Asociación para las Naciones Unidas en España
United Nations Association of Spain

JUNIO 2023

Las nuevas tecnologías y sus amenazas

Nos encontramos en un momento de gran incertidumbre, adulación y miedo ante las nuevas tecnologías sin saber realmente lo que son, sus usos, y las amenazas que causan.

¿Qué es el Ciberterrorismo?

De momento no existe una definición única que defina el concepto. Sin embargo, según la UNODC se considera que ciberterrorismo es un crimen cibernético perpetrado para coaccionar a un gobierno o población concreta, y causar o amenazar con causar daño (Denning, 2001). Es decir, el uso de medios tecnológicos por parte de grupos terroristas para cometer una intrusión, un fallo o un ataque en los sistemas informáticos o las redes de telecomunicaciones de infraestructuras o instituciones políticas, económicas o sociales.

El ciberterrorismo se realiza en remoto desde cualquier parte del mundo lo que aumenta las vulnerabilidades de las víctimas y dificulta procesos judiciales o legislativos. Algunos ejemplos de ciberterrorismo son: lanzar un ataque informático, suplantar o robar una identidad digital, enviar un programa espía, introducir un virus troyano para controlar en remoto el equipo de otro usuario y robar información, y secuestrar datos privados a usuarios para luego pedir un rescate, así conseguir dinero para financiar otras operaciones delictivas.

En el Hospital Clínic de Barcelona tomó lugar uno de los secuestros de información más grandes de España. El Consejero de Salud, Manel Balcells, definió el ciberataque como terrorismo del siglo XXI, el hackeo afectó sustancialmente la actividad del hospital, el cual tuvo que aplazar cientos de cirugías y extracciones, además de no poder atender infartos o ictus en urgencias en el momento del hackeo. El problema persiste y el hospital sigue sin recuperar sus datos, el Departamento de Salud y la Agencia de Ciberseguridad de Cataluña declararon que no negociarán con los hackers que piden 4,5 millones de dólares para devolver los datos robados.

Fuente: Ester Delgado, El País (2023)

¿Cómo afecta a los derechos de los individuos?

Según el Consejo de Europa y las Naciones Unidas toda persona tiene derechos digitales, que son una extensión de los derechos humanos ya existentes, estos pueden ser: derecho a una vida privada, patrimonio, dignidad, seguridad, integridad psicológica, y la no intervención de comunicaciones privadas.

El ciberterrorismo ocurre con mucha más frecuencia de la que nos podemos imaginar, de hecho, según Cybersecurity Statistics hay 2,200 ataques al día, aproximadamente uno cada 39 segundos. Hay diferentes niveles de ciberterrorismo desde hackeos a gobiernos, hackeos son la obtención de información privada de forma ilegal, hasta la suplantación de identidad digital.

En el ciberespacio las amenazas pasan desapercibidas para los usuarios, por lo tanto, es necesario fomentar la educación digital, que las personas conozcan las amenazas a las que se exponen con la finalidad de su uso responsable y la toma de acciones preventivas, para salvaguardar sus derechos humanos. Entre las acciones que se pueden tomar para prevenir estos ataques se encuentran usar contraseñas fuertes, no hacer clics en enlaces o páginas sospechosas, utilizar softwares de seguridad como antivirus, firewalls y detección programas malignos, evitar el uso de redes de Wi-Fi para hacer transacciones o enviar datos con programas malignos, evitar el uso de redes de Wi-Fi para hacer transacciones o enviar datos confidenciales, mantener copias de seguridad y ser consciente de los riesgos actuales.

Guerras Híbridas con Ciberterrorismo

Las guerras modernas ya no son solo con armas de fuego o estados que deciden combatir los unos contra los otros. Ahora los actores estatales y no estatales pueden utilizar tácticas cibernéticas para socavar las infraestructuras críticas, interrumpir las comunicaciones, robar información confidencial, difundir propaganda, desestabilizar economías y llevar a cabo acciones destructivas en el ámbito virtual. Al realizar esto la población pierde estabilidad y confianza en las estructuras gubernamentales por lo cual es una táctica muy difícil de combatir una vez realizada.

