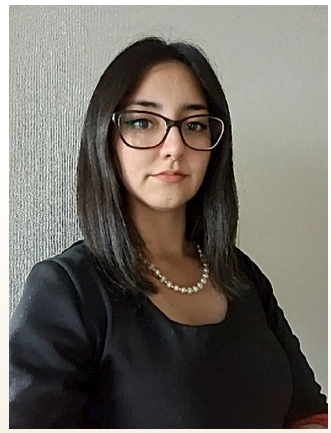
Escenarios Actuales, año 27, noviembre, Nº 3 (2022), pp. 143-155
Centro de Estudios e Investigaciones Militares
Santiago de Chile
ISSN 0717-6805

Inteligencia Artificial: el campo de la innovación en defensa



Denisse Olguín Arias[1]

Resumen

El campo tecnológico considerado más esencial en las estrategias de defensa del siglo XXI es la inteligencia artificial (IA). Aquellos países que logren dominar esta tecnología, marcarán un enorme cambio en la geopolítica de este siglo. Sin embargo, este dominio implicará una brecha entre los países que tengan estas capacidades y aquellos que no dispongan de las mismas. Esto conducirá a una nueva forma de colonización tecnológica que aumentará las dependencias de unos con otros. Por otra parte, los riesgos que puedan surgir de esta nueva tecnología van más allá de la ética; lo que conlleva a que países más avanzados podrán controlar las tecnologías de los países menos avanzados. Esto aumenta las fragilidades de países latinoamericanos, que se encuentran en este campo muy por detrás de Estados Unidos y de China.

Abstract

The technological field considered most essential in the defense strategies of the 21st century is artificial intelligence (AI). Those countries that manage to master this technology will mark a huge change in the geopolitics of this century. However, this dominance will imply a gap between countries that have these capabilities and those that do not. This will lead to a new form of technological colonization that will increase dependencies on each other. On the other hand, the risks that may arise from this new technology go beyond ethics; which means that more advanced countries will be able to control the technologies of less advanced countries. This increases the weaknesses of Latin American countries, which are far behind the United States and China in this field.

Palabras clave
Inteligencia artificial (IA)
Militar defensa geopolítica
Estados Unidos
China
Europa
Latinoamérica

Keywords
Artificial intelligence (AI)
Military defense geopolitics
United States
China
Europe
Latin America

1 Ingeniera en Automatización y Robótica en la Universidad Andrés Bello, Máster en Ingeniería Aeronáutica en la Universidad Técnica Federico Santa María. Investigadora de Electrónica y TIC's, Centro de Estudios en Ciencia y Tecnología (CECTAP), Academia Politécnica Militar (ACAPOMIL).

Introducción

La inteligencia artificial (IA) es un área del campo tecnológico que tiene un gran impacto en aplicaciones tanto civiles como militares de variados países. Se puede decir que este desarrollo se debe a cuatro elementos fundamentales:

1. El enorme volumen de datos disponibles.
2. Posibilidad de manipulación con las tecnologías de Big Data.
3. Desarrollo de algoritmos cada vez más robustos, con la capacidad de autogenerar nuevos algoritmos; semejante a la reproducción celular en los seres vivos.
4. La gran capacidad de procesamiento de la información que ofrecen los actuales sistemas informáticos, gestionando con gran rapidez decenas de miles de millones de datos en tamaños que alcanzan los zetabytes.[2]

Si bien ya existen sistemas que se encuentran en operación, están en marcha nuevos desarrollos basados en el potencial que ofrece la IA, tales como la recopilación y análisis de la información logística, de actividades cibernéticas, de vehículos semiautónomos y autónomos, entre otros y, en el campo de la defensa, existen variadas aplicaciones, donde la guerra, tal como se conoce, sería conducida prácticamente sin el elemento humano en los campos de batalla.

La IA ya ha sido utilizada en actividades militares de Estados Unidos en Irak, en Siria y en otros lugares, y es aplicada casi a diario en misiones de información, muchas de las cuales son desconocidas, ya que tanto los que las ejercen a modo de ataque, como aquellos que las reciben y se aprestan a su defensa, prefieren mantenerlas en la más absoluta reserva. A lo que se añade la aplicación de la IA en el dominio del espacio exterior: en noviembre del año 2021, Rusia destruyó uno de sus satélites mediante un misil antisatélite[3] de ascenso directo. En este contexto, es importante destacar que las tecnologías de IA aplicadas al campo militar son un enorme desafío para aquellos países que no dispongan de estas nuevas tecnologías, implicando una enorme brecha entre aquellos países que dispongan de nuevos sistemas basados en IA de aquellos que no lo posean.

Hoy en día los estudios desarrollados más avanzados en IA se presentan en el área académica (a nivel universitario) y en el mundo empresarial, de manera que las fuerzas armadas deberán apoyarse en el sector privado y académico; considerando que, si estos no están muy avanzados, las fuerzas armadas podrían encontrarse con la imposibilidad de tener las capacidades necesarias por la dificultad de adquirir tales tecnologías en los mercados internacionales, debido al cierre de estos por tratarse de productos de alto valor estratégico para la seguridad. Por tanto, la dificultad de adquisición de sistemas de defensa basados en IA determinará la capacidad de responder a los nuevos desafíos de seguridad que se presentarán en el siglo XXI, sin contar la necesidad de dotar de personal a las fuerzas armadas que sea capaz de comprender, analizar y manipular esta nueva tecnología, considerando, además, que podría no estar disponible de forma inmediata para su utilización en el tiempo y en la forma requerida

2 Un zetabyte consiste en 1021 bytes, siendo un byte la unidad de computación más pequeña, que se compone a su vez de 8 bits.

