ضمان أمن التكنولوجيات الرقمية للجيل التالي من المفاعلات النووية

بقلم جوان ليو

تجلب جميع الابتكارات فوائد محتملة يمكن أن تثمر عن تحوُّل في الصناعات ولكنها قد تجلب معها أيضاً مخاطر محتملة. وفي المجال النووي، تدمج المفاعلات النووية المتقدمة، بما في ذلك المفاعلات النمطية الصغيرة، تكنولوجياتٍ مبتكرةً، ولا سيّما التكنولوجيات الرقمية التي تثمر عن حلول جديدة.

وثمة اهتمام متنامٍ بالمفاعلات النمطية الصغيرة. ولهذه المفاعلات النووية المتقدمة قدرة محدودة على توليد القوى النووية - تصل عادةً إلى 300 ميغاواط (كهربائي) لكلّ وحدة، وهو ما يعادل تقريباً ثلث قدرة مفاعلات القوى النووية التقليدية. غير أنّ استخدام التكنولوجيا الرقمية المتطورة في هذه المفاعلات الجديدة يجلب تحدّيات جديدة من حيث الأمان والأمن النوويين. ويوجَد اليوم على الصعيد العالمي أكثر من 80 تصميماً ومفهوماً للمفاعلات النمطية الصغيرة، وهذه التصاميم والمفاهيم في مراحل تطوير مختلفة.

وقال رودني بوسكويم إي سيلفا، مسؤول أمن تكنولوجيا المعلومات في الوكالة: "يتمثّل أحد التحديات الماثلة أمام نشر المفاعلات النمطية الصغيرة في كيفية تسريع تطوير التكنولوجيا الخاصة بها وإثبات مستوى استعدادها، وفي الوقت نفسه الحفاظ على الامتثال لمعايير الأمان والأمن النوويين". "وهو ما يعزز الحاجة إلى نُظم الأجهزة والتحكم الرقمية وحلول الأمن الحاسوبي التي يتعيّن مراعاتها والحفاظ عليها طوال دورة حياة المفاعلات النمطية الصغيرة".

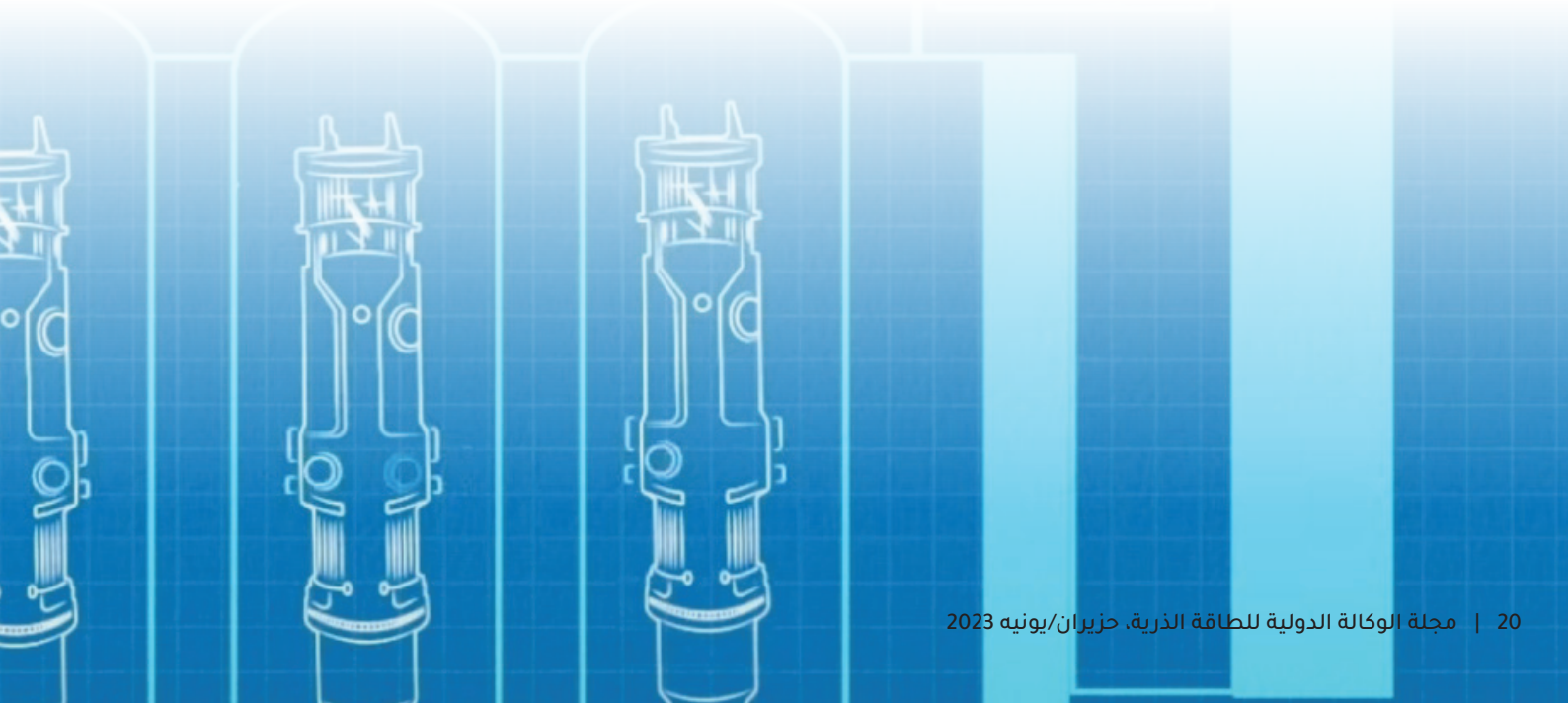
> **"الحاجة إلى تبادُل المعلومات ربما تستحدث مسارات يمكن أن يستغلها المجرمون السيبرانيون، وعليهِ تستلزم تطبيق اعتبارات أمنية سيبرانية قوية على البنية الأساسية للاتصالات"**
>
> — مايك سانت جون جرين، خبير الأمن الحاسوبي، المملكة المتحدة

