IAEA BULLETIN

مجلة الوكالة الدولية للطاقة الذرية

منشور الوكالة الرئيسي | حزيران/يونيه 2023 | www.iaea.org/ar/bulletin

الأمن الحاسوبي في العالم النووي

مجلة الوكالة الدولية للطاقة الذرية

يصدرها مكتب الإعلام العام والاتصالات
الوكالة الدولية للطاقة الذرية

Vienna International Centre

العنوان:
International Atomic Energy Agency
Vienna International Centre
PO Box 100, 1400 Vienna, Austria

الهاتف: 0-2600 (1 -43)

البريد الإلكتروني: iaeabulletin@iaea.org

مديرة التحرير: إيما ميدجلي
التصميم والإنتاج: ريتو كين

مجلة الوكالة متاحة على الموقع التالي:
www.iaea.org/ar/**bulletin**

الغلاف:
(Adobestock.com)

تابعونا على

IAEA

تكمن مهمة الوكالة الدولية للطاقة الذرية في منع انتشار الأسلحة النووية ومساعدة جميع البلدان، لا سيما في العالم النامي، على الاستفادة من استخدام العلوم والتكنولوجيا النووية استخداماً سلميًّا ومأموناً وآمناً.

وقد تأسَّست الوكالة كمنظمة مستقلة في إطار منظومة الأمم المتحدة في عام 1957، وهي المنظمة الوحيدة ضمن هذه المنظومة التي لديها الخبرة في مجال التكنولوجيات النووية. وتساعد مختبرات الوكالة المتخصصة الفريدة من نوعها على نقل المعارف والدراية إلى الدول الأعضاء في الوكالة في مجالات مثل الصحة البشرية والأغذية والمياه والصناعة والبيئة.

وتقوم الوكالة كذلك بدور المنصة العالمية لتعزيز الأمن النووي. وقد أسَّست الوكالة سلسلة الأمن النووي لتصدر في إطارها المنشورات المحتوية على الإرشادات المتوافق عليها دوليًّا بشأن الأمن النووي. وتركِّز أنشطة الوكالة أيضاً على تقديم المساعدة للتقليل إلى أدنى حد من مخاطر وقوع المواد النووية وغيرها من المواد المشعة في أيدي الإرهابيين والمجرمين، أو خطر تعرُّض المرافق النووية لأعمال شريرة.

وتوفِّر معايير الأمان الصادرة عن الوكالة المبادئ الأساسية والمتطلبات والتوصيات اللازمة لضمان الأمان النووي وتجسيد توافق الآراء الدولي حول ما يشكِّل مستوى عالياً من الأمان لحماية الناس والبيئة من التأثيرات الضارة للإشعاعات المؤينة. وقد وُضِعت معايير الأمان الخاصة بالوكالة لتطبيقها في جميع أنواع المرافق والأنشطة النووية التي تُستَخدَم للأغراض السلمية، وكذلك لتطبيقها في الإجراءات الوقائية الرامية إلى الحد من المخاطر الإشعاعية القائمة.

وتتحقَّق الوكالة أيضاً، من خلال نظامها التفتيشي، من مدى امتثال الدول الأعضاء للالتزامات التي قطعتها على نفسها بموجب معاهدة عدم انتشار الأسلحة النووية وغيرها من اتفاقات عدم الانتشار، والمتمثلة في عدم استخدام المواد والمرافق النووية إلا للأغراض السلمية.

ويشمل عمل الوكالة جوانب متعددة، وتشارك فيه طائفة واسعة ومتنوعة من الشركاء على الصعيد الوطني والإقليمي والدولي. وتُحدَّد برامج الوكالة وميزانياتها من خلال مقررات جهازي تقرير سياسات الوكالة، أي مجلس المحافظين المؤلَّف من 35 عضواً والمؤتمر العام الذي يضم جميع الدول الأعضاء.

ويوجد المقر الرئيسي للوكالة في مركز فيينا الدولي. كما توجد مكاتب ميدانية ومكاتب اتصال في جنيف ونيويورك وطوكيو وتورونتو. وتدير الوكالة مختبراتٍ علميةً في كلٍّ من موناكو وزايبرسدورف وفيينا. وعلاوةً على ذلك، تدعم الوكالة مركز عبد السلام الدولي للفيزياء النظرية في تريستي بإيطاليا وتوفر له التمويل اللازم.

تعاون الدور الأساسي للأمن الحاسوبي في الأمن والأمان النوويين

بقلم: رافائيل ماريانو غروسي، المدير العام للوكالة

وتيرة الابتكارات الرقمية مذهلة، فنحن أمام تكنولوجيات، مثل الذكاء الاصطناعي، تخطو خطواتٍ واسعة باتت تغيّر قواعد اللعبة حتى في غضون الأشهر القليلة الماضية. وستساعدنا هذه التطورات على تحسين العمليات التشغيلية التي يتمّ التحكم بها رقميًّا وتكنولوجيات الأتمتة في المرافق النووية، وما لذلك من فوائد محتملة على صعيد تحسين الكفاءة التشغيلية، وخفض تكاليف العمالة، وتحسين الأمان والأمن.

وبالفعل تتضمن تصاميم المفاعلات النووية المتقدمة، مثل المفاعلات النمطية الصغيرة والمفاعلات الصّغرية، خططاً لاستخدام الذكاء الاصطناعي والتعلّم الآلي لتمكين ميزات مبتكرة مثل الأتمتة، والتحكم الإشرافي والصيانة عن بُعد، وغرف التحكم المشتركة. لكن الابتكارات الرقمية، مثل الذكاء الاصطناعي والتعلّم الآلي، تنطوي أيضاً على تهديدات. وهي تستلزم اليقظة الدائمة لضمان سلامة الأصول الحسّاسة وحماية المعلومات في المرافق النووية والإشعاعية.

ولطالما استُخدمت البوابات والحرّاس لضمان حماية المرافق النووية من التخريب أو الجهات الفاعلة الخبيثة، إلا أننا أصبحنا اليوم نعتمد بشكل متزايد على النُّظم الرقمية. وتُستخدم نُظم الأجهزة والتحكم في المرافق النووية في تطبيقات الأمان والأمن الرئيسية. ومن شأن ذلك أن يحسّن الكفاءة، إلا أنّ علينا أن نكون متيقظين بشدة في حماية الأمن الحاسوبي. وتدرك البلدان في جميع أنحاء العالم أولوية مثل هذا الأمر.

وتضطلع الوكالة بدور فريد في ترسيخ التعاون فيما بين البلدان وتمكين عملية تقاسُم الدراية التكنولوجية وأفضل الممارسات في اعتماد التكنولوجيات السريعة التطور. وفي الوقت نفسه، نقوم بإسداء المشورة للبلدان عن كيفية الحدّ إلى أدنى مستوى ممكن من مواطِن الضعف المحتملة المصاحبة التي تؤثر في الأمن الحاسوبي والتخفيف من أثرها. وفي العامين الماضيين فحسب، زادت أنشطتنا العالمية للمساعدة في مجال الأمن الحاسوبي بأكثر من الرُّبع، مع التركيز بشكل خاص على الدعم على المستوى الوطني للوائح/عمليات التفتيش المتعلقة بالأمن الحاسوبي وتمارين الأمن الحاسوبي.

وما فتئت الوكالة تتصدّى لتحديات الأمن النووي التي تواجهها دولها الأعضاء بمجموعة من الأنشطة، بما في ذلك من خلال توفير الوثائق الإرشادية والتدريبات التي تمكّنها من وضع برامج وطنية متينة في مجال أمن المعلومات والأمن الحاسوبي. وتُستخدم هذه الإرشادات أيضاً كمعيار لتقييم برنامج أمن المعلومات والأمن الحاسوبي في بلد ما خلال الخدمة الاستشارية الدولية الخاصة بالحماية المادية، المعروفة باسم الخدمة الاستشارية IPPAS.

وبالإضافة إلى ذلك، نحن بصدد إطلاق دورة دراسية لتدريب الخبراء على وَضْع اللوائح المتعلقة بالأمن الحاسوبي. وقريباً سيتمكن عدد أكبر من البلدان من الوصول إلى الدورات التدريبية التي تنظّمها الوكالة في مجال الأمن الحاسوبي من خلال إطلاق منصة تعلُّم إلكترونية افتراضية.

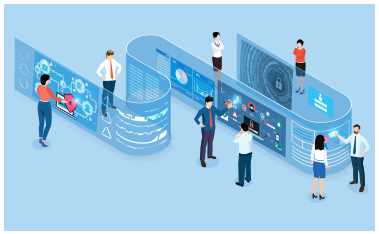
وفي موازاة ذلك، تدعم الوكالة التمارين الوطنية والإقليمية المتعلقة بالأمن الحاسوبي والتي من شأنها أن تزيد الوعي بخطر الهجمات السيبرانية وتأثيرها المحتمل على الأمن النووي. ونحن نعزز التعاون فيما بين الخبراء الدوليين وصانعي السياسات ونمكّن البحوث المصاحبة.

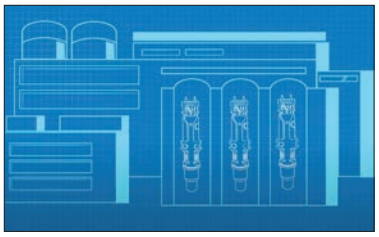
ومن المتوقع أن تنمو أنشطة الوكالة في مجال الأمن الحاسوبي، مع تزايد لجوء البلدان، بما فيها البلدان المنخفضة والمتوسطة الدخل، إلى التكنولوجيا النووية للوفاء بأولوياتها، بما في ذلك في مجال الطاقة النظيفة، ورعاية مرضى السرطان، والتغذية، والبحوث.

وخلال المؤتمر الدولي المعني بالأمن الحاسوبي في العالم النووي: الأمن من أجل الأمان، سنلتئم لمناقشة أبرز القضايا والحلول ورسم خريطة طريق للمُضيّ إلى الأمام، ما يمكّن القطاع النووي من تحقيق الاستفادة القصوى من الابتكارات الرقمية مع التفوّق في الوقت نفسه على كلّ مَن قد يستخدمها لإلحاق الضرر.

”من المتوقع أن تزيد أنشطة الوكالة في مجال الأمن الحاسوبي، حيث أن البلدان، بما في ذلك البلدان المنخفضة والمتوسطة الدخل، تتجه بشكل متزايد إلى استخدام التكنولوجيا النووية من أجل تلبية أولوياتها، بما في ذلك الطاقة النظيفة ورعاية مرضى السرطان والتغذية والبحث.“

— رافائيل ماريانو غروسي،
المدير العام للوكالة الدولية للطاقة الذرية





أسئلة وأجوبة

رؤية عالمية

تحديثات الوكالة

التصدّي لتهديدات الأمن الحاسوبي: تطوُّر برنامج المساعدة التابع للوكالة

بقلم فاسيليكي تافيلي

للتحوُّل إلى مجتمعات متصلة رقميًّا بالشبكات، حيث الأنشطة اليومية مترابطة فيما بينها بمساعدة النُّظم الحاسوبية والذكاء الاصطناعي والتكنولوجيات الرقمية، تأثيرٌ كبير على الأمان والأمن النوويين. ولا يمكن المبالغة في الحديث عن الدور الأساسي الذي تضطلع به التكنولوجيات الرقمية في الحفاظ على وظائف الأمان والأمن في المرافق التي تتعامل مع المواد النووية أو غيرها من المواد المشعّة.

وقالت إيلينا بوغلوفا، مديرة شعبة الأمن النووي بالوكالة: "للنُّظم الحاسوبية والتكنولوجيات الرقمية أهمية بالغة بالنسبة للمرافق والأنشطة المرتبطة بها حيث تُستخدم المواد النووية وغيرها من المواد المشعّة"، مؤكّدةً على حاجة جميع البلدان إلى تنفيذ برنامج للأمن الحاسوبي وتحسين الدفاع في العُمق عن الأمن النووي. وأضافت قائلة: "مع تقدُّم التكنولوجيا ، تتطلب حماية سرية وسلامة ومدى توافر المعلومات والأصول الحساسة التزامَ جانب اليقظة بشكل متواصل لدرء المخاطر والتخفيف منها، وبرنامجاً رصيناً لأمن المعلومات والأمن الحاسوبي".

وتمَّ للمرة الأولى تحديد الحاجة للتصدّي لتهديدات الأمن الحاسوبي، والهجمات السيبرانية الخبيثة، وأيّ مواطِن ضعف محتملة قد تُحدثها التكنولوجيات الرقمية، وأهمية الأمن الحاسوبي لأغراض الأمن النووي في قرار الأمن النووي الذي اعتمده المؤتمر العام للوكالة في دورته الخامسة والخمسين عام 2011. فقد أشار القرار إلى الجهود التي تبذلها الوكالة "لإذكاء الوعي بالتهديد المتنامي المتمثل في هجمات الفضاء الإلكتروني وأثرها المحتمل على الأمن النووي". وشجّع هذا القرار أيضاً الوكالة على إعداد وثائق إرشادية مناسبة، وتوفير دورات تدريبية، واستضافة المزيد من اجتماعات الخبراء الخاصة بالأمن السيبراني في المرافق النووية لمساعدة البلدان على حماية نفسها من الهجمات السيبرانية.