3 AMOS, Jonathan. (16 noviembre 2021). Russian anti-satellite missile test draws condemnation. BBC News: https://www.bbc.com/news/science-environment-59299101 (consultado el 22 de agosto de 2022).

por los acontecimientos, en un contexto geopolítico mundial altamente cambiante.

Todo este panorama es nuevo en los sistemas de defensa en países de Latinoamérica, que requieren desarrollar una estrategia integrada para poner en marcha nuevos sistemas basados en IA, pero con un trabajo conjunto de la industria privada, las universidades y las propias fuerzas armadas. Además, deberá dotarse de los mecanismos de confidencialidad y de protección de la información con la ayuda que la propia inteligencia militar pueda brindar en este sentido.

Dada la importancia de la IA en los sistemas militares, este artículo presenta un panorama inicial que permita la reflexión sobre la necesidad de proporcionar IA a los sistemas de defensa, tanto para soportar las necesidades actuales como las futuras. Aunque la IA puede aportar ventajas en el contexto de la defensa, también abre la posibilidad de importantes retos; pues dotar a las misiones de la posibilidad de operaciones autónomas, podría igualmente tener resultados imprevistos. Es por esto que se presenta la necesidad de desarrollar toda una nueva capacidad estratégica que permita una manipulación segura de esta nueva tecnología en los planes militares, sin excluir, a su vez, las consideraciones éticas y legislativas, así como la formación de mandos y de equipos especializados en el área.

Tecnologías alrededor de la IA

La mayoría de las personas suele decir que "*lo importante no es lo que se conoce, sino lo que se hace con lo que se conoce*". Una frase muy acertada cuando se habla en el ámbito de la estrategia militar. Con esto, se puede deducir que las tecnologías que se encuentran en sistemas basados en IA deben facilitar como primera función el análisis de complejas situaciones para simplificar y favorecer la toma de decisiones, permitiendo la construcción de escenarios futuros.

Una IA presenta variadas formas y técnicas informáticas para que un sistema pueda "aprender" sin la necesidad de ser explícitamente programadas para tal función: se trata de algoritmos trabajados informáticamente que muestran diversas denominaciones, por ejemplo, los utilizados en teoría de juegos (aprendizaje por refuerzo o *reinforcement learning* en inglés), los algoritmos genéticos, las máquinas de vectores de soporte (*suport-vector machines*) o las redes neuronales, las cuales trabajan de igual modo que las redes de neuronas biológicas, es decir, las informaciones que entran en ellas son capaces de producir resultados después de un proceso de aprendizaje interno que se realiza de manera automática.

En este conjunto tecnológico de redes neuronales, se destacan las máquinas que gestionan los algoritmos denominados *Deep Learning*, sistemas que utilizan diferentes estructuras de redes neuronales que, en capas sucesivas, aumentan su capacidad de aprendizaje a medida que son alimentadas con mayores cantidades de datos. En la actualidad, este tipo de máquinas con *Deep Learning*, tienen una capacidad similar al conocimiento humano para la comprensión del lenguaje hablado, reconocimiento de escritura, en sistemas de traducción automática, en el manejo de vehículos autónomos, en los asistentes digitales, en la manipulación de juegos más complejos de estrategia como lo es el ajedrez o el juego chino Go. Un claro ejemplo es la máquina AlphaGo, que en el año 2016 derrotó a Lee Sedol, el mejor jugador del mundo de este antiguo juego de fichas chino, en donde el

tablero puede contener hasta 10.170 combinaciones diferentes.[4] Esta estructura tecnológica se engloba en la ciencia de datos, la que incluye métodos matemáticos, procesos y sistemas de computación que manipulan datos masivos para la toma de decisiones en situaciones complejas, dando un énfasis en el análisis predictivo y en la construcción de escenarios futuros, puesto que saber y conocer lo que puede ocurrir es uno de los elementos esenciales en cualquier proceso de toma de decisiones.

Otro punto importante sobre la IA es convertir los datos adquiridos en datos "inteligentes", es decir, entregarlos como información útil para la toma de decisiones, ya sea para aquellos que deben tomar decisiones complejas en cualquier actividad, o bien para nutrir máquinas inteligentes diseñadas para decidir por ellas mismas lo que se debería hacer en situaciones complejas, tal como es el caso de los vehículos autónomos.

La IA no puede trabajar por sí sola para otorgar una respuesta autónoma e inteligente a un sistema. Se construye y trabaja en base a un conjunto de tecnologías en el que cada una de ellas interacciona con las demás para dar soluciones a problemas complejos. Para el caso de un vehículo autónomo, en primera medida se deberán incorporar múltiples sensores que, a su vez, serán guiados y administrados por otros sistemas, como podrían ser máquinas con capacidad de aprender o máquinas que incorporan algoritmos que procesen el lenguaje natural. La figura 1 muestra un esquema simple con las diferentes tecnologías que pueden constituir un sistema de IA.