Como mencionamos anteriormente el ciberterrorismo puede incluir ataques contra sistemas de control industrial, infraestructuras energéticas, redes de comunicación, sistemas financieros y gubernamentales, entre otros. Un ejemplo de este tipo de acciones hostiles fue en 2007 cuando Rusia intentó bloquear virtualmente la infraestructura de internet de Estonia como retribución después de que el país quitase un centro conmemorativo de la Unión Soviética que había existido desde la II Guerra Mundial. Asimismo, Rusia ha empleado este tipo de tácticas en otros países como Georgia, Crimea y en las elecciones de 2016 de Trump, favoreciendo sus resultados y la publicación favorable de información relacionada con el expresidente. Este tipo de ataques se usan con la doctrina teórica de Valery Gerasimov quien habló sobre la emergencia de una guerra híbrida y cómo Rusia podía ponerla en práctica, aunque por supuesto se debe de recalcar que Rusia niega cualquier uso de ciberataques para obtener influencia política.

La Inteligencia Artificial

¿Qué es la IA? ¿Cuál es su rol? ¿Tiene un límite? ¿Qué tanto cambiarán nuestras vidas? En las siguientes secciones se intenta proveer un poco de claridad al "misterio" de estas innovaciones y contestar algunas de las preguntas mencionadas, ya que suelen ser las más comunes entre las personas de cualquier sociedad.

Entre académicos no existe una definición única y común para la descripción de lo que es la Inteligencia Artificial ni hasta qué punto se pueden desarrollar sus funciones. Muchas personas se preguntan si es un buscador inteligente como ChatGPT, un robot que sustituirá a los humanos en sus trabajos o un conjunto de robots que llegarán a dominar el mundo; *sí, por más distópico que parezca muchas personas temen al poder de la IA, y con cierta razón*. La definición que le daremos en este artículo a la IA es que es una máquina que puede llevar a cabo tareas humanas incluyendo la creación de otras máquinas.

Primero, debemos entender que la IA no nos entiende. Cuando buscadores inteligentes o asistentes virtuales nos dan información en un chat no son conscientes de lo que hacen ni entienden la información que nos brindan. Estas herramientas funcionan con una combinación de programación y probabilidades desde una base de datos que les permite darnos lo que estamos buscando sin poder o tener que interpretarlo. Muchas personas se confunden al ver que las respuestas de los modelos de lenguaje como ChatGPT o Baart son tan humanizadas e incluso llegan a pensar que se vuelven seres sentientes.

Los cambios en la vida cotidiana de las personas cuyos trabajos no están relacionados con la tecnología aún no están siendo tan radicales, por lo tanto, muchas personas no se dan cuenta de todo lo que ha cambiado con la existencia de la IA. Desde "Robots Asesinos" que son los nuevos soldados utilizados en las guerras, vigilancia extrema en países (no) democráticos, hasta autogeneración de imágenes en la aplicación de adobe Photoshop. Diariamente salen nuevas funciones o AI específicos para llevar a cabo una tarea, cada vez mejor y más avanzada. ¿Puede la IA conquistar el mundo? No, la IA está muy lejos de ser tan avanzada como en las películas, ni siquiera es consciente de su propia existencia y la captación de datos no es en vivo, lo que significa que necesita una base de datos introducida por humanos constantemente para poder proveernos datos actualizados. Las personas han dado por supuesto que la IA funciona bien y que por ello puede llegar a "dominarnos" pero realmente la pregunta que deberíamos hacernos es: ¿La IA funciona? Y si la respuesta es sí: ¿En una escala cuantificada, qué tan funcional es? En esta segunda pregunta muchas de las tecnologías no han alcanzado ni el 10% de su poder ni realizan tan "bien" su trabajo.

Militarización de la IA

La militarización de la Inteligencia Artificial (IA) se refiere al uso de sistemas de IA con fines militares y en operaciones de defensa. Esto implica la aplicación de tecnologías de IA en el ámbito militar. Las fuerzas armadas están creando sistemas que emplean la IA para diversas tareas, como el mando y el control, la fuerza letal, el apoyo a la toma

de decisiones y la logística. Estas capacidades parecen desarrollarse con mayor rapidez que los debates sobre los posibles peligros, como si determinados usos causarían problemas de seguridad, alimentarían una carrera armamentística o eliminarían las barreras que impiden el inicio de una guerra nuclear. Hay diferentes áreas en las que se están usando como vigilancia, ciberseguridad, análisis de datos, entre otros.

La IA tiene potencial para contribuir a la salud y bienestar de individuos, comunidades y estados e incluso de contribuir a los goles de las ODS del 2030. Sin embargo, sus aplicaciones pueden afectar la paz y la seguridad internacional, especialmente con la militarización de herramientas y sistemas nacionales militares. Mayoritariamente estas aplicaciones están siendo desarrolladas por entidades privadas o instituciones académicas para usos principalmente civiles.

La inteligencia artificial no está exenta de riesgos, especialmente cuando se trata del ejército nacional. La opinión pública se interesa por los sistemas de armas autónomas letales (LAWS) porque son fácilmente imaginables y plantean importantes problemas de seguridad, jurídicos, filosóficos y éticos.

Es probable que los ejércitos utilicen la IA para ayudar en la toma de decisiones. Esto podría lograrse proporcionando datos para guiar la toma de decisiones humana o incluso asumiendo todo el proceso por completo. Esto puede ocurrir, por ejemplo, en lugares donde la comunicación es imposible o en lugares como el ciberespacio, donde las cosas se mueven demasiado rápido para que las personas puedan comprenderlas.

La capacidad de un operador o comandante humano para ejercer un mando y control directos sobre los sistemas militares puede verse reforzada como consecuencia de ello, pero también es posible que ocurra lo contrario. La IA permite la creación de sistemas complejos que pueden ser difíciles de comprender, lo que plantea problemas de transparencia y de capacidad para determinar si el sistema funciona como se espera o se pretende.

Los gobiernos no solo se utilizan estas aplicaciones contra otros estados, sino que también con sus propias poblaciones para analizar comportamiento de terroristas, amenazas a la seguridad nacional o incluso para vigilancia. Un claro ejemplo es China. En los últimos años, los problemas de privacidad han aumentado también en China. China cuenta ahora con uno de los sistemas de gobernanza de datos más sólidos del mundo sobre el papel, gracias a la aprobación el año pasado de dos importantes leyes: la Ley de Protección de Datos Personales y la Ley de Seguridad de Datos. Sin embargo, las fuerzas de seguridad pública chinas estaban altamente capacitadas para rastrear y vigilar a sospechosos de delitos y disidentes del régimen incluso antes del desarrollo de sistemas tecnológicos de vanguardia que utilizan IA. Las capacidades de vigilancia del aparato de seguridad pública han mejorado ahora con el despliegue de la tecnología de reconocimiento facial. Por ejemplo, hay pruebas convincentes de que algunas tecnologías de reconocimiento facial se están utilizando en la región de Xinjiang para perseguir especialmente a personas de ascendencia uigur.

Estados Unidos está intentando retrasar el avance de la militarización de la IA en China con la estricta implementación de sanciones a compañías privadas

y regulaciones como la Lista de Entidades o la prohibición de exportación de Semiconductores, y lo mismo intenta hacer China al bajar la exportación de metales imprescindibles para la producción de tecnologías tanto para energías renovables como para cualquier tipo de aplicaciones tecnológicas.

Fuente: New York Times

ChatGPT

ChatGPT es un modelo de lenguaje de la IA. Para muchos es una herramienta realmente útil, pero lo que no se tiene en cuenta es que puede dar información falsa, malos o incluso peligrosos consejos sobre acciones como realizar explosivos, manufacturar drogas ilegales y participar en otras actividades ilegales. Aunque es crucial señalar que las directrices de Chat GPT prohíben la generación de contenidos nocivos, la falta de control total sobre los resultados suscita preocupación por la posibilidad de que se produzcan desinformación y daños.

Además, la incapacidad de Chat GPT para verificar la información o comprobar los hechos de sus respuestas también puede dar lugar a consejos inexactos.

El consejero delegado de OpenAI, Sam Altman, se enfrenta a una audiencia en el Senado de EE.UU. sobre Inteligencia Artificial (IA). Su empresa creó el chatGPT. La herramienta ha llegado a ser tan avanzada que puede escribir redacciones, guiones, poemas y resolver la codificación de software de la misma forma que lo haría un humano.

Miembros del Senado buscan las posibles amenazas que la IA puede suponer para los humanos en el futuro y si debe ser regulada por el gobierno. Expertos como el Dr. Geoffrey Hinton han manifestado recientemente su preocupación por el rápido desarrollo de la nueva tecnología.

La senadora Blumenthan preguntó a Altman si cree que es buena idea explicar a los usuarios la fiabilidad de los contenidos que utilizan. Sugirió que los contenidos recibieran "tarjetas de puntuación" para reflejar su fiabilidad. Altman está de acuerdo y cree que las auditorías independientes son importantes. Cree que, aunque hay un elemento de error cuando se utiliza tecnología de IA, se puede crear otro tipo de software para detectar errores y precisión. Además, hay grandes motivaciones para reducir la velocidad del avance de la IA. La IA utiliza la capacidad de resolver problemas basándose en la información que se le proporciona ya sea subjetiva u objetiva.

OpenAI es la empresa que está detrás de ChatGPT. Fue fundada en 2015 con 1.000 millones de dólares de apoyo con inversores de Silicon Valley. Chat GPT-4 es la nueva versión de ChatGPT. Puede reconocer y explicar imágenes. Su capacidad puede ser más sofisticada y ofrecer sugerencias de recetas a partir de fotos de ingredientes, por ejemplo.

Sin embargo, no todo es color de rosa. En un acto reciente durante su visita a la India, Altman declaró: "Me fío menos de las respuestas generadas por ChatGPT que de cualquier otra persona en la Tierra". En resumen, aunque ChatGPT y otras aplicaciones de la IA han venido para cambiar nuestro día a día, se ha enfrentado a críticas por su tendencia a ofrecer respuestas inexactas. Se sabe que en múltiples ocasiones alucina y crea escenarios ficticios.

Posición de las Naciones Unidas

Las NU defiende el desarrollo de la IA como una herramienta ética y para el desarrollo sostenible del ser humano, ayudándonos a cumplir los ODS y a cambiar las reglas del juego de una forma positiva. Sin embargo, el Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Volker Türk, y en 2021 también Michelle Bachelet, denuncian estrictamente los peligros de la IA y la necesidad de su regulación antes de continuar su desarrollo. El 8 de mayo Türk dio un discurso en el que menciona el incremento en la propagación de los discursos de odio y de desinformación en el espacio digital, así como el posible uso de la IA para reprimir la libertad de expresión. Además, así como se mencionó anteriormente, denunció la desaparición del derecho a la intimidad y la brecha digital que amplía las desigualdades. Dada la importancia de la utilización y creación de la IA se está desarrollando una propuesta para un **Pacto Digital Mundial** para presentarlo este 2024 en la Cumbre del Futuro basado en un proceso inclusivo y transparente, que quiere atender las necesidades de aquellas personas a las que las innovaciones digitales benefician tanto como a las que no. Asimismo, resaltó la responsabilidad del sector privado en el respeto de los derechos humanos, mencionando los Principios Rectores de las Naciones Unidas sobre las Empresas y los Derechos Humanos como una guía. También se destaca el papel de los gobiernos en la regulación de las actividades del sector privado y en garantizar el acceso universal a Internet. Se enfatiza la importancia de la transparencia, la rendición de cuentas y la ética en el desarrollo de la inteligencia artificial, así como la necesidad de prevenir posibles repercusiones negativas.

El **Pacto Digital Mundial** se refiere a un marco propuesto para abordar los desafíos y oportunidades asociados con la tecnología digital y garantizar que su desarrollo y uso estén guiados por los principios de los derechos humanos. También, busca establecer normas y principios comunes que rijan el comportamiento de los actores involucrados en el ámbito digital, incluyendo gobiernos, empresas, organizaciones de la sociedad civil y otros actores relevantes. Además, promoverá un enfoque inclusivo y transparente, asegurando la participación de estados, individuos y el sector privado en su desarrollo y aplicación. Intentará equilibrar el uso y los beneficios de la tecnología digital con la protección de los derechos humanos, abordando temas como la privacidad, la libertad de expresión, la igualdad de acceso, la seguridad en línea y la rendición de cuentas. El objetivo no está 100% decidido pero será para establecer un marco universal y vinculante que ayude a orientar las políticas, regulaciones y prácticas relacionadas con el ámbito digital, con el fin de fomentar un entorno digital seguro, inclusivo y respetuoso de los derechos humanos en todo el mundo.

Según Türk una vez hayan "líneas rojas regulatorias", transparencia, colaboración entre actores y se mantengan los derechos humanos como la prioridad de la innovación digital se construirá una gobernanza adecuada para un futuro digital saludable y ayudaremos en la consecución de los Objetivos de Desarrollo Sostenible.

