Cómo la inteligencia artificial cambiará la seguridad informática y la seguridad física de la información en el mundo nuclear

Mitchell Hewes

Las tecnologías de inteligencia artificial (IA) y aprendizaje automático podrían tal vez revolucionar el mundo y dar paso a un progreso y una innovación sin precedentes al transformar la forma en que creamos, consumimos y utilizamos la información. Las tecnologías de IA, conforme se vuelvan cada vez más sofisticadas, transformarán las industrias, racionalizarán los procesos e incluso podrán influir en nuestra manera de vivir. El sector nuclear no es la excepción, y cabe esperar que los beneficios de la IA se reflejen en muchos procesos y operaciones de las instalaciones nucleares y radiológicas.

Al mismo tiempo, el rápido avance de la IA también conlleva múltiples riesgos. Los agentes con fines dolosos pueden utilizar la IA para perpetrar ataques más avanzados y selectivos o explotarla para poner en riesgo la integridad de las redes, los sistemas y la información de carácter estratégico de las instalaciones nucleares y radiológicas.

Beneficios para la seguridad informática y la seguridad física de la información

El OIEA se prepara para las transformaciones que traerá consigo la IA fomentando la cooperación internacional en este ámbito a fin de garantizar que todos los países puedan beneficiarse de las oportunidades y, al mismo tiempo, prepararse para mitigar los riesgos. A través de mecanismos como reuniones técnicas y proyectos coordinados de investigación (PCI), el OIEA apoya el desarrollo, la difusión y la aplicación de técnicas de IA, así como las contramedidas y la defensa contra agentes con fines dolosos.

Tal vez la ventaja más significativa de la IA en el ámbito de la seguridad informática y la seguridad física de la información sea la menor dependencia de la intervención y el análisis humanos. Los sistemas basados en la IA pueden funcionar ininterrumpidamente para monitorizar las redes y los sistemas en busca de amenazas. Al automatizar estas tareas, los profesionales de la seguridad física nuclear tienen tiempo para centrarse en tareas más estratégicas y responder con mayor eficiencia a los incidentes cuando ocurren.

“Las capacidades de aprendizaje adaptativo de la IA pueden aprovecharse para mejorar la seguridad informática y la seguridad física de la información, ya que detectan con rapidez las amenazas y proporcionan automáticamente a los expertos humanos la información que necesitan para coordinar las actividades de respuesta, —afirma Fan Zhang, Profesora Adjunta del Instituto de Tecnología de Georgia en los Estados Unidos de América, que participó en un PCI de apoyo a la investigación para reforzar la seguridad informática—. No sustituirá la mano de obra, sino que creará recursos y conocimientos que harán de la detección y la respuesta tempranas en el ámbito de la seguridad informática objetivos realistas”.

Gracias a los algoritmos avanzados de aprendizaje automático, la IA también puede ayudar a las instalaciones nucleares y radiológicas a reforzar sus defensas contra los ciberataques mediante la detección de anomalías en los datos de los sistemas informáticos. Los sistemas de seguridad física asistidos por IA pueden monitorizar y analizar constantemente grandes cantidades de datos para determinar si se produce alguna actividad anómala en el funcionamiento normal de las instalaciones. Mediante los ciberataques se pueden introducir datos falsos para engañar con fines dolosos a los operadores de las instalaciones nucleares. En este caso, los sistemas asistidos por IA se pueden aprovechar para alertar a los responsables de una central nuclear de la más mínima variación en el funcionamiento normal. Al proporcionar un mayor conocimiento de la situación, la IA también permite detectar de forma temprana las acciones delictivas e impulsa la respuesta necesaria en caso de incidentes.

Desafíos que han de afrontarse

Los beneficios que ofrece la IA en las instalaciones nucleares y radiológicas dependen en gran medida de cómo se haya preparado el sistema de IA. La IA es tan inteligente como los datos de entrenamiento con los que trabaja y puede ser manipulada para ofrecer lecturas y resultados falsos si no dispone de los datos de entrada correctos, lo que sigue siendo un obstáculo importante para su uso en la esfera de la seguridad física nuclear. Incluso con los avances recientes en la tecnología de la IA, no es viable utilizarla como sustituto de un ser humano. La protección física, la contabilidad y el control de materiales nucleares y las mediciones directas —actividades esenciales para garantizar la seguridad física nuclear— requieren la intervención humana.