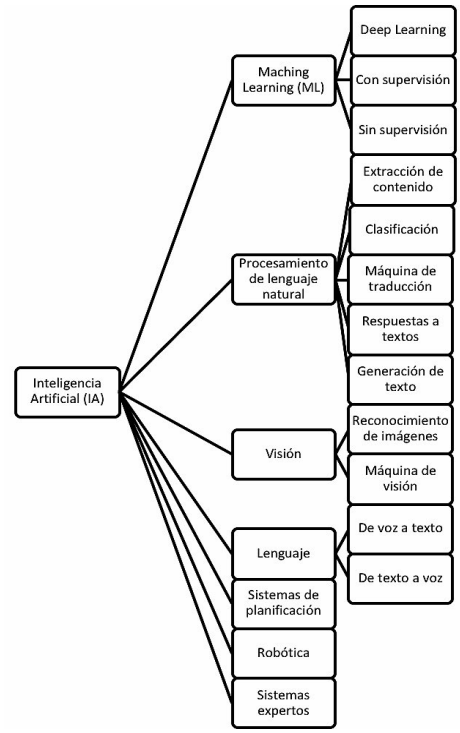


Figura Nº 1: Diversas tecnologías utilizadas en sistemas basados en inteligencia artificial.

Fuente: Elaboración propia.

Gran cantidad de algoritmos están construidos y basados en reglas y, en ocasiones, se han confundido los sistemas expertos como la base fundamental de la IA. Es importante destacar que un sistema experto es un mecanismo lógico compuesto de tres elementos esenciales:

1. Conocimiento-base (knowledge-base).
2. Mecanismo de inferencia.
3. Un programa informático para facilitar la interacción de los usuarios, la construcción del conocimiento-base, y desarrollar un esquema de razonamiento posterior.[5]

4 Deep Mind: https://deepmind.com/research/case-studies/alphago-the-story-so-far (consultado el 24 de agosto de 2022).
5 BUCHANNAN, Bruce. C. y SHORTLIFFE, Edward. H. Rule-Based Expert Systems. Addison-Wesley, 1984, p. 4-19.

Por otra parte, el conocimiento-base es el archivo de sucesos y las asociaciones entre ellos, que se conocen de un área concreta de análisis. Este conocimiento está representado por reglas según un esquema lógico "SI-ENTONCES" (basada en el álgebra de Boole). Por ejemplo, se tiene tres variables: A, B y C pertenecientes a un mismo conjunto. "SI" existe la evidencia de que A y B son ciertos, "ENTONCES" se puede concluir que C será cierto. Aunque el mecanismo de inferencia puede adquirir múltiples formas, es una estructura que controla la relación entre las reglas, de manera que los datos conocidos infieren las reglas para llegar a concluir el conocimiento de aquellos datos desconocidos.

Por tanto, la inteligencia artificial trabaja con un conjunto de tecnologías informáticas basadas en procesos lógico-matemáticos que se encuentran en evolución permanente. En la figura 2 se presenta una proyección del desarrollo de sistemas con IA, sugiriendo la posibilidad de la sustitución de la capacidad humana en muchos aspectos.

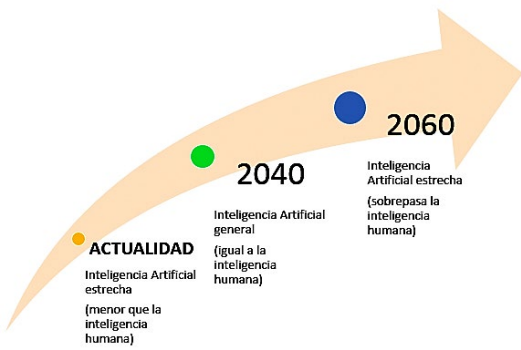


Figura Nº 2: Proyección de la inteligencia artificial.

Fuente: MOHAMED, Ziyad, *op. cit.*, p. 5.

Aplicación de sistemas basados en IA para la defensa

Las aplicaciones de la IA tienen un importante campo de aplicación, especialmente en asuntos de análisis de inteligencia, logística, ciberseguridad y sistemas de mando y control, así como también en vehículos autónomos y semiautónomos para aplicaciones militares, pero, dado que estas tecnologías se desarrollan principalmente en el mundo civil, surgen de manera persistente problemas de desconfianza cuando se trasladan al mundo militar.

Esta desconfianza abre las posibilidades de que un país que se encuentra en constante combate invierta en empresas que desarrollen tecnologías avanzadas de IA. En este caso, adquiriría complejos sistemas y algoritmos de IA capaces de detectar de manera autónoma fallos en equipos militares, o bien sistemas de IA capaces de realizar intrusiones no deseadas en equipos militares en escenarios bélicos o de defensa.

