Inteligencia Artificial en la Seguridad de TI

Gustavo Rondo Montes
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz – Bolivia
gurondo777@gmail.com

***Resumen*—Este artículo tiene la finalidad de mostrar un panorama general de la aplicación de la Inteligencia Artificial enfocada a la seguridad de las tecnologías de información, una opinión que se da hoy en día, es que no solo se debería constituir una mente artificial simulada de buena fe que pudiera superar el Test de Turing de un ser humano, sino que también debería tener la capacidad de simular a un profesional en ciberseguridad muy bien adiestrado, capaz de replicar las decisiones tomadas por el ingeniero en seguridad con más experiencia pero en una escala muy superior. Antes de lograr una Inteligencia Artificial brillante propia de la ciencia ficción, debemos pasar por algunas etapas de prueba, si bien dichas etapas tienen un gran valor en sí mismas, cuando madure como tecnología, constituirá uno de los desarrollos más asombrosos de la historia, cambiando la condición del ser humano de manera similar e incluso superior a cambios trascendentales como la electricidad, la aviación e Internet.**

Palabras clave—Conocimiento, inteligencia artificial, tecnología de información.

I. Introducción

El software de Inteligencia Artificial (IA) o aprendizaje automático (ML, *Machine Learning* por sus siglas en inglés) tiene la capacidad de "aprender" a partir de las consecuencias de eventos pasados para poder predecir e identificar amenazas en ciberseguridad. Según un informe de Webroot, la IA es utilizada por aproximadamente el 87 % de los profesionales en ciberseguridad de los Estados Unidos [1].

En el mundo de la seguridad, la Inteligencia Artificial constituye un caso claro de elemento potencialmente positivo. La industria está notoriamente desequilibrada, con agentes maliciosos que intentan aprovechar miles de vulnerabilidades para lanzar sus ataques al tiempo que intentan desplegar un arsenal de herramientas cada vez mayor para evadir la detección una vez que han roto la seguridad de un sistema.

Con los recursos avanzados, la inteligencia y la motivación para completar un ataque, los intrusos son capaces de generar ataques de alto nivel estos ataques se producen cada día, es así que la victoria resulta eventualmente imposible para los defensores.

La velocidad analítica y la potencia de nuestra seguridad "de ensueño" mediante el uso de IA como mínimo debería poder hacer frente a este tipo de escalada, nivelando el terreno de juego para los profesionales de la seguridad que actualmente tienen que realizar una defensa constante contra atacantes que pueden escoger un punto débil en su tiempo libre. En su lugar, incluso los ataques bien planeados y ocultos podrían detectarse y ser derrotados rápidamente.

Obviamente, queda mucho por hacer para lograr una seguridad perfecta mediante el uso de la IA. Dicha IA no solo debería constituir una mente simulada de buena fe que pudiera superar el Test de Turing, sino que también debería ser un profesional en ciberseguridad muy bien adiestrado, capaz de replicar las decisiones tomadas por el ingeniero en seguridad con más experiencia, pero en una escala muy superior.

Antes de lograr una Inteligencia Artificial brillante propia de la ciencia ficción, debemos pasar por algunas etapas de prueba, si bien dichas etapas tienen un gran valor en sí mismas. Constantemente asistimos a avances verdaderamente asombrosos. Cuando madure como tecnología, constituirá uno de los desarrollos más asombrosos de la historia, cambiando la condición del ser humano de manera similar e incluso superior a cambios trascendentales como la electricidad, la aviación e Internet, ya que estamos en la era "pre IA".

II. Problemática

El futuro de la industria de la ciberseguridad parece que pasa por la inteligencia artificial (IA).

Prácticamente 7 de cada 10 empresas así lo creen. Y es que el 69 % de aquellas que han sido consultadas por el *Instituto de Investigación de Capgemini* se muestra convencida de que no tendrá capacidad para responder a los ciberataques y las amenazas críticas que caracterizan al panorama empresarial actual si no usan IA. El motivo de fondo es que el mundo está cambiando con la introducción del internet de las cosas, los avances en la nube, la llegada del 5G o el uso de tecnologías de interfaz conversacional, por ejemplo.

Según un 60 % de los directivos, la IA es útil en el campo de la seguridad porque incrementa la eficiencia y la productividad de los analistas, que gastarían menos tiempo en falsos positivos. Un 64 % aprecia que se reduzca el coste derivado de detectar brechas y responder ante el descubrimiento de las mismas. Un porcentaje mayor, el 69 %, destaca su contribución en la precisión a la hora de descubrir problemas. Y otro 74 % valora que se disminuye el tiempo de respuesta [2].