وقالت بوغلوفا: "في متابعة قرار المؤتمر العام في عام 2011، أخذت أنشطة الوكالة تركّز على تحسين قدرات الأمن الحاسوبي على مستوى الدولة ومستوى المرافق"، مضيفةً أن هذه الأنشطة أُدرجت بعد ذلك في خطط الأمن النووي اللاحقة الصادرة عن الوكالة، بما في ذلك تفاصيل التنفيذ الراهن لأنشطة الوكالة في مجال الأمن الحاسوبي الواردة في خطة الأمن النووي للفترة 2022-2025.

> **"النمو الملحوظ المتوقع في استخدام التطبيقات النووية السلمية، وتحديداً برامج القوى النووية، يحتّم علينا اعتبار أمن المعلومات والأمن الحاسوبي جزءاً لا يتجزأ من الأمن النووي ".**
>
> — إيلينا بوغلوفا، مديرة شعبة الأمن النووي في الوكالة

كيف تساعد الوكالة البلدان على وضع أو تحسين أمنها الحاسوبي؟

يُعدُّ إنشاء برنامج مُحكَم ومحدَّث للأمن الحاسوبي عنصراً أساسيًّا لحماية البلدان من الهجمات السيبرانية في البنية الأساسية الحساسة بكل أنواعها. وقد سارعت الوكالة إلى تقديم المساعدة للبلدان في جميع مراحل وَضْع البرامج الوطنية لأمن المعلومات والأمن الحاسوبي، بما في ذلك توفير الوثائق الإرشادية والتدريب.

وتوفر أربعة منشورات إرشادية لسلسلة الأمن النووي الصادرة عن الوكالة وثلاثة منشورات تقنية إضافية إرشاداتٍ في مجال أمن المعلومات والأمن الحاسوبي. وتُستخدم الإرشادات كأساس لوضع أطر وطنية للأمن الحاسوبي، بما في ذلك استراتيجيات وطنية، وأيضاً لأغراض لوائح الأمن الحاسوبي والتدريب في هذا المجال.

ويتمثل أحد المبادئ الأساسية للإرشادات الصادرة عن الوكالة في صَوْن الوظائف الحساسة في المرافق النووية من خلال حماية نُظم المعلومات والنُّظم الحاسوبية للحفاظ على بيئة مأمونة وآمنة للمرافق والمواد على حدّ سواء. ويتحقق ذلك من خلال وَضْع برنامج للأمان الحاسوبي (انظر الصفحة 6)؛ وتحديد وظائف الأمن النووي؛ واستخدام إدارة المخاطر لتحديد العواقب المحتملة للأمن المخترَق؛ وتحديد مستوى الأمن الحاسوبي المطلوب للأصول الرقمية الحساسة؛ وتنفيذ نَهْج متدرّج ومفاهيم الدفاع في العمق في مجال الأمن الحاسوبي. وينبغي تصميم هذه العناصر وتنفيذها على نحو يحُول دون الاختراق، ويساعد على تعزيز قدرة المشغّل على اكتشاف الاقتحامات والتصدّي لها، وكذلك التخفيف من التأثير المحتمل للهجمات السيبرانية.

وتوفر الوكالة، بناء على طلب البلدان، فرصاً تدريبية متنوعة لطائفة من الفئات المستهدفة. ويشمل ذلك السلطات المختصة، والمشغلين، والبائعين، والكيانات الأخرى التي يمكن أن تضطلع بمسؤوليات في مجال تنفيذ الأمن الحاسوبي. ويمكن لهذه الفئات أيضاً أن تستفيد من خبرة الوكالة في إجراء تمارين الأمن الحاسوبي كجزء من برنامج الأمن النووي.

بالإضافة إلى ذلك، هناك أربع دورات تعلُّم إلكتروني في مجال الأمن الحاسوبي، وهي متاحة مجاناً باللغات

العربية والصينية والفرنسية والإسبانية والروسية والإنكليزية من خلال منصة الوكالة للتعلم الإلكتروني الخاصة بشبكة التعليم والتدريب، ويمكن الوصول إليها عن طريق التسجيل أو عن طريق حساب على بوابة نيوكليس NUCLEUS. وستتوافر أيضاً قريباً منصة ابتكارية جديدة في مجال التدريب الافتراضي (انظر الصفحة 12).

وعلى نحو موازٍ، تدعم الوكالة تمارين الأمن الحاسوبي الوطنية أو الإقليمية كجزء من جهودها الرامية لزيادة الوعي بتهديد الهجمات السيبرانية وتأثيرها المحتمل على الأمن النووي. وتتضمن التمارين سيناريوهات مختلفة حيث تُستهدف نُظم المعلومات والنُظم الحاسوبية الحساسة بشكل مباشر أو غير مباشر كجزء من هجوم على كلّ من الحماية المادية والنُظم الإلكترونية.

وتأتي البحوث متممةً لأنشطة الأمن الحاسوبي التي تضطلع بها الوكالة، ولا سيما من خلال الآلية الراسخة للمشاريع البحثية المنسَّقة. فقد أُطلقت مشاريع بحثية منسَّقة في السنوات الأخيرة لتعزيز جهود الأوساط البحثية العالمية في مجال أمن المعلومات والأمن الحاسوبي، وزيادة جاهزية التصدّي للتحديات والمخاطر الناشئة (انظر الصفحة 18).

ماذا يُخفي المستقبل؟

برنامج الأمن الحاسوبي لأغراض الأمن النووي التابع للوكالة آخذ بالتطور المستمر. واعتماد المفاعلات النمطية الصغيرة والمفاعلات المتقدمة على التكنولوجيات المتقدمة والأجهزة الرقمية، والتأثير المتوقع للذكاء الاصطناعي، وظهور بيئات التعلُّم الافتراضي كلها أمور تنطوي على تحدّيات وهي مجالات لتوسيع نطاق الدعم المقدَّم إلى الدول.

وقالت بوغلوفا: "نشهدُ وعياً متنامياً على نحو متزايد بالتداعيات المحتملة أو الفعلية على الأمان والأمن النوويين فيما بين البلدان، والهيئات التنظيمية، والمشغلين، وسائر الجهات المعنيّة". وأضافت قائلةً: "النمو الملحوظ المتوقع في استخدام التطبيقات النووية السلمية، وتحديداً برامج القوى النووية، يحتّم علينا اعتبار أمن المعلومات والأمن الحاسوبي جزءاً لا يتجزأ من الأمن النووي"

الهجوم السيبراني

يُستخدم مصطلح "الهجوم السيبراني" لوصف عمل شرير يُنفَّذ بنيّة سرقة بند مستهدف محدد أو تعديله أو منع الوصول إليه أو إتلافه، من خلال الوصول غير المأذون به إلى نظام حاسوبي حساس أو تنفيذ إجراءات داخل هذا النظام. وتستهدف الهجمات السيبرانية سمة واحدة أو أكثر من سمات الأمن الحاسوبي، أي السرية والسلامة والتوافر، فيما يخصُّ معلومات حساسة موجودة في أصل رقمي حساس أو الأصل الرقمي الحساس نفسه، ويمكن استخدامها لتنفيذ أو يسير ارتكاب عمل شرير ضد أحد المرافق أو الأنشطة أو ارتكاب عمل إجرامي أو عمل آخر متعمد غير مأذون به باستخدام مواد نووية أو مواد مشعة أخرى.

ويمكن تنفيذ الهجوم السيبراني عن طريق الوصول المادي المباشر إلى المعلومات أو أصول المعلومات، أو عن طريق الوصول الإلكتروني، أو باستخدام مزيج من الطريقتين، ويمكن أن ينفِّذ الخصم الهجوم مباشرة أو أن ينفِّذه (أو يساعد الخصم على تنفيذه) طرفٌ داخلي، عن علم منه أو دون علم، تحت تأثير الخصم.

وينبغي معاملة الهجمات السيبرانية فور الكشف عنها على أنَّها حادثات متصلة بالأمن الحاسوبي.

هذا التعريف مأخوذ من المنشور المعنون "الأمن الحاسوبي لأغراض الأمن النووي " العدد G-42 من سلسلة الأمن النووي الصادرة عن الوكالة)

ما مقوّمات وضع برنامج للأمن الحاسوبي

بقلم فاسيليكي تافيلي وترينت نيلسون

تمثّل المرافق التي تتعامل مع المواد النووية أو غيرها من المواد المشعة، وتضطلع بالأنشطة المرتبطة بها، بنيةً أساسيةً حسّاسةً تستلزم مستويات عالية من الأمان والأمن. وباتباع نَهْج شامل ذي طبيعة استباقية إزاء الأمن الحاسوبي، يمكن للمؤسسات حماية أصول المعلومات الحسّاسة والنُّظم الحاسوبية في هذه المرافق مما قد يُخِلُّ بها. ويكمن أساس النَّهج الذي أوصت به الوكالة بشأن الأمن الحاسوبي في قيام الدول بتحديد متطلباتٍ لاستراتيجية وطنية أو سياسة وطنية، ما يمكّن من سرية وحماية المعلومات الحسّاسة ونُظم الحوسبة المتعلقة بالحماية المادية، والأمان النووي، وحصر المواد النووية ومراقبتها. ويمكن أن تأخذ هذه المتطلبات أيضاً شكل لوائح وطنية تنصُّ على إعداد وتنفيذ برنامج للأمن الحاسوبي*.

وبرنامج الأمن الحاسوبي هو إطار شامل يتضمّن العناصر الرئيسية لخطة فعّالة لتنفيذ سياسات وإجراءات الأمن الحاسوبي التي ستُستخدم طوال عمر مرفق نووي أو مرفق ينطوي على مصادر مشعّة. وهو يهدف إلى حماية أصول المعلومات الحسّاسة ونُظم الحوسبة ذات الأهمية البالغة للحفاظ على وظائف الأمان والأمن من التهديدات السيبرانية من أجل التخفيف من أثر الهجمات السيبرانية.

الاستراتيجية الوطنية

تستلزم استراتيجية الأمن الحاسوبي الشاملة والفعّالة نهجاً منظّماً يدمج عناصر مختلفة، بما في ذلك اللوائح، والبرامج، وتدابير الأمن الوقائية، وقدرات التصدّي للحفاظ على نُظم الأمن النووي الوطنية.

اللوائح

توفّر اللوائح الفعّالة إطاراً قانونيًّا لحماية النُّظم الحاسوبية الحسّاسة وتضمن أن يوجد لدى المؤسسات برنامج أمن حاسوبي قائم مع الضوابط المناسبة المعمول بها.

العناصر الرئيسية لبرنامج الأمن الحاسوبي:

الأدوار والمسؤوليات

للأدوار والمسؤوليات التنظيمية مع المساءلة أهميةٌ حيويةٌ بالنسبة للإدارة الفعّالة، خصوصاً عندما يتعلق الأمر بالبنية الأساسية الحسّاسة. والدراية بالتسلسل الهرمي التنظيمي والخطوط الواضحة لتسلسل السلطة، وهيكل الإبلاغ أمران ضروريان لغرس تعاون وتآزر يتسمان بالكفاءة والفعالية ضمن برنامج الأمن الحاسوبي.

إدارة المخاطر ومواطِن الضعف والامتثال

تتضمن إدارة مخاطر الأمن الحاسوبي تقييمَ مواطِن ضعف الأصول الرقمية والنُّظم الحاسوبية الحسّاسة وعواقبها المحتملة من أجل تنفيذ ضوابط أمن حاسوبي في نَهْج متدرّج لدرء الهجمات السيبرانية. وينبغي أن يتناسب مستوى التدابير الأمنية المطبقة مع مستوى المخاطر المرتبطة بالمعلومات و/أو النُّظم الحاسوبية التي تتمّ حمايتها. ومن خلال النظر في عواقب مواطِن الضعف أو التهديد، يمكن للمؤسسات تحديد مستوى التدابير الأمنية اللازمة للتخفيف من المخاطر.

تصميم الأمن وإدارته

يُعدُّ تصميم الأمن الحاسوبي جانباً بالغ الأهمية للحماية من التهديدات السيبرانية. وتشمل مبادئ التصميم الأساسية وضع نَهْج متدرّج والدفاع في العمق، حيث تُنفَّذ طبقات متعددة من الضوابط الأمنية المقسَّمة إلى مناطق للحؤول دون وقوع الهجمات والتخفيف من أثرها. ويجب أيضاً دَمْج متطلبات الأمن على امتداد دورة حياة تطوير النظام بما في ذلك أن تخضع منظمات الأطراف الثالثة لسياسات واتفاقات واضحة بما يضمن أن تكون الإجراءات الأمنية متسقة وفعّالة.

إدارة الأصول الرقمية

يعتمد الأمن الحاسوبي الفعّال على عملية منهجية لتحديد قائمة شاملة لجميع وظائف المرافق وأصولها ونُظمها بما في ذلك الأصول الرقمية الحسّاسة الضرورية لحماية العمليات النووية أو للحفاظ على الاستخدام المأمون والآمن للمواد النووية وغيرها من المواد المشعّة. وتوفر هذه القائمة أيضاً تدفقات البيانات وأوجُه الاعتماد المتبادل فيما بينها التي تُعدُّ مهمةً للمؤسسة لدعم ضوابط الوصول، والنُّسخ الاحتياطية، والتدابير الأمنية الأخرى لحماية هذه الأصول من التخريب أو السرقة.

الإجراءات الأمنية

توفر سياسات وإجراءات الأمن النووي التشغيلية التوجيهَ مع المساءلة لدعم مَنْع السرقة، أو التخريب، أو الاستخدام غير المأذون به للمواد والمرافق النووية. وتضمن هذه السياسات أن يخضع الوصول إلى المعلومات والأصول الحسّاسة لضوابط صارمة، وأن يتمَّ التحقُّق من الأفراد الذين لديهم إمكانية الوصول وتدريبهم بشكل مناسب.

