كيف سيغيِّر الذكاء الاصطناعي ملامح أمن المعلومات والأمن الحاسوبي في القطاع النووي

بقلم ميتشل هيفيز

> "الذكاء الاصطناعي لن يحل محل القوى العاملة ولكن الموارد والرؤى التي يوفِّرها ستجعل الكشف المبكر عن تهديدات الأمن الحاسوبي والتصدي لها هدفاً يمكن تحقيقه فعلياً".
>
> — السيد فان جانغ، أستاذ مساعِد في معهد جورجيا التقني، بالولايات المتحدة الأمريكية

من شأن تكنولوجيات الذكاء الاصطناعي والتعلُّم الآلي أن تحدث ثورة في العالم وأن تفتح الأبواب لتقدُّم وابتكار لم يسبق لهما مثيل عن طريق تحويل كيفية إنتاجنا واستخدامنا للمعلومات وكيفية تصرُّفنا على أساسها. وستفضي تكنولوجيات الذكاء الاصطناعي التي تزداد تعقيداً وتطوراً اليوم إلى تحويل الصناعات وتبسيط الإجراءات، وقد تؤثِّر حتى في الطريقة التي نعيش بها حياتنا. وليس القطاع النووي مستثنى من هذه التحولات. فمن المرجَّح أن تبرُز فوائد الذكاء الاصطناعي في الكثير من الإجراءات والعمليات في المرافق النووية والمرافق الإشعاعية.

ولكن التقدم السريع في مجال الذكاء الاصطناعي يحمل معه أيضاً في الوقت ذاته العديد من المخاطر. فالجهات الفاعلة الخبيثة يمكن أن تستخدم الذكاء الاصطناعي لشن هجمات أكثر تعقيداً وموجَّهة بمزيد من الدقة، أو أن تستغله للإخلال بسلامة الشبكات والنظم والمعلومات الحساسة في المرافق النووية والمرافق الإشعاعية.

فوائد الذكاء الاصطناعي في مجال أمن المعلومات والأمن الحاسوبي

تستعد الوكالة للتحولات التي سيحدثها الذكاء الاصطناعي عن طريق تعزيز التعاون الدولي في هذا المجال لضمان استفادة جميع البلدان مما سيُتاح من فرص، ولكنها تستعد أيضاً للتخفيف مما سينشأ من مخاطر. ومن خلال آليات مختلفة مثل الاجتماعات التقنية والمشاريع البحثية المنسقة، تدعم الوكالة تطوير تقنيات الذكاء الاصطناعي والتوعية بها وتطبيقها، وتدعم كذلك التدابير المضادة والدفاعات التي تتيح مواجهة الجهات الفاعلة الخبيثة.

وتقليص الاعتماد على التحليل البشري والتدخل البشري هو ربما أهم مزايا الذكاء الاصطناعي في مجال أمن المعلومات والأمن الحاسوبي. فالنظم القائمة على الذكاء الاصطناعي يمكن أن تُشغَّل على مدار الساعة وطيلة أيام الأسبوع لرصد أي تهديدات قد تتعرض لها الشبكات والنظم. وعند أتمتة هذا النوع من المهام، يصبح لدى المهنيين العاملين في مجال الأمن النووي الوقت اللازم للتركيز على مهام أكثر اتساماً بالطابع الاستراتيجي وللتصدي للحادثات بمزيد من الكفاءة وقت حصولها.

وفي هذا الصدد، قال السيد فان جانغ، وهو أستاذ مساعِد في معهد جورجيا التقني، بالولايات المتحدة الأمريكية، كان قد شارك في مشروع بحثي منسق للوكالة من أجل دعم البحوث المتعلقة بسبل تعزيز الأمن الحاسوبي إنه "يمكن تسخير قدرات التعلُّم التكيُّفي الخاصة بالذكاء الاصطناعي من أجل تحسين أمن المعلومات والأمن الحاسوبي، وذلك عن طريق تحديد التهديدات بسرعة وتزويد الخبراء البشر تلقائياً بما يحتاجون إليه من معلومات لتنسيق أنشطة التصدي". وأضاف السيد جانغ أن "الذكاء الاصطناعي لن يحل محل القوى العاملة ولكن الموارد والرؤى التي يوفِّرها ستجعل الكشف المبكر عن تهديدات الأمن الحاسوبي والتصدي لها هدفاً يمكن تحقيقه فعلياً".