Y esto se está reflejando en las inversiones. Prácticamente la mitad de los consultados (48 %) dice que en 2020 aumentarán los presupuestos para IA en ciberseguridad y que lo harán un 29 %. Hasta ahora solo 1 de cada 5 empresas usaba IA en ciberseguridad, pero se espera que el año que viene 2 de cada 3 hayan desplegado esta tecnología [2].

Más allá de las ventajas, que animan a cambiar la forma de hacer las cosas, todavía hay desafíos que superar, sobre todo la dificultad para transformar pruebas de concepto en despliegues

Para referenciar este artículo (IEEE):

[N] G. Rondo, «Inteligencia Artificial en la Seguridad de TI», *Revista PGI. Investigación, Ciencia y Tecnología en Informática,* nº 8, pp. 99-101, 2020.

completos o la cuestión de la integración de infraestructuras, sistemas de datos y aplicaciones.

III. Objetivo

Dar a conocer y comprender la importancia de la seguridad en las tecnologías de información enfocándolos desde la perspectiva de la inteligencia artificial.

IV. Hipótesis

Es posible mediante la inteligencia artificial poder suplir las necesidades de seguridad que demanda las tecnologías de información.

V. Revisión de literatura

Es fácil pensar que todo aquello denominado como '*smart*' sea algo inteligente, pero esto no es obligatoriamente así. Un ejemplo recurrente dentro de la industria son los analíticos inteligentes, la mayoría de los cuales, a pesar de tener esta denominación, son simplemente algoritmos predefinidos que dependen de alguien para que los modifique, actualice y mejore; en otras palabras, no necesariamente aprenden algo nuevo con el paso del tiempo.

En su forma más básica, la IA alude a la capacidad de la máquina para aprender por sí misma, diferente al aprendizaje automático (*machine learning*), el cual se refiere a cómo se está aplicando la IA en la evaluación de datos, tanto en un nivel superficial como en uno profundo. También tenemos los analíticos, que suelen ser un concepto que abarca todos los resultados que se le presentan al usuario, pero que no necesariamente están relacionados con la IA.

A. La Inteligencia Artificial y el análisis de video

Tradicionalmente el análisis de video se ha basado en reglas decretadas por un programador humano que establece parámetros fijos para cada situación que el sistema debe reconocer. En comparación, la tecnología de análisis de contenido basada en IA puede aprender directamente del video sobre los objetos, sus relaciones entre sí y su comportamiento [1].

Esto hace posible identificar los objetos de manera "inteligente" y clasificar las situaciones. El sistema podrá comprender si tiene un comportamiento normal o anormal y alertar al operador sobre actividades inusuales, lo que llevará a desarrollar sistemas predictivos en el futuro.

La inteligencia artificial y el aprendizaje automático se aplican a dispositivos y equipos para obtener funciones que el ser humano no podría alcanzar; por ejemplo, sentarse y mirar todas las imágenes de las cámaras simultáneamente.

Nuestra atención no funciona de esa manera, pero las máquinas son extremadamente buenas y detalladas en esto. Aprovechar datos y videos de los dispositivos es la base para combinar la inteligencia de la máquina con el juicio humano.

En otras palabras, la inteligencia artificial es la evolución del análisis de video, pero en lugar de crear algoritmos alrededor de algo que estamos viendo, está construyendo sistemas que realmente aprenden lo que está sucediendo sobre la marcha. Inherentemente, la calidad seguirá mejorando con el tiempo, y eso nos ayudará a impulsar una mejor adopción con una mejor calidad.

B. Aprendizaje de lo Superficial a lo Profundo

Debido a las limitaciones de la capacidad de procesamiento del *hardware*, el aprendizaje automático sólo podía implementar un aprendizaje superficial de conjuntos de datos muy grandes. Con los recientes y significativos avances en el poder de procesamiento de las unidades de procesamiento gráfico (GPU), ahora podemos utilizar un enfoque de aprendizaje profundo en el que logramos ver datos en muchos más niveles o dimensiones; de ahí la palabra "profundo".

Milestone, por ejemplo, se ha trasladado a esta nueva plataforma de cómputo de GPU al recodificar nuestro *software* para usar un nuevo tipo de codificación llamada paralelización. La paralelización de *software* es una técnica de codificación para dividir un solo problema en cientos de problemas más pequeños. El *software* puede ejecutar esos 100 o mil procesos en mil núcleos de procesamiento, en lugar de esperar a que un núcleo procese los datos mil veces [3].

