LITORALPRESS

Fecha: 11-11-2024
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: El lado B de la inteligencia artificial

Pág. : 24
Cm2: 540,9

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

El lado B de la inteligencia artificial

POR MARCO ZECCHETTO

El desarrollo de la inteligencia artificial y, en particular, la IA generativa, ha traído diversos beneficios para las empresas y la sociedad. Sin embargo, su uso para actividades delictivas, como ciberataques y espionaje industrial, además de otras reñidas con la ética, como armamento autónomo para guerras, ya son una realidad.

En el caso de la ciberdelincuencia, la IA generativa se ha convertido en un potencial vector de ataque, especialmente en el robo de credenciales y accesos a organizaciones a través de campañas de *phishing* (suplantación de identidad) utilizando técnicas de *deepfake*, es decir, archivos de imagen, audio o video alterados a través de IA para que parezcan reales.

Según el Identity Fraud Report 2024 de Onfido -firma especializada en servicios de verificación de identidad- los intentos de fraude a través de *deepfake* en el mundo, aumentaron 3.000% en 2023.

La gerenta de IBM Security para Argentina, Chile, Uruguay y Paraguay, Pamela Skokanovic, afirmó que la IA generativa ha permitido escalar estos ataques y las campañas de *phishing* con *deepfake* -en el escenario empresarial- se han enfocado en el "audio generativo" o suplantación de voz, que "puede ser utilizada para engañar a los ejecutivos, como los directores financieros, para que realicen transacciones".

> Desde sofisticados ciberataques de suplantación de identidad, espionaje y plagio industrial, hasta drones y tanques autónomos para la guerra, son algunas de las otras aplicaciones de la nueva tecnología.

Skokanovic explicó que la manipulación de una conversación puede suceder en tiempo real, a través de técnicas como el *audio jacking* -ataque basado en IA generativa para interceptar y manipular conversaciones en vivo sin ser detectados- y software maliciosos.

"Los cibercriminales pueden interceptar y reemplazar palabras específicas en una conversación en vivo. Este tipo de ataque es difícil de detectar, ya que se ajusta al contexto original de la conversación. Sin embargo, es más probable que se observe en campañas dirigidas a personas de alto perfil con un historial de charlas o conferencias en público que pueden aprovechar para falsificar la voz", afirmó.

Por su parte, el socio de Cyber de Deloitte y experto en ciberseguridad, Nicolás Corrado, dijo que otro riesgo asociado a esta tecnología es la inyección de *prompt*, un tipo de ataque en que el delincuente manipula las instrucciones que se dan a un modelo de IA generativa para que actúe de una manera diferente a la determinada por el usuario.

"Por ejemplo, podemos hacer que la IA lea un depósito de US$ 1 y después vea en la inyección que es US$ 1 millón. Si esto lo hacemos por *back office* (tareas administrativas de una empresa) y lo implementamos en un banco, uno podría generar un depósito de US$ 1 millón en vez de US$ 1", ejemplificó.

Espionaje industrial

La IA también abre nuevas posibilidades para descifrar secretos corporativos, plagiar y violar la propiedad industrial, aunque hoy no son muchos los casos conocidos donde se ha vinculado directamente el uso de esta tecnología para estos fines.

En 2023, la agencia de imágenes Getty Images inició un procedimiento judicial ante el Tribunal Superior de Justicia de Londres contra Stability AI -la empresa detrás del modelo de generación de imágenes Stable Diffusion- alegando que la compañía copió y procesó ilegalmente millones de imágenes protegidas por derechos de autor y los metadatos asociados, propiedad de Getty Images o representados por ésta, sin contar con una licencia.

El CEO de Hackmetrix -startup de cumplimiento y certificación en ciberseguridad- Adriel Araujo, señaló que el uso de IA, en muchos casos, "no es necesariamente más sofisticado que las técnicas de espionaje tradicionales", pero ha revolucionado las prácticas de espionaje industrial al hacerlas "más rápidas, eficientes y accesibles".

Por ejemplo, se están utilizando drones -que pueden entrar a áreas restringidas sin ser detectados- equipados con tecnología de visión por computadora. En este caso, las imágenes capturadas se analizan con IA, lo que permite identificar patrones o anomalías y compararlas con registros previos, "para detectar cambios sutiles y obtener información clave casi al instante".

Otra técnica común es la infiltración mediante *insiders digitales*, donde, a través de *deepfake*, se simulan empleados o proveedores con acceso legítimo para insertar *malware* (software malicioso) o robar información confidencial, "sin levantar sospechas", afirmó.

IA en guerra: armamento automatizado y ética

En noviembre de 2021, la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (Unesco), publicó la "Recomendación sobre la ética de la inteligencia artificial", el primer marco normativo universal sobre ética de la IA.

