, siempre protegiendo la integridad de los encargados de hacer cumplir la ley. En este sentido, el control humano sobre este tipo de máquinas es esencial para garantizar la protección humanitaria y un control legal efectivo.

Al respecto, cabe señalar que el Departamento de Defensa de los Estados Unidos, en la Directiva N.º 3000.09, del 12 de noviembre de 2012, define las armas autónomas como

> […] un sistema que, una vez activado, puede seleccionar y enfrentarse a objetivos sin la intervención de un operador humano. Esto incluye los sistemas de armas autónomos supervisados por humanos que están diseñados para permitir a los operadores anular el sistema automático, pero pueden seleccionar y atacar objetivos sin mayor intervención humana después de su activación. (Departamento de Defensa de Estados Unidos, 2012, p. 13)

En ese orden de ideas, los sistemas de armas autónomos sin control humano es un instrumento que selecciona y ataca objetivos de acuerdo con criterios que han establecido los ingenieros de programación y con unas reglas operacionales, pero no pueden ser detenidos por la intervención humana después de que se ha lanzado el ataque. Cabe señalar que actualmente existen más de 380 armas semiautónomas que fueron desarrolladas por Israel, China, Estados Unidos y otros países (Sossa & Reyes, 2021).

Aunque no han sido empleadas en conflictos armados, se espera que en un futuro no muy lejano se puedan utilizar con el desarrollo de la robótica y la IA, para lo cual los países desarrollados, especialmente las potencias, destinan importantes recursos financieros al campo militar, de manera que la sustitución de soldados por tecnología no parece un escenario lejano (Acosta, 2020).

Ahora bien, todo sistema automático de armas no es necesariamente un sistema totalmente autónomo, ya que la intervención humana en la programación debe respetar todo tipo de parámetros exigidos por la ley, en la medida que requiere el uso de un operador. Actualmente, muchos armamentos militares poseen grandes niveles de automatización y tienen la capacidad de ser semiautomáticos, por ejemplo los drones, que pueden realizar actividades de forma automática, como despegar y aterrizar, sin la necesidad de que sea dirigido por un ser humano gracias a las rutas que se programan con el Global Position System (GPS).

En el caso de Estados Unidos, gran parte del presupuesto que destina a la defensa lo enfoca en desarrollar IA, lo cual le ha permitido tener una ventaja significativa respecto a China, sus principal competidor. Específicamente, estas tecnologías se relacionan con los siguientes campos:

- *Operaciones no tripuladas:* incluye los sistemas aéreos, terrestres o marinos tanto de superficie, como de inmersión con sistemas no tripulados y cada vez más autónomos.
- *Operaciones navales y aéreas a grandes distancias:* mediante bases expedicionarias flotantes o a través de aviones cisterna no tripulados que permitan aumentar significativamente el radio de acción de los aparatos de las Fuerzas de los Estados Unidos sin depender de aliados poco fiables (Vigevano, 2021).
- *Operaciones no-observables:* comprende las tecnologías furtivas que van mucho más allá de la "invisibilidad" al radar. Aspectos como la composición del material, la pintura, las emisiones infrarrojas y muchos otros factores complican la invisibilidad a niveles insospechados (Gutiérrez, 2014).
- *Guerra submarina:* es otro de los campos dominados por los Estados Unidos, pero China está construyendo submarinos no tripulados que serían capaces de llevar a cabo ataques de estilo kamikaze contra buques enemigos.
- *Ingeniería e integración de sistemas:* es la clave de todo el edificio militar estadounidense. Consiste en un sistema de sistemas, centrado en nuevos niveles de cooperación interarmas dentro de cada ejército e interejércitos dentro del conjunto de sus fuerzas armadas, que permite un mayor control sobre el campo de batalla.

Por lo tanto, es significativo que muchos países hayan creado todo tipo de marcos jurídicos para regular la protección de datos personales, ya que con el empleo de la IA y la disponibilidad de *big data* existe el riesgo de que se vulnere la información del titular de los datos, por ejemplo la suplantación o la creación de perfiles exactos para generar todo tipo de extorsiones; para fines políticos ilegales

o lo que se denomina *guerra cognitiva,* es decir, hacerles crear a las masas una serie de eventos catastróficos por las decisiones de sus gobernantes sin ningún tipo de criterio u objetividad.

En resumen, la estrategia de los Estados Unidos se enfoca en sobrepasar los avances chinos con la finalidad de salvaguardar a los combatientes humanos, para lo cual desarrolla sistemas aéreos, navales y terrestres no tripulados controlados a distancia e incluso autónomos que tengan la capacidad del factor sorpresa y puedan atacar en cualquier lugar y momento a partir del desarrollo de una red global de observación y ataque (Acosta et al., 2020).