Es interesante también revisar lo que se piensa y ejecuta respecto de las nuevas tecnologías de IA aplicadas al campo militar en China, dado que la tendencia occidental es considerar solamente los desarrollos tecnológicos que suceden en esta parte del mundo, particularmente, en Estados Unidos. Un informe presentado por *China Defense News*,[6] asegura que el mundo *"está actualmente en vísperas de una revolución de la inteligencia, con la sociedad humana pasando de la era de internet a la era de la inteligencia".*

La IA impulsada por el Big Data, los nuevos algoritmos y la supercomputación, están cambiando e

6 HANG HUI, Chen. Inteligencia artificial: cómo alterar el futuro de la guerra. Diponible en: http://www.mod.gov.cn/jmsd/2018-01/02/content_4801253.htm (consultado el 29 de agosto de 2022).

incluso modificando todos los sectores en donde la guerra ya no es una excepción. Asegurando que: "*desde los submarinos hasta los drones, y desde el software de mantenimiento predictivo hasta los asistentes inteligentes para la toma de decisiones, la IA está cambiando los escenarios de la guerra con una amplitud y profundidad sin precedentes, impulsando una nueva ola de cambios militares y modificando silenciosamente la forma y el rostro de la guerra*".

Hoy en día el tiempo es el elemento clave, siendo necesario calcular y predecir los posibles resultados de un conflicto armado. Es por esto que surge la importancia de la IA, que, con algoritmos avanzados y sistemas de supercomputación, puede ayudar y facilitar la predicción de resultados con mayor precisión. De ahí nace la importancia de nuevas tecnologías, como pueden ser los sistemas de armas inteligentes, las contramedidas autónomas o las armas hipersónicas.

Otra potencia, como es el caso de Rusia (sin entrar en los sistemas militares utilizados en el actual conflicto con Ucrania), ha desarrollado una especial estrategia en el contexto de la IA militar, dando prioridad a las tecnologías y capacidades que pueden utilizarse para debilitar los sistemas de mando y control, como también las comunicaciones del adversario. Sin embargo, Rusia se encuentra por detrás en aspectos de desarrollo de IA en comparación a como lo aborda China o Estados Unidos. Por otra parte, la industria de semiconductores de altas capacidades de computación es esencial para el trabajo y tratamiento de sistemas y máquinas basadas en IA. Aquí, Rusia se vuelve enormemente dependiente de Estados Unidos, de la República de Corea o de Taiwán. Sin embargo, mientras que la cultura de innovación occidental se caracteriza por una tendencia a utilizar tecnologías de vanguardia como solución a los problemas estratégicos y tácticos en el dominio militar, el enfoque ruso de las aplicaciones militares de la IA se ve más pragmático.[7] Dicho esto, los estrategas rusos consideran que la guerra de la información es el elemento primordial y central en los conflictos contemporáneos, llegando a considerar la guerra de la información basada en la IA como una *"partida estratégica para ganar la guerra en los conflictos entre Estados"*.[8] Y, según el pensar de los estrategas rusos, es el campo de la IA lo que permitirá a Rusia enfrentarse más eficazmente al entorno de la información en los escenarios de guerras cibernéticas, en el nuevo contexto de guerras electrónicas.[9] Por supuesto, no olvidar la capacidad actual de Rusia en la construcción de vehículos autónomos como lo es el URAN-9; un tanque de combate de gran capacidad operativa (sistemas que se definen como *Unmanned Ground Vehicles* o *UGV*).[10]

Las tecnologías basadas en IA, aparte de ser dirigidas a sistemas de mando y control, incluyendo todas aquellas que se encuentran en el contexto de la ciberguerra, se enfocan, como lo es el URAN-9, a los vehículos autónomos no tripulados y, en especial, a los drones o vehículos aéreos no tripulados (*Unmanned Aerial Vehicles o*

7 Chatam House. Advanced Military Technology in Russia. https://www.chathamhouse. org/2021/09/advanced-military-technology-Russia (consultado el 29 de Agosto de 2022).

8 *Ibídem*.

9 *Ibídem*.

10 CRANNY-Evans, S. (05 de octubre de 2021). Russia to conduct mass testing of Uran-9 UGV in 2022. Janes News: https://www.janes.com/defence-news/news-detail/russia-to-conduct-mass-testing-of-uran-9-ugv-in-2022 (consultado el 30 de agosto de 2022).

UAV). De estas tecnologías es conveniente realizar una distinción entre vehículos autónomos y vehículos automatizados. En los primeros, a partir de la información recibida desde sus distintos sensores y de sus sistemas de IA, será el propio vehículo quien piense y tome la decisión sobre el curso que ha de tomar para lograr alcanzar el objetivo marcado o la tarea asignada. Por su parte, los segundos actuarán según reglas determinadas a la manera lógica "SI-ENTONCES", referidas para los sistemas expertos, entregando como resultado un comportamiento constante en todos los casos; es decir, para un conjunto de entradas (*inputs*) se obtendrán un conjunto único de salidas (*outputs*).[11]

En general, las tecnologías de aplicación militar basadas en sistemas de IA pueden dividirse en cinco grandes grupos:[12]

1. Inteligencia, vigilancia y reconocimiento
2. Logística
3. Ciberoperaciones
4. Desinformación (profunda)
5. Mando y control
6. Vehículos autónomos y semiautónomos
7. Sistemas de armas letales autónomas

Desde otro punto de vista, en la figura 3 se expone algunos riesgos presentes en la aplicación de IA en el campo militar.