وبفضل خوارزميات التعلُّم الآلي المتقدمة، من شأن الذكاء الاصطناعي أيضاً أن يساعد المرافق النووية والمرافق الإشعاعية على تدعيم دفاعاتها لمواجهة الهجمات على الفضاء الإلكتروني من خلال تحديد البيانات الشاذة في النظم الحاسوبية. وتتيح نظم الأمن المدعومة بالذكاء الاصطناعي رصد كم هائل من البيانات وتحليلها باستمرار لتحديد ما إذا كان ثمة أنشطة شاذة في سياق العمل العادي للمرفق. ويمكن أن يدخِل منفِّذو الهجمات على الفضاء الإلكتروني بيانات مزيفة إلى النظم الحاسوبية ليضلِّلوا بصورة كيدية مشغِّلِي المرافق النووية. وفي حالات كهذه، يمكن الاستفادة من النظم المدعومة بالذكاء الاصطناعي لتحذير الجهات المسؤولة عن تشغيل محطات القوى النووية وتنبيهها حتى إلى أبسط التغيرات في العمليات الاعتيادية. ويعزِّز الذكاء الاصطناعي الوعي بالظروف القائمة، وبذلك يتيح أيضاً الكشف عن الأنشطة الجرمية في وقت مبكر والتصدي لها على وجه السرعة وبالطريقة المناسبة.

التحديات التي يتعين معالجتها

تعتمد الفوائد التي يقدِّمها الذكاء الاصطناعي في المرافق النووية والمرافق الإشعاعية اعتماداً كبيراً على الطريقة التي يُنمَّى بها نظام الذكاء الاصطناعي. وترتبط قوة الذكاء الاصطناعي ارتباطاً عضوياً بمتانة البيانات المستخدمة لتنميته ويمكن التلاعب بالنظم القائمة على الذكاء الاصطناعي لتعطي معلومات ونتائج خاطئة إذا لم تكن تحتوي على المدخلات الصحيحة. ولا يزال ذلك عائقاً كبيراً أمام استخدام الذكاء الاصطناعي في مجال الأمن النووي. وعلى الرغم من التقدم الذي شهدته تكنولوجيا الذكاء الاصطناعي حديثاً، ليس من الممكن استخدامها بديلاً للبشر. فالحماية المادية، وحصر المواد النووية ومراقبتها، والقياسات المباشرة تستلزم تدخلاً بشرياً لأنها أنشطة أساسية في ضمان الأمن النووي.

وأحد التحديات الإضافية المقترنة باستخدام الذكاء الاصطناعي فيما يخص الأمن النووي هو التمكُّن من فهم الطريقة التي ينتِج بها نموذج قائم على الذكاء الاصطناعي قرارات أو توقعات معيَّنة وسبب إنتاجه هذه القرارات أو التوقعات بالتحديد. وأوضح السيد سكوت بورفيس، رئيس قسم إدارة المعلومات التابع لشعبة الأمن النووي في الوكالة، أن "الشفافية والقدرة على شرح المخرجات – حين يكون باستطاعة البشر فهم سبب القرارات أو التوقعات التي ينتِجها الذكاء الاصطناعي – هما من أكبر المشاكل المرتبطة بنماذج الذكاء الاصطناعي. ومن الصعب في أحيان كثيرة فهم الطريقة التي تتوصل بها هذه النماذج إلى نتائجها. وبذلك، يصبح من الصعب أيضاً وضع الثقة بمخرجاتها وضمان سلامة هذه المخرجات". وأضاف السيد بورفيس قائلاً إن "الوضع يزداد صعوبةً إلى حد بعيد عندما تُستخدم هذه النماذج محل أجهزة الاستشعار التي توفِّر قياسات مباشرة والخبرات البشرية المكتسبة على أساس الخصائص الفريدة لكل مرفق. ولا يصح عندئذ وضع الثقة بسلامة النظم إلا إذا كان هناك فهم مسبق وشامل ومتقدم لخوارزميات الذكاء الاصطناعي يتيح معرفة الطريقة التي تُتخذ بها القرارات وسبب اتخاذها".

وتشمل إرشادات الوكالة بشأن الأمن الحاسوبي لأغراض الأمن النووي الممارسات الفضلى المتعلقة بالضوابط والموازين التي يؤمِّنها البشر. والهدف من هذه الإرشادات هو تعزيز الوعي داخل المرافق بالإجراءات التي يمكن أتمتتها باستخدام الذكاء الاصطناعي وتلك التي يجب أن يستمر الإشراف البشري عليها، على الأقل إلى حين معرفة المخاطر التي تنطوي عليها هذه التكنولوجيا الجديدة السريعة التطور. وتُعَدُّ الإرشادات المذكورة أيضاً مورداً أساسياً قد يمكِّن البلدان من اتخاذ تدابير هامة في مجال الأمن الحاسوبي للكشف عن الهجمات على الفضاء الإلكتروني ومنعها والتصدي لها.

وفضلاً عن ذلك، وضَعت الوكالة مشروعاً بحثياً منسقاً لدعم البحوث المتعلقة بسبل تعزيز الأمن الحاسوبي. ويُشار إلى أن هذا المشروع المعنون "تعزيز تحليل الحادثات المتعلقة بالأمن الحاسوبي في المرافق النووية" يضم ممثلين من 13 بلداً يعملون معاً لتحسين القدرات في مجال الأمن الحاسوبي، بما يشمل تقنيات الذكاء الاصطناعي في المرافق النووية من أجل الكشف عن الأنشطة الشاذة التي تشير إلى وجود هجمات موجَّهة تستهدف الفضاء الإلكتروني.

السباق نحو اعتماد تكنولوجيات الذكاء الاصطناعي

أثبَت الذكاء الاصطناعي ما لديه من إمكانات يمكن أن تعود بالفائدة على الأشخاص الذين يستخدمون التكنولوجيا النووية لغايات سلمية. وفي وقت يزداد فيه استخدام الذكاء الاصطناعي لتعزيز الإجراءات والعمليات في المرافق النووية والمرافق الإشعاعية، لا بد أيضاً من تعزيز التوعية بالمخاطر المقترنة باعتماد الذكاء الاصطناعي على نطاق أوسع. ويجب أن تحافظ المؤسسات على متانة برامجها الخاصة بالأمن الحاسوبي لضمان الأمن النووي وأن تستفيد في الوقت عينه من قدرات الذكاء الاصطناعي.

ويستلزم تحقيق ذلك نقلة نوعية جذرية في الطريقة التي يُنظر بها إلى مسألتَي الثقة والطابع الحساس للمعلومات. ويجب مراعاة كل مكامن الضعف التي يُحتمل أن تؤدي إلى تعطُّل النظم، حتى تلك التي لا تتعلق بتصميمها. ويمكن للجهات الفاعلة الخبيثة أن تستفيد من الذكاء الاصطناعي لاستحداث برامجيات خبيثة أكثر تطوراً وتعقيداً، أو أتمتة الهجمات على الفضاء الإلكتروني، أو استغلال أوجه التحيز والضعف في النماذج، أو تجاوز تدابير الأمن عن طريق تقليد سلوكيات المستخدمين المشروعة. وسيتطلب سباق التسلح هذا بين المدافعين عن أمن النظم ومنفِّذي الهجمات عليها بذل جهود مستمرة في مجالَي الابتكار والتكيُّف.

ومن شأن زيادة استخدام تكنولوجيا الذكاء الاصطناعي لتعزيز تدابير الأمن الحاسوبي في المرافق النووية أن تقدِّم فوائد مهمة، بما يشمل تعزيز الكشف عن التهديدات، واتخاذ تدابير أمن استباقية، وتقليص الاعتماد على التدخل البشري، وتحسين سبل التصدي للحادثات. وعن طريق الاستفادة من مزايا الذكاء الاصطناعي ومعالجة ما يحمله من مخاطر في الوقت ذاته، يمكن للمؤسسات أن تعزِّز الأمن الحاسوبي لديها إلى حد بعيد لمواجهة التهديدات السيبرانية الآخذة في التطور.

من شأن الذكاء الاصطناعي أيضاً أن يساعد المرافق النووية والمرافق الإشعاعية على تدعيم دفاعاتها لمواجهة الهجمات على الفضاء الإلكتروني من خلال تحديد البيانات الشاذة في النظم الحاسوبية.
(صورة: أدوبي شوك)