الحلول والتحدّيات الحاسوبية

تعتمد التصاميم المبتكرة للمفاعلات النمطية الصغيرة على نُظم الأجهزة والتحكم الرقمية التي تمكّن ميزاتها المبتكرة. وتُبرز التكنولوجيات الرقمية المتزايدة اللازمة للأتمتة، والتحكم الإشرافي والصيانة عن بُعد، إلى جانب الميزات الجديدة الأخرى، الحاجة إلى حلول حاسوبية.

وبعض المفاعلات النمطية الصغيرة مصمَّمة لنشر القوى النووية في مناطق معزولة ولعدد محدود من الموظفين العاملين في الموقع، الأمر الذي قد يتطلب رصداً مستمراً وموثوقاً عن بُعد. ونظراً لتصميم نُظم الأجهزة والتحكم الرقمية، ينبغي أن يكون تطبيق تدابير الأمن الحاسوبي شرطاً أساسيًا للاتصال الآمن بين مواقع المفاعلات النمطية الصغيرة ومراكز الدعم. وقال مايك سانت جون جرين، خبير الأمن الحاسوبي المقيم بالمملكة المتحدة: "الحاجة إلى تبادُل المعلومات ربما تستحدث مسارات يمكن أن يستغلها المجرمون السيبرانيون، وعليهِ تستلزم تطبيق اعتبارات أمنية سيبرانية قوية على البنية الأساسية للاتصالات". وأضاف قائلاً: "يجب حماية سرية المعلومات وتوافرها وسلامتها لعمليات التشغيل عن بُعد لضمان التشغيل المأمون والموثوق للمفاعلات النمطية الصغيرة والبنية الأساسية المرتبطة بها".

والذكاء الاصطناعي والتعلّم الآلي يدعمان أيضاً العمليات التشغيلية للمفاعلات النمطية الصغيرة. ويشير الذكاء الاصطناعي إلى التكنولوجيات التي



تستحدث نُظماً قادرة على تتبُّع المشكلات المعقدة، بينما تتعلم تكنولوجيات التعلّم الآلي كيفية إكمال مهمة معيّنة بناءً على البيانات المتاحة. ومن خلال الجمع بين المحاكاة الرقمية للمرافق النووية ونُظم التحكم بالرصد بنُظم الذكاء الاصطناعي، تسعى الصناعة النووية إلى تحسين الوظائف المعقدة، الأمر الذي يمكن أن يزيد من الكفاءة التشغيلية. غير أن هذه الفوائد تقترن باحتمالية شنّ هجمات سيبرانية. فعلى سبيل المثال، تعتمد الخوارزميات القائمة على البرمجيات اللازمة للذكاء الاصطناعي والتعلّم الآلي على قواعد بيانات يمكن التلاعب بها للتسبّب بقرارات ذكاء اصطناعي خاطئة.