Figura Nº 3: Riesgos asociados al uso militar de la IA.

Fuente: MORGAN, Forrest E. *et al.* Military Applications of Artificial Intelligence. Ethical Concerns.

¿Cómo afecta la IA en la ciberseguridad?

Diariamente se producen miles de ciberataques contra instituciones privadas y públicas de todo el mundo, siendo unos países más atacados que otros, principalmente aquellos que son potencias económicas avanzadas. Los ataques de piratas informáticos (*hackers*) o la diseminación de *ransomware*[13] son por cientos de miles anualmente, en contra de grandes compañías privadas o incluso contra potentes agencias de inteligencia, como fue el caso de los *Shadow Brokers*, donde fueron capaces de acceder a los sistemas de la agencia de inteligencia americana NSA (*National Security Agency*) en el mes de agosto de 2016.[14] Asimismo fue el caso del denominado Petya, que alcanzó a manipular los ordenadores de medio mundo,

11 CUMMINGS, Mary L. (enero 2017). Artificial Intelligence and the Future of Warfare. Chatham House: https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificialintelligence-future-warfare-cummings-final.pdf (consultado el 30 de agosto de 2022).

12 Congressional Research Service. Artificial Intelligence and National Scurity. 10 de noviembre de 2020. https://sgp.fas.org/crs/natsec/R45178.pdf (consultado el 15 de marzo de 2022).

13 Son programas informáticos hostiles (virus, gusanos informáticos, programas espía, etc.), denominados *malware* en inglés, que se basan, en el caso del *ransomware*, en la extorsión e impiden a los usuarios la posibilidad de acceder a sus propios archivos salvo que se pague la cantidad exigida.

14 GOODIN, Dan. (14 de abril de 2017). NSA-leaking Shadow Brokers just dumped its most damaging release yet. Ars Technica: https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-justdumped-its-most-damaging-release-yet/ (consultado el 30 de agosto de 2022).

incluido el conocido ciberataque a los sistemas de distribución de energía eléctrica de Ucrania.[15] De igual modo, es importante recordar que más de 60.000 ficheros pertenecientes al Gobierno de Estados Unidos aparecieron accesibles públicamente en los servicios en la nube de Amazon (*Amazon Web Services*), por una mala operación de un ingeniero de dicha empresa.[16] Estos errores evidencian la enorme cantidad de ciberataques que ocurren diariamente contra empresas o instituciones públicas en todo el mundo.

Como se ha mencionado, las aplicaciones de la IA en el campo militar son fundamentalmente operacionales y tácticas y, muchas de ellas, van dirigidas a la toma de decisiones. La IA es un componente que puede proporcionar ventajas defensivas y ofensivas. Sin embargo, como también se ha presentado en este artículo, también puede proporcionar riesgos a sus propias capacidades, es decir, a la vez de presentar nuevas capacidades abre las puertas para dar ventajas a un oponente que se encuentre tecnológicamente mucho más avanzado. Un caso paradigmático de esta estrategia es el programa lanzado por el US *Strategic Operations Control* (SOCOM), que "*no es sino el Mando de Operaciones Estratégicas para la defensa de Estados Unidos, que tiene en marcha una hoja de ruta invirtiendo fuertemente en tecnologías apoyadas por la IA, donde el aprendizaje automático es uno de los puntales de tal estrategia, que mantiene en lo esencial tres objetivos principales:*

1. *Personal operativo experto en técnicas de IA*
2. *Desarrollo de aplicaciones específicas de IA para las fuerzas armadas*
3. *Análisis del alcance y potencial de las aplicaciones de IA en el campo militar*".[17]

Cuando se consideran los aspectos estratégicos de un conflicto armado, la inteligencia artificial viene a potenciar las capacidades de comando, control, comunicaciones e inteligencia, las cuales incluyen aspectos relacionados con el seguimiento y guiado de misiles y la intercepción de los misiles enemigos. Es aquí cuando es necesario las aplicaciones en aspectos relacionados con la ciberseguridad, lo cual presenta la otra cara de la moneda: los actuales métodos de defensa ante potentes ciberataques de potenciales adversarios presentan vulnerabilidades, y estos pueden disponer de nuevas armas inteligentes contra las que no sea posible una respuesta eficaz, provocando que exista una línea delgada entre los métodos de ciberdefensa y de ciberataque.

El Departamento de Defensa de Estados Unidos considera que la IA es un instrumento esencial para predecir, identificar y responder a ciberataques y otras amenazas físicas que provengan de diversas fuentes. Para esto trabajan en cooperación con el sector público-privado, seleccionando aliados comerciales y personal académico con el fin de desarrollar nuevos sistemas con énfasis en áreas

15 Este video muestra la situación que se produjo entre el personal técnico que se ocupaba del control de la red de distribución de electricidad de Ucrania. https://www.wired.com/video/watch/watch-hackers-take-over-a-ukranian-power-station (consultado el 30 de agosto de 2022).

16 ZAVIA, Matías. (03 de febrero de 2017). Cómo un comando mal escrito por un ingeniero de Amazon dejó una buena parte de Internet inaccesible durante horas. Gizmodo en español: https://es.gizmodo.com/como-un-comando-mal-escrito-por-un-ingeniero-deamazon-1792910295 (consultado el 01 de septiembre de 2022).