Con respecto a las diferentes amenazas que presenta la militarización de la IA el Secretario General de la ONU, António Guterres, en su programa para el desarme "Asegurar nuestro futuro común", subraya la necesidad de que los Estados miembros de la ONU comprendan mejor la naturaleza y las implicaciones de las tecnologías nuevas y emergentes con posibles aplicaciones militares y la necesidad de mantener el control humano sobre los sistemas de armamento. Subraya que el diálogo entre los gobiernos, la sociedad civil y el sector privado es un complemento cada vez más necesario de los procesos intergubernamentales existentes.

Nota conclusiva

Los ataques cibernéticos realizados por grupos terroristas pueden comprometer la seguridad de sistemas informáticos, redes de telecomunicaciones términos de protección de los derechos de los individuos. Los derechos digitales, como el derechoa la privacidad, la seguridad y la integridad, pueden ser vulnerados por estos ataques. e infraestructuras políticas, económicas o sociales. Es fundamental promover la educación digital y fomentar el uso responsable de la tecnología para salvaguardar los derechos humanos y tomar medidas preventivas contra el ciberterrorismo.

Además, se ha observado una creciente militarización de la inteligencia artificial (IA) en el ámbito de defensa y seguridad. La aplicación de la IA en operaciones militares plantea preocupaciones sobre la transparencia, el control y los posibles riesgos para la paz y la seguridad internacional.

En general, tanto el ciberterrorismo como la militarización de la IA plantean desafíos significativos en términos de seguridad, derechos individuales y ética. Es necesario abordar estos desafíos a niveles nacionales e Internacionales con regulaciones adecuadas, educación digital y una mayor conciencia sobre los riesgos y beneficios de estas tecnologías.

Yuliana Vázquez Hernández

Estudiante de Global Governance, Economics & Legal Order

ESADE

Fuentes de referencia:

- Bachmann, M., & Gunneriusson, H. (2016). Hybrid wars: The 21st-century's new threat. Scientia Militaria - South African Journal of Military Studies, 44(2), 1-20. https://ung.edu/institute-leadership-strategic-studies/_uploads/files/bachmann-gunneriusson-hybrid-wars-16-sep-2016-scientia-militaria.pdf

- Big Data and Security (2019). The AI surveillance symbiosis in China: Joint development of military-civil fusion in national strategic emerging industries. Center for Strategic and International Studieshttps://bigdatachina.csis.org/the-ai-surveillance-symbiosis-in-china/

- Firstpost (2022, 19 de enero). Sam Altman, the inventor of ChatGPT, doesn't trust anything that his AI chatbot says. https://www.firstpost.com/world/sam-altman-the-inventor-of-chatgpt-doesnt-trust-anything-that-his-ai-chatbot-says-12714112.html

- Lavanguardia.com (2020, 10 de diciembre). La economía geopolítica a cuatro patas de la inteligencia artificial. Vanguardia Dossier. https://www.lavanguardia.com/vanguardia-dossier/20201210/49848571042/economia-geopolitica-patas-inteligencia-artificial.html

- OHCHR. (2023, mayo 15). Global digital compact must be guided by human rights, says Turk. Recuperado de https://www.ohchr.org/es/statements/2023/05/global-digital-compact-must-be-guided-human-rights-says-turk

- OHCHR. (2021, septiembre 1). Artificial intelligence risks privacy and demands urgent action, says Bachelet. Recuperado de https://www.ohchr.org/es/press-releases/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet

- OHCHR. (2023, junio 1). New and emerging technologies need urgent oversight and robust transparency, says OHCHR. Recuperado de https://www.ohchr.org/es/press-releases/2023/06/new-and-emerging-technologies-need-urgent-oversight-and-robust-transparency

- Pool Marketing (2022, 27 de febrero). The dark side of ChatGPT has real-world consequences. https://poolmarketing.medium.com/the-dark-side-of-chatgpt-has-real-world-consequences-90bff03a00bf

- Stimson Center (2020). The Militarization of Artificial Intelligence. https://www.stimson.org/2020/the-militarization-of-artificial-intelligence/

- Tokio School (s.f.). Inteligencia Artificial y Política. https://www.tokioschool.com/noticias/inteligencia-artificial-politica/

- United Nations (2020). Towards ethics in artificial intelligence. The United Nations Chronicle. https://www.un.org/en/chronicle/article/towards-ethics-artificial-intelligence

- World Summit AI (2023, 14 de junio). OpenAI CEO faces US Senate hearing.

Publicado por:

Asociación para las Naciones Unidas en España
United Nations Association of Spain

Con el apoyo de:

Generalitat de Catalunya