Otro desafío que presenta la IA en relación con la seguridad física nuclear es comprender cómo y por qué un modelo de IA ha tomado determinada decisión o ha hecho una predicción concreta. “La transparencia y la explicabilidad, que implica que las personas pueden entender la lógica que fundamenta las decisiones o las predicciones de la IA, son algunos de los problemas más importantes de los modelos de IA. A menudo no es fácil comprender cómo estos modelos llegan a

sus conclusiones, lo que dificulta confiar en sus resultados y garantizar la integridad de estos —señala Scott Purvis, Jefe de la Sección de Gestión de la Información de la División de Seguridad Física Nuclear del OIEA—. Ello se vuelve sumamente problemático cuando estos modelos sustituyen a los sensores que proporcionan mediciones directas y a la experiencia humana adquirida con las características singulares de cada instalación. Resulta poco factible ofrecer garantía alguna de la integridad del sistema sin un conocimiento avanzado previo exhaustivo de los algoritmos de IA para reconocer cómo y por qué se toman las decisiones".

Las orientaciones del OIEA sobre seguridad informática en aras de la seguridad física nuclear comprenden prácticas óptimas relativas a los sistemas de control humanos que sirven de guía a las instalaciones a la hora de determinar qué procesos pueden automatizarse mediante la IA y cuáles deben seguir contando con supervisión humana, al menos hasta que se conozcan los riesgos de esta tecnología en rápido desarrollo. También constituyen un recurso esencial que puede permitir a los países poner en marcha importantes medidas de seguridad informática para detectar y prevenir los ciberataques, así como para responder a ellos.

Además, el OIEA elaboró un PCI de apoyo a la investigación para reforzar la seguridad informática. Titulado "Mejora del análisis de incidentes de seguridad informática en instalaciones nucleares", el PCI reunió a representantes de 13 países con el fin de trabajar en la mejora de las capacidades de seguridad informática en instalaciones nucleares, incluidas las técnicas de IA, para detectar anomalías que indiquen ciberataques selectivos.

La carrera por adoptar tecnologías de IA

La IA ha demostrado su potencial para beneficiar a las personas que utilizan la tecnología nuclear con fines pacíficos. A medida que aumenta su uso para mejorar los procesos y las operaciones en las instalaciones nucleares y radiológicas, también debe aumentar la concienciación sobre los riesgos asociados a su adopción generalizada. Las organizaciones deben mantener un programa de seguridad informática robusto para garantizar la seguridad física nuclear mientras se benefician de la IA.

Para ello es necesario un cambio de paradigma fundamental en la forma de entender la confianza y el carácter estratégico. Hay que tener en cuenta todos los posibles puntos de fallo de un sistema, incluso los que no están relacionados con su diseño. Los agentes con fines dolosos pueden aprovechar la IA para crear programas maliciosos más sofisticados, automatizar ciberataques, explotar sesgos y vulnerabilidades de los modelos o eludir las medidas de seguridad física imitando el comportamiento de los usuarios legítimos. Esta "carrera de armamentos" entre defensores y detractores exigirá innovación y adaptación constantes.

La IA también puede ayudar a las instalaciones nucleares y radiológicas a reforzar sus defensas contra los ciberataques mediante la detección de anomalías en los datos de los sistemas informáticos. (Imagen: AdobeStock)

Un mayor uso de la tecnología de la IA para mejorar las medidas de seguridad informática en las instalaciones nucleares podría ofrecer importantes beneficios, entre ellos, una detección de amenazas optimizada, medidas de seguridad proactivas, una menor dependencia de la intervención humana y una mejor respuesta a los incidentes. Si aprovechan los beneficios de la IA y, al mismo tiempo, hacen frente a sus riesgos, las organizaciones pueden mejorar de manera considerable su seguridad informática ante la evolución de las ciberamenazas.