17 SOCOM. Plans New Artificial Intelligence Strategy. https://www.nationaldefensemagazine.org/articles/2019/8/9/socom-plans-new-artificial-intelligencestrategy (consultado el 01 de septiembre de 2022).

del tratamiento de datos, evaluación y pruebas de nuevos sistemas basados en IA y, principalmente, en el área de la ciberseguridad.[18]

Sin embargo, los sistemas inteligentes basados en IA pueden aumentar las vulnerabilidades de cualquier defensa ante potenciales ciberataques, en los que, contrariamente a lo que se establezca, un potencial enemigo podría utilizar *malware* para hacerse con el control, manipular o engañar al respecto del comportamiento de los sistemas de IA diseñados para el ataque o la defensa. Un claro ejemplo es el proyecto *Maven* de Estados Unidos,[19] capaz de extraer de forma autónoma objetos de interés de imágenes en movimiento o fijas, buscando lograr una gran capacidad de ciberataque a la hora de ser detectado. Ahora bien, es un hecho que los ciberataques existen porque los sistemas informáticos son vulnerables. Siempre existirá alguien capaz de encontrar la manera de corromper un algoritmo por muy robusto que este sea. Se debe entender que los ciberataques se dirigen a interrumpir, alterar, confundir, degradar e incluso destruir los sistemas y redes informáticas del adversario. De igual modo lo hacen con la información.

Al lado de los ciberataques se encuentra también la ciberexplotación, que se enfoca en la adquisición de información sensible de forma ilegal, sin perturbar el correcto funcionamiento de los sistemas. De igual modo, el ciberespionaje se vuelve un entorno complejo, algo a lo que algunos denominan como "sombras en la nube".[20] Tanto los ciberataques como la ciberexplotación, basados en sistemas de IA no se enfocan únicamente a los sistemas de computación o a los sistemas de armas fijos o móviles, sino que también tiene como objetivo las redes de comunicaciones, de manera que, a mayor procedimiento técnico de los sistemas militares, mayores son los peligros y los riesgos de ser interceptados. Por otra parte, de acuerdo con la RAND Corporation,[21] el ciberespacio se compone de tres capas que interactúan en los otros espacios indicados: la capa física, la capa sintáctica y la capa semántica, tal como se aprecia en la figura 4. Todo un conjunto susceptible de ser destruido en una u otra forma o de poder destruir a un posible oponente.

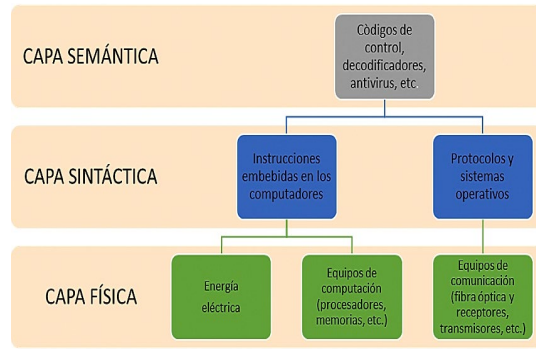


Figura Nº 4: Estructura del ciberespacio.

Fuente: LIBICKI, M. C., Cyberdeterrence and Cyberwar. RAND Corporation, 2009.

18 U.S. Department of Defense. Summary of the 2018 Department of Defense Artificial Intelligence Strategy. Harnessing AI to Advance Our Security and Prosperity. https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF?source=GovDelivery (consultado el 06 de septiembre de 2022).

19 PELLERIN, Cheryl. (21 de julio de 2017). Project Maven to deploy computer algorithms to war zone by year's end. U.S. Department of Defense: https://www.defense.gov/News/News-Stories/Article/Article/1254719/project-maven-to-deploycomputer-algorithms-to-war-zone-by-years-end/ (consultado el 06 de septiembre de 2022).

20 DEIBERT, Ronald. y ROHOZINSKI, Rafal. Shadows in the Cloud. Investigating Cyber Espionage 2.0. https://www.nartv.org/mirror/shadows-in-the-cloud.pdf (consultado el 11 de marzo de 2022).

21 LIBICKI, Martin. C., Cyberdeterrence and Cyberwar. RAND Corporation, 2009. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (consultado el 28 de marzo de 2022).

En definitiva, la IA es útil para ayudar en la toma de decisiones en el contexto del ciberespacio debido a que la rapidez es esencial y los sistemas basados en esta tecnología son capaces de gestionar enormes volúmenes de datos a gran velocidad. Sin embargo, aunque sea posible desarrollar sistemas militares autónomos o semiautónomos que otorguen una gran capacidad operativa, los sistemas militares bajo la tecnología de la IA son igualmente vulnerables a los ciberataques, dejando la puerta abierta a importantes consideraciones respecto de su uso e, incluso, se puede pensar en la posibilidad de la adquisición de armas del exterior manipuladas por los propios vendedores para debilitar las capacidades operativas del país. La dimensión global del ciberespacio en operaciones militares puede ser muy negativa si no se dispone de capacidades humanas como tecnológicas para desarrollar los propios sistemas y máquinas basadas en IA, al margen de mercados internacionales, ya sean de países aliados o de otros no aliados.[22]

¿Cómo afecta la IA en la geopolítica?

