INSTITUTO DE INVESTIGACIONES ESTRATÉGICAS
DE LA ARMADA DE MÉXICO

TI 01/24
01/10/2024

Capitán de Navío
Rommel Toledo Ramírez

Inteligencia Artificial: Antagonismos para la Seguridad Nacional de México

RESUMEN

Resumen (Español): Este artículo aborda las implicaciones de la inteligencia artificial (IA) en la seguridad nacional de México, un tema de creciente importancia en el contexto de la rápida evolución tecnológica global. El ensayo analiza cómo la IA puede transformar aspectos fundamentales de la seguridad nacional, identificando amenazas y antagonismos.

Palabras clave: Inteligencia Artificial, Seguridad Nacional, México, Ciberseguridad, Amenazas.

ABSTRACT

Abstract (Inglés): This article addresses the implications of artificial intelligence (AI) on Mexico's national security, a topic of increasing importance in the context of rapid global technological evolution. The study analyzes how AI can transform fundamental aspects of national security, identifying threats and antagonisms.

Keywords: Artificial Intelligence, National Security, Mexico, Cybersecurity, Threats.

INTRODUCCIÓN

La evolución tecnológica ha impactado todos los campos del poder nacional. La llegada de Internet trajo progreso, pero también nuevas amenazas. El ciberespacio se ha convertido en un espacio crítico para las naciones, sumándose a los tres dominios tradicionales de la guerra (tierra, mar y aire)[1] (Setzer, 2022). Estas amenazas en el ciberespacio han crecido exponencialmente, afectando a naciones, gobiernos, empresas y ciudadanos.

Incidentes notables incluyen los ciberataques atribuidos a Rusia en la guerra con Ucrania, demostrando el poder y sofisticación de las operaciones cibernéticas (Grace B. Mueller et al., 2023). Por otro lado, los ataques asimétricos por colectivos de ciberdelincuentes, comprometen sistemas críticos, robando información sensible e inutilizando servicios a la ciudadanía.

1 La OTAN reconoce al ciberespacio desde 2016 y al espacio exterior desde 2019 como dominios operacionales.

La inteligencia artificial (IA) ha influido enormemente en la evolución de las amenazas informáticas, proporcionando herramientas más poderosas y automatizadas para atacar y evadir la detección. Los ataques impulsados por IA son cada vez más difíciles de detectar y prevenir, incrementando la importancia de la ciberseguridad.

Ademas, la reciente inclusión de la IA ha permeado todos los aspectos de la sociedad, impactando también la seguridad nacional, internacional y la geopolítica. China y Estados Unidos han emergido como actores principales en la IA, invirtiendo recursos significativos en su desarrollo, aplicándola en la ciberseguridad y la guerra, lo que afecta la estabilidad y seguridad internacionales. (Sarah Cook, 2018). La competencia tecnológica entre estas potencias tiene implicaciones más allá de la economía, introduciendo nuevas dinámicas en las relaciones internacionales. La interconexión de infraestructuras críticas, como energía, transporte y comunicaciones, las hace objetivos atractivos para ciberataques.

Otro aspecto a considerar, es como la desinformación global también se ha incrementado con la IA, permitiendo la creación de contenido falso, noticias manipuladas y videos deepfake[2], que pueden propagarse rápidamente y manipular la opinión pública. Estos riesgos son significativos para la sociedad y la política, como se vio en las elecciones presidenciales de los Estados Unidos de América en 2016 en el caso conocido como “El escándalo de Cambridge Analytica” (Nicholas Confessore, 2018).

En México, la situación no es diferente, el número de ataques a entes gubernamentales ha aumentado, mientras la preparación para mitigarlos ha disminuido, afectando la posición nacional en el índice mundial de ciberseguridad, cayendo del lugar 70 (en 2018) al 92 (en 2021) (National Cyber Security Index, 2021).

Abordar estos desafíos de manera integral y proactiva, mediante la identificación precisa de amenazas, análisis de riesgos y medidas efectivas de ciberseguridad, es esencial para proteger la seguridad nacional en el entorno digital. La colaboración nacional e internacional es crucial para compartir información y recursos en la lucha contra las amenazas cibernéticas impulsadas por IA. De la misma manera que es imprescindible analizar los efectos de la introducción de la IA en los aspectos de la vida diaria, que sin duda se verá trastocada por esta tecnología emergente.

En resumen, los ciberataques, tanto simétricos como asimétricos, y el papel creciente de la IA en ellos, presentan desafíos significativos para la Seguridad Nacional de México. Comprender y mitigar estas amenazas es impresindible para garantizar la protección de infraestructuras críticas, así como de la estabilidad política, económica y social en la era de la Inteligencia Artificial.

2 Es un término que se refiere a una técnica de manipulación de medios que utiliza la inteligencia artificial, para crear contenido multimedia falso y convincente.

El propósito de este ensayo es analizar las implicaciones que tiene la IA en los distintos campos del poder, y por ende en la seguridad nacional de México. Principalmente los antagonismos asociados con la implementación, lenta pero inexorable, de tecnologías de IA. Al explorar estos aspectos, el documento pretende llamar la atención del lector sobre las posibles afectaciones que la IA puede tener en nuestra sociedad.

DESARROLLO

Teorías de seguridad nacional en la Era del Ciberespacio y la Inteligencia Artificial

El concepto de seguridad nacional ha evolucionado con la llegada del ciberespacio como dominio crítico. Joseph S. Nye[3] destaca la relevancia de la ciberseguridad y el poder blando. Joseph S. Nye, Jr. es un destacado politólogo estadounidense, conocido por sus significativas contribuciones en el campo de las relaciones internacionales y la teoría del poder. Es profesor en la Universidad de Harvard y exsecretario Adjunto de Defensa de EE.UU. Nye es especialmente famoso por desarrollar el concepto de "poder blando", que se refiere a la capacidad de un país para influir en otros a través de medios culturales y diplomáticos, en contraposición al "poder duro" basado en la fuerza militar y económica. Sus trabajos abordan temas como el poder global, la ciberseguridad y la geopolítica, explorando cómo la tecnología y la información afectan la dinámica del poder y la seguridad nacional en el mundo moderno.Según Nye, la capacidad de un Estado para proteger su soberanía y a sus ciudadanos se extiende al dominio digital, donde la información y la conectividad son recursos estratégicos (Nye, 1990). Nye señala que el poder en la era digital se manifiesta a través de la influencia y el control de la información en el ciberespacio. Esto abarca tanto medidas defensivas como ciberataques y guerra informática. La seguridad nacional no solo depende de la defensa contra amenazas externas, sino también de la protección de activos digitales (Nye, 2020).

El ciberespacio, por su naturaleza global e interconectada, no reconoce fronteras tradicionales, lo que obliga a reevaluar las estrategias de seguridad nacional. Los ciberataques pueden originarse desde cualquier lugar y afectar infraestructuras críticas, desestabilizando así a un Estado (Burns & Price, 2012). La ciberseguridad se convierte en un componente integral de la seguridad nacional. Nye enfatiza la necesidad de anticipar y responder proactivamente a las amenazas cibernéticas, combinando tecnología avanzada, inteligencia cibernética y políticas de resiliencia (Nye, 2020).

Manipulación de la sociedad y guerra de la información

3 Joseph S. Nye, Jr. es un destacado politólogo estadounidense, conocido por sus significativas contribuciones en el campo de las relaciones internacionales y la teoría del poder. Es profesor en la Universidad de Harvard y exsecretario Adjunto de Defensa de EE.UU. Nye es especialmente famoso por desarrollar el concepto de "poder blando", que se refiere a la capacidad de un país para influir en otros a través de medios culturales y diplomáticos, en contraposición al "poder duro" basado en la fuerza militar y económica. Sus trabajos abordan temas como el poder global, la ciberseguridad y la geopolítica, explorando cómo la tecnología y la información afectan la dinámica del poder y la seguridad nacional en el mundo moderno.

En el ciberespacio, la información es una herramienta poderosa de influencia. Bruce Schneier[4] explora cómo la manipulación de datos y la desinformación se utilizan para influir en la sociedad y decisiones políticas. Schneier destaca que la manipulación de la información puede alterar la percepción pública y el discurso político, afectando procesos democráticos como las elecciones (Cueto, 2023).

La IA ha amplificado la capacidad de manipular la información. Los algoritmos avanzados pueden crear y difundir contenido falso con gran eficiencia, representando un desafío significativo para la integridad informativa. Schneier advierte sobre los riesgos de la IA en la generación de desinformación, destacando cómo puede influir en la opinión pública y decisiones políticas (Schneier, 2016).

La guerra de la información afecta la estabilidad y seguridad de los países. Schneier argumenta que protegerse contra la manipulación de la información es vital para la seguridad nacional. Esto implica no solo salvaguardar la infraestructura digital, sino también fomentar la resiliencia de la sociedad frente a la desinformación y promover la alfabetización mediática (PBS News, 2023).

Inteligencia artificial y seguridad nacional

El impacto de la IA en la seguridad nacional es un campo que ha sido abordado por diversos autores, filósofos y analistas, entre ellos Nick Bostrom[5] en su libro "Superintelligence: Paths, Dangers, Strategies", advierte sobre los riesgos de una IA superinteligente que podría actuar de manera impredecible o contraria a los intereses humanos. En cuanto a la seguridad nacional, una IA superinteligente podría manipular o sabotear infraestructuras críticas (Bostrom, 2017).

Eliezer Yudkowsky[6], del Machine Intelligence Research Institute, se enfoca en los aspectos éticos y de seguridad de la IA. Subraya la importancia de desarrollarla con objetivos seguros y éticos, crucial para la seguridad nacional, ya que resalta la necesidad de controlar y orientar adecuadamente el uso de la IA en aplicaciones críticas (Yudkowsky, 2008).

La intersección de las visiones de Bostrom y Yudkowsky sugiere que, aunque la IA ofrece capacidades mejoradas para la inteligencia y la eficiencia operativa, requiere una gestión cuidadosa y consideración ética

4 Bruce Schneier es una figura prominente y respetada en el campo de la seguridad informática y la criptografía. Reconocido como un experto en seguridad, autor prolífico y conferencista destacado, Schneier ha desempeñado un papel crucial en la formulación y promoción de conceptos clave en el ámbito de la ciberseguridad. Su contribución va más allá de la teoría, ya que ha trabajado activamente para aumentar la conciencia pública sobre cuestiones de privacidad y seguridad en la era digital. Con libros como "Secrets and Lies" y "Applied Cryptography", Schneier ha logrado explicar conceptos complejos de manera accesible, permitiendo que tanto expertos como el público en general comprendan mejor los desafíos y las soluciones en la esfera de la seguridad cibernética.

5 Nick Bostrom es un filósofo y profesor universitario en la Universidad de Oxford, conocido principalmente por su trabajo en los campos de la ética del riesgo existencial y de la inteligencia artificial. Bostrom ha adquirido relevancia por su enfoque en cómo las tecnologías avanzadas, especialmente la inteligencia artificial, podrían afectar a la humanidad de maneras fundamentales. Es autor de la obra influyente "Superintelligence: Paths, Dangers, Strategies", en la cual examina los riesgos y las estrategias relacionadas con el desarrollo de una IA que sobrepase la inteligencia humana.

6 Eliezer Yudkowsky es un investigador y escritor estadounidense en el campo de la inteligencia artificial, conocido por su enfoque en la ética y seguridad de la IA avanzada. Como cofundador del Machine Intelligence Research Institute (MIRI), Yudkowsky ha contribuido significativamente al estudio de la IA "amigable" y a las estrategias para mitigar riesgos potenciales asociados con sistemas de IA autónomos y avanzados.

para asegurar que su aplicación en la seguridad nacional no comprometa los valores humanos ni la estabilidad global.

Marco normativo mexicano

El marco legal del ciberespacio es sumamente importante para garantizar el uso seguro de las tecnologías digitales, incluido el tema de la IA. Sin embargo, la tecnología avanza más rápido que la legislación. Existen leyes y reglamentos que abordan aspectos del ciberespacio, desde la protección de datos hasta la ciberseguridad, sin embargo, al día de hoy, no hay una sola ley específica sobre IA o ciberespacio.

El marco jurídico mexicano, encabezado por la Constitución Política de los Estados Unidos Mexicanos en su artículo 6°. garantiza el derecho al acceso a las tecnologías de la información y comunicación (CPEUM, 1917).

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares establece principios para la recopilación, procesamiento y almacenamiento de datos personales, obligando a las entidades a obtener consentimiento y garantizar la seguridad de los datos (LFPDPPP, 2010).

La Ley Federal de Telecomunicaciones y Radiodifusión regula las telecomunicaciones y radiodifusión, promoviendo la competencia y accesibilidad en el ámbito digital. Establece la base para la Estrategia Digital Nacional (LFTR, 2014).

El Código Penal Federal incluye disposiciones sobre delitos cibernéticos, penalizando el acceso no autorizado a sistemas informáticos y otros delitos digitales. Sin embargo, la palabra **ciberespacio** no aparece en dicho precepto legal (CPF, 1931).

La Ley de Seguridad Nacional define principios y acciones para proteger la seguridad interior y soberanía nacional, pero no menciona la ciberseguridad (LSN, 2005). El Artículo 5 identifica amenazas a la seguridad nacional, algunas de las cuales pueden incluir ataques cibernéticos.

Ejemplos de ataques cibernéticos que pudieran caer en los supuestos de esta ley incluyen el ataque a la Comisión Nacional del Agua (CONAGUA) en 2023 y el hackeo a la Secretaría de la Defensa Nacional (SEDENA), que expuso información altamente sensible de dicha institución (BBC News Mundo, 2022; Bravo, 2023).

En cuanto a la actualización este marco jurídico, existen iniciativas de ley en ciberseguridad, como la Ley Federal de Ciberseguridad (LFC, 2023) y la Ley Nacional de Seguridad en el Ciberespacio (LSNC, 2020), que buscan desarrollar políticas nacionales de ciberseguridad y enfrentar riesgos en el ciberespacio.

Además, han existido estrategias gubernamentales como la Estrategia Nacional de Ciberseguridad (2018) y la Estrategia Digital Nacional 2021-2024 abordan la ciberseguridad, aunque con críticas por su enfoque y austeridad (José Otero, 2021).

En cuanto a la IA, se han propuesto varias iniciativas de ley como la Ley de Regulación Ética de la Inteligencia Artificial y la Robótica (LREIAEUM, 2023), la Ley para la Agencia Mexicana para el Desarrollo de la Inteligencia Artificial (LAMDIA, 2023), y la Ley Federal que regula la Inteligencia Artificial (Riquelme, 2024). Al momento de la redacción de este artículo, ninguna de las iniciativas mencionadas han sido aprobadas.

Definición y principios de la inteligencia artificial

Definiciones en el ámbito académico y práctico

John McCarthy[7] definió originalmente la IA en 1956 como "la ciencia y la ingeniería de crear máquinas inteligentes, especialmente programas de computadora inteligentes" (John McCarthy, 2007). La IA abarca diversas ramas y aplicaciones, y es usada hoy día en diversos aspectos aspectos en la industria, la informática, e incluso en el transporte.

En la práctica, la IA se manifiesta en sistemas que pueden aprender, adaptarse y ejecutar tareas de manera autónoma, desde algoritmos básicos hasta complejas redes neuronales capaces de tomar decisiones y resolver problemas sin intervención humana directa.

Evolución histórica de la IA

En 1950, Alan Turing[8] propuso la Prueba de Turing para evaluar si una máquina puede mostrar inteligencia humana. Marvin Minsky y John McCarthy pioneros en esa misma década fundanron el MIT AI Lab. En las décadas de 1960 y 1970 se enfrentaron desafíos y períodos de escepticismo conocidos como "inviernos de IA" (Gold, 2023). Ya en los años 90, IBM desarrolló Deep Blue, que derrotó al campeón mundial de ajedrez Gary Kasparov, mostrando avances en procesamiento de IA (Anyoha, 2017). Desde la década de 2000, el enfoque en el aprendizaje automático y el aprendizaje profundo ha transformado la IA. Desarrollos como AlexNet en 2012 revolucionaron la visión por computadora, y sistemas avanzados como GPT-4 de OpenAI representan una nueva era en la comprensión del lenguaje natural (Ferrer-Bonsoms Cruz, 2023).

7 John McCarthy fue un influyente científico de la computación y pionero en la materia. Su relevancia radica en ser el creador del término "inteligencia artificial" y en su contribución al desarrollo de los fundamentos teóricos y algoritmos clave en este campo. Su trabajo sentó las bases para la investigación y el avance continuo de la inteligencia artificial.

8 Matemático británico y pionero en la ciencia de la computación. Jugó un papel clave en descifrar los códigos Enigma durante la Segunda Guerra Mundial y es conocido por la Prueba de Turing, un método para evaluar la inteligencia de una máquina. Su trabajo sentó las bases de la computación moderna y la inteligencia artificial.

El desarrollo exponencial de la capacidad de procesamiento y el acceso a grandes volúmenes de datos en la ultima década, han permitido avances en el aprendizaje profundo[9], que imita la red neuronal del cerebro humano para procesar datos y generar patrones para la toma de decisiones. Herramientas como ChatGPT[10] son ahora de uso cotidiano en escuelas y centros de trabajo, así como los autos de conducción autónoma que circulan en diversas ciudades del mundo, sistemas que no serian posibles sin la IA.

Diferenciación de la IA con tecnologías y conceptos afines

Es importante distinguir la IA de otras tecnologías. La "automatización" se refiere al uso de sistemas para realizar tareas humanas, pero no siempre implica IA. El "aprendizaje automático", una subdisciplina de la IA, permite a los sistemas aprender y mejorar sin programación explícita. Aunque central en la IA contemporánea, no abarca todas sus aplicaciones. La "robótica" se enfoca en el diseño y funcionamiento de robots, que pueden incorporar IA para procesar información y tomar decisiones. La IA es un componente de la robótica cuando se utiliza para aprender de las interacciones con el entorno (Russel & Norvig, 2009).

Definiciones adicionales de la IA: Suave y general

Existen dos categorías primordiales de IA: la "IA suave" y la "IA general". La "IA suave" aborda problemas específicos y limitados sin pretender replicar todas las capacidades cognitivas humanas (por ejemplo, la conducción de un vehículo). La "IA general" o Inteligencia Artificial General (IAG) aspira a desarrollar sistemas con capacidad cognitiva equiparable o superior a la humana, capaces de realizar cualquier tarea intelectual que un ser humano pueda llevar a cabo (Fjelland, 2020).

Ejemplos de aplicaciones en diferentes sectores

La IA se ha convertido en una herramienta transformadora en varios sectores:

- Salud: La IA es esencial en el diagnóstico, personalización de tratamientos y análisis de imágenes médicas, alcanzando precisión comparable, y a veces superior a la de especialistas humanos (Arenas, 2021).
- Finanzas: La IA mejora el análisis de riesgos, detección de fraudes y automatización de procesos, optimizando estrategias de inversión (Tello, 2023).
- Transporte: Clave en el desarrollo de vehículos autónomos, utiliza sensores y algoritmos para una navegación segura (Lewis et al., 2021).

9 El deep learning, o aprendizaje profundo, es un subcampo del aprendizaje automático que utiliza redes neuronales artificiales con varias capas (profundas) para modelar complejidades en datos de alta dimensión.
10 ChatGPT es un modelo de lenguaje desarrollado por la empresa OpenAI que utiliza inteligencia artificial para comprender y generar texto basado en la entrada que recibe. Es capaz de mantener conversaciones, responder preguntas, proporcionar explicaciones, redactar textos y realizar muchas otras tareas relacionadas con el lenguaje natural.

- Comercio y servicio al cliente: La IA ha mejorado la experiencia del cliente con chatbots[11] y sistemas de recomendación personalizada (Ullerup, 2023).
- Seguridad y vigilancia: Utilizada en el análisis de video, detección de actividades sospechosas y ciberseguridad para detectar y responder a amenazas (Elliott & Soifer, 2022).
- Militar: Desarrolla sistemas de vigilancia avanzados, drones autónomos y optimiza la logística y estrategias de combate, mejorando la toma de decisiones en conflictos (Cox, 2021).
- Estos ejemplos destacan la capacidad de la IA para mejorar procesos y abrir nuevas oportunidades en diversos sectores, desde la salud hasta la seguridad y el comercio.

Liderazgo global en el desarrollo de la IA

La "Carrera" global por la IA

La competencia global por el liderazgo en la IA es un aspecto dinámico y estratégico en el ámbito tecnológico y geopolítico contemporáneo. Esta carrera abarca avances científicos, tecnológicos, económicos, militares e influencias globales, haciendo de la IA un elemento esencial para el desarrollo y la seguridad nacional.

Principales países y entidades líderes en IA

Estados Unidos ha mantenido un liderazgo destacado en la IA, siendo hogar de Silicon Valley[12] y de prestigiosas universidades y empresas tecnológicas como Google, Apple, Facebook y Microsoft. Estas empresas dominan el mercado de IA y lideran la investigación y el desarrollo, con el apoyo del gobierno estadounidense que reconoce la IA como esencial para la seguridad nacional y económica (Lynner Parker, 2020).

China ha emergido como el principal competidor en la carrera por la supremacía en IA, con ambiciosas iniciativas para superar a Estados Unidos para el año 2030. Empresas como Alibaba, Tencent y Baidu lideran la investigación y aplicación de la IA en China, respaldadas por el gobierno con financiamiento y políticas favorables (Manning, 2023).

La Unión Europea adopta un enfoque regulado y ético, destacándose por su énfasis en la IA responsable y el respeto a la privacidad y derechos humanos. La Comisión Europea propone regulaciones para alinear el desarrollo de la IA con estos valores (European Parliament, 2023c).

11 Es un programa de software diseñado para simular conversaciones con usuarios humanos, especialmente a través de Internet. Utiliza la inteligencia artificial para responder preguntas y asistir en tareas, a menudo implementado en sitios web, aplicaciones y plataformas de mensajería.
12 Región en el área de la Bahía de San Francisco, California, conocida como un importante centro de innovación tecnológica y sede de muchas empresas de tecnología y startups. Es famoso por su papel crucial en el desarrollo de la industria de alta tecnología desde la segunda mitad del siglo XX

Otros actores globales, como el Reino Unido, Canadá, Japón y Corea del Sur, también contribuyen significativamente al campo de la IA, desarrollando tecnologías avanzadas y estableciendo marcos regulatorios y políticas para promover el desarrollo ético y sostenible de esta tecnología (Sears, 2023).

La competencia global por la IA refleja su importancia en las estrategias nacionales, llevando a inversiones en investigación y desarrollo, políticas específicas y alianzas estratégicas para fortalecer su posición en el escenario mundial.

El papel de méxico en la IA

Estado actual de la IA en México

México no ocupa una posición líder en el desarrollo de la IA a nivel global, ni siquiera en América Latina. Según el Índice de Preparación del Gobierno para la IA 2023, México se sitúa en el lugar 68 a nivel mundial y 8° en América Latina (Hankins et al., 2023). Sin embargo, ha comenzado a reconocer la relevancia de la IA en el crecimiento económico y social, observándose esfuerzos en el ámbito público y privado para integrar estas tecnologías.

Iniciativas gubernamentales, académicas y del sector privado

La Estrategia IA-MX 2018 posicionó a México como uno de los primeros diez países en adoptar una estrategia formal para el desarrollo de la IA, fruto de la colaboración entre el gobierno, empresas de tecnología y la academia (Gobierno de México, 2018). Esta estrategia se centró en un marco de gobernanza, identificación de usos de la IA en la industria y el impulso al liderazgo internacional de México. Sin embargo, con el cambio de gobierno en 2018, la prioridad se desplazó hacia la infraestructura y conectividad, dejando la estrategia de IA en un segundo plano (Zamarrón, 2023).

En junio de 2020, México, junto con otros países, fundó la Alianza Global sobre la Inteligencia Artificial (AGIA), una iniciativa internacional para guiar el desarrollo y uso responsable de la IA. En el ámbito académico, universidades y centros de investigación como el ITESM y la UNAM lideran proyectos innovadores y colaboraciones internacionales, contribuyendo significativamente al avance de la IA en México (Doddoli, 2023; González, 2019).

El sector privado también muestra un creciente interés en la IA, con empresas y startups[13] incorporando soluciones basadas en IA en sus operaciones y servicios, reflejando un aumento significativo de inversiones en tecnologías afines (Castellanos, 2023).

13 Extranjerismo usado para denominar a una empresa de reciente creación y de base tecnológica.

El futuro de la inteligencia artificial y la perspectiva de la IA general

Hacia la Inteligencia Artificial General

El futuro de la IA es incierto pero prometedor. Una meta ambiciosa es el desarrollo de la Inteligencia Artificial General, capaz de comprender, aprender y aplicar su inteligencia a una amplia gama de tareas, superando la capacidad humana. La IAG se destacaría por su versatilidad y adaptabilidad, aplicándose a cualquier problema intelectual y colaborando efectivamente con humanos.

Sin embargo, la creación de una IAG plantea desafíos significativos en términos de seguridad y control, requiriendo garantías de que actúe de manera segura y alineada con los valores humanos. La IAG podría transformar el mercado laboral y la estructura socioeconómica, necesitando una revisión de los sistemas educativos, laborales y de bienestar social. En el ámbito ético, la IAG desafiará las concepciones actuales sobre la ética aplicable a la IA (Burrows, 2021; Fjelland, 2020).

Para la seguridad nacional, la transición hacia la IAG exigirá un enfoque proactivo en formación de capacidades, legislación y adaptación social y económica. La IAG podría ofrecer avances en inteligencia, defensa y gestión de crisis, pero también presentar nuevos desafíos en ciberseguridad y equilibrio geopolítico. La anticipación y manejo estratégico de estas innovaciones serán clave para aprovechar sus beneficios y mitigar sus riesgos.

Inteligencia artificial, antagonismos y afectaciones a la Seguridad Nacional

El desarrollo e integración de la inteligencia artificial en el ámbito de la seguridad nacional constituyen uno de los desafíos más significativos para las naciones en el siglo XXI. La teoría del poder blando de Joseph S. Nye, mencionada anteriormente, es fundamental para entender las dinámicas actuales de seguridad nacional e internacional, subrayando la importancia de persuadir y atraer más que coaccionar.

Actores mundiales ante la Inteligencia Artificial

Estados Unidos de América

Estados Unidos de América, en sus documentos estratégicos de IA ((U. S. Government Accountability Office, 2021) y (National Security Commission on Artificial Intelligence, 2021)) aborda los antagonismos de ésta con un enfoque regulatorio sólido, estableciendo normativas claras para guiar su implementación y uso, especialmente en contextos de alto riesgo. La seguridad nacional es un campo de especial interés, con la IA convirtiéndose en una herramienta vital en la estrategia de defensa, generando inquietudes sobre su posible uso indebido por competidores estratégicos.

Se presta atención a los derechos humanos y la privacidad, considerando los riesgos de vigilancia excesiva y sesgo en los sistemas de IA. También se examina el impacto de la IA en la economía y el mercado laboral, reconociendo su potencial para transformar estos ámbitos y provocar el desplazamiento de trabajadores.

La cooperación internacional y la competencia global son manejadas con cautela, con Estados Unidos esforzándose por mantener su liderazgo mientras maneja la competencia global, especialmente con China. Se enfatiza un desarrollo ético de la IA, promoviendo prácticas justas y transparentes, y preservando el control humano sobre los sistemas críticos de IA.

Esta estrategia holística equilibra los beneficios potenciales de la IA con una conciencia clara de los riesgos asociados, incluyendo políticas internas detalladas y participación activa en iniciativas y acuerdos internacionales para modelar un futuro seguro y ético para la IA.

Organización del Tratado del Atlántico Norte (OTAN)

La OTAN, aborda en (Stanley-Lockman & Christie, 2021), (NATO, 2023) y (NATO, 2021)) los antagonismos de la IA con un enfoque decidido en la seguridad y defensa, reconociendo su potencial para redefinir el concepto de guerra. La inclusión de la IA abarca desde la automatización de funciones rutinarias hasta análisis complejos para reforzar operaciones de combate. La adquisición y desarrollo de tecnologías de IA presentan desafíos en sistemas capaces de ejecutar operaciones complejas y de alto riesgo en contextos bélicos. Se requiere una consideración ética y legal cuidadosa, además de recursos computacionales avanzados.

La OTAN vigila el posible mal uso de la IA por competidores como China y Rusia, evaluando y mitigando riesgos para asegurar un empleo ético y conforme al derecho internacional. Organiza ejercicios de ciberdefensa y promueve principios de transparencia, trazabilidad y gobernanza en la IA, preparándose para enfrentar desafíos y riesgos asociados.

Unión Europea (UE)

La UE aborda en ((European Parliament, 2023b) y (European Parliament, 2023a)) la IA desde una perspectiva holística, buscando equilibrar sus beneficios con la mitigación de riesgos. Ha establecido el Acta de IA, un marco regulatorio pionero que clasifica los sistemas de IA según el nivel de riesgo. Este enfoque regula desde riesgos inaceptables hasta riesgos limitados.

La UE protege derechos y libertades fundamentales, asegurando que el desarrollo y uso de la IA respeten la privacidad, protección de datos, transparencia y no discriminación. Se enfoca en la aplicación de la IA en la prevención del crimen y el sistema de justicia penal.

La UE adapta la formación y educación para preparar a las generaciones futuras ante los cambios tecnológicos. Promueve un desarrollo ético de la IA y fomenta la cooperación internacional, estableciéndose como un actor clave en la promoción de un uso ético y seguro de la IA.

China

China adopta un enfoque multifacético hacia la IA, combinando esfuerzos regulatorios gubernamentales con innovación industrial y colaboración global. Desarrolla un marco regulatorio robusto, enfatizando la seguridad y responsabilidad en la evolución de la IA.

China lanzó la Iniciativa Global de Gobernanza de la IA (GAIGI), promoviendo un entorno de desarrollo abierto y equitativo. El gobierno chino destaca los intereses colectivos sobre los individuales, especialmente en decisiones algorítmicas y protección de datos, con amplias facultades para utilizar información ciudadana en beneficio de la seguridad pública.

Industria y academia promueven una IA ética, con empresas y startups impulsando autorregulación e investigación en ética de la IA. Este enfoque equilibra la ambición tecnológica con la prudencia regulatoria, buscando integrar la IA de manera responsable y beneficiosa para el bien común.

Desde la perspectiva estadounidense, se observa que China utiliza sus iniciativas en América Latina para avanzar en sus objetivos estratégicos y obtener ventajas económicas, políticas y militares, buscando liderar en tecnología de IA. La presencia de tecnología china de IA en la región es notable, contrastando con una menor adopción de tecnología estadounidense. Aunque Estados Unidos tiene ventajas en el desarrollo de IA, existe el riesgo de perder influencia en el mercado latinoamericano y caribeño, lo que afectaría su seguridad nacional a largo plazo. Para mantener su posición, Estados Unidos debería mejorar las capacidades de la región en seguridad y fortalecer la colaboración con el sector privado, la academia y las instituciones de seguridad (Andres, 2021).

Para el estudio de la visión de la República Popular China, se analizó a (Yang, 2024), (Kuo, 2024), (Tiezzi, 2023), (Arcesati, 2021) y (China Government, 2023).

Brasil

Brasil, el país más preparado en la materia de América latina, está definiendo su enfoque frente a la IA, centrándose en crear un entorno legal propicio para su desarrollo responsable. Avanza hacia una legislación específica, destacando proyectos como el nº 21/2020, que establece derechos y responsabilidades en el uso de la IA, abordando cuestiones éticas como privacidad y no discriminación.

Brasil promueve una Estrategia Brasileña de IA, estableciendo principios éticos y estimulando la investigación e innovación. Adapta programas educativos para preparar a las generaciones futuras ante los cambios tecnológicos.

Este enfoque holístico refleja el compromiso de Brasil con un marco regulatorio que tenga en cuenta los impactos sociales y éticos de la IA, avanzando hacia una comprensión y aplicación responsable de esta tecnología.

Se revisó a (Coordenação de Comissões Especiais, Temporárias e & Parlamentares de Inquérito, 2022), (Shimoda Uechi & Guimarães Moraes, 2023), (Roman, 2021) y (Ministry of Science, Technology and innovations. Brasil, 2021) para esta redactar esta información.

Análisis de antagonismos a la Seguridad Nacional mexicana causados por la IA

Del estudio de la historia, alcances y efectos de la IA en las estrategias de los cinco entes del derecho internacional previamente mencionados, se pueden dilucidar los posibles antagonismos que se han generado y se generaran por la introducción de esta tecnología en nuestra sociedad.

Los antagonismos en seguridad nacional son obstáculos o interferencias que pueden originarse por acciones de Estados, agentes no estatales o eventos naturales y antropogénicos. Se dividen en riesgos (sin intención hostil) y amenazas (con intención hostil), además de desafíos que requieren medidas específicas sin encajar en las dos categorías anteriores. Esta clasificación ayuda a desarrollar estrategias de respuesta y mitigación (CODENAL & CESNAV, 2018).

Los campos del poder, que incluyen los ámbitos político, económico, social, militar, tecnológico y diplomático, son componentes fundamentales del poder nacional de un Estado. La interconexión de estos campos permite coordinar acciones efectivas para preservar la soberanía, integridad y desarrollo del país (CODENAL & CESNAV, 2018).

Principales hallazgos

En un análisis de los antagonismos causados por la IA en diversos ámbitos de la seguridad nacional, se logró una clasificación meticulosa de los mismos, agrupándolos en categorías validadas por un panel de expertos (Toledo, 2024). Estas categorías reflejan los principales retos y áreas de afectación significativas, abarcando ciberseguridad, manipulación social y política, economía, geopolítica y aspectos sociales y éticos. Hallándose 52 antagonismos: amenazas (22), riesgos (07) y desafíos (23), los cuales están distribuidos en todos los campos del poder de la siguiente manera:

- Campo diplomático: 9 antagonismos, destacando complejidades en relaciones internacionales.

- Campo económico: 10 antagonismos, resaltando alteraciones en mercados y dinámicas laborales.
- Campo militar: 8 antagonismos, subrayando retos en seguridad y defensa.
- Campo político: 9 antagonismos, reflejando tensiones en gobernanza.
- Campo social: 9 antagonismos, impactando la cohesión social y derechos humanos.
- Campo tecnológico: 7 antagonismos, evidenciando preocupaciones en innovación, privacidad y ética.

Ademas, se categorizaron los antagonismos identificados y su relevancia en el entorno de seguridad nacional de acuerdo al tipo de afectación que provocan:

- Ciberseguridad y Ciberguerra**:** Esta categoría aborda los retos asociados con la seguridad en el espacio digital, incluyendo ataques cibernéticos avanzados y vulnerabilidades en sistemas críticos potenciados por la IA, que afectan tanto infraestructuras militares como civiles.
- Desinformación, Manipulación Social y Política**:** Considera los desafíos relacionados con el uso de la IA para influir o manipular la opinión pública, las decisiones políticas y la cohesión social, lo que incluye la polarización política y la propagación de desinformación.
- Laborales y Económicos**:** Incluye los efectos de la IA en el mercado laboral y la economía, tales como el desplazamiento laboral, las desigualdades económicas, y los desafíos en la dependencia tecnológica y la fuga de capitales.
- Innovación y Educación**:** Se refiere a los retos que enfrentan la innovación tecnológica y la educación ante la rápida evolución de la IA, incluida la necesidad de capacitación y ajustes en los sistemas educativos.
- Privacidad y Ética**:** Aborda las implicaciones éticas y los riesgos para la privacidad derivados del uso de la IA, con especial atención a la protección de datos personales y las consideraciones morales en su aplicación.
- Impacto Cultural y de Identidad**:** Examina cómo la IA puede influir en la identidad cultural, las relaciones sociales y la salud mental, resaltando la importancia de preservar los valores culturales ante la influencia tecnológica.
- Tecnológicos y Dependencia**:** Enfoca los retos tecnológicos específicos y la dependencia de tecnologías extranjeras, así como los desequilibrios en el desarrollo tecnológico entre diferentes sectores.

- Geopolítica y Proteccionismo**:** Analiza el impacto de la IA en las dinámicas geopolíticas y el proteccionismo tecnológico, considerando las presiones económicas y la competencia global en el desarrollo y adopción de la IA.

Escenarios de afectación de las amenazas ocasionadas por la IA a los campos del poder Nacional

A continuación se muestran escenarios hipotéticos para cada uno de los campos del poder, mostrando, por simplicidad, solo el impacto o afectación que pudieran tener en la Nación los antagonismos del tipo "amenaza".

Escenario: Campo Diplomático de México

México se enfrenta a una crisis diplomática debido al uso malintencionado de inteligencia artificial por parte de actores estatales y no estatales.

- Espionaje y Vigilancia Internacional: Un país extranjero usa IA para espiar y obtiene información confidencial de México, ocasionando un escándalo diplomático, deterioro de la confianza y afectación de tratados bilaterales.
- Desinformación y Guerra de Información: Campañas de desinformación potenciadas por IA desacreditan al gobierno mexicano, provocando protestas internas, cuestionamiento internacional de la estabilidad y disminución de inversiones.
- Falsa Atribución de Ciberataques: Un ciberataque en un país vecino se atribuye falsamente a México, lo que ocasiona un aumento de la presión diplomática, afectación de relaciones regionales y riesgo de aislamiento.

Escenario: Campo Económico de México

México enfrenta una crisis económica exacerbada por el mal uso de la inteligencia artificial.

- Ataques Cibernéticos Potenciados por IA: Una serie de ciberataques sofisticados, potenciados por IA, golpea las infraestructuras críticas de México, incluyendo el sector financiero, energético y de telecomunicaciones, hay interrupciones significativas en los servicios básicos, caos en el sector financiero y una desaceleración económica generalizada.
- Desinformación y Manipulación de Datos: Campañas de desinformación, utilizando IA, siembran dudas sobre la estabilidad económica y la integridad de las empresas mexicanas. Se toman decisiones empresariales erróneas, aparece pérdida de confianza pública y disminución de las inversiones extranjeras.

- Inestabilidad en los Mercados Financieros: Algoritmos de IA, manipulados por actores malintencionados, causan fluctuaciones impredecibles en los mercados financieros de México, ocasionando pérdidas significativas para los inversores, volatilidad económica y una mayor incertidumbre en el mercado.
- Manipulación Extranjera a través de IA: Actores extranjeros utilizan IA para influir en decisiones económicas nacionales, como la política fiscal y la regulación de industrias clave. Se toman decisiones económicas desfavorables para el país, existe afectación de la soberanía económica y presión política interna.
- Robo de Propiedad Intelectual y Espionaje Empresarial: Empresas mexicanas son víctimas de espionaje cibernético y robo de propiedad intelectual, realizado mediante técnicas avanzadas de IA. Se pierde la competitividad e innovación, existe disminución de la confianza de los inversores y una caída en el desarrollo tecnológico nacional.

Escenario: Campo Militar de México

México enfrenta una crisis militar potenciada por el uso malintencionado de inteligencia artificial.

- Ciberataques Avanzados Potenciados por IA: Infraestructuras militares críticas de México son atacadas por sofisticados ciberataques potenciados por IA. Estos ataques comprometen sistemas de comunicaciones y logística, paralizando operaciones clave. Se interrumpen las operaciones militares, hay pérdida de información confidencial y debilitamiento de la capacidad de respuesta militar.
- Guerra Híbrida y Asimétrica: Actores estatales y no estatales utilizan IA para llevar a cabo tácticas de guerra híbrida y asimétrica, incluyendo ataques cibernéticos, desinformación y operaciones encubiertas. Hay dificultad para identificar y responder a los actores responsables, aumento de la complejidad en las operaciones militares y riesgo de escalada del conflicto.
- Automatización en el Campo de Batalla: Sistemas autónomos y drones guiados por IA son desplegados en zonas de conflicto. Estos sistemas enfrentan problemas operativos y toman decisiones autónomas en situaciones de combate. Surgen desafíos éticos y operacionales, potenciales fallos en misiones críticas y controversias sobre el uso de armas autónomas.
- Vulnerabilidad a la Inteligencia Adversaria: Adversarios utilizan técnicas avanzadas de IA para espiar y comprometer sistemas militares mexicanos, obteniendo acceso a información sensible y estrategias militares. Esto provoca un aumento de la vulnerabilidad de las operaciones militares, riesgo de filtración de información estratégica y debilitamiento de la seguridad nacional.
- Desinformación y Guerra Psicológica: Campañas de desinformación, potenciadas por IA, se dirigen a las fuerzas armadas mexicanas y al público en general, con el objetivo de socavar la moral y crear

confusión. Existe disminución de la moral de las fuerzas armadas, erosión de la confianza pública en las instituciones militares y dificultades en la gestión de crisis.

Escenario: Campo Político de México

México se encuentra en una situación de crisis política debido al uso perverso de la inteligencia artificial.

- Polarización y Manipulación Política**:** La IA es utilizada para amplificar campañas de desinformación que afectan la opinión pública y provocan una creciente polarización política, resultando en protestas y una creciente desconfianza hacia el gobierno.
- Vulnerabilidades en Procesos Electorales: Durante las elecciones nacionales, la IA es empleada para manipular los resultados, socavando la integridad y confianza en el sistema electoral mexicano, lo que lleva a una crisis de legitimidad y demandas de anulación de la elección.
- Influencia en la Toma de Decisiones Políticas: La dependencia del gobierno en sistemas de IA para la toma de decisiones políticas introduce sesgos y falta de transparencia, lo que genera controversias y acusaciones de parcialidad en las políticas implementadas.
- Ataques Cibernéticos a Infraestructuras Gubernamentales: Ciberataques dirigidos a infraestructuras críticas gubernamentales, potenciados por IA, buscan desestabilizar las operaciones gubernamentales, causando interrupciones en servicios públicos esenciales y disminuyendo la eficiencia del gobierno.
- Guerra de Información y Propaganda Extranjera: Actores extranjeros utilizan IA para llevar a cabo una guerra de información, influenciando la política interna mexicana mediante desinformación y propaganda, exacerbando divisiones sociales y políticas.
- Espionaje Político Potenciado por IA: El espionaje extranjero a través de técnicas avanzadas de IA compromete la seguridad y soberanía nacionales al obtener información confidencial sobre estrategias y decisiones políticas mexicanas.

Escenario: Campo Social de México

México enfrenta una crisis social provocada por el uso de inteligencia artificial que afecta profundamente la cultura, los valores colectivos y la privacidad de los individuos.

- Manipulación de Comportamientos y Opiniones: La IA se utiliza para influir y manipular opiniones sociales mediante campañas dirigidas en redes sociales. Algoritmos avanzados crean contenido personalizado que polariza a la sociedad y erosiona los valores colectivos. La desinformación

amplificada por IA cambia percepciones y comportamientos, debilitando la cohesión social y generando conflictos culturales.

- Pérdida de Privacidad y Autonomía: La recopilación y análisis masivo de datos personales por IA erosiona la privacidad y autonomía individual. Empresas y entidades gubernamentales monitorean y predicen comportamientos, creando una sensación de vigilancia constante. Esto lleva a abusos de poder y decisiones automatizadas que afectan la vida diaria, generando desconfianza en las instituciones y promoviendo un clima de miedo.

Escenario: Campo Tecnológico de México

México se enfrenta a una crisis tecnológica debido a las vulnerabilidades en seguridad cibernética que surgen con la adopción de tecnologías avanzadas.

- Vulnerabilidades y Seguridad Cibernética**:** Con la rápida adopción de tecnologías avanzadas en múltiples sectores, México experimenta un aumento significativo en los ataques cibernéticos. Los ciberdelincuentes y actores estatales malintencionados aprovechan las vulnerabilidades en los sistemas tecnológicos para lanzar ataques sofisticados que comprometen datos sensibles y sistemas críticos. Estos ataques afectan desde infraestructuras críticas como la energía y las telecomunicaciones hasta servicios financieros y de salud. Las brechas de seguridad resultan en la interrupción de servicios esenciales, pérdidas financieras sustanciales y una disminución de la confianza pública en las capacidades tecnológicas del país.

  Estos escenarios, aunque hipotéticos, son posibles y, en algunos casos, ya están ocurriendo en mayor o menor medida en otras regiones del mundo. México deberá analizar estos antagonismos y actuar en consecuencia para proteger sus intereses nacionales y garantizar su seguridad y estabilidad en la era de la inteligencia artificial.

  En resumen, estos escenarios resaltan la necesidad de que México adopte un enfoque proactivo y estratégico para enfrentar las amenazas emergentes asociadas con la inteligencia artificial. La implementación de políticas y estrategias adecuadas, la inversión en tecnología y ciberseguridad, y la colaboración internacional serán esenciales para proteger la seguridad nacional y garantizar un futuro seguro y próspero a futuro.

CONCLUSIONES

A lo largo de este ensayo, hemos explorado la profunda influencia de la inteligencia artificial en la seguridad nacional, no solo de México, sino también de otros entes del orbe, destacando los múltiples antagonismos que surgen de su integración en diversos campos del poder nacional. La IA, como herramienta es poderosa y disruptiva, presenta tanto oportunidades significativas como amenazas potencialmente devastadoras,

especialmente en términos de ciberseguridad, desinformación y manipulación social y política, impactos económicos, y desafíos éticos y de privacidad.

En el ámbito de la ciberseguridad, la IA ha incrementado la sofisticación y frecuencia de los ataques cibernéticos, exponiendo vulnerabilidades críticas en infraestructuras esenciales como la energía, telecomunicaciones, servicios financieros y de salud. Estos ataques no solo generan pérdidas económicas y operativas, sino que también minan la confianza pública en las capacidades tecnológicas del país.

La desinformación y manipulación social son otros antagonismos destacados. La IA se utiliza para amplificar campañas de desinformación, polarizando a la sociedad y erosionando la cohesión social. Este fenómeno es especialmente peligroso en el contexto político, donde la manipulación de la opinión pública puede desestabilizar gobiernos y afectar la gobernabilidad.

En el ámbito económico, la IA plantea desafíos significativos, como el desplazamiento laboral y la exacerbación de las desigualdades económicas. La automatización y la dependencia tecnológica pueden llevar a una mayor concentración de capital y poder en manos de unos pocos, aumentando las brechas sociales y económicas.

A nivel ético y de privacidad, la IA plantea dilemas cruciales sobre la protección de datos personales y la moralidad en su aplicación. La recopilación y análisis masivo de datos pueden llevar a abusos de poder y a una vigilancia constante que erosiona la autonomía individual y la privacidad.

La intersección de estos antagonismos destaca la necesidad urgente de continuar investigando y desarrollando políticas efectivas en el ámbito de la IA. México debe invertir en tecnología y ciberseguridad, fomentar la educación y capacitación en la materia, y promover la cooperación internacional para establecer normas y mejores prácticas que mitiguen las amenazas transfronterizas.

El desarrollo de estrategias holísticas y colaborativas es esencial para navegar los desafíos que plantea la IA. Esto incluye la formulación de marcos normativos que equilibren la innovación con la protección de derechos y la seguridad nacional, y la adaptación de los sistemas educativos y laborales para preparar a la fuerza laboral ante los cambios tecnológicos.

En conclusión, la inteligencia artificial representa un campo de batalla crítico para la seguridad nacional de México. La anticipación y el manejo estratégico de las innovaciones en IA serán claves para aprovechar sus beneficios y mitigar sus riesgos. Es imperativo que México adopte un enfoque proactivo y estratégico para enfrentar las amenazas emergentes asociadas con ella, garantizando un futuro seguro y próspero para todos

sus ciudadanos. La investigación continua y la formulación de políticas robustas no solo mejorarán nuestras capacidades, sino que también fortalecerán nuestra posición en el panorama global de la inteligencia artificial.

BIBLIOGRAFÍA

Andres, E. S. (2021). *United States National Security concerns with Chinese Artificial Intelligence Initiatives in Latin America*. NPS.

Anyoha, R. (2017, agosto 28). The History of Artificial Intelligence. *Science in the News*. https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/

Arcesati, R. (2021, junio 24). *Lofty principles, conflicting incentives: AI ethics and governance in China | Merics*. https://merics.org/en/report/lofty-principles-conflicting-incentives-ai-ethics-and-governance-china

Arenas, G. (2021, septiembre 10). *Inteligencia artificial al servicio de la medicina: Así ayuda a conseguir diagnósticos más certeros*. El País. https://elpais.com/sociedad/siempre-innovando/2021-09-10/inteligencia-artificial-al-servicio-de-la-medicina-asi-ayuda-a-conseguir-diagnosticos-mas-certeros.html

BBC News Mundo. (2022, septiembre 30). Qué se sabe de Guacamaya, el cibergrupo clandestino que reveló los problemas de salud de AMLO y ha robado secretos a varios de países de América Latina. *BBC News Mundo*. https://www.bbc.com/mundo/noticias-america-latina-63098421

Bostrom, N. (2017). *Superintelligence: Paths, dangers, strategies* (Reprinted with corrections 2017). Oxford University Press.

Bravo, J. (2023, abril 26). *La Cuarta Transformación está hackeada—Proceso* [Semanario]. Procesa. https://www.proceso.com.mx/opinion/2023/4/26/la-cuarta-transformacion-esta-hackeada-306042.html

Burns, R. N., & Price, J. (Eds.). (2012). *Securing cyberspace: A new domain for national security*. Aspen Institute.

Burrows, L. (2021, octubre 19). *The present and future of AI* [University]. Harvard School of Engineering. https://seas.harvard.edu/news/2021/10/present-and-future-ai

Castellanos, D. S. (2023, diciembre 20). *Startups en Latinoamérica: ¿qué esperar de la financiación y capital de riesgo en 2024?* Bloomberg Línea. https://www.bloomberglinea.com/2023/12/20/startups-en-latinoamerica-que-esperar-de-la-financiacion-y-capital-de-riesgo-en-2024/

China Government. (2023, octubre 24). *Global AI Governance Initiative*. Embassy of the People's Republic of China in Grenada. http://gd.china-embassy.gov.cn/eng/zxhd_1/202310/t20231024_11167412.htm

CODENAL & CESNAV. (2018). *Glosario de Términos Unificados de Seguridad Nacional*.

Código Penal Federal, 338 (1931). https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf

Constitución Política de los Estados Unidos Mexicanos, 361 (1917). https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

Coordenação de Comissões Especiais, Temporárias e & Parlamentares de Inquérito. (2022). *RELATÓRIO FINAL COMISSÃO DE JURISTAS RESPONSÁVEL POR SUBSIDIAR ELABORAÇÃO DE SUBSTITUTIVO SOBRE INTELIGÊNCIA ARTIFICIAL NO BRASIL* (p. 908).

https://legis.senado.leg.br/sdleg-getter/documento/download/777129a2-e659-4053-bf2e-e4b53edc3a04

Cox, D. G. (2021, junio). *Artificial Intelligence and Multi-Domain Operations*. Army University Press. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2021/Cox-AI-MDO/

Cueto, J. C. (2023, abril 17). La extensión del espionaje y manipulación que TikTok realiza es igual a la de Facebook. *BBC News Mundo*. https://www.bbc.com/mundo/noticias-65251036

Doddoli, C. (2023, marzo 29). *Inteligencia Artificial aplicada a la solución de problemas nacionales*. Ciencia UNAM. https://ciencia.unam.mx/leer/1390/inteligencia-artificial-aplicada-a-la-solucion-de-problemas-nacionales

Elliott, D., & Soifer, E. (2022). AI Technologies, Privacy, and Security. *Frontiers in Artificial Intelligence*, *5*. https://www.frontiersin.org/articles/10.3389/frai.2022.826737

European Parliament. (2023a). *Artificial intelligence Act* (PE 698.792; p. 12). https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf

European Parliament. (2023b, junio 20). *Artificial intelligence: Threats and opportunities*. https://www.europarl.europa.eu/topics/en/article/20200918STO87404/artificial-intelligence-threats-and-opportunities

European Parliament. (2023c, agosto 6). *EU AI Act: First regulation on artificial intelligence | News | European Parliament*. https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

Ferrer-Bonsoms Cruz, C. (2023, abril 26). *Qué es GPT-4: Funcionamiento, características, novedades y cómo puedes probar la IA más avanzada de OpenAI*. Business Insider España. https://www.businessinsider.es/gpt-4-ia-avanzada-openai-1225948

Fjelland, R. (2020). Why general artificial intelligence will not be realized. *Humanities and Social Sciences Communications*, *7*(1), Article 1. https://doi.org/10.1057/s41599-020-0494-4

Gobierno de México. (2018, marzo 22). *Estrategia de Inteligencia Artificial MX 2018 | Presidencia de la República*. https://www.gob.mx/epn/articulos/estrategia-de-inteligencia-artificial-mx-2018

Gold, E. (2023, abril 10). *The History of Artificial Intelligence from the 1950s to Today*. freeCodeCamp.Org. https://www.freecodecamp.org/news/the-history-of-ai/

González, C. (2019, noviembre 21). *Así será el innovador Hub de Inteligencia Artificial del Tec*. https://conecta.tec.mx/es/noticias/guadalajara/investigacion/asi-sera-el-innovador-hub-de-inteligencia-artificial-del-tec

Grace B. Mueller, Benjamin Jensen, Brandon Valeriano, Ryan C. Maness, & Jose M. Macias. (2023, julio 13). *Cyber Operations during the Russo-Ukrainian War*. Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war

Hankins, E., Fuentes Nettel, P., Martinescu, L., Grau, G., & Rahim, S. (2023). *2023 Government AI Readiness Index*. Oxford Insights.

Iniciativa de Ley Federal de Ciberseguridad (2023). https://www.diputados.gob.mx/LeyesBiblio/iniclave/65/CD-LXV-II-2P-292/02_iniciativa_292_25abr23.pdf

Iniciativa de Ley Nacional de Seguridad en el Ciberespacio (2020). http://sil.gobernacion.gob.mx/Archivos/Documentos/2020/10/asun_4093498_20201019_1603158505.pdf

Iniciativa de Ley para la Agencia Mexicana para el Desarrollo de la Inteligencia Artificial, 26 (2023). http://gaceta.diputados.gob.mx/PDF/65/2023/oct/20231011-II-3-1.pdf

Iniciativa de Ley para la Regulación Ética de la Inteligencia Artificial para los Estados Unidos Mexicanos (2023). http://sil.gobernacion.gob.mx/Archivos/Documentos/2023/04/asun_4543395_20230413_1680209417.pdf

John McCarthy. (2007, noviembre 12). *What is AI? / Basic Questions*. Stanford University. http://jmc.stanford.edu/artificial-intelligence/what-is-ai/index.html

José Otero. (2021, agosto 19). *Análisis de la Estrategia Digital Nacional 2021-2024*. El Economista. https://www.eleconomista.com.mx/opinion/Analisis-de-la-Estrategia-Digital-Nacional-2021-2024-20210819-0026.html

Kuo, M. A. (2024, enero 3). *China and Global Governance of AI*. https://thediplomat.com/2024/01/china-and-global-governance-of-ai/

Lewis, J. A., Lostri, E., & Cheng, C. (2021). *AI Strategies and Autonomous Vehicles Development*. https://www.csis.org/analysis/ai-strategies-and-autonomous-vehicles-development

Ley de Seguridad Nacional, 27 (2005). https://www.diputados.gob.mx/LeyesBiblio/pdf/LSN.pdf

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 18 (2010). https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Ley Federal de Telecomunicaciones y Radiodifusión, 173 (2014). https://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR.pdf

Lynner Parker. (2020, junio 11). *The American AI Initiative: The U.S. strategy for leadership in artificial intelligence*. https://oecd.ai/en/wonk/the-american-ai-initiative-the-u-s-strategy-for-leadership-in-rtificial-intelligence

Manning, C. (2023, octubre 17). *CODE WAR: How China's AI Ambitions Risk U.S. National Security American Security Project*. American Security Project. https://www.americansecurityproject.org/perspective-code-war-how-chinas-ai-ambitions-threaten-u-s-national-security/

Ministry of Science, Technology and innovations. Brasil. (2021). *Summary of the Brazilian Artificial Intelligence Strategy* (p. 16). https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-summary_brazilian_4-979_2021.pdf

National Cyber Security Index. (2021, junio 25). *Index*. National Cyber Security Index. https://ncsi.ega.ee/

National Security Commission on Artificial Intelligence. (2021). *NSCAI Final Report* (p. 756). National Security Commission on Artificial Intelligence. https://reports.nscai.gov/final-report/

NATO. (2021, octubre 22). *Summary of the NATO Artificial Intelligence Strategy*. NATO. https://www.nato.int/cps/en/natohq/official_texts_187617.htm

NATO. (2023, junio 22). *Emerging and disruptive technologies*. NATO. https://www.nato.int/cps/en/natohq/topics_184303.htm

Nicholas Confessore. (2018, abril 4). *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far—The New York Times* [Diario]. The New York Times. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Nye, J. S. (1990). *Bound to lead: The changing nature of American power*. Basic Books.

Nye, J. S. (2020, agosto 6). *El otro cambio de poder global | by Joseph S. Nye, Jr.* Project Syndicate. https://www.project-syndicate.org/commentary/new-technology-threats-to-us-national-security-by-joseph-s-nye-2020-08/spanish

PBS News. (2023, febrero 4). *Security expert warns of AI tools' potential threat to democracy | PBS News Weekend*. https://www.pbs.org/newshour/show/security-expert-warns-of-ai-tools-potential-threat-to-democracy

Riquelme, R. (2024, febrero 27). *Ricardo Monreal presenta iniciativa para regular la inteligencia artificial*. El Economista. https://www.eleconomista.com.mx/tecnologia/Ricardo-Monreal-presenta-iniciativa-para-regular-la-inteligencia-artificial-20240227-0055.html

Roman, J. (2021, octubre 5). *Artificial Intelligence in Brazil: The Brazilian Strategy for Artificial Intelligence (BSAI/EBIA) and Bill No. 21/2020*. IRIS-BH. https://irisbh.com.br/en/artificial-intelligence-in-brazil-the-brazilian-strategy-for-artificial-intelligence-bsai-ebia-and-bill-no-21-2020/

Russel, S., & Norvig, P. (2009). *Artificial Intelligence: A Modern Approach* (1a ed.). Pearson.

Sarah Cook. (2018, septiembre 28). *China's Cyber Superpower Strategy: Implementation, Internet Freedom Implications, and U.S. Responses | Freedom House*. Freedom House. https://freedomhouse.org/article/chinas-cyber-superpower-strategy-implementation-internet-freedom-implications-and-us

Schneier, B. (2016). *Data and Goliath: The hidden battles to collect your data and control your world* (First published as a Norton paperback 2016). W.W. Norton & Company.

Sears, J. (2023, diciembre 23). *TRAIN'—The AI Race Heats Up: Mapping the Emerging Geography of Innovation*. LinkedIn. https://www.linkedin.com/pulse/train-ai-race-heats-up-mapping-emerging-geography-innovation-sears-pxlre/

Setzer, M. G. J. (2022, junio). *The Cyber and Information Domain and the Space Domain: Links and Interdependencies—Joint Air Power Competence Centre*. Join Air power Competence Center. https://www.japcc.org/essays/the-cyber-and-information-domain-and-the-space-domain-links-and-interdependencies/

Shimoda Uechi, C. A., & Guimarães Moraes, T. (2023, julio 23). *Brazil's path to responsible AI*. https://oecd.ai/en/wonk/brazils-path-to-responsible-ai

Stanley-Lockman, Z., & Christie, E. H. (2021, octubre 25). *An Artificial Intelligence Strategy for NATO*. NATO Review. https://www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html

Tello, J. S. (2023, mayo 24). *El impacto de la IA en el mundo de las finanzas, un vistazo al futuro*. Expansión. https://expansion.mx/opinion/2023/05/24/el-impacto-de-la-ia-en-el-mundo-de-las-finanzas-un-vistazo-al-futuro

Tiezzi, S. (2023, noviembre 9). *China Renews Its Pitch on AI Governance at World Internet Conference*. https://thediplomat.com/2023/11/china-renews-its-pitch-on-ai-governance-at-world-internet-conference/

Toledo, R. (2024). *Las amenazas derivadas del uso de la inteligencia artificial y sus afectaciones a la seguridad nacional*. CESNAV.

U. S. Government Accountability Office. (2021). Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities | U.S. GAO (GAO-21-519SP; p. 112). U. S. Government Accountability Office. https://www.gao.gov/products/gao-21-519sp

Ullerup, A. (2023, noviembre 23). 7 ways AI revolutionises commerce and transforms customer experiences. IMPACT. https://impactcommerce.com/insights/7-ways-ai-revolutionises-commerce-and-transforms-customer-experiences/

Yang, Z. (2024, enero 17). Four things to know about China's new AI rules in 2024. MIT Technology Review. https://www.technologyreview.com/2024/01/17/1086704/china-ai-regulation-changes-2024/

Yudkowsky, E. (2008). Artificial Intelligence as a positive and negative factor in global risk. En E. Yudkowsky, Global Catastrophic Risks. Oxford University Press. https://doi.org/10.1093/oso/9780198570509.003.0021

Zamarrón, I. (2023, junio 6). Este 'think tank' quiere armar la estrategia de inteligencia artificial para el próximo presidente. Forbes México. https://www.forbes.com.mx/este-think-tank-quiere-armar-la-estrategia-de-inteligencia-artificial-para-el-proximo-presidente/

Andres, E. S. (2021). United States National Security concerns with Chinese Artificial Intelligence Initiatives in Latin America. NPS.

Anyoha, R. (2017, agosto 28). The History of Artificial Intelligence. Science in the News. https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/

Arcesati, R. (2021, junio 24). Lofty principles, conflicting incentives: AI ethics and governance in China | Merics. https://merics.org/en/report/lofty-principles-conflicting-incentives-ai-ethics-and-governance-china

Arenas, G. (2021, septiembre 10). Inteligencia artificial al servicio de la medicina: Así ayuda a conseguir diagnósticos más certeros. El País. https://elpais.com/sociedad/siempre-innovando/2021-09-10/inteligencia-artificial-al-servicio-de-la-medicina-asi-ayuda-a-conseguir-diagnosticos-mas-certeros.html

BBC News Mundo. (2022, septiembre 30). Qué se sabe de Guacamaya, el cibergrupo clandestino que reveló los problemas de salud de AMLO y ha robado secretos a varios de países de América Latina. BBC News Mundo. https://www.bbc.com/mundo/noticias-america-latina-63098421

Bostrom, N. (2017). Superintelligence: Paths, dangers, strategies (Reprinted with corrections 2017). Oxford University Press.

Bravo, J. (2023, abril 26). La Cuarta Transformación está hackeada—Proceso [Semanario]. Procesa. https://www.proceso.com.mx/opinion/2023/4/26/la-cuarta-transformacion-esta-hackeada-306042.html

Burns, R. N., & Price, J. (Eds.). (2012). Securing cyberspace: A new domain for national security. Aspen Institute.

Burrows, L. (2021, octubre 19). The present and future of AI [University]. Harvard School of Engineering. https://seas.harvard.edu/news/2021/10/present-and-future-ai

Castellanos, D. S. (2023, diciembre 20). Startups en Latinoamérica: ¿qué esperar de la financiación y capital de riesgo en 2024? Bloomberg Línea. https://www.bloomberglinea.com/2023/12/20/startups-en-latinoamerica-que-esperar-de-la-financiacion-y-capital-de-riesgo-en-2024/

China Government. (2023, octubre 24). Global AI Governance Initiative. Embassy of the People's Republic of China in Grenada. http://gd.china-embassy.gov.cn/eng/zxhd_1/202310/t20231024_11167412.htm

CODENAL & CESNAV. (2018). Glosario de Términos Unificados de Seguridad Nacional.

Código Penal Federal, 338 (1931). https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf

Constitución Política de los Estados Unidos Mexicanos, 361 (1917). https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

Coordenação de Comissões Especiais, Temporárias e & Parlamentares de Inquérito. (2022). RELATÓRIO FINAL COMISSÃO DE JURISTAS RESPONSÁVEL POR SUBSIDIAR ELABORAÇÃO DE SUBSTITUTIVO SOBRE INTELIGÊNCIA ARTIFICIAL NO BRASIL (p. 908). https://legis.senado.leg.br/sdleg-getter/documento/download/777129a2-e659-4053-bf2e-e4b53edc3a04

Cox, D. G. (2021, junio). Artificial Intelligence and Multi-Domain Operations. Army University Press. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2021/Cox-AI-MDO/

Cueto, J. C. (2023, abril 17). La extensión del espionaje y manipulación que TikTok realiza es igual a la de Facebook. BBC News Mundo. https://www.bbc.com/mundo/noticias-65251036

Doddoli, C. (2023, marzo 29). Inteligencia Artificial aplicada a la solución de problemas nacionales. Ciencia UNAM. https://ciencia.unam.mx/leer/1390/inteligencia-artificial-aplicada-a-la-solucion-de-problemas-nacionales

Elliott, D., & Soifer, E. (2022). AI Technologies, Privacy, and Security. Frontiers in Artificial Intelligence, 5. https://www.frontiersin.org/articles/10.3389/frai.2022.826737

European Parliament. (2023a). Artificial intelligence Act (PE 698.792; p. 12). https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf

European Parliament. (2023b, junio 20). Artificial intelligence: Threats and opportunities. https://www.europarl.europa.eu/topics/en/article/20200918STO87404/artificial-intelligence-threats-and-opportunities

European Parliament. (2023c, agosto 6). EU AI Act: First regulation on artificial intelligence | News | European Parliament. https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

Ferrer-Bonsoms Cruz, C. (2023, abril 26). Qué es GPT-4: Funcionamiento, características, novedades y cómo puedes probar la IA más avanzada de OpenAI. Business Insider España. https://www.businessinsider.es/gpt-4-ia-avanzada-openai-1225948

Fjelland, R. (2020). Why general artificial intelligence will not be realized. Humanities and Social Sciences Communications, 7(1), Article 1. https://doi.org/10.1057/s41599-020-0494-4

Gobierno de México. (2018, marzo 22). Estrategia de Inteligencia Artificial MX 2018 | Presidencia de la República. https://www.gob.mx/epn/articulos/estrategia-de-inteligencia-artificial-mx-2018

Gold, E. (2023, abril 10). The History of Artificial Intelligence from the 1950s to Today. freeCodeCamp.Org. https://www.freecodecamp.org/news/the-history-of-ai/

González, C. (2019, noviembre 21). Así será el innovador Hub de Inteligencia Artificial del Tec. https://conecta.tec.mx/es/noticias/guadalajara/investigacion/asi-sera-el-innovador-hub-de-inteligencia-artificial-del-tec

Grace B. Mueller, Benjamin Jensen, Brandon Valeriano, Ryan C. Maness, & Jose M. Macias. (2023, julio 13). Cyber Operations during the Russo-Ukrainian War. Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war

Hankins, E., Fuentes Nettel, P., Martinescu, L., Grau, G., & Rahim, S. (2023). 2023 Government AI Readiness Index. Oxford Insights.

Iniciativa de Ley Federal de Ciberseguridad (2023). https://www.diputados.gob.mx/LeyesBiblio/iniclave/65/CD-LXV-II-2P-292/02_iniciativa_292_25abr23.pdf

Iniciativa de Ley Nacional de Seguridad en el Ciberespacio (2020). http://sil.gobernacion.gob.mx/Archivos/Documentos/2020/10/asun_4093498_20201019_1603158505.pdf

Iniciativa de Ley para la Agencia Mexicana para el Desarrollo de la Inteligencia Artificial, 26 (2023). http://gaceta.diputados.gob.mx/PDF/65/2023/oct/20231011-II-3-1.pdf

Iniciativa de Ley para la Regulación Ética de la Inteligencia Artificial para los Estados Unidos Mexicanos (2023). http://sil.gobernacion.gob.mx/Archivos/Documentos/2023/04/asun_4543395_20230413_1680209417.pdf

John McCarthy. (2007, noviembre 12). What is AI? / Basic Questions. Stanford University. http://jmc.stanford.edu/artificial-intelligence/what-is-ai/index.html

José Otero. (2021, agosto 19). Análisis de la Estrategia Digital Nacional 2021-2024. El Economista. https://www.eleconomista.com.mx/opinion/Analisis-de-la-Estrategia-Digital-Nacional-2021-2024-20210819-0026.html

Kuo, M. A. (2024, enero 3). China and Global Governance of AI. https://thediplomat.com/2024/01/china-and-global-governance-of-ai/

Lewis, J. A., Lostri, E., & Cheng, C. (2021). AI Strategies and Autonomous Vehicles Development. https://www.csis.org/analysis/ai-strategies-and-autonomous-vehicles-development

Ley de Seguridad Nacional, 27 (2005). https://www.diputados.gob.mx/LeyesBiblio/pdf/LSN.pdf

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 18 (2010). https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Ley Federal de Telecomunicaciones y Radiodifusión, 173 (2014). https://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR.pdf

Lynner Parker. (2020, junio 11). The American AI Initiative: The U.S. strategy for leadership in artificial intelligence. https://oecd.ai/en/wonk/the-american-ai-initiative-the-u-s-strategy-for-leadership-in-rtificial-intelligence

Manning, C. (2023, octubre 17). CODE WAR: How China's AI Ambitions Risk U.S. National Security American Security Project. American Security Project. https://www.americansecurityproject.org/perspective-code-war-how-chinas-ai-ambitions-threaten-u-s-national-security/

Ministry of Science, Technology and innovations. Brasil. (2021). Summary of the Brazilian Artificial Intelligence Strategy (p. 16). https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-summary_brazilian_4-979_2021.pdf

National Cyber Security Index. (2021, junio 25). Index. National Cyber Security Index. https://ncsi.ega.ee/

National Security Commission on Artificial Intelligence. (2021). NSCAI Final Report (p. 756). National Security Commission on Artificial Intelligence. https://reports.nscai.gov/final-report/

NATO. (2021, octubre 22). Summary of the NATO Artificial Intelligence Strategy. NATO. https://www.nato.int/cps/en/natohq/official_texts_187617.htm

NATO. (2023, junio 22). Emerging and disruptive technologies. NATO. https://www.nato.int/cps/en/natohq/topics_184303.htm

Nicholas Confessore. (2018, abril 4). Cambridge Analytica and Facebook: The Scandal and the Fallout So Far—The New York Times [Diario]. The New York Times. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Nye, J. S. (1990). Bound to lead: The changing nature of American power. Basic Books.

Nye, J. S. (2020, agosto 6). El otro cambio de poder global | by Joseph S. Nye, Jr. Project Syndicate. https://www.project-syndicate.org/commentary/new-technology-threats-to-us-national-security-by-joseph-s-nye-2020-08/spanish

PBS News. (2023, febrero 4). Security expert warns of AI tools' potential threat to democracy | PBS News Weekend. https://www.pbs.org/newshour/show/security-expert-warns-of-ai-tools-potential-threat-to-democracy

Riquelme, R. (2024, febrero 27). Ricardo Monreal presenta iniciativa para regular la inteligencia artificial. El Economista. https://www.eleconomista.com.mx/tecnologia/Ricardo-Monreal-presenta-iniciativa-para-regular-la-inteligencia-artificial-20240227-0055.html

Roman, J. (2021, octubre 5). Artificial Intelligence in Brazil: The Brazilian Strategy for Artificial Intelligence (BSAI/EBIA) and Bill No. 21/2020. IRIS-BH. https://irisbh.com.br/en/artificial-intelligence-in-brazil-the-brazilian-strategy-for-artificial-intelligence-bsai-ebia-and-bill-no-21-2020/

Russel, S., & Norvig, P. (2009). Artificial Intelligence: A Modern Approach (1a ed.). Pearson.

Sarah Cook. (2018, septiembre 28). China's Cyber Superpower Strategy: Implementation, Internet Freedom Implications, and U.S. Responses | Freedom House. Freedom House. https://freedomhouse.org/article/chinas-cyber-superpower-strategy-implementation-internet-freedom-implications-and-us

Schneier, B. (2016). Data and Goliath: The hidden battles to collect your data and control your world (First published as a Norton paperback 2016). W.W. Norton & Company.

Sears, J. (2023, diciembre 23). TRAIN'—The AI Race Heats Up: Mapping the Emerging Geography of Innovation. LinkedIn. https://www.linkedin.com/pulse/train-ai-race-heats-up-mapping-emerging-geography-innovation-sears-pxlre/

Setzer, M. G. J. (2022, junio). The Cyber and Information Domain and the Space Domain: Links and Interdependencies—Joint Air Power Competence Centre. Join Air power Competence Center. https://www.japcc.org/essays/the-cyber-and-information-domain-and-the-space-domain-links-and-interdependencies/

Shimoda Uechi, C. A., & Guimarães Moraes, T. (2023, julio 23). Brazil's path to responsible AI. https://oecd.ai/en/wonk/brazils-path-to-responsible-ai

Stanley-Lockman, Z., & Christie, E. H. (2021, octubre 25). An Artificial Intelligence Strategy for NATO. NATO Review. https://www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html

Tello, J. S. (2023, mayo 24). El impacto de la IA en el mundo de las finanzas, un vistazo al futuro. Expansión. https://expansion.mx/opinion/2023/05/24/el-impacto-de-la-ia-en-el-mundo-de-las-finanzas-un-vistazo-al-futuro

Tiezzi, S. (2023, noviembre 9). China Renews Its Pitch on AI Governance at World Internet Conference. https://thediplomat.com/2023/11/china-renews-its-pitch-on-ai-governance-at-world-internet-conference/

Toledo, R. (2024). Las amenazas derivadas del uso de la inteligencia artificial y sus afectaciones a la seguridad nacional. CESNAV.

U. S. Government Accountability Office. (2021). Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities | U.S. GAO (GAO-21-519SP; p. 112). U. S. Government Accountability Office. https://www.gao.gov/products/gao-21-519sp

Ullerup, A. (2023, noviembre 23). 7 ways AI revolutionises commerce and transforms customer experiences. IMPACT. https://impactcommerce.com/insights/7-ways-ai-revolutionises-commerce-and-transforms-customer-experiences/

Yang, Z. (2024, enero 17). Four things to know about China's new AI rules in 2024. MIT Technology Review. https://www.technologyreview.com/2024/01/17/1086704/china-ai-regulation-changes-2024/

Yudkowsky, E. (2008). Artificial Intelligence as a positive and negative factor in global risk. En E. Yudkowsky, Global Catastrophic Risks. Oxford University Press. https://doi.org/10.1093/oso/9780198570509.003.0021

Zamarrón, I. (2023, junio 6). Este 'think tank' quiere armar la estrategia de inteligencia artificial para el próximo presidente. Forbes México. https://www.forbes.com.mx/este-think-tank-quiere-armar-la-estrategia-de-inteligencia-artificial-para-el-proximo-presidente/