وقالت سي وين، طالبة دكتوراه من جامعة شينغوا في الصين: "هذه النظم ربما تكون خاضعة لحَقْن بالشفرة البرمجية، كأن يكون ذلك، على سبيل المثال، بتلقيمها عن قصد ببيانات خاطئة، في أثناء عملية تطوير البرمجيات أو توفيرها أو تثبيتها. ويتمثل التحدي العام في كيفية تحقيق شفافية كافية لخوارزميات الذكاء الاصطناعي/التعلّم الآلي. ويجب أن يكون الاستخدام المقبول للذكاء الاصطناعي/التعلّم الآلي معرّفاً تعريفاً واضحاً بمستويات مقبولة من المخاطر".

إدراج الأمن في التصميم

يتفق الخبراء على وجوب النظر في الأمن الحاسوبي للمرافق النووية منذ البداية. ويستند هذا النهج الاستباقي، المعروف باسم إدراج الأمن في التصميم، على أفضل الممارسات والدروس المستفادة من التجارب، ويطبّق مفهومَ "الإدراج في التصميم" ذاته الذي ينطبق أيضاً على الأمن النووي، والضمانات، والإخراج من الخدمة.

ويهدف إدراج الأمن الحاسوبي في التصميم إلى الحدّ من المخاطر الأمنية عند المصدر من خلال نَهْج يأخذ في الحسبان الأمن المنظّم والمتسق خلال جميع مراحل عمر المرفق أو العملية. وقال بوسكويم إي سيلفا: "يتعيّن النظر في تدابير الأمن الحاسوبي والحفاظ عليها طوال دورة حياة المفاعلات النمطية الصغيرة، من التصميم إلى التشغيل إلى الإخراج من الخدمة". وأضاف قائلاً: "عند النظر في الأمن، بما في ذلك الأمن السيبراني، منذ البداية، يمكن لمطوّري المرافق تقديم خيارات تصاميم تجعل المرافق أكثر أماناً وأمناً وكفاءةً وجدوى من حيث التكلفة".

دور الوكالة الدولية للطاقة الذرية

تجمع الوكالة الخبراء، من المنظمات النووية وغيرها من المنظمات، لمناقشة وتحديد قضايا وتحديات الأمن الحاسوبي فيما يتعلق بالسّمات التكنولوجية والتشغيلية للمفاعلات النمطية الصغيرة. فعلى سبيل المثال، في شباط/فبراير 2022، استضافت الوكالة اجتماعاً تقنيًا عن نُظم الأجهزة والتحكم والأمن الحاسوبي للمفاعلات النمطية الصغيرة، بهدف تعزيز التعاون وتيسير تبادُل المعلومات فيما بين الخبراء الدوليين. واتفق المشاركون على أن ثمة حاجة لتنسيق النُّهج واللوائح الوطنية لجعل السوق الدولية للمفاعلات النمطية الصغيرة مجديةً. وقال خورخي كازانوفا، الذي حضر الاجتماع كممثل للهيئة الرقابية النووية في الأرجنتين: "حلول الأجهزة والتحكم بشأن المفاعلات النمطية الصغيرة تفتح مجالاً تقنيًا جديداً كليًا. فالأتمتة المتنامية اللازمة لأنماط التشغيل الجديدة، والاستخدام المكثف للنُّظم الرقمية، يتطلبان تدابير للأمن الحاسوبي وحلولاً هندسية من مستوى التصميم بما يضمن التشغيل المأمون والآمن للمحطات".

وفي آذار/مارس 2023، عقدت الوكالة أيضاً حلقة عمل لمواصلة استكشاف تطوير القدرات التقنية فيما يتعلق بالأمن الحاسوبي ونُظم الأجهزة والتحكم للمفاعلات النمطية الصغيرة. وعلاوة على ذلك، تعتزم الوكالة إطلاق مشروع بحثي منسَّق عن هذا الموضوع في عام 2024.

يوجَد اليوم على الصعيد العالمي أكثر من 80 تصميماً ومفهوماً للمفاعلات النمطية الصغيرة، وهذه التصاميم والمفاهيم في مراحل تطوير مختلفة.