إدارة الموظفين

الجدارة بالثقة والوعي والتدريب أمور بالغة الأهمية لإدارة الموظفين في الصناعة النووية. وينبغي تقييم الجدارة بالثقة لضمان أن يكون الموظفون موثوقين ومختصين وفي مأمن من أي تنازع للمصالح يمكن أن يُخِلَّ بالأمان والأمن. والحفاظ على موظفين مؤهلين وجديرين بالثقة أمر ذو أهمية بالغة لضمان الأمان والأمن النووية.

---

* يَرِدُ المزيد من التفاصيل في العدد T-17 (الصيغة المنقَّحة (Rev.1)) من سلسلة الأمن النووي الصادرة عن الوكالة، "Computer Security Techniques for Nuclear Facilities" (تقنيات الأمن الحاسوبي المستخدمة في المرافق النووية).

خطوات إلى الأمام في مجال الحماية المادية

الخدمة الاستشارية الدولية الخاصة بالحماية المادية تيسِّر تدعيم الأمن الحاسوبي

بقلم فاسيليكي تافيلي

على مدى ثلاثين سنة تقريباً، استخدمت بلدان عديدة الخدمة الاستشارية الدولية الخاصة بالحماية المادية والتابعة للوكالة (الخدمة الاستشارية IPPAS) للحصول على المشورة من أجل ضمان الحماية المادية لجميع أنواع المرافق التي تُستعمل فيها المواد النووية والمواد المشعة الأخرى، بما يشمل محطات القوى النووية ووحدات العلاج الإشعاعي في المستشفيات. ولكن بفضل التقدم التكنولوجي، باتت النظم الرقمية اليوم عنصراً أساسياً من العمليات في هذا النوع من المرافق. ونشأ عن ذلك الكثير من التحديات الجديدة على صعيد الأمن النووي.

وبغية التصدي للهجمات على الفضاء الإلكتروني التي تُعَدُّ خطراً حقيقياً يهدِّد المرافق، بما فيها المرافق النووية، أُضيفَت في عام 2012 وحدة أمن المعلومات والأمن الحاسوبي لأغراض الحماية المادية إلى الوحدات الأخرى المشمولة بالخدمة الاستشارية IPPAS. ومنذ ذلك الحين، تقدِّم البلدان عدداً متزايداً من الطلبات للاستفادة من هذه الوحدة في إطار استعراضات الخدمة الاستشارية IPPAS، وذلك لدعم عملها في مواجهة تهديدات أمن الفضاء الإلكتروني.

والخدمة الاستشارية IPPAS هي من العناصر الرئيسية لبرنامج الوكالة الخاص بالأمن النووي. وفي إطار هذه الخدمة، تُستعرض الممارسات القائمة في البلدان عن طريق مقارنتها بمقتضيات الصكوك الدولية المعنية وإرشادات الوكالة في مجال الأمن النووي. وعند الطلب، تُقدَّم المساعدة إلى البلدان من خلال الخدمة الاستشارية IPPAS لمساندتها في تعزيز المنظومات والنظم والتدابير الوطنية المتعلقة بالأمن النووي عن طريق توفير المشورة لها بشأن تطبيق الصكوك القانونية الدولية.

وقالت السيدة هيذر لوني، رئيسة قسم الأمن النووي للمواد والمرافق التابع لشعبة الأمن النووي في الوكالة إن "الخدمة الاستشارية IPPAS تطورت منذ إيفاد بعثتها الأولى قبل سبع وعشرين سنة، وباتت تعالج التحديات والاحتياجات الملازمة لهذا العصر". وأضافت أن "الحماية المادية من السرقة وأعمال التخريب والاستخدام غير المأذون به للمواد النووية والمواد المشعة الأخرى لا يمكن أن تؤمَّن بلا اتخاذ تدابير في مجال الأمن الحاسوبي. وحين تطلب البلدان إيفاد بعثة إليها في إطار الخدمة الاستشارية IPPAS، يمكنها الاستفادة من المشورة بشأن المسائل التي يمكن تحسينها والسبل المتوافرة لإجراء هذه التحسينات".

> **"الحماية المادية من السرقة وأعمال التخريب والاستخدام غير المأذون به للمواد النووية والمواد المشعة الأخرى لا يمكن أن تؤمَّن بلا اتخاذ تدابير في مجال الأمن الحاسوبي. وحين تطلب البلدان إيفاد بعثة إليها في إطار الخدمة الاستشارية IPPAS، يمكنها الاستفادة من المشورة بشأن المسائل التي يمكن تحسينها والسبل المتوافرة لإجراء هذه التحسينات."**
>
> — السيدة هيذر لوني، رئيسة قسم الأمن النووي للمواد والمرافق التابع لشعبة الأمن النووي في الوكالة

ويقوم النهج المتَّبع في سياق الخدمة الاستشارية IPPAS على خمس وحدات (modules) تغطي ما يلي: استعراض وطني لمنظومة الأمن النووي فيما يتعلق بالمواد النووية والمرافق النووية؛ واستعراض لنظم وتدابير الأمن في المرافق النووية؛ واستعراض خاص بأمن عمليات نقل المواد؛ واستعراض لأمن المواد المشعة وما يرتبط بذلك من المرافق والأنشطة؛ واستعراض لأمن المعلومات والأمن الحاسوبي. وقد أُوفِد حتى الآن ما مجموعه 97 من بعثات الخدمة الاستشارية IPPAS منذ تاريخ إيفاد البعثة الأولى في عام 1996. وطلب 22 بلداً إدراج الوحدة الخاصة بأمن المعلومات والأمن الحاسوبي في استعراض الخدمة الاستشارية IPPAS.

ما ينبغي أن تتوقعه البلدان خلال تقييم أمن المعلومات والأمن الحاسوبي؟

كخطوة أولى، يقوم فريق تابع للخدمة الاستشارية IPPAS، ومؤلف من خبراء دوليين في مجال الأمن النووي، بالنظر في الطريقة التي وضِعَت بها السياسات الوطنية المتعلقة ببرامج أمن المعلومات والأمن الحاسوبي وكيفية إدارتها. وبعد ذلك، ينظر الفريق في الإطار التشريعي والرقابي عن طريق مقارنة الإجراءات والممارسات القائمة في البلد المعني بالالتزامات المنصوص عليها في اتفاقية الحماية المادية للمواد النووية وتعديلها الصادر في عام 2005، وبالإرشادات المقدمة في منشورات سلسلة الأمن النووي الصادرة عن الوكالة. ويمكِّن ذلك الخبراء من تحديد ما إذا كان يتوافر لدى البلدان ما يلزم من السياسات والإجراءات لتأمين المستوى الكافي من الأمن الحاسوبي في المرافق النووية والمرافق الإشعاعية الحرجة.

وعلى مستوى المرافق، يُجرى استعراض للأمن الحاسوبي من أجل التدقيق في كيفية إدارة الأمن الحاسوبي، وبرنامج الأمن الحاسوبي (انظر الصفحة 6)، وضوابط الدخول، وبنية الأمن الحاسوبي الدفاعي، وطريقة كشف الأحداث المتعلقة بالأمن الحاسوبي والتصدي لها. ويمكن أن يجري الفريق أيضاً تقييماً في عدد من المجالات المتقاطعة، مثل إدارة المخاطر، والنُهُج المتدرجة، وثقافة الأمن النووي، وإدارة الموارد البشرية.

وفي عامَي 2015 و2018 على التوالي، استضافت اليابان بعثة من بعثات الخدمة الاستشارية IPPAS وبعثة المتابعة التي تلتها. وأفاد السيد هيرويوكي سوغاوارا، مدير الأمن النووي الدولي في شعبة الأمن النووي لدى الهيئة الرقابية النووية في اليابان بما يلي: "كان استعراض الوضع الراهن لتدابير الأمن الحاسوبي وتعزيز تحسينها استناداً إلى اقتراحات خبراء الاستعراض تجربة قيِّمة لليابان". وأضاف: "بناءً على نتائج استعراض الخدمة الاستشارية IPPAS، قررنا أن نعزِّز تدابير الأمن الحاسوبي وأن نزيد عدد المفتشين الذين هم من ذوي الخبرات في الميدان. وفضلاً عن ذلك، أدرجت الهيئة الرقابية النووية موضوع تهديدات الأمن الحاسوبي في تقييمها الوطني للتهديدات وطلبت من حامِلي الرخص أن يتخذوا تدابير صارمة لضمان الأمن الحاسوبي وأن يعزِّزوا محتويات خطط الأمن الحاسوبي الخاصة بهم عن طريق تضمينها تدابير مضادة لمواجهة الهجمات على الفضاء الإلكتروني".

وفي فرنسا، أفضت بعثة الخدمة الاستشارية IPPAS التي أُوفِدت إلى البلد في عام 2018 إلى تسليط المزيد من الأضواء على أهمية الأمن الحاسوبي في الإطار الوطني للأمن النووي. وذكر فريديريك بون، وهو مدير مشروع الأمن الحاسوبي في مكتب الأمن النووي التابع لمديرية الدفاع والأمن في الوزارة المعنية بالتحول في مجال الطاقة، أن "بعثة الخدمة الاستشارية IPPAS تطلبت التزاماً قوياً من جانب مختلف الجهات المعنية، وأتاحت لفرنسا فرصة تدعيم منظومة الأمن النووي الخاصة بها والتشجيع على تطبيقها". وتابع قائلاً إنه "تمت زيادة عدد الموظفين المختصين بالأمن الحاسوبي ووضِعَت مبادئ توجيهية رقابية تماشياً مع المعايير الدولية ومع إرشادات الوكالة في مجال الأمن النووي".

وتحفظ الوكالة قاعدة بيانات الممارسات الجيدة للخدمة الاستشارية الدولية المعنية بالحماية المادية منذ عام 2016 من أجل تقاسم نتائج بعثات الخدمة الاستشارية IPPAS مع الأوساط الدولية المعنية بالأمن النووي، وهو ما يعزِّز أثر المساعدة التي تقدِّمها الوكالة إلى بلدان العالم. وأوضحت السيدة لوني أن "حفظ قاعدة البيانات هذه وتقاسم هذا النوع من الأمثلة يتيحان توسيع نطاق فوائد بعثات الخدمة الاستشارية IPPAS كي تتجاوز حدود البلد المضيف وتشمل الأوساط الدولية المعنية بالأمن النووي، ويضاعفان أثر المساعدة التي توفرها الوكالة للدول الأعضاء فيها".

وترتبط أكثرية الممارسات الجيدة المتَّبعة على مستوى الدول بموضوع إدارة الأمن النووي الذي يمثِّل أساس الأمن الحاسوبي والتنسيق. وإضافةً إلى ذلك، تتوافر 40 ممارسة جيدة تتعلق بالأمن الحاسوبي على مستوى الدول وعلى مستوى المرافق، ويمكن للدول الأعضاء في الوكالة الاطِّلاع عليها من خلال جهات الاتصال المعيَّنة.

وتواصِل الوكالة دعم ما تبذله البلدان من جهود لتعزيز منظوماتها الوطنية الخاصة بالأمن النووي. ويُشار إلى أن عدد الطلبات الواردة من البلدان للاستفادة من بعثات الخدمة الاستشارية IPPAS في عامَي 2023 و2024 لا يزال عالياً.

منذ عام 1996، تقدِّم الخدمة الاستشارية الدولية الخاصة بالحماية المادية والتابعة للوكالة (الخدمة الاستشارية IPPAS) المساعدة إلى البلدان لتحديد سبل تعزيز حماية المواد والمرافق النووية.

(الصورة: الوكالة)

الوكالة تساعد البلدان الأفريقية على وضع لوائح الأمن الحاسوبي

بقلم أندريا راهانديني

من المتوقع أن يزداد الطلب في أفريقيا على النظائر المشعة في السنوات المقبلة، مع تزايد عدد البلدان التي تتوسع في الاستخدام السلمي للتكنولوجيا النووية. وقد أدّى تصاعد معدلات الإصابة بالسرطان إلى زيادة كبيرة في الطلب على الخدمات في مجالات العلاج الإشعاعي وعلم الأشعة والطب النووي. ومن ناحية أخرى، يتزايد الاعتماد على التطبيقات النووية في ميادين الصناعة والزراعة والعلوم. وقد أفضى ذلك إلى الطلب على زيادة إنتاج النظائر المشعة في مفاعلات البحوث. وتعمل هذه المفاعلات البالغة الأهمية بالاستعانة بنظم حاسوبية يمكن أن تكون عرضة للهجمات السيبرانية. وعلى غرار محطات القوى النووية، فمفاعلات البحوث بدورها مرافق نووية تتطلب خططاً مماثلة لحمايتها من أجل منع الهجمات الخبيثة المحتملة والتخفيف من آثارها والتصدي لها. وتعدُّ حماية المرافق النووية بجميع أنواعها من الهجمات المحتملة من هذا القبيل عنصراً أساسيًّا في استخدام التكنولوجيا النووية بطريقة مأمونة وآمنة في أفريقيا.