En ese orden de ideas, los nuevos escenarios tecnológicos han demostrado que la protección a la vida privada y a los datos personales pueden ser vulnerados de diferentes formas. Esto no afecta solamente a un país, sino también a millones de personas en todo el mundo, pues traspasa los límites fronterizos, como sucedió recientemente en el campo geopolítico electoral con Cambridge Analytica. Esta compañía se especializa en aplicar test a una gran cantidad de personas con el interés de enviar mensajes personalizados para influir sus gustos en el ámbito comercial y electoral, de manera que los ciudadanos consuman determinados productos u orienten su intención de voto a favor de un candidato. El caso más emblemático sucedió en las elecciones presidenciales de los Estados Unidos en las que fue elegido Donald Trump (Hill & Dance, 2020). Estos eventos señalan la necesidad de establecer una serie de límites que deben ser analizados por las agencias de seguridad del Estado.

Ahora bien, las tecnologías de IA son un recurso más a disposición del personal encargado de analizar y procesar la información, el cual facilita la creación colectiva de conocimiento por su fácil acceso. Sin embargo, es importante establecer lineamientos para proteger legalmente los datos personales para que los resultados de estos análisis no caigan en manos criminales o de corporaciones que los vulneren flagrantemente para intereses electorales o comerciales. En ese sentido, la IA y el *big data* pueden proporcionar un entorno de enseñanza y aprendizaje para el análisis de la información que se realiza en los procesos de inteligencia.

En definitiva, los nuevos retos y desafíos de la IA contribuyen a generar ámbitos de innovación para crear todo tipo de tendencias. En el campo militar, la IA y el *big data* permiten enlazar las bases de datos de información de los usuarios, con el fin de analizar y determinar la solución o acción correctiva entre realizar seguimiento entre lo planeado vs lo ejecutado para asegurar el cumplimiento de los objetivos. Por estas razones, cada día cobra mayor fuerza la necesidad de establecer lineamientos para la protección legal de los datos personales en el uso de aplicaciones.

Conclusiones

La IA y la tecnología *big data* en el análisis de la información son conceptos determinantes en el proceso de Inteligencia. Esto se debe tener en cuenta en los diferentes niveles del planeamiento estratégico, pues el empleo de estas capacidades puede afectar el ambiente operacional y la toma de decisiones, en especial el planeamiento de la gran estrategia. De igual forma, el uso de IA y *big data* hace que las capacidades de Inteligencia se especialicen y actualicen cada vez más para hacer análisis lo más aproximado a la realidad, en la medida en que permiten formular escenarios de futuro más concretos frente a este nuevo desafío.

Del mismo modo, es importante determinar las variables y expectativas que tienen todas las partes con las que se interactúa para establecer su veracidad y credibilidad, de manera que sea posible concretar los objetivos y evaluar cuáles metas tienen una mayor posibilidad de ser cumplidas. Por lo anterior, es necesario desarrollar más sistemas efectivos de control y seguimiento para facilitar que el planeamiento se ajuste mejor a la realidad.

Dado que el desarrollo de la innovación y la tecnología, la IA y el *big data* pueden tener propósitos positivos o negativos, existe la posibilidad de que sean usados para generar ventajas que permitan explotar situaciones favorables ajustadas a la verdad o al engaño. En ese orden de ideas, la utilización de la IA y la tecnología *big data* en el planeamiento y la ejecución de escenarios de guerra o confrontaciones híbridas contemporáneas tienen una importancia determinante en la toma de decisiones, ya que se realizan como un conjunto de tareas y métodos conexos entre sí que comprometen el empleo de las Fuerzas y diferentes campos del poder para tomar una posición de ventaja relativa sobre el adversario, las amenazas y los factores de inestabilidad.

En este sentido, la Inteligencia militar se fortalece cuando incrementa sus capacidades y medios con el propósito de generar más inteligencia. Al realizar un mejor proceso de análisis con la ayuda de estas herramientas, los tomadores de decisiones pueden planear mejor operaciones coordinadas que faciliten el cumplimiento de la misión y el estado final deseado en los diferentes teatros o áreas de operaciones internas y externas.

Por esta razón se debe estar al tanto de la revolución que generan estas tecnologías, pues si se usan, por ejemplo, para desarrollar una IA que muestre el centro de gravedad del adversario, puede multiplicar la ventaja, hacer que las decisiones sobre la ejecución de las operaciones sea más eficiente y reducir al mínimo posible

las acciones del recurso humano, pero haciéndolas más letales. Asimismo, las tecnologías armamentistas, por más desarrolladas que sean, se vuelven vulnerables si se logra impactar con audacia las variables que constituyen las fortalezas de un Estado, de forma que se transformen en una desventaja en el área de injerencia o en su misma área.

Actualmente, el mundo está apuntando a los desarrollos tecnológicos de todo tipo, se ha ido transformando a través de las crisis y, por lo tanto, ha tenido que innovar para supervivir, lo cual hace necesario, para bien o para mal, cambiar el pensamiento porque el mundo real está pasando al virtual. Desde el punto de vista estratégico, la IA y la tecnología *big data* fortalecerán las relaciones de las agencias de Inteligencia, de manera que desarrollarán tareas de inteligencia estratégica y contrainteligencia para neutralizar las amenazas comunes y proteger los intereses nacionales, con el fin de generar mayor control. En cuanto al carácter operacional, la Inteligencia militar debe desarrollar acuerdos para fortalecer sus capacidades y medios, con el propósito de generar operaciones coordinadas que afecten directamente a las organizaciones armadas ilegales que delinquen en el territorio nacional.

No obstante, se debe indicar que si no se establece algún tipo de regulación jurídica para usar y desarrollar la IA, se puede abrir una peligrosa puerta a una serie de actividades criminales y a graves vulneraciones a los Derechos Humanos. En este contexto, se debe recordar la distinción entre un mal uso de la IA "no intencionado" y el mal uso "con intencionalidad", por ejemplo con fines terroristas, lo cual representa un riesgo a la seguridad y la defensa nacionales (Romero, 2019). Por lo tanto, para limitar estas amenazas es fundamental establecer un marco jurídico internacional y vinculante que regule esta tecnología.

En el contexto actual de guerra híbrida, emplear la IA en el estudio de los factores económicos, políticos y sociales que potencian directamente el poder de combate, permitirá realizar de forma integral las tareas, obtener una ventaja militar y, de esta manera, ganar la iniciativa para neutralizar todo tipo de amenazas que atenten contra la soberanía y las políticas de Estado. En ese sentido, contar con estas herramientas permite tener un enfoque transversal en el desarrollo de las operaciones que preste especial atención a la participación de la Inteligencia militar.

Finalmente, la IA y el big data son instrumentos que siempre deberán depender del análisis y el control de una persona, quien debe determinar qué sirve y qué no en el planeamiento. Por lo tanto, también es fundamental que cuente con un marco jurídico que lo regule y con la asesoría adecuada para blindar todas las decisiones que tome cuando incorpore dichas tecnologías.

Referencias

Acosta, A., Aguilar-Esteva, V., Carreño, R., Patiño, M., Patiño, J., & Martínez, M. (2020). Nuevas tecnologías como factor de cambio ante los retos de la inteligencia artificial y la sociedad del conocimiento. *Revista Espacios, 41*(05), 25-32. https://tinyurl.com/35dm93jd

Ahedo Ruiz, J., & Danvila del Valle, I. (2014). Las nuevas tecnologías como herramientas que facilitan la educación. En J. Días-Cuesta (Ed.), *Estrategias innovadoras para la docencia dialógica y virtual* (pp. 25-40). ACCI.

Arcos, R. (2015). Reservas de inteligencia: Una comunidad ampliada de inteligencia. *Inteligencia y Seguridad,* (8), 11-38. https://tinyurl.com/yc77ra2d

Barceló, M. (2001). A.I. (inteligencia artificial). *Byte España,* (78), 98-99. https://tinyurl.com/32x36khf

Bonami, P., Piazentini, L., & Dala-Possa, A. (2020). Educación, big data e inteligencia artificial: Metodologías mixtas en plataformas digitales. *Comunicar, 65*(25), 43-52. https://doi.org/10.3916/C65-2020-04

Bostrom, N. (2016). *Superinteligencia: Caminos, peligros, estrategias.* Teell.

Bravo, G. (2010). El proceso de inteligencia, vigilancia, adquisición de blancos y reconocimiento. *Revismar,* (1), 58-64. https://tinyurl.com/3w85djeu

Chipuxi, V., & Paucar, J. (2020). *Propuesta de un modelo de cadena de suministro basado en tecnología Blockchain* [Tesis de pregrado, Universidad Central del Ecuador]. Repositorio UCE. https://tinyurl.com/yc6t2h4b

Daza, M. (2020). *Grado de conocimiento y nivel de implementación de la tecnología Blockchain en empresas colombianas* [Tesis de maestría, Pontificia Universidad Javeriana]. Repositorio PUJ. https://tinyurl.com/bdv3w9ys

Departamento de Defensa de Estados Unidos. (2012). DOD Directive 3000.09, "Autonomy in Weapon System". https://tinyurl.com/466nkb9b

Fernández, M. (2020). *Tecnología Blockchain en la logística portuaria* [Tesis de pregrado, Universidad de Cantabria]. Repositorio UNICAN. https://tinyurl.com/vhh4ztb3

Galindo, C. (2005). De la seguridad nacional a la seguridad democrática: Nuevos problemas, viejos esquemas. *Estudios Socio-Jurídicos,* (7), 496-543. https://tinyurl.com/2vh6a55c

Gutiérrez Abarzúa, H. (2014). El concepto ISTAR: ¿Una herramienta válida para la función de inteligencia de las Fuerzas Militares del siglo XXI? *Revista Fuerzas Armadas,* (230), 55-63. https://doi.org/10.25062/0120-0631.859

Hill, K., & Dance, G. (2020, 10 de febrero). Una aplicación de reconocimiento facial ha identificado a víctimas de abuso infantil. https://tinyurl.com/2m3tj3yd

Hueso, L. (2019). Riesgos e impactos del big data, la inteligencia artificial y la robótica: Enfoques, modelos y principios de la respuesta del derecho. *Revista General de Derecho Administrativo,* (50), 1-37.

Martínez Devia, A. (2019). La inteligencia artificial, el big data y la era digital: ¿Una amenaza para los datos personales? *Revista La Propiedad Inmaterial,* (27), 5-23. https://doi.org/10.18601/16571959.n27.01

Ministerio de Tecnologías de la Información y Comunicaciones. (2016). Investigación, desarrollo e innovación. *Ciberseguridad,* 10-12. https://tinyurl.com/5xkx5k6b

Navarro Bonilla, D. (2014). El ciclo de inteligencia y sus límites: Producción de información. *Cuadernos Constitucionales de la Cátedra Fadrique Furió Ceriol,* (48), 51-65. https://tinyurl.com/58yw8ncj

Orozco, L. E. (2003). La calidad de la universidad: Más allá de toda ambigüedad. https://tinyurl.com/9rsx47tj

Palomo-Zurdo, R. J. (2018). Blockchain: La descentralización del poder y su aplicación en la defensa. *Boletín IEEE,* (10), 885-904. https://tinyurl.com/2s43yc2y

Pashchuk, Y. (2013). *Medios de implementación de Instar en el sistema de Inteligencia de las Fuerzas de Ucrania.* Universidad Nacional de la Fuerza Aérea (KNAFU). https://tinyurl.com/y5d6ujv8

Pérez, J. (2023). Ramón López de Mántaras, experto en inteligencia artificial: "La IA sola no resolverá absolutamente nada. Serán los humanos". *Diario El País,* https://tinyurl.com/52vwc9m2

Romero, S. (2019). Inteligencia artificial como herramienta de estrategia y seguridad para defensa de los Estados. *Revista de la Escuela Superior de Guerra Naval del Perú ESUP, 16*(1). https://tinyurl.com/56a4vwah

Rosales Pardo, I. R. (2005). La inteligencia en los procesos de toma de decisiones en la seguridad y defensa. *Cuadernos de Estrategia,* (130), 39-64. https://tinyurl.com/2u9yczne

Rubio, I. (2018, 15 de noviembre). Necesitamos la inteligencia artificial para sobrevivir como especie. https://tinyurl.com/4yy47rz2

Sarda, J. M. (2016, 22 de septiembre). *En la inteligencia de un Estado se pueden mostrar varios tipos de amenazas a las estructuras organizacionales del mismo que pueden afectar los procesos de información. Toma de decisiones y manejo de amenazas.* Universidad de Valencia.

Sossa Azuela, H., & Reyes Cortés, F. (2021). *Inteligencia artificial aplicada a robótica y automatización.* Marcombo; Alfaomega.

Valencia Bermúdez, M. P., Puerta Bohada, J. S., Collazos Ballén, N., Urrea, D., & Cañas C. (2019). Influencia de la cuarta revolución industrial en Colombia. *Punto de Vista, 10*(16), 1-18 https://doi.org/10.15765/pdv.v11i16.1419

Valls, M. (2018). La inteligencia artificial y su encaje en las estrategias de seguridad nacional. *Boletín IEEE*, (12), 472-485. https://tinyurl.com/4y38fw4c

Vigevano, M. (2021). Inteligencia artificial aplicable a los conflictos armados: Límites jurídicos y éticos. *Arbor, 197*(800), Artículo e600. https://tinyurl.com/s73rua84