Comment l'intelligence artificielle changera la sécurité de l'information et la sécurité informatique dans le monde nucléaire

Par Mitchell Hewes

Les technologies de l'intelligence artificielle (IA) et d'apprentissage automatique pourraient révolutionner le monde, ouvrant la voie à des progrès et à des innovations sans précédent en transformant notre manière de produire l'information, de la consommer et de l'utiliser. À mesure que les technologies de l'IA deviennent de plus en plus sophistiquées, elles transformeront les industries, rationaliseront les processus et pourraient même influer sur nos modes de vie. Le nucléaire ne fait pas exception, et on peut s'attendre à des avantages de l'IA dans de nombreux processus et opérations des installations nucléaires et radiologiques.

Dans le même temps, les progrès rapides de l'IA comportent également une multitude de risques. Des acteurs malveillants peuvent utiliser l'IA pour lancer des attaques plus élaborées et ciblées ou s'en servir pour compromettre l'intégrité des réseaux, des systèmes et des informations sensibles dans les installations nucléaires et radiologiques.

Avantages pour la sécurité de l'information et la sécurité informatique

L'AIEA se prépare aux transformations induites par l'IA en encourageant la coopération internationale dans ce domaine afin que tous les pays puissent bénéficier des possibilités qu'elle offre tout en se préparant à atténuer les risques. Par des mécanismes tels que des réunions techniques et des projets de recherche coordonnée (PRC), l'AIEA soutient la mise au point, la diffusion et l'application de techniques issues de l'intelligence artificielle, ainsi que les contre-mesures et la défense contre les acteurs malveillants.

L'avantage le plus important de l'IA dans le domaine de la sécurité de l'information et de la sécurité informatique est peut-être la réduction de la dépendance à l'égard de l'analyse et de l'intervention humaines.

Les systèmes d'IA peuvent fonctionner 24 heures sur 24 et 7 jours sur 7 pour surveiller les réseaux et les systèmes et détecter les menaces. En automatisant ces tâches, les professionnels de la sécurité nucléaire peuvent se concentrer sur des activités plus stratégiques et intervenir plus efficacement en cas d'incident.

« Les capacités d'apprentissage adaptatif de l'IA peuvent être mises à profit pour renforcer la sécurité de l'information et la sécurité informatique en détectant rapidement les menaces et en fournissant automatiquement aux experts humains les informations dont ils ont besoin pour coordonner les interventions », explique Fan Zhang, professeur adjoint à l'Institut de technologie de Géorgie (ÉtatsUnis d'Amérique), qui a participé à un projet de recherche coordonnée de l'AIEA visant à soutenir la recherche sur le renforcement de la sécurité informatique. « Certes, l'IA ne remplacera pas le personnel, mais elle fournira des ressources et des connaissances qui rendront concrètement réalisables la détection et l'intervention rapides dans le domaine de la sécurité informatique ».

Tirant profit d'algorithmes avancés d'apprentissage automatique, l'IA peut également aider les installations nucléaires et radiologiques à renforcer leurs défenses contre les cyberattaques en décelant les données anormales dans les systèmes informatiques. Les systèmes de sécurité reposant sur l'IA peuvent surveiller et analyser en permanence de grandes quantités de données pour déterminer si une activité présente une anomalie par rapport au fonctionnement normal de l'installation. Les cyberattaques peuvent induire en erreur les exploitants d'installations nucléaires en générant des données falsifiées. Dans ce cas, les systèmes reposant sur l'IA peuvent être mis à contribution pour alerter les responsables d'une centrale nucléaire du moindre écart par rapport au fonctionnement normal. Par une meilleure compréhension de la situation, l'IA permet également la détection rapide des actes criminels et déclenche l'intervention nécessaire en cas d'incident.

Défis à relever

Les avantages de l'IA dans les installations nucléaires et radiologiques dépendent grandement de la manière dont le système d'IA a été entraîné. L'efficacité de l'IA dépend des données d'apprentissage avec lesquelles elle travaille, et elle peut être manipulée pour donner de fausses indications et de faux résultats si les données fournies ne sont pas correctes. Cette vulnérabilité reste un obstacle majeur à son utilisation en sécurité nucléaire. Même avec les progrès récents des technologies d'IA, elle ne saurait remplacer l'être humain. La protection physique, la comptabilité et le contrôle des matières nucléaires et les mesures directes, activités essentielles à la sécurité nucléaire, nécessitent une action humaine.