وفي إطار العمل على مواجهة هذه التهديدات، تستفيد بلدان عديدة في أفريقيا من الخبرات المكتسبة في مصر وغانا ونيجيريا، حيث يمتلك كلٌّ من هذه البلدان ويشغِّل مفاعلاً نوويًّا للبحوث. وبدعم من الوكالة، تعمل هذه البلدان الثلاث على وضع وتعزيز لوائح الأمن الحاسوبي، وتنفيذ برامج لضمان تأمين مرافقها بصورة مناسبة من الأعمال الحاسوبية الخبيثة التي يمكن أن تؤثر في الأمان والأمن النووين للمرافق

وقال السيد ترينت نيلسون، وهو مسؤول أول في مجال أمن المعلومات والأمن الحاسوبي في شعبة الأمن النووي التابعة للوكالة: "إنَّ أهمية الأمن الحاسوبي ما فتئت تتزايد لأنَّ التكنولوجيات الرقمية والنظم الحاسوبية مدمجة في الجوانب المتصلة بالأمان النووي والأمن النووي وبالجوانب التشغيلية في المرافق والعمليات المنطوية على مواد نووية ومواد مشعة أخرى". وأضاف أنَّ "الوكالة تعمل مع بلدان في أفريقيا على وضع لوائح الأمن الحاسوبي واستعراضها وتحسينها".

وفي مصر، تعمل الوكالة مع هيئة الرقابة النووية والإشعاعية المصرية على استعراض اللوائح القائمة بشأن الأمن الحاسوبي وسد الثغرات المحتملة في الجوانب الرقابية. ونُظِّمت في عام 2022 دورة تدريبية وطنية لإرساء القدرات الوطنية على إجراء عمليات التفتيش المتعلقة بالأمن الحاسوبي في المرافق النووية. وبالاستعانة بإرشادات الأمن النووي الصادرة عن الوكالة والتقنيات المتاحة للمفتشين، زوَّدت الدورة المشاركين بالمعارف والخبرات العملية اللازمة لتحسين تقييم فعالية الأمن الحاسوبي في المرافق النووية والإشعاعية.

وكانت السيدة نادية نوار، وهي مهندسة حواسيب في مرفق إنتاج النظائر المشعة التابع لهيئة الطاقة الذرية المصرية، واحدة من بين اثنين وعشرين مهنيًّا شاركوا في هذه الدورة التدريبية. وقالت السيدة نوار: "لقد تعلمتُ كيف تجري الهيئة الرقابية عمليات التفتيش المتعلقة بالأمن الحاسوبي وما هي الترتيبات الضرورية للأمن الحاسوبي التي يجب أن تنفذها الجهة المشغلة. ومنذ المشاركة في الدورة، صار بإمكاننا استعراض العناصر الرقابية المتعلقة بالأمن الحاسوبي والتحقق منها بفعالية أكبر. وقد ساعدتنا الدورة على وضع وتنفيذ برنامج للأمن الحاسوبي من أجل حماية المعلومات الحساسة في المرفق والأصول الرقمية الحساسة المعرضة للهجمات السيبرانية".

وفيما يخصُّ غانا، فقد أوفدت الوكالة بعثة خبراء إلى ذلك البلد في نيسان/أبريل 2023 لتقييم لوائح الأمن الحاسوبي الوطنية الحالية المعمول بها لدى الهيئة الرقابية النووية في غانا وبرنامج عمليات التفتيش الذي تنفذه الهيئة.

وقال السيد نيلسون كودزوتسي أغبيمافا، قائد فريق قسم الأمن السيبراني النووي في الهيئة الرقابية النووية في غانا: "لقد طرح تطوير الأمن الحاسوبي في غانا تحديات عديدة، بما في ذلك الافتقار للمعارف التقنية المحلية حول الموضوع، والجمع بين القضايا القانونية والدراية التقنية، وكيفية إدارة الموارد المطلوبة. وخلال عملية إرساء الإطار الرقابي، التمسنا الدعم من الوكالة وبلدان أخرى في إجراء استعراضات الخبراء لضمان اتباع نهج شامل ومنظَّم إزاء الأمن الحاسوبي".

وعلى ذات المنوال، أوفدت أيضا الوكالة بعثة خبراء إلى نيجيريا في تشرين الأول/أكتوبر 2022. وقالت السيدة إيثيل أوفوغبو، كبيرة المسؤولين الرقابيين

> **"ساعدتنا الدورة على وضع وتنفيذ برنامج للأمن الحاسوبي من أجل حماية المعلومات الحساسة في المرفق والأصول الرقمية الحساسة المعرضة للهجمات السيبرانية".**
>
> — السيدة نادية نوار، مهندسة حواسيب في مرفق إنتاج النظائر المشعة التابع لهيئة الطاقة الذرية المصرية

في الهيئة الرقابية النووية النيجيرية: "خلال الاستعراض الذي قادته الوكالة للخطة المتكاملة لدعم الأمن النووي في بلدنا في عام 2019، حُدِّدت الحاجة إلى وضع إطار تشريعي ورقابي فعال للأمن الحاسوبي. وبناءً على ذلك، قيَّمت الوكالة اللوائح الوطنية للأمن الحاسوبي وحددت الثغرات وقدمت الإرشادات اللازمة. وشملت النتائج إعداد مشروع اللائحة النيجيرية للأمن الحاسوبي في الأنشطة والمرافق النووية والإشعاعية". وتعمل نيجيريا في الوقت الراهن على استعراض مشروع اللائحة وتخطط لعقد دورة تدريبية حول عمليات التفتيش الحاسوبية.

وبالنظر إلى الزيادة في عدد طلبات المساعدة الواردة من البلدان، تعمل الوكالة على إعداد وثيقة تقنية لمساعدة البلدان على وضع العناصر الرئيسية في لوائح الأمن الحاسوبي. والوكالة جاهزة أيضاً لمساعدة العديد من البلدان الأخرى على صياغة اللوائح في مجال الأمن الحاسوبي حين تُطلق دورتها الدراسية بشأن صياغة عناصر لوائح الأمن الحاسوبي في آب/أغسطس 2023. وتهدف هذه الدورة الدراسية إلى مساعدة بلدان متعددة في الوقت نفسه على وضع لوائحها الوطنية للأمن الحاسوبي، بدلاً من تقديم المساعدة من الوكالة إلى فرادى البلدان كلٍّ على حدة. وبعد حلقة العمل الاستهلالية التي ستُعقد في آب/أغسطس، ستنظَّم الدورة الدراسية على أساس نصف سنوي في جميع المناطق. وستتاح الفرصة أمام المشاركين للعمل معاً من أجل صياغة استراتيجيتهم الوطنية للأمن الحاسوبي - بوصفها الأساس الرقابي لإرساء برنامج مُحكم للأمن الحاسوبي.

سيتم إطلاق دورة دراسية لصياغة عناصر لوائح الأمن الحاسوبي في آب/أغسطس 2023 بهدف مساعدة البلدان على وضع لوائحها الوطنية في مجال الأمن الحاسوبي

الابتكار في التدريب الافتراضي على الأمن الحاسوبي للمرافق النووية والإشعاعية

بقلم أنجاريكا ستروهال

تعمل اتجاهات التكنولوجيا الرقمية المتغلغلة في كلّ مكان والمتنامية باستمرار على تغيير حياتنا بسرعة وبشكل هائل. وتعتمد البنى الأساسية الحسّاسة اليوم، التي تشمل القوى النووية والاستخدامات السلمية الأخرى للتكنولوجيا النووية، اعتماداً كبيراً على التكنولوجيات الرقمية من أجل تشغيلها السّلس والموثوق. ومن المرجح أن تكون وعود التكنولوجيات الجديدة الآخذة بالتطور بوتيرة متسارعة، مثل الذكاء الاصطناعي، لحلّ المشكلات وتحسين العمليات التشغيلية التي يتم التحكم بها رقميًّا مفيدةً في تحسين التطبيقات النووية. وعليهِ، فإنها تُستخدم ويؤخذ بها اليوم في تصاميم المفاعلات المتقدّمة.

وعلى الرغم من أن هذه التكنولوجيات الرقمية تجلب معها العديد من الفوائد، إلا أنها، للأسف، قد تستحدث العديد من مواطِن الضعف المحتملة وغير المعروفة. ومردُّ ذلك إلى التهديد القائم للاختراقات السيبرانية أو الهجمات السيبرانية الخبيثة التي تستهدف المرافق النووية والتي قد تستغل هذه التكنولوجيات نفسها.

وكان من شأن عدد ونطاق الهجمات السيبرانية المعقدة بشكل متزايد أن أوجدَ طلباً ملحًّا داخل أروقة الصناعة النووية للتدريب على الأمن الحاسوبي للمرافق النووية والإشعاعية. وللمساعدة على تلبية هذا الطلب، أعدّت الوكالة الدولية للطاقة الذرية سلسلة من الدورات التدريبية التي تتناول مواضيع مختلفة، ابتداءً من أساسيات الأمن الحاسوبي، ووصولاً إلى الأمن الحاسوبي الأكثر تقدّماً لنُظم الأجهزة والتحكم.

ومن خلال توفير هذه الدورات التدريبية المخصَّصة والمتطورة والمتقدمة، والتي تتضمن تعلُّماً تجريبيًّا عمليًّا، تكون الوكالة قد حدّدت الحاجة إلى منصة إلكترونية بسيطة يمكنها توحيد منهاج الدراسة وتتيح استخدامه على نطاق أوسع وأكثر شمولية من قبل كيانات التدريب – دون مساعدة حضورية من الوكالة. فقد أبرزت قيود السفر إبّان جائحة كوفيد-19 والاستخدام الواسع النطاق للتكنولوجيات الافتراضية هذه الحاجة وسرّعت عملية تطوير المنصة.

وتهدف أداة التدريب الافتراضي، المسمّاة Learners (المتعلمون)، إلى توفير دورات تدريبية مرنة وشائقة في مجال الأمن الحاسوبي للأوساط النووية من خلال تقديم مواد تدريبية وتجربة التمارين العملية ضمن بيئة افتراضية. وكلُّ ما يحتاجه المشارك هو جهاز حاسوب واتصال موثوق بالإنترنت للوصول إلى جميع مواد الدورة التدريبية اللازمة. وقالت إيلينا بوغلوفا، مديرة شعبة الأمن النووي في الوكالة: "من المتوقع أن تضطلع المنصة الجديدة بدور محوري في تحسين الوعي بالأمن الحاسوبي والتدريب لأغراض الأمن النووي، وبناء مجتمع راسخ من الخبراء، والإسهام في تحسين الأمان والأمن في المرافق النووية وتلك المرافق المرتبطة بالمواد المشعة".

وابتداءً من حزيران/يونيه 2023، ستجعل الوكالة منصة Learners متاحة عالميًّا من أجل تحسين الأمن الحاسوبي في المرافق النووية، وكذلك في المرافق والأنشطة المنطوية على مصادر مشعة.

التدريب في مجال الأمن الحاسوبي والأنشطة الأخرى

وأبرمَ المعهد النمساوي للتكنولوجيا (AIT) – وهو مركز متعاون مع الوكالة في مجال أمن المعلومات والأمن الحاسوبي لأغراض الأمن النووي – شراكةً مع الوكالة لإنشاء منصة Learners.

وقال هيلموت ليوبولد، رئيس مركز الأمان والأمن الرقميين في المعهد النمساوي للتكنولوجيا: "تحقق بيئة التعلّم الافتراضية قيمة هائلة لزيادة القدرات التشغيلية وكذلك الاستراتيجية من خلال دعم أغراض التدريب المختلفة". وأضاف قائلاً: "من خلال محاكاة البيئات الفعلية، تمكّن هذه المنصة المتعلمين من اكتساب المهارات والخبرات العلمية الضرورية لإدارة الأمن النووي بشكل فعّال".

تعلُّم تحسين الأمن الحاسوبي

منصة Learners التابعة للوكالة متاحة عند الطلب لتحسين التدريب على الأمن النووي. وهذه المنصة مصمَّمة لتكون سهلة الاستخدام للجمهور على المستوى الدولي وتوفر دعماً متعدد اللغات. وتتسم المنصة بميزات مختلفة، مثل التمارين الموجّهة، والتعقيبات الفورية، وتكامل العرض التقديمي، والدعم المتعدد الشاشات. وهو ما يجعل المنصة قابلة للتكيّف ويمكن الوصول إليها للاستخدام من قبل منظمات التدريب والمستخدمين المباشرين.

ومنصّة Learners مصمَّمة كمنصة لتطوير وتوفير واستخدام بيئات المحاكاة التفاعلية، وبُنيت باستخدام تكنولوجيات المصادر المفتوحة. تشمل الوحدات الإضافية نُهجاً موحّدة لمنصات الحوسبة، وإتاحة البنية الأساسية وإتاحة البرمجيات، ما يمكّن من سهولة المشاركة وتبادُل المعارف مع المزوّدين الحاليين بالتدريب التابعين للوكالة والمنظمات الأخرى التي تعتزم استخدام المنصة.

وأُعِدَّ اثنا عشر تمريناً عمليًّا تم تقسيمها إلى ست مجالات مواضيعية قائمة على إرشادات الأمن النووي الصادرة عن الوكالة بشأن الأمن الحاسوبي. وأضافت بوغلوفا قائلة: "باستخدام بيئات افتراضية تمثل المرافق الفعلية، تعزز منصة Learners تنمية المهارات العملية وتدعم وصولاً أكثر إنصافاً إلى المعارف والمهارات".