En el año 2017, el presidente de la Federación de Rusia, Vladimir Putin, comentando con un grupo de periodistas y estudiantes rusos declaró que: *"Quien se convierta en el líder en esta esfera* (la inteligencia artificial) *se convertirá en el gobernante del mundo"*.[23] El poder, en el contexto de las relaciones internacionales durante el siglo XXI, estará determinado por la tecnología.

En este nuevo escenario, Estados Unidos y China surgen como las dos grandes potencias que, probablemente, dominarán el ciberespacio. Por otra parte, Latinoamérica parece carecer de estas capacidades tecnológicas y corre el riesgo de padecer una suerte de "cibercolonización", considerando los peligros que esto implica para la independencia y la autonomía en un contexto global.[24]

En la historia, los imperios se han caracterizado por implantar su poder en un extenso territorio, imponiendo sus modos de ejercer política y sus normas sociales en dicho territorio, la IA viene a ser el instrumento clave en la constitución de imperios en el ciberespacio.[25]

Tal como se ha mencionado durante el desarrollo de este artículo, una de las claves en el desarrollo de las capacidades de IA, aparte de la computación y la creación de potentes algoritmos, se encuentra en los datos. Es ahí donde la manipulación de datos masivos ha permitido el crecimiento y cambio en el contexto económico global y el desarrollo de las grandes empresas tecnológicas mundiales, tales como Google (*Alphabet*), Apple, Amazon, Facebook (actualmente, Meta) o Microsoft que, junto con los consorcios chinos Tencent y Alibaba, constituyen el poder tecnológico global.

Por otra parte, la petrolera saudí Saudi Aramco tiene el privilegio de ingresar a este selecto grupo de empresas, cuyo valor de capitalización bursátil supera en cada caso los 600.000 millones de dólares

22 Stanley Center for Peace and Security. The Militarization of Artificial Intelligence. 2009. https://front.un-arm.org/wp-content/uploads/2020/06/Stanley-Stimson-UNODA-2020- TheMilitarization-ArtificialIntelligence.pdf (consultado el 09 de septiembre de 2022).

23 MIAILHE, Nicolás. Géopolitique de l'Intelligence artificielle: le retour des empires? Politique étrangère, Vol. 83, Issue 3, 2018.

24 *Ibídem*.

25 *Ibídem*.

(en valores de 2020).[26] Estas empresas ya dominan el ciberespacio gracias a sus potentes sistemas basados en IA, además de llevar a cabo la manipulación de miles de millones de datos de todo tipo de usuarios de todo el mundo. Este se ha convertido en un poder geopolítico poco considerado, pero que actúa y predomina determinantemente en las inversiones de múltiples gobiernos en todo el mundo, así como también se aprecia en muchos de los desarrollos tecnológicos de empresas y universidades. [27]

Simplemente, la IA está cambiando el equilibrio de poder en el mundo. Todo lo relativo a la IA es un nuevo eje que cambiará no solo el ciberespacio, sino lo que algunos denominan como "geoespacio".[28]

Reflexiones finales

La inteligencia artificial, como se ha explicado en este artículo, es el campo de la tecnología en donde se determinará un nuevo orden mundial. Como ha sido la tónica de la historia humana, estará determinado por las estructuras de poder político y militar, en donde China y Estados Unidos se convertirán en las dos grandes potencias de este siglo, sin olvidar a otros países que juegan igualmente a ocupar y defender aquellos espacios geopolíticos que consideran propios.

Sin embargo, como se ha expresado en estas páginas, las aplicaciones de IA en el dominio militar aportan considerables ventajas, pero también importantes riesgos. Dichos riesgos provienen esencialmente de los desarrollos tecnológicos que se van dando en este nuevo campo de actuación.

También existe la posibilidad de que países contrarios aprovechen sus mejores potencialidades para convertir la IA en un arma de doble filo, volviéndose en contra de aquellos que supuestamente tienen grandes capacidades en sus desarrollos de inteligencia artificial. A esto se une lo que se ha decidido denominar como "cibercolonización", que permitirá que muchos países pasen a ser dependientes de otros y, por tanto, ocupen un lugar secundario en su peso geopolítico y geoeconómico a nivel mundial.

Por otra parte, se presenta con nitidez la falencia y carencia en desarrollos tecnológicos en el campo de la inteligencia artificial en Latinoamérica quedando muy por detrás de Estados Unidos, de China e incluso de Rusia.

Por tanto, hoy en día contar con un sistema de IA ya es una necesidad en el campo de la defensa y se vuelve absolutamente crucial para poder participar con independencia en los retos geopolíticos que presenta el siglo XXI.

Sirva el presente artículo como una llamada de atención para poner en marcha con urgencia un plan integrado de aplicaciones de IA en la defensa, en el que las fuerzas armadas deberán ser el motor de dicha integración, con mandos y personal especializados y con un programa específico que analice, desarrolle y englobe todas las capacidades disponibles.