Con la paralelización, hay un gran avance en la rapidez con la que podemos resolver un problema. Y cuanto más rápido podamos resolver un problema, con más profundidad se pueden procesar los conjuntos de datos.

C. Desafíos en un Futuro Inteligente

Históricamente el gran desafío de la IA ha sido la potencia, pues se necesita una gran cantidad de cómputo para procesar todos estos datos. Sin embargo, con NVIDIA, el proceso de computación ya no es un problema [4].

Ahora el reto para la arquitectura e infraestructura general de estos proyectos pasa por cómo asegurarlos. Es una gran cantidad de datos y, si es valioso para nosotros, probablemente también lo sea para otra persona. Así que, ¿cómo podemos mantener el control sobre eso? Ese es probablemente el agujero más grande que vemos en la mayoría de las implementaciones: una falta de atención hacia los elementos de ciberseguridad.

Aún estamos en la infancia de la inteligencia artificial. Pasará bastante tiempo antes de que la IA tenga el potencial de reemplazar las capacidades de un equipo humano. El escenario más probable es que la inteligencia artificial se aproveche para procesar muchos más datos en mucho menos tiempo, lo que permitirá a los usuarios finales tomar mejores decisiones con mayor rapidez.

Necesitamos personas, sólo queremos darles mejores datos para su toma de decisiones; gente que haga un dictamen de los datos proporcionados, y el video sin duda será una herramienta crucial en este proceso, asegurando el acceso visual en tiempo real, convirtiendo los datos en información visual.

Combinar la inteligencia de la máquina con el juicio humano es un requisito previo para aprovechar al máximo los datos generados por los entornos IoT (Internet de las Cosas). Y no tengo dudas de que el video será la base para que las personas confiemos en estos datos en el futuro [5].

En la actualidad, existen pocas soluciones que verdaderamente implementen la inteligencia artificial en la industria de la seguridad. Muchas soluciones están "entrenadas para IA", lo que significa que en el laboratorio sus algoritmos se entrenan utilizando capacidades de IA. Pero, una vez que se desarrolla ese algoritmo, se implementa como solo un dispositivo inteligente y no se produce más aprendizaje. La

única vez que estos algoritmos mejorarán es cuando se actualicen para incluir un aprendizaje mejorado [6].

VI. Conclusiones

La aplicación de la IA en el campo de la ciberseguridad, aunque es emergente, es la gran apuesta. Las medidas defensivas deben ir por delante de los atacantes y los algoritmos de Inteligencia Artificial se están presentando como la tecnología idónea para combatirlos.

Esta capacidad de optimización de recursos, que se nos presenta para poder adelantarnos a las amenazas, puede ser decisiva para evitar un aumento en el volumen de riesgos y daños al que empresas y usuarios (por desgracia, pero con remedio) ya se están enfrentando.

Referencias

[1] Webroot and opentext. (2018 – 2019) Resources-internet-security-faq. Recuperado de: https://www.webroot.com/us/en.

[2] Silicon insights for it profesionals (2020) Visite la página seguridad-sin-inteligencia-artificial Recuperado de: https://www.silicon.es/

[3] J.A. Tuszynki, et al. Dielectric Polarization, Electrical Conduction, Information Processing and Quatum Computation in Microtubules. Are they plausible? Philisophical Transactions of the Royal Society London 356: 1897-1926, 1998.

[4] C.G. Langton. Artificial Life. Santa Fe Institute in the Science of Complexity. New York: AddisonWesley,1998.

[5] H. Garret and C. Grisham. Biochemistry. Chapter 17. 2nd ed. Harcourt Brace College Publishers. Sauder College Publishing. New York 1999. - R. Kurzweil. The Age of Spiritual Machines: When the computers exceed human intelligence. Penguin Books, 1999.

[6] J. Satinover. The quantum Brain: The search for freedom and the next generation of man. John Wiley & Sons, Inc. New York, 2001.

Breve CV del autor

Gustavo Rondo Montes es Ingeniero de Sistemas por la Universidad Salesiana de Bolivia; Diplomado en Telecomunicaciones; Diplomado en Auditoria de Sistemas. Actualmente realiza la Maestría en Informática Forense Seguridad de la Información y Auditoria de Sistemas en el Postgrado en Informática UMSA. Email: gurondo777@gmail.com.