وتُعدُّ منصة Learners أحد جوانب العمل الذي تضطلع به الوكالة لزيادة الوعي، وتعزيز التعاون، وتوفير الدعم للدول للتصدي لتهديدات الأمن السيبراني المتفاقمة في القطاع النووي. وأتيحت أنشطة بناء القدرات لأكثر من 120 بلداً خلال الأعوام الخمسة الماضية. وعلاوة على ذلك، كان من شأن الدعم المقدَّم من خلال بعثات الخبراء؛ والدورات التدريبية الوطنية والإقليمية والدولية؛ والاجتماعات التقنية؛ والحلقات الدراسية الشبكية تعزيزُ التعاون النشط، وتقاسُم المعارف، وتطوير المهارات. وبالإضافة إلى ذلك، تدعم الوكالة البلدان في تنظيم تمارين واسعة النطاق في مجال الأمن السيبراني.

تمرين عملي ومركز إيضاحي

وللمضي قُدُماً، من المهم للغاية مواصلة الاستثمار في مثل هذه المبادرات لبناء القدرات لضمان أعلى معايير الأمن النووي في جميع أنحاء العالم. ومن المقرر افتتاح المركز التدريبي والإيضاحي في مجال الأمن النووي التابع للوكالة والمزوَّد بأحدث التقنيات في النصف الثاني من عام 2023 للإسهام في تعزيز قدرات البلدان على التصدّي للإرهاب النووي من خلال اكتساب خبرات التمارين العملية. وستدمج الدورات التدريبية المبتكرة التي يطرحها المركز التدريبي والإيضاحي في مجال الأمن النووي مواضيع تتعلق بالأمن الحاسوبي وستشمل سيناريوهات للهجمات السيبرانية التي من الممكن أن تستهدف المرافق النووية أو المرافق والأنشطة المنطوية على مصادر مشعة.

> **"من خلال محاكاة البيئات الفعلية، تمكّن هذه المنصة المتعلمين من اكتساب المهارات والخبرات العلمية الضرورية لإدارة الأمن النووي بشكل فعّال".**
>
> — هيلموت ليوبولد، رئيس مركز الأمان والأمن الرقميين في المعهد النمساوي للتكنولوجيا

الفعاليات بحسب المناطق

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)

كيف تساعد تمارين الأمن الحاسوبي على زيادة التأهب للتصدي للهجمات السيبرانية في سياق الأمن النووي

بقلم إيما ميدجلي

جرت العادة تاريخيًا على أن تركّز المرافق النووية على ضمان أمن ما لديها من المواد النووية ضد الهجمات الشريرة من خلال إرساء تدابير للحماية المادية مثل الأسلحة النارية والحرّاس والبوابات. ولا تزال هذه التدابير تُستخدم بنجاح لتشييد تحصينات حول المرافق النووية من أجل منع سرقة المواد النووية أو المواد المشعة الأخرى أو تنفيذ أعمال تخريبية أو الوصول غير المأذون به إلى نُظم التحكم. بيد أنَّ العقود الأخيرة شهدت تفاقم تهديدات الهجمات السيبرانية في عالمنا الذي تسوده الوسائط الرقمية بصورة متزايدة. وجميع البلدان معرَّضة لهذه الهجمات، حتى البلدان الأكثر تقدُّماً على صعيد برامج القوى النووية وبرامج البحوث. ولذلك فإنَّ وضع أُطر وطنية للأمن الحاسوبي وللتصدي للتهديدات السيبرانية التي تستهدف المرافق النووية قد صار أمراً ضروريًا. ومن خلال عقد التمارين الواسعة النطاق، تدعم الوكالة البلدان في تحسين الحماية من الهجمات السيبرانية وتساعدها على تعزيز الكشف عن الهجمات السيبرانية على المرافق النووية واستراتيجيات التصدي لها.

وقد وضعت الوكالة تمارين للأمن الحاسوبي في محطات القوى النووية والمرافق الإشعاعية، ويجري تنفيذ هذه التمارين على المستوى الوطني في جميع أنحاء العالم. وتمكّن هذه التمارين البلدان من التمرن والتأهب للتصدي لأسوأ سيناريو قد تواجهه، وهو اختراق الأمن السيبراني في أحد المرافق النووية. ويمكن أن يؤدي التمرُّن على السيناريوهات النظرية إلى تحديد مواطن الضعف في السياسات والإجراءات والعمليات؛ والوقوف على الثغرات التي يجب سدها من خلال تقنيات التخفيف من الآثار و/أو بناء القدرات و/أو التغيير المؤسسي. وبالإضافة إلى مساعدة الدول على تنفيذ التمارين الواسعة النطاق لاختبار الأمن الحاسوبي في المرافق النووية، توفر إرشادات الأمن النووي الصادرة عن الوكالة بشأن الأمن الحاسوبي أيضاً مورداً أساسيًا يمكن أن يكفل للبلدان إرساء تدابير مهمة لأغراض الأمن الحاسوبي بغية الكشف عن الهجمات السيبرانية ومنعها والتصدي لها.

وقال السيد ترينت نيلسون، وهو مسؤول أول في مجال أمن المعلومات والأمن الحاسوبي في شعبة الأمن النووي التابعة للوكالة: "لا بدَّ من وضع السياسات وتحديد الأدوار والمسؤوليات وإرساء إجراءات مفصلة للتصدي لحادثات الأمن الحاسوبي قبل وقوع أي حادثة. وهنا يمكن أن تقدم الوكالة المساعدة في جوانب عديدة: من التمارين والإرشادات إلى تقاسم أفضل الممارسات والإجراءات لضمان التواصل الفعال وتوفير تدابير وافية لحماية الأمن".

وتشمل العوامل التي تجعل المرافق النووية عرضة للهجمات السيبرانية العناصر البشرية والتعقيدات التي تنطوي عليها سلسلة الإمداد، وتقاسم المعلومات الحساسة بين جهات معنية متعددة تستخدم نظماً حاسوبية لدعم الوظائف النووية.

وأضاف السيد ترينت نيلسون: "على سبيل المثال، في حال تنفيذ هجوم على جهة موردة وتزييف طلب عمل، مما يدفع موظفاً تقنيًا لديه حق الوصول المأذون به إلى القيام بعمل خاطئ مستتر. وهذا ليس إلا مثالاً واحداً على الأساليب التي يمكن أن تستخدمها الجهات الفاعلة الخبيثة لتخطي النظم الأمنية".

وعند العمل على التقليل من تأثير أي هجوم سيبراني محتمل، يتمثَّل أحد العناصر المهمة في إرساء الوعي والتواصل الفعال بين الأطراف المعنية، لأنَّ الجهات الفاعلة الخبيثة يمكن أن تستهدف أي جماعة أو فرد ضمن هذه الأطراف. وفي سياق الدفاع عن المرافق النووية، هناك أربع جهات فاعلة رئيسية، ألا وهي: الهيئة الرقابية؛ والجهة المشغلة للمرفق؛ ومنظمات الدعم التقني (أفرقة التصدي لحادثات الأمن الحاسوبي و/أو مراكز عمليات الأمن الحاسوبي)؛ ومنظمات الأطراف الثالثة، مثل الجهات البائعة ومنظمات الدعم. ويُعدُّ إجراء التمارين وسيلة جيدة لاختبار التواصل والإبلاغ والإخطار بين الجهات المعنية، وللتأكد والتحقق من الأمان والأمن في الهياكل التنظيمية.

وفي حين أنَّ السيناريو الأمثل هو أن يستحيل على المهاجمين السيبرانيين اختراق نظم الأمن الحاسوبي في المرافق النووية، فالجهات الفاعلة الخبيثة سريعة التطور والبشر معرضون لارتكاب الأخطاء بطبيعتهم، ومن ثم فمن شبه المستحيل التنبؤ بما ستنطوي عليه الهجمة الكبيرة المقبلة. ولذلك فالكشف عن الهجمات في الوقت المناسب أمر جوهري. وعُقد مؤخراً في سلوفينيا تمرين انطوى على هجوم سيبراني نظري من

> **"لا بدَّ من وضع السياسات وتحديد الأدوار والمسؤوليات وإرساء إجراءات مفصلة للتصدي لحادثات الأمن الحاسوبي قبل وقوع أي حادثة."**
>
> — السيد ترينت نيلسون، مسؤول أول في مجال أمن المعلومات والأمن الحاسوبي في شعبة الأمن النووي التابعة للوكالة

أجل المساعدة على التأكد والتحقق من قدرات الكشف والتصدي للدفاع ضد الهجمات السيبرانية.

وقال السيد سامو تومازيتش، رئيس شعبة الأمن السيبراني في إدارة الأمان النووي في سلوفينيا: "إنَّ لأمن الحاسوبي ليس مشروعاً ولا عملية إجرائية، بل هو رحلة تدوم مدى الحياة وتتطلب بذل الجهد والانتباه والتمرُّن بصورة مستمرة. والتمارين من النوع الذي عُقد في سلوفينيا تمكِّن جميع الكيانات المعنية في القطاع النووي من تقييم مدى إحكام خططها للتصدي للحادثات في حال النجاح في تنفيذ هجوم سيبراني".

وفي حالة وقوع حادثة خطيرة تتعلق بالأمن الحاسوبي ويمكن أن تتسبب في حدث متصل بالأمان النووي أو الأمن النووي، يجب أن يتدخل أحد أفرقة التصدي لحادثات الأمن الحاسوبي، بالإضافة إلى الأطراف المعنية المعتادة في المرفق النووي. وعلى سبيل المثال، يمكن أن تترتب على الحادثات من هذا القبيل مخالفة السياسات أو الإجراءات الأمنية؛ أو تأثيرات تمس بالأصول أو النظم الرقمية الحساسة؛ أو فقدان معلومات حساسة وفقدان السيطرة على وظائف جوهرية للأمان النووي.

وفي هذه الحالة، ففور الوقوف على وقوع حادثة مرتبطة بالأمن الحاسوبي أو على الإخلال بالأمن الحاسوبي، يعمل فريق التصدي لحادثات الأمن الحاسوبي مع الأطراف المعنية بالمرفق من أجل تحري الحادثة، وجمع بيانات التحليل الجنائي، وتحليل ماهية الحادثة ومكان وقوعها، والمساعدة على احتواء حالة التسلُّل والقضاء عليها لمساعدة الجهات المشغلة على إعادة المرفق النووي إلى حالة الاتصال العادية. وفي نهاية عملية التصدي، تُجَمّع أدلة التحليل الجنائي الحاسوبي للمساعدة على إجراء أي تحقيقات جنائية بشأن الهجوم، ولضمان تقاسم المعلومات بفعالية لزيادة تعزيز إجراءات الأمن الحاسوبي في المرفق النووي في المستقبل.

وفي التمرين الذي عُقد في سلوفينيا، كان الكشف عن الهجمات السيبرانية عاملاً أساسيًا في تمكين التصدي للحادثة الأمنية النظرية واختبار إجراءات التصدي للحادثات والتحقق منها. وتدعم هذه التمارين اختبار العلاقة بين الأمان والأمن والتأهب للطوارئ، وتُعزز نظم الأمن النووي من خلال تحديد مواطن الضعف المحتملة وإعداد التغييرات اللازمة لتحسين تأهبها بوجه عام من أجل التصدي للتهديدات التي يمكن أن تمس بالأمن السيبراني. وبالإضافة إلى ذلك، تتيح هذه التمارين فرصة لاختبار قنوات الاتصال الوطنية والدولية المستخدمة في الإخطار والإبلاغ. وعموماً، يُعدُّ إجراء تمارين الأمن الحاسوبي بانتظام جانباً مهمًّا من المحافظة على أمن المرافق النووية.

يتمثَّل أحد العناصر المهمة في التقليل من احتمال تأثير أي هجوم سيبراني في إرساء الوعي والتواصل الفعال بين الأطراف المعنية.

(صورة: أدوبي شوك)

تعزيز تقنيات الكشف عن الحالات الشاذة المتعلقة بالأمن الحاسوبي من خلال المشاريع البحثية المنسقة

بقلم رودني بوسكيم إي سيلفا وأندريا راهانديني

يستلزم تحديد الحالات الشاذة في عمليات النظم الحاسوبية التي تتحكم بوظائف الأمان والأمن الحرجة توافرَ خبرات واسعة النطاق، وينبغي اختبار التدابير المطلوبة وتحليلها وتعديلها لكي تكون متينة.

وفي هذا الصدد، قال السيد سكوت بورفيس، رئيس قسم إدارة المعلومات التابع لشعبة الأمن النووي في الوكالة: "يؤدي الكشف عن الحالات الشاذة دوراً مهماً في التقييم المبكر للتهديدات التي يُحتمل أن تستهدف النظم الحاسوبية في المرافق النووية والمرافق الإشعاعية". وتابع قائلاً: "في العادة، تستند تقنيات الكشف عن الحالات الشاذة إلى تطبيقات الذكاء الاصطناعي مثل التعلم الآلي، والأساليب القائمة على الإحصاءات والمعارف، أو غيرها من التكنولوجيات". وتُستخدم هذه التكنولوجيات لتحديد الانحرافات عن الاتصالات الشبكية أو قياسات العمليات المتوقعة، مما قد يكون مؤشراً أولياً إلى اختراق جهة متسللة دفاعات أحد النظم الحاسوبية، ويمكن أن تتيح الكشف عن الهجمات السيبرانية في الوقت الفعلي.