26 PAGANINI, Pierluigi. Data, the New Power in Geopolitics. ISPI (Italian Institute for International Political Studies). 2021. Recuperado de: https://www.ispionline.it/en/pubblicazione/data-new-power-geopolitics-30657#:~:text=The%20governments%20that%20invested%20moredata%20is%20the%20new%20power (consultado el 13 de septiembre de 2022).

27 *Ibídem*. En este artículo de P. Paganini se muestran las 17 universidades más importantes en el desarrollo de IA, siendo las más relevantes las que se encuentran en Estados Unidos.

28 PANDYA, Jayshree. The Geopolitics of Artificial Intelligence. Forbes. Rescatado de: https://www.forbes.com/sites/cognitiveworld/2019/01/28/the-geopolitics-of-artificialintelligence/?sh=25d27d1a79e1 (consultado el 15 de septiembre de 2022).

Bibliografía

AMOS, Jonathan. *Russian anti-satellite missile test draws condemnation. BBC News*. (16 noviembre 2021). Recuperado de: https://www.bbc.com/news/science-environment-59299101

BUCHANAN, Bruce G. y SHORTLIFFE, Edward. H. *Rule-Based Expert Systems.* Addison-Wesley, 1984, pp. 4-19.

Chatam House. *Advanced Military Technology in Russia.* Recuperado de: https://www.chathamhouse.org/2021/09/advanced-military-technology-russia

Congressional Research Service. *Artificial Intelligence and National Security.* 10 de noviembre de 2020. Recuperado de: https://sgp.fas.org/crs/natsec/R45178.pdf

CRANNY-Evans, S. *Russia to conduct mass testing of Uran-9 UGV in 2022.* Janes News. (05 de octubre de 2021). Recuperado de: https://www.janes.com/defence-news/news-detail/russia-to-conduct-mass-testing-of-uran-9-ugv-in-2022

CUMMINGS, Mary. L. *Artificial Intelligence and the Future of Warfare.* Chatham House. (enero 2017). Recuperado de: https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificialintelligence-future-warfare-cummings-final.pdf

Deep Mind. Recuperado de: https://deepmind.com/research/case-studies/alphago-the-story-so-far

DEIBERT, Ronald y ROHOZINSKI, Rafal. *Shadows in the Cloud. Investigating Cyber Espionage 2.0.* Recuperado de: https://www.nartv.org/mirror/shadows-in-the-cloud.pdf

GOODIN, Dan. *NSA-leaking Shadow Brokers just dumped its most damaging release yet. Ars Technica.* (14 de abril de 2017). Recuperado de: https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-justdumped-its-most-damaging-release-yet/

HANG HUI, Chen. Inteligencia artificial: cómo alterar el futuro de la guerra. Recuperado de: http://www.mod.gov.cn/jmsd/2018-01/02/content_4801253.htm

LIBICKI, Martin. C. *Cyberdeterrence and Cyberwar.* RAND Corporation, 2009. Recuperado de: https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

MIAILHE, Nicolás. "Géopolitique de l'Intelligence artificielle: ¿le retour des empires?" *Politique étrangère,* Vol. 83, Issue 3, 2018.

MOHAMED, Ziyad. *Artificial Intelligence, Definition, Ethics, and Standards.* The British University in Egypt, 2018-2019.

MORGAN, Forrest E. *et al. Military Applications of Artificial Intelligence.* Ethical Concerns.

PAGANINI, Pierluigi. *Data, the New Power in Geopolitics*. ISPI (Italian Institute for International. Political Studies). 2021. Recuperado de: https://www.ispionline.it/en/pubblicazione/data-new-power-geopolitics-30657#:~:text=The%20governments%20that%20invested%20more,data%20is%20the%20new%20power

PANDYA, Jayshree. *The Geopolitics of Artificial Intelligence.* Forbes. Recuperado de: https://www.forbes.com/sites/cognitiveworld/2019/01/28/the-geopolitics-of-artificialintelligence/?sh=25d27d1a79e1

PELLERIN, Cheryl. *Project Maven to deploy computer algorithms to war zone by year's end. U.S.* Department of Defense. (21 de julio de 2017). Recuperado de: https://www.defense.gov/News/News-Stories/Article/Article/1254719/project-maven-to-deploycomputer-algorithms-to-war-zone-by-years-end/

SOCOM. Plans *New Artificial Intelligence Strategy.* Recuperado de: https://www.nationaldefensemagazine.org/articles/2019/8/9/socom-plans-new-artificial-intelligencestrategy

Stanley Center for Peace and Security. *The Militarization of Artificial Intelligence.* 2009. Recuperado de: https://front.un-arm.org/wp-content/uploads/2020/06/Stanley-Stimson-UNODA-2020-TheMilitarization-ArtificialIntelligence.pdf

U.S. Department of Defense. *Summary of the 2018 Department of Defense Artificial Intelligence Strategy.* Harnessing AI to Advance Our Security and Prosperity. Recuperado de: https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF?source=GovDelivery

ZAVIA, Matías S. Cómo un comando mal escrito por un ingeniero de Amazon dejó una buena parte de Internet innacesible durante horas. *Gizmodo en español*. (3 de febrero de 2017). Recuperado de: https://es.gizmodo.com/como-un-comando-mal-escrito-por-un-ingeniero-deamazon-179291.