Un autre défi que pose l'IA en matière de sécurité nucléaire est de comprendre comment et pourquoi un modèle d'IA a pris une décision ou fait une prédiction particulière. « La transparence et l'explicabilité, c'est-à-dire la possibilité pour l'homme de comprendre le raisonnement qui sous-tend les décisions ou les prédictions de l'IA, font partie des principaux problèmes des modèles d'IA. Il est souvent difficile de comprendre comment ces modèles parviennent à leurs conclusions, et donc de faire

confiance à leurs résultats et d'en garantir l'intégrité », explique Scott Purvis, chef de la Section de la gestion de l'information à la Division de la sécurité nucléaire de l'AIEA. « Le problème s'accentue lorsque ces modèles remplacent les capteurs fournissant des mesures directes et l'expérience humaine des caractéristiques uniques de chaque installation. Il devient irréaliste de garantir l'intégrité du système à moins d'avoir au préalable une compréhension approfondie des algorithmes d'AI afin de savoir comment et pourquoi les décisions sont prises ».

Les orientations de l'AIEA sur la sécurité informatique pour la sécurité nucléaire contiennent notamment des meilleures pratiques de contrôle humain, afin d'aider les exploitants d'installations à mieux savoir quels processus peuvent être automatisés par l'IA ou doivent rester sous supervision humaine, au moins jusqu'à ce que les risques de cette technologie en plein essor soient connus. Elles constituent également une ressource essentielle que les pays peuvent utiliser pour mettre en place d'importantes mesures de sécurité informatique afin de détecter les cyberattaques, de les prévenir et d'y faire face.

En outre, l'AIEA a mis en place un PRC pour soutenir la recherche sur le renforcement de la sécurité informatique. Intitulé « Amélioration de l'analyse des incidents de sécurité informatique dans les installations nucléaires », le PRC a réuni des représentants de 13 pays qui ont travaillé à l'amélioration des capacités de sécurité informatique, notamment des techniques d'IA, dans les installations nucléaires afin de détecter les anomalies indiquant des cyberattaques ciblées.

La course à l'adoption des technologies de l'IA

L'IA a montré qu'elle pouvait bénéficier aux personnes qui utilisent la technologie nucléaire à des fins pacifiques. À mesure que son utilisation pour améliorer les processus et les opérations dans les installations nucléaires et radiologiques se répand, la prise de conscience des risques inhérents à son adoption massive doit également se généraliser. Les organismes doivent maintenir un programme de sécurité informatique solide pour garantir la sécurité nucléaire tout en tirant parti de l'IA.

Pour y parvenir, il faut changer radicalement la perception de la confiance et de la sensibilité. Chaque point de défaillance potentiel d'un système doit être pris en compte, même ceux qui ne sont pas liés à sa conception. Les acteurs malveillants peuvent se servir de l'IA pour créer des logiciels malveillants plus sophistiqués, automatiser les cyberattaques, exploiter les biais et les vulnérabilités des modèles ou contourner les mesures de sécurité en imitant le comportement d'utilisateurs légitimes. Cette « course aux armements » entre défenseurs et attaquants appelle des innovations et des adaptations constantes.

L'IA peut également aider les installations nucléaires et radiologiques à renforcer leurs défenses contre les cyberattaques en décelant les données anormales dans les systèmes informatiques. (Image : AdobeStock)

L'utilisation accrue des technologies de l'IA pour renforcer les mesures de sécurité informatique dans les installations nucléaires pourrait offrir des avantages importants, notamment une meilleure détection des menaces, des mesures de sécurité proactives, une diminution de la dépendance à l'égard de l'action humaine et une plus grande efficacité des interventions en cas d'incident. En tirant parti des avantages de l'IA tout en veillant à en maîtriser les risques, les organisations peuvent renforcer considérablement leur sécurité informatique face à l'évolution des cybermenaces.