والتكنولوجيات المذكورة مهمة لأنه يمكن لجهة فاعلة خبيثة ذات قدرات عالية في المجال السيبراني أن تدخِل برامجيات خبيثة تخل بوظائف الأمان أو الأمن في النظم الرقمية، وأن تزوِّر البيانات المستمدة من أجهزة الاستشعار والمؤشرات التي تُرسل إلى الجهات المشغلة. ويعني ذلك أن الجهة المشغلة قد لا تكون على عِلم بحدوث نشاط خبيث وسيستند رد فعلها في بادئ الأمر إلى ما يظهر على شاشات غرفة التحكم، وهو أمر قد يضلِّلها ويجعلها تتخذ تدابير خاطئة. وعليه، فإن الجهة المشغلة لا يمكن أن تُعلَم على النحو الصحيح بحدوث هجوم سيبراني من هذا القبيل إلا من خلال الكشف المؤتمت عن أصغر الحالات الشاذة.

وبغية معالجة هذا المجال المهم من مجالات العمل وغيره من التحديات المتعلقة بالأمن الحاسوبي، أطلقت الوكالة مشروعاً بحثياً منسقاً محدداً في عام 2016.

ويشكل البحث والتطوير من خلال المشاريع البحثية المنسقة جزءاً لا غنى عنه من الأنشطة التي تقوم بها الوكالة من أجل ضمان الأمن الحاسوبي لأغراض الأمن النووي. وتنتج هذه المشاريع بحوثاً واستنتاجات عملية كثيرة تكمِّل الجهود التي تبذلها الوكالة باستمرار من أجل تعزيز قدرات البلدان على منع حادثات الأمن الحاسوبي والكشف عنها والتصدي لها والتعافي منها بعد وقوعها، لأن هذه الحادثات قد تؤثر بصورة مباشرة أو غير مباشرة في أمان المرافق النووية والمرافق الإشعاعية وأمنها.

وأضاف السيد بورفيس أن "أساليب الخصوم تزداد تعقيداً وتطوراً وتفرض قدراتهم في المجال السيبراني تحديات متزايدة على مطوِّري أدوات الكشف عن الحالات الشاذة" وأن "تطوير تقنيات للكشف عن الحالات الشاذة يتطلب الحصول على بيانات واقعية ومتسقة فعلياً بشأن عمليات الشبكات والمحطات من أجل تدريب نماذج الكشف واختبارها".

وضع سيناريوهات للهجمات السيبرانية من أجل بناء القدرات

أفضى المشروع البحثي المنسق الذي أُطلق في عام 2016 تحت عنوان "تعزيز تحليل الحادثات المتعلقة بالأمن الحاسوبي في المرافق النووية" إلى نتائج مهمة مثل إتاحة إجراء المزيد من البحوث بشأن أدوات وتقنيات محددة الهدف كان من المستحيل دراستها في السابق من دون أن يكون هناك خطر الكشف عن معلومات حساسة خاصة بالمرافق النووية والمرافق الإشعاعية.

وأنشأ فريق المشروع البحثي المنسق، الذي يتألف من باحثين من 13 بلداً و17 منظمة، مرفقاً وهمياً يُعرف باسم محطة "أشيرا" (Asherah) للقوى النووية. وقد طوَّرت جامعة ساو باولو جهاز محاكاة (ANS) باستنادها إلى هذا المرفق. ووضَع الفريق بالتعاون مع الجامعة سيناريوهات واقعية لهجمات سيبرانية يمكن أن تحدث داخل المرافق النووية. وبفضل سيناريوهات الهجمات السيبرانية هذه، تسنى استطلاع تدابير الأمن الحاسوبي وتقييم فعاليتها، والبحث في العواقب التشغيلية المحتملة التي قد تنجم عن الإخلال بأصول رقمية. وعلاوةً على ذلك، عمل الفريق على جمع البيانات وتحليلها وعلى تطوير تقنيات للكشف عن الهجمات السيبرانية واختبارها.

وقال السيد ريكاردو ماركيس، وهو أستاذ في كلية البوليتيكنيك التابعة لجامعة ساو باولو بالبرازيل:

"من التقليدي أن يستخدم المزارعون الأسمدة النيتروجينية لتحسين محاصيلهم. ولكنهم قد يضيفون كمية من النيتروجين أكثر مما تستطيع النباتات امتصاصه. ولا يؤدي ذلك إلى إنتاج انبعاثات إضافية من أكسيد النيتروز فحسب، بل أيضاً يجعل النباتات أقل إنتاجية ويؤثر على دخل المزارعين".

— محمد زمان، عالم تربة في المركز المشترك بين الفاو والوكالة لاستخدام التقنيات النووية في الأغذية والزراعة.

"طوَّرنا جهاز المحاكاة ANS واستخدمناه بغية إنشاء مستودع بيانات لتدريب نماذجنا الخاصة بالتعلم الآلي وتقييم كفاءتها. وجمَع المشروع البحثي المنسق الذي أطلقته الوكالة شركاء دوليين لإجراء البحوث وتوفير معارف جديدة في هذا المجال". وأضاف أن "التعاون بين المشاركين في المشروع البحثي المنسق كان أساسياً لتأكيد صحة العمل المنجز".

وإضافةً إلى ذلك، استُخدمت نتائج المشروع البحثي المنسق لتوفير التعليم والتدريب بصورة متواصلة لعدد كبير من طلاب الدراسات العليا والباحثين في مجالات تخصص مختلفة. وأدى هذا الأمر إلى مواصلة تعزيز البحوث والجهود بغية الاستمرار في تحسين الأمن الحاسوبي في المرافق النووية والمرافق الإشعاعية.

وأفادت السيدة سي وين، وهي طالبة دكتوراه من جامعة شينغهوا في الصين، بما يلي: "أجريتُ قسماً من بحوثي، بصفتي طالبة دكتوراه، باستخدام جهاز المحاكاة ANS وواجهته المخصصة للتفاعل بين الإنسان والآلة، وهي واجهة تسمح للمستخدم بمراقبة ما يحدث والتفاعل مع جهاز المحاكاة الذي تم تطويره في إطار المشروع البحثي المنسق الذي أطلقته الوكالة". وتابعت قائلةً: "أجريتُ بحوثاً بشأن تقنيات الكشف عن الحالات الشاذة، وكان جهاز المحاكاة ANS أساسياً لإصدار البيانات اللازمة لتدريب خوارزمية كشف أُعدَّت لمحطات القوى النووية ولتقييمها. ومن دون التعاون بين جميع المعاهد المشارِكة والأدوات التي وضعها فريق المشروع البحثي المنسق، كان من المستحيل أن يكون الأمن السيبراني للنظم الرقمية الخاصة بمحطات القوى النووية موضوع بحثي الخاص بدرجة الدكتوراه".

ونتائج المشروع البحثي المنسق – بما يشمل جهاز محاكاة ANS والأدوات والإرشادات – متاحة لمعاهد البحوث المهتمة في جميع أنحاء العالم. ويمكن الحصول عليها من خلال ملء نموذج الطلب المتاح على البوابة الإلكترونية للمعلومات المتعلقة بالأمن النووي التابعة للوكالة، وتقديمه إلى الوكالة من خلال الهيئة الوطنية المختصة.

وفي الآونة الأخيرة، وتحديداً في عام 2023، أطلقت الوكالة مشروعاً بحثياً منسقاً جديداً بعنوان "تعزيز الأمن الحاسوبي في نظم الكشف عن الإشعاعات" بهدف البحث في المنهجيات والتقنيات التي تتيح تعزيز الأمن الحاسوبي في معدات الكشف عن الإشعاعات. وستتطرق المشاريع البحثية التي من المقرر تنفيذها في إطار المشروع البحثي المنسق الجديد، بمشاركة 12 منظمة (بما فيها مختبرات وطنية وجامعات ومعاهد بحوث وطنية) من 11 بلداً، إلى موضوع استخدام التكنولوجيات الرقمية الناشئة، مثل الحوسبة السحابية، وسيواصَل فيها استكشاف تقنيات مبتكرة للكشف عن الحالات الشاذة وتطويرها.

طوَّرت جامعة ساو باولو جهاز محاكاة استناداً إلى مرفق وهمي يُعرف باسم محطة "أشيرا" (Asherah) للقوى النووية.

(الصورة: الوكالة)

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".

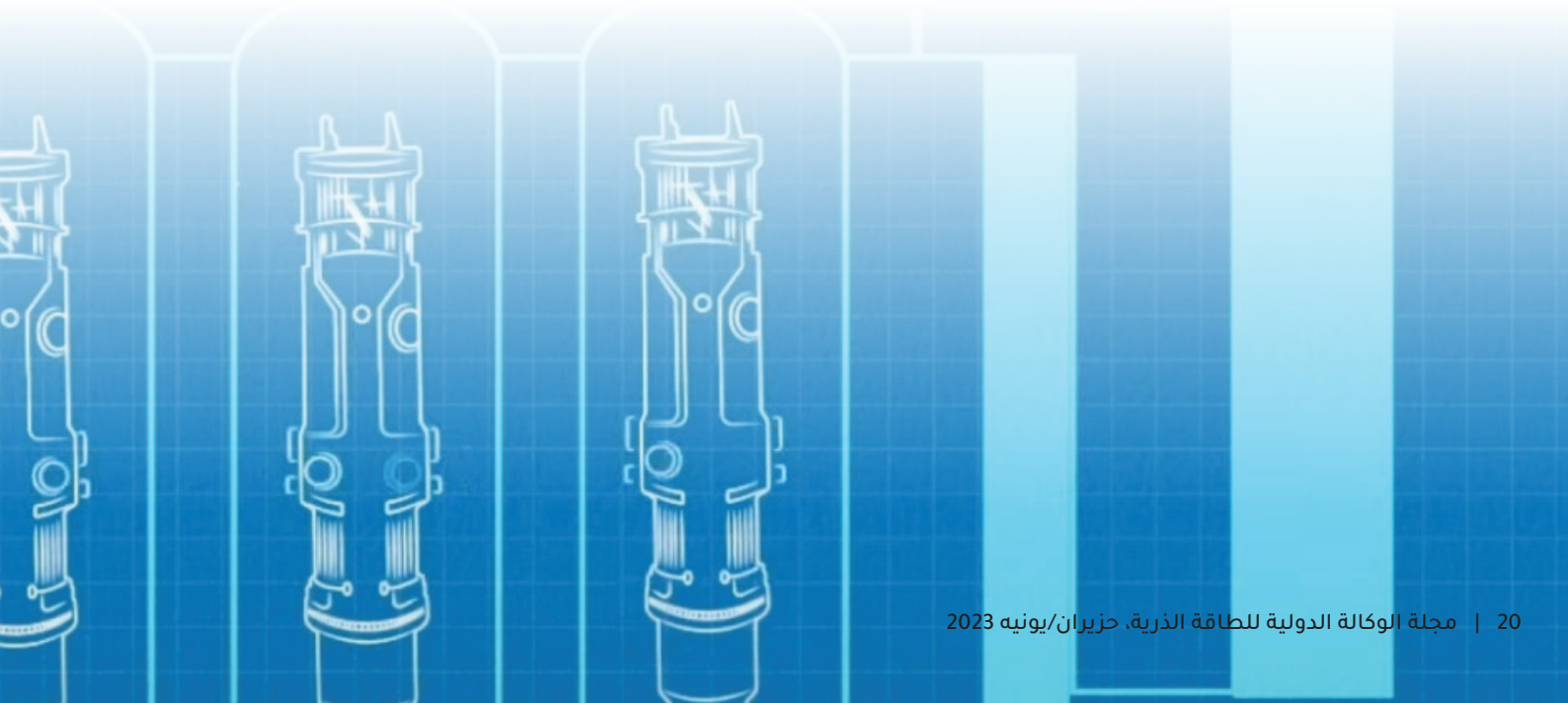
> **"الحاجة إلى تبادُل المعلومات ربما تستحدث مسارات يمكن أن يستغلها المجرمون السيبرانيون، وعليهِ تستلزم تطبيق اعتبارات أمنية سيبرانية قوية على البنية الأساسية للاتصالات"**
>
> — مايك سانت جون جرين، خبير الأمن الحاسوبي، المملكة المتحدة

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.

تعزيز الأمن الحاسوبي لأغراض الأمان والأمن النوويين

بقلم السيدة ليدي إيفرار

نائبة المدير العام ورئيسة إدارة الأمان والأمن النوويين في الوكالة

للأمان النووي والأمن النووي نفس الهدف ونفس الرؤية، وهما حماية الأفراد والمجتمعات والبيئة من الآثار الضارة التي يمكن أن تنجم عن الإشعاع المؤين. وصحيح أن الأنشطة التي تعالج الأمان النووي تختلف عن تلك التي تعالج الأمن النووي، ولكن لا بد من وضع نهج منسق جيداً لإدارة أوجه الترابط بين تلك الأنشطة. ومن المهم الحرص على تنفيذ التدابير المتعلقة بالأمان والأمن النوويين بطريقة تضمن الاستفادة من فرص التعزيز المتبادل التي يمكن أن تُتاح، من دون الإخلال بالأمان ولا بالأمن.

ومن المسلَّم به أن النظم والتدابير الخاصة بالأمن المادي في المرافق النووية والمرافق الإشعاعية هي ضرورية لحماية المعدات والنظم والأجهزة المخصصة عادةً للحفاظ على الأمان النووي ولصونها من أي عمل تخريبي متعمد يمكن أن يؤدي إلى إطلاق انبعاثات تكون لها عواقب إشعاعية. وفي التصاميم والتطبيقات القديمة، كان ينبغي في العادة حماية نظم الأمان من خلال اتخاذ تدابير خاصة بالحماية المادية فقط. بيد أن اتجاهات التكنولوجيا التي نشهدها اليوم والتي تنتشر على نطاق واسع وتزداد باستمرار تعزِّز إلى حد بعيد دور النظم الرقمية في ضمان كفاءة العمليات في المرافق النووية والمرافق الإشعاعية، ولا سيما عندما ترتبط بتلك المسؤولة عن وظائف المرفق المهمة، مثل نظم الأجهزة والتحكم، بما يشمل تلك التي تُستخدم لأغراض الأمان والأمن على حد سواء.