El documento, que fue adoptado por los 193 estados miembros, no incluyó defensa por falta de acuerdo entre los países. Una exclusión amparada por las potencias militares que tienen una industria armamentística y que ha generado discusiones internacionales.

En septiembre se realizó en Corea del Sur la segunda cumbre sobre In-

LITORALPRESS

Fecha: 11-11-2024
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: **El lado B de la inteligencia artificial**

Pág. : 25
Cm2: 307,2

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

"SON VARIAS LAS POTENCIAS MILITARES QUE TIENEN INICIATIVAS DE APLICACIÓN DE IA EN DESARROLLO, PERO NO TODAS ESTÁN DISCUTIENDO LOS LÍMITES", DICE EL COMANDANTE DEL BATALLÓN DE CIBERDEFENSA DEL EJÉRCITO DE CHILE.

teligencia Artificial Responsable en el Ámbito Militar (Reaim, en inglés), la que abordó el impacto potencial de la IA en la seguridad internacional ante conflictos, riesgos y beneficios de uso militar de armas con IA y uso responsable.

La cumbre culminó con la declaración "Blueprint for Action", que respaldaron 61 de los 90 países que participaron -China no lo firmó- y que establece una hoja de ruta para definir normas y principios de IA en el ámbito militar, como mantener una participación humana adecuada.

El teniente coronel comandante del batallón de Ciberdefensa del Ejército de Chile, Juan Pablo del Castillo, dijo que hoy son varias las potencias militares importantes que tienen iniciativas de aplicación de IA en desarrollo, "pero no todos están discutiendo los límites, por lo menos desde el lado occidental".

Del Castillo señaló que las principales discusiones éticas que despierta la aplicación de esta tecnología están asociadas a los sistemas de armas con toma de decisiones autónomas, los que clasifican y determinan si un objetivo es o no una amenaza, y puede tomar la decisión de disparar sin consultar a un humano.

"Esto es diferente de los procesos de *targeting* (selección y respuesta ante un objetivo), en donde hay un protocolo de decisión, asesoramiento jurídico, un marco legal, un paso a paso para poder disminuir los daños colaterales, apegado a la ley", comentó.

Robust, es un prototipo de vehículo de combate completamente autónomo con IA, desarrollado por el Gobierno de Israel en conjunto con Elbit Systems.

3.000%
AUMENTARON LOS ATAQUES CON DEEPFAKE EN 2023, SEGÚN ONFIDO.

La preocupación estaría en la toma de decisión sin mediación humana, lo que plantea interrogantes: "¿Tendrá fallos la IA? ¿Qué se levanta con los sesgos de los datos que tenga?, ese es el temor que está en la comunidad científica global, de cuáles son los alcances y los límites que se pueden establecer", señaló del Castillo.

El analista internacional y académico de la Universidad de Valparaíso, Guillermo Holzmann, comentó que ante un conflicto armado, la aplicación de IA hace más eficiente la función de mando, lo que implica "entrar a guerras multidominio donde se están controlando vía satélite las operaciones terrestres y navales, utilizando vehículos no tripulados, cambia todos los elementos que definían la guerra convencional".

No obstante, comentó que hoy los vehículos de combate con sistemas de IA en su mayoría son operados a distancia por humanos y que la transición hacia vehículos completamente autónomos con capacidad de decisión en la línea de batalla, involucra temas de infraestructura tecnológica y riesgos vinculados a sesgos algorítmicos.

"Exige necesariamente una infraestructura en el dominio espacial y cibernético, a nivel de satélites y de intercomunicación para compartir datos en tiempo real", afirmó Holzmann.

Además, la implementación de la IA en vehículos de guerra y armamentos estará marcada por los algoritmos y los datos biométricos con los que se entrenen los modelos.

"Por ejemplo, si un grupo terrorista islámico radical accede a un vehículo con armamento autónomo y tiene IA, los algoritmos que le van a colocar es que toda aquella persona que biométricamente responda a un occidental hay que asesinarlo. Entonces, ahí hay un tema importante", dijo.

Según Holzmann, no existe suficiente información pública para determinar qué países están desarrollando prototipos de tanques o vehículos con IA con capacidad de tomar decisiones de ataque autónomas. Sin embargo, estima que los más avanzados podrían ser Estados Unidos, China, Turquía y el Reino Unido.

En 2022, el Ministerio de Defensa de Israel presentó las primeras pruebas de Robust (Robotic Autonomous Sense and Strike), un vehículo de combate completamente autónomo con inteligencia artificial, desarrollado en conjunto con la empresa Elbit Systems.

El prototipo incorpora conducción autónoma con IA y cuenta con un artillero virtual con capacidad para reconocer y seguir múltiples objetivos y priorizar ataques según el contexto.

Para Holzmann, Israel, dada su capacidad tecnológica, "podría tener las condiciones para poder mantener un flujo permanente de transmisión de datos a un tanque autónomo".