ويستلزم ضمان أمن هذه النظم مراقبة صارمة لتحديد مواطن الضعف وردع الدخول غير المأذون به إلى نظم التحكم الرقمية الذي قد يؤدي إلى الإخلال بوظائف الأمان أو الأمن. وفي هذا الإطار، تزداد أهمية موضوع الأمن الحاسوبي على صعيد الترابط بين الأمان والأمن، وتتم معالجته بوصفه جزءاً من مجالات رئيسية أخرى تشمل البنية الأساسية الرقابية؛ وترتيبات الهندسة المتعلقة

بتصميم المنشآت النووية وتشييدها؛ ومراقبة الدخول إلى المنشآت النووية؛ وتصنيف المصادر المشعة؛ والتصرف في المصادر المشعة والمواد المشعة، بما يشمل الوقود المستهلك ونواتج النفايات المشعة؛ والكشف عن المصادر غير الخاضعة للمراقبة واستردادها؛ وخطط التصدي للطوارئ وخطط الطوارئ.

وعلى المستوى الوطني، ينبغي أن يراعي واضعو السياسات الأمن النووي والأمان النووي معاً عند وضع اللوائح الخاصة بالأمن الحاسوبي. وإسناد المسؤوليات بوضوح، إضافةً إلى القيادة وإدارة المخاطر، هي أسس الترابط بين الأمان والأمن ولها نفس القدر من الأهمية فيما يخص تنفيذ تدابير فعالة لضمان الأمن الحاسوبي. ولكن في الوقت ذاته، يمثِّل الأمن الحاسوبي بطبيعته تحدياً عالمياً.

وفي هذا السياق، هناك اعتراف واسع النطاق بأهمية التعاون الدولي والدور المركزي الذي تؤديه الوكالة. ويُسلَّط الضوء على الترابط بين الأمان النووي والأمن النووي في معايير الأمان وإرشادات الأمن النووي الصادرة عن الوكالة. وتعمل الوكالة، منذ نحو عقد من الزمن، على تطوير مجموعة شاملة من أدوات المساعدة في المجال التقني المتمثل في أمن المعلومات والأمن الحاسوبي، وعلى توفيرها للبلدان بغية دعمها في اتخاذ تدابير فعالة للتصدي للهجمات السيبرانية التي يمكن أن تؤثر في الأمن النووي.

وعلاوةً على ذلك، تقدِّم الوكالة الدعم لغرض إيجاد أوجه تآزر بين النظم والتدابير الخاصة بالأمان والأمن النوويين لكي تكمِّل الخطوات المتخذة في المجالين إحداها الأخرى بدلاً من أن تخل إحداها بالأخرى.

وبالنظر إلى المستقبل، ستواصل أوجه التقدم التكنولوجي تعزيز أهمية الأمن الحاسوبي المتين لأغراض الأمان والأمن النوويين على مستوى الدول وعلى مستوى المرافق. فالتكنولوجيات السريعة التطور، مثل الذكاء الاصطناعي، هي تكنولوجيات واعدة من حيث حل بعض المشاكل وتحسين العمليات التي يتم التحكم فيها رقمياً. غير أنها تفرض في الوقت نفسه تحديات جديدة لا بد من معالجتها. وبالمثل، يُنظر حالياً في التكنولوجيات اللاسلكية وتكنولوجيات الأتمتة ويتم استخدامها اليوم في تصاميم المفاعلات النووية المتقدمة مثل المفاعلات النمطية الصغيرة والمفاعلات الصغرية. وفي ظل التطور المستمر والسريع للتهديدات السيبرانية، يستلزم الدعم الذي تقدِّمه الوكالة إلى الدول الأعضاء لتلبية احتياجاتها في مجال تعزيز الأمن الحاسوبي لأغراض الأمان والأمن النوويين قدرة على التحرك السريع بغية مواكبة جميع الفرص والتحديات الجديدة التي تنتج من هذه التكنولوجيات الجديدة، وذلك من أجل توفير أعلى قدر من الكفاءة في المعايير وأفضل الممارسات والتدريبات والمبادئ التوجيهية. وهذا هو ما تسعى إدارة الأمان النووي في الوكالة إلى تحقيقه باستمرار.

”على المستوى الوطني، ينبغي أن يراعي واضعو السياسات الأمن النووي والأمان النووي معاً عند وضع اللوائح الخاصة بالأمن الحاسوبي.“

— السيدة ليدي إيفرار، نائبة المدير العام ورئيسة إدارة الأمان والأمن النوويين في الوكالة

مواجهة التهديدات في عالم مُرقمَن على نحو متزايد

بقلم: فولفغانغ بيكو

في أيار/مايو 2022، أصبح المعهد النمساوي للتكنولوجيا (AIT) أول مركز متعاون مع الوكالة لأمن المعلومات والأمن الحاسوبي لأغراض الأمن النووي. ويقدّم المعهد النمساوي للتكنولوجيا الدعم للدورات التدريبية والتمارين الإقليمية والدولية في مجال الأمن الحاسوبي لفائدة المرافق والأنشطة النووية، وسيُعِدُّ وحدات إيضاحية تقنية بهدف زيادة الوعي بالتهديدات السيبرانية، وسيسهم في إعداد المواد التدريبية للمركز التدريبي والإيضاحي الجديد في مجال الأمن النووي في زايبرسدورف. ولفهم هذا التعاون بشكل أفضل، تحدّثنا إلى هيلموت ليوبولد، رئيس مركز الأمان والأمن الرقميَّين في المعهد النمساوي للتكنولوجيا.

ما المخاطر والتهديدات الناشئة في الأمن الحاسوبي بشكل عام؟

يُصنَع العديد من الأجهزة الرقمية الحديثة اليوم مع الأخذ في الحسبان وجود شبكات أوسع نطاقاً. والعديد منها بحاجة إلى الوصول إلى الإنترنت لكي تعمل. وينطوي كلُّ تطوير للبرمجيات على أخطاء محتملة يمكن أن تتسبَّب بمواطِن ضعف. من شأن الواجهات البينية ضعيفة الحماية والمستخدمين الذين يتصرفون بشكل غير مسؤول زيادة عدد التهديدات الأمنية لتشغيل نُظم تكنولوجيا المعلومات. يستغل المهاجمون مَواطِن الضعف في الأنظمة الرقمية من أجل النفاذ إليها.

وتتطور أساليب وأدوات الهجوم بما يتماشى مع تطوُّر عمليات الابتكارات الرقمية. وباتت برمجيات المخترقين "الهاكرز" متاحة الآن بسهولة على الإنترنت، ما يجعل شنّ الهجمات أسهل – حتى بالنسبة للمهاجمين الذين هُم أقلّ تأهيلاً. ونحن نواجه منظومة متنوعة للهجمات السيبرانية المدفوعة بالجريمة المنظمة، والتجسس الاقتصادي والصناعي، والإرهاب السيبراني.

لذلك، تهدّد اليومَ مجموعة واسعة من الهجمات السيبرانية المستخدمين والشركات والسلطات، ويمكنها مهاجمة البنية الأساسية الرقمية لدول بأكملها بالتزامن مع حملات التضليل المستهدفة، ما يهزُّ أُسسَ مجتمعاتنا.

هل تواجه الصناعة النووية التحديات نفسها؟

تستخدم الشركات والمستهلكون الأفراد في المقام الأول تكنولوجيا المعلومات القائمة على البيانات والموجهة نحو الاتصالات. وفي المقابل، تستخدم المرافق الإنتاجية والبنى الأساسية الحيوية ما يُسمّى بالتكنولوجيا التشغيلية التي ترصد وتتحكم في سلوكيات ونتائج عمليات إنتاجية محدَّدة.

وتقليديًا، كانت التكنولوجيا التشغيلية أقلّ ترابطاً بكثير من تكنولوجيا المعلومات. ومع ذلك، ومع تقدُّم التكنولوجيا، تقارَب المجالان، ويتم وَصْل برمجيات وأجهزة التكنولوجيا التشغيلية على نحو متزايد بشبكات أوسع نطاقاً.

”نحن نعمل بشكل وثيق مع زملائنا في الوكالة الدولية للطاقة الذرية في إعداد وحدات تدريبية، وعروض توضيحية، وتمارين للمركز التدريبي والإيضاحي في مجال الأمن النووي.“

— هيلموت ليوبولد، رئيس مركز الأمان والأمن الرقميَّين، المعهد النمساوي للتكنولوجيا

ويثير هذا التطور إشكاليةً، فالوعي بالأمن السيبراني أقلّ انتشاراً في مجال التكنولوجيا التشغيلية منه في مجال تكنولوجيا المعلومات.

وبالتالي، تصبح هذه التهديدات الجديدة لأمن تكنولوجيا المعلومات ذات أهمية للتكنولوجيا التشغيلية الخاصة بالإنتاج الصناعي والبنية الأساسية الحسّاسة. وتزداد أيضاً أهمية ذلك بالنسبة للصناعة

النووية، التي كانت تقليديًا تتّبع نهجاً متحفظاً وأبقت أنظمة التحكم معزولة.

ما الأنشطة التي يقوم بها المعهد النمساوي للتكنولوجيا لتعزيز الأمن السيبراني في مجال الأمن النووي؟

يقوم برنامج البحوث في المعهد النمساوي للتكنولوجيا بدراسة متمعّنة عن كيفية تأثير سيناريوهات التهديد الناشئة في نُظم التكنولوجيا التشغيلية ويهدف إلى تطوير الدراية والتوصل إلى حلول جديدة لزيادة مرونة البنى الأساسية الحيوية ضدّ الهجمات السيبرانية. وهذا العمل هو الأساس لوضع معايير أمان عالمية جديدة، وإجراءات اعتماد لعناصر النُظم الحاسمة الأهمية وهياكل النُظم الجديدة لتضمين تدابير الأمن السيبراني المتينة في نُظم التكنولوجيا التشغيلية عند البدء بتصميمها.

ويقدّم المعهد النمساوي للتكنولوجيا أيضاً تدريباً وتعليماً شاملَيْن للتأهُّب ضد هجمات الأمن السيبراني. وفي عمليات المحاكاة المعقدة لنظم تكنولوجيا المعلومات 'الافتراضية'، أو ما يُسمّى 'النطاقات السيبرانية'، يتفاعل المستخدمون ومطوّرو النُظم وموظفو التشغيل وممثلو الحكومات مع سيناريوهات واقعية للهجمات السيبرانية. وتُعدُّ عمليات المحاكاة بالغة الأهمية لضمان صمود نُظم تكنولوجيا المعلومات والتكنولوجيا التشغيلية والتي يمكنها صدّ التهديدات السيبرانية بشكّل فعال.

ما مزايا بيئة التعلم الافتراضية التي طوّرها المعهد النمساوي للتكنولوجيا والوكالة الدولية للطاقة الذرية؟

التجربة العملية هي عملية التعلُّم الأكثر فعاليةً. وقام كلّ من المعهد النمساوي للتكنولوجيا والوكالة الدولية للطاقة الذرية بتطوير 'النطاق السيبراني' الذي يوفر إنشاء 'توائم رقمية' للبنى الأساسية الرقمية الحيوية القائمة، والذي يوفر أيضاً التدريب على سيناريوهات التطبيق الواقعية للغاية.

وهنا، يمكن للمستخدمين من الحكومة والصناعة تقييم واختبار فعالية آليات الحماية وعمليات الأعمال.

وتدعم التجارب من 'النطاق السيبراني' إنشاء قدرات دفاعية مستدامة للمؤسسات العامة والخاصة على حدّ سواء.

إلى جانب التدريب الافتراضي، كيف يسهم عمل المعهد النمساوي للتكنولوجيا وخبراته في مجال الأمن الحاسوبي في تعزيز الأمن النووي؟

يمكننا المساعدة على درء هجمات المهاجمين، على سبيل المثال، بتطوير برمجيات ترصد الأجهزة "الطرفية" التيعادةً ما تربط الشبكات الداخلية للمؤسسات بالإنترنت. غالباً ما يستخدم المهاجمون هذه الأجهزة كنقاط دخول للنُظم قبل أن يتسببوا في الضرر.

ونحن نستخدم خبرتنا في كشف الاختلالات لتدريب البرمجيات التحليلية التي ترصد الأجهزة الطرفيّة المستخدَمة عادةً في نوع معيّن من المرافق النووية.

وويمكن لهذه البرمجيات أن تطلق إنذاراً أو أن تتخذ إجراءات مضادّة في حال تصرّف جهاز ما بطريقة غريبة. ونتيجة لذلك، يمكن للمشغلين اكتشاف الهجمات السيبرانية وردعها بالسرعة اللازمة قبل أن تتمكّن من إحداث ضرر كبير.

قبل عام واحد، عُيّن المعهد النمساوي للتكنولوجيا كأول مركز متعاون مع الوكالة لأمن المعلومات والأمن الحاسوبي لأغراض الأمن النووي، وما يزال المركز الوحيد من هذا القبيل اليوم. ماذا يعني هذا بالنسبة لعمل المعهد النمساوي للتكنولوجيا؟

نحن فخورون للغاية بتعييننا كمركز متعاون ونواصل دعم تقديم دورة تدريبية إقليمية بشأن الأمن الحاسوبي لنُظم القياس والتحكم في المجال النووي. وعُقدت الدورة مرّتين في عام 2022، بالاستعانة ببعض نتائج مشروعنا المشترك لتطوير منصة تعليمية افتراضية.

وشاركنا أيضاً في أنشطة تتعلق بالأمن الحاسوبي في تطوير مفاعلات نمطية صغيرة.

وحاليًا، نساعد الوكالة في الاستعدادات الجارية للمؤتمر الدولي بشأن الأمن الحاسوبي في العالم النووي 2023: الأمن من أجل الأمان، حيث سنجري عروضاً توضيحية لمنصة التدريب الافتراضية الخاصة بنا، وسنترأس جلسات نقاشية، وسنقدّم أوراقاً تتعلق ببحوثنا في هذا القطاع، إلى جانب أنشطة أخرى.

ما مشاركة المعهد النمساوي للتكنولوجيا في المركز التدريبي والإيضاحي في مجال الأمن النووي؟

نحن نعمل بشكل وثيق مع زملائنا في الوكالة الدولية للطاقة الذرية في إعداد وحدات تدريبية، وعروض توضيحية، وتمارين للمركز التدريبي والإيضاحي في مجال الأمن النووي. ونحن ندمج وحدات الأمن الحاسوبي في الدورات التدريبية المرتبطة بالحماية المادية للمواد النووية والمواد المشعة الأخرى، وكذلك تلك المرتبطة بالكشف عن المواد النووية والمواد المشعة الأخرى غير الخاضعة للتحكم الرقابي والتصدّي لها. والهدف من هذا الترتيب هو ترسيخ مفهوم أن الأمن الحاسوبي هو جزء لا يتجزأ من الأمن النووي ولا ينفصل عنه.

كيف يجعل التعاون الدولي العالم آمناً من التهديدات السيبرانية

تايغ سميث هو منظّم الفريق العامل A9 المنبثق عن اللجنة الفرعية 45A في اللجنة الدولية للتقنيات الكهربائية (IEC). وعُيّن من قبل لجنة لقيادة الفريق العامل A9 الذي يتعامل مع الأمن الحاسوبي في اللجنة الدولية للتقنيات الكهربائية.

اللجنة الدولية للتقنيات الكهربائية هي منظمة عالمية غير ربحية تعمل على تطوير المعايير الدولية لتصميم وتصنيع وتشغيل المعدات الكهربائية، بما في ذلك تلك المستخدَمة في محطات القوى النووية. تأسّست اللجنة الدولية للتقنيات الكهربائية في عام 1906، وتجمع أكثر من 170 بلداً وتنشر 10000 من المعايير الدولية الصادرة عن عنها.

تواجه الصناعة النووية تحدّياً لا يُستهان به في الحفاظ على الأمن الحاسوبي بسبب الاستخدام الواسع النطاق للأجهزة الرقمية. وهذا الاتجاه واضح للعيان في حياتنا اليومية، فقد شاعت وانتشرت الثلاجات الذكية، والإنارة الذكية، وسائر الأجهزة الذكية التي يتمّ التحكم فيها عن بُعد عبر الحوسبة السحابية. ونجد عناصر رقمية في العديد من النُّظم في المرافق النووية، التي لم تكن تحتوي في السابق على أيّ مكوّنات رقمية. وتوفر قوتها في الحوسبة، وطبيعتها القابلة لإعادة البرمجة، وقدرتها على الربط فيما بينها كفاءةً لا مثيلَ لها في دعم العمليات التشغيلية، والأمان النووي، والأمن النووي.

وتوضَع تصاميم المفاعلات النمطية الصغيرة وتصاميم سائر المفاعلات الجديدة الأخرى في عالم قائم في المقام الأول على التقنية الرقمية مع استخدام أكثر انتشاراً للنُّظم الحاسوبية من التصاميم السابقة. وقد تُصمَّم للعمل عن بُعد أو حتى بشكل مستقل، باستخدام البنية الأساسية للشبكة الحاسوبية للتواصل مع منصة تشغيل مركزية. ويمكن لهذا النَّهج أن يُستغلّ من جهات فاعلة خبيثة كجزء من هجوم ضد أحد تلك المرافق.

ومع ذلك، فإن هذا التحديث الرقمي للصناعة النووية يجلب معه المزيد من التحديات لأنه بدون أمن حاسوبي كافٍ يمكن أن تستغل جهاتٌ فاعلة خبيثة نقاط الضعف أو مواطِن الضعف كجزء من هجوم ضد أحد تلك المرافق.

ومن أجل مواجهة التحديات التي يفرضها مشهد التكنولوجيا الرقمية بتطوراته السريعة في المرافق النووية، وتلبية الحاجة إلى دعم النُّهج المنسَّقة فيما بين البلدان والمرافق، اعتمدت اللجنة الدولية للتقنيات الكهربائية نهجاً قائماً على العواقب المحتملة وموضوعاً عن عِلم بالمخاطر يتماشى مع إرشادات أمن المعلومات والأمن الحاسوبي ضمن سلسلة الأمن النووي الصادرة عن الوكالة. وبدلاً من اتّباع نَهْج يقوم على الإيعاز بما يجب فعله، ننصح باتّباع نَهْج متدرّج، ما يمكّن المؤسسات من تحديد مستوى التحكم المطلوب لمنتج ما أو عملية ما بناءً على العواقب المحتملة للهجمة السيبرانية. وعلى سبيل المثال، تتمثل الخطوة الأولى لوضع برنامج للأمن الحاسوبي في استعراض وظائف المرافق النووية، وتقييم تأثيرها على الأمان والأمن، وتحديد المستوى المناسب لمتطلبات الأمن.

المنع والكشف والتخفيف من الأثر

التنبؤ بكيفية تطوُّر الهجمات السيبرانية في المستقبل ليس بالأمر الهيّن، لذلك عملت اللجنة الدولية للتقنيات الكهربائية عن كثب مع الوكالة بأن وضعت معايير توصي بأن تركّز برامج الأمن الحاسوبي في المرافق

النووية على الكشف، والتصدّي، والتعافي بالإضافة إلى المنع. وحتى إذا ما نجحت عناصر هجمة سيبرانية ما، ينبغي أن تكون هناك آليات قيد التطبيق لاستعادة وضمان الأداء السليم للوظائف الضرورية بما يكفل عدم الإخلال بالأمان والأمن.

ويمكن للرَّقمنة السريعة في عالمنا، جنباً إلى جنب مع نمو الذكاء الاصطناعي والتعلُّم الآلي، أن تجعل الأمن الحاسوبي في المرافق النووية يبدو كمهمّة عسيرة. وللتعاون الدولي أهمية بالغة من أجل الاستمرار في تشغيل هذه المرافق على نحو مأمون وآمن على الرغم من هذه التحديات. فطوال أكثر من نصف قرن، تعاونت الوكالة، والمجتمع الدولي، والصناعة النووية في توحيد المعايير لدعم أمان وأمن التكنولوجيا النووية السلمية. وبعد أن باتت القضايا العالمية مثل تغيُّر المناخ وأمن الطاقة أكثر إلحاحاً، تتطلع بلدان عدّة إلى اللجوء إلى التكنولوجيا النووية الجديدة والمبتكرة كوسيلة لتوليد طاقة منخفضة الكربون، ما يجعل توحيد المعايير أكثر أهميةً للحفاظ على أمان وأمن المرافق النووية.

التعاون في العالم النووي

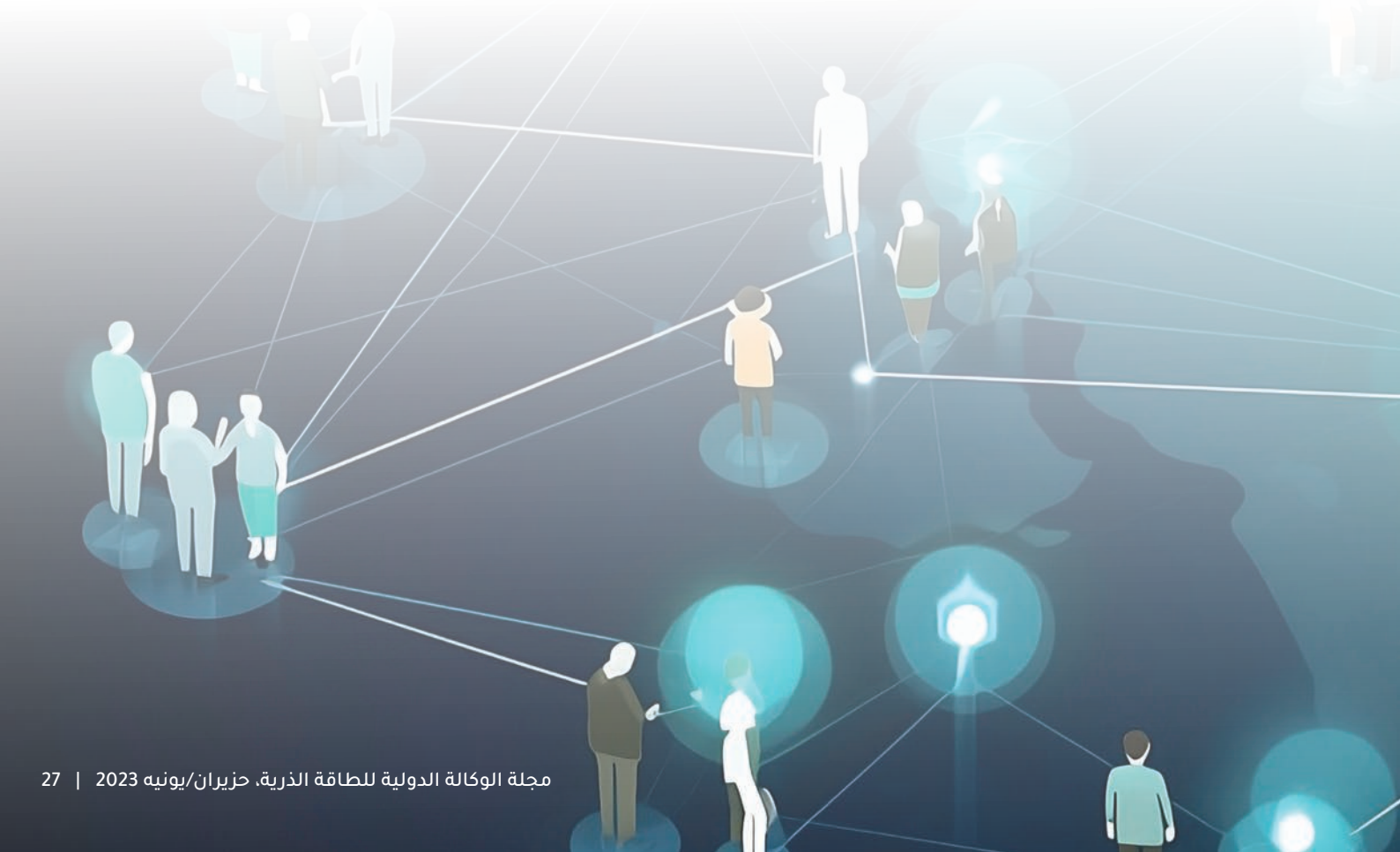
الوكالة الدولية للطاقة الذرية واللجنة الدولية للتقنيات الكهربائية مساهمان أساسيان في الجهود الدولية المبذولة لوضع معايير لأمن المعلومات والأمن الحاسوبي في المرافق النووية. وتقوم الوكالة بإعداد منشورات إرشادية ضمن سلسلة الأمن النووي يتمّ التوافق عليها دوليًا، لتحديد المفاهيم والقواعد اللازمة لضمان أمن المعلومات والأمن الحاسوبي كعنصرين أساسيّين لتحقيق أهداف الأمن النووي. وتوفر سلسلة الأمن النووي إرشادات بشأن تنظيم موارد الدولة، وإعداد لوائح القطاع، ومفاهيم تنفيذ نَهْج هندسةٍ مستنير سيبرانيًا في المرافق النووية.

وتعمل اللجنة الدولية للتقنيات الكهربائية عن كثب مع الوكالة، وذلك بصفةِ اللجنة منظمة دولية معنيّة بالمعايير وتروّج لأفضل الممارسات وتقاسُم المعارف. وبموجب مذكرة التفاهم بين اللجنة الدولية للتقنيات الكهربائية والوكالة الدولية للطاقة الذرية، يضع العلماء والخبراء الذين يعملون مع اللجنة الدولية للتقنيات الكهربائية معاييرَ وتقارير تقنية بشأن تنفيذ الإرشادات الصادرة عن الوكالة من خلال متطلبات برنامجية وهندسية محددة. ويمكن الاستفادة من هذه المتطلبات في تصميم وتطوير النُّظم الرقمية، الحالية والمستقبلية، والتي يمكن اعتمادها إزاء النماذج التنظيمية المتوافقة مع الإرشادات الصادرة عن الوكالة. ومن ثمَّ يمكن للخبراء الذين يمثلون تجربة الصناعة النووية في تنفيذ معايير اللجنة الدولية للتقنيات الكهربائية أن يدعموا عملية وضع الإصدارات المماثلة المستقبلية من الإرشادات الصادرة عن الوكالة.

ويسهم العلماء والخبراء في عمل اللجنة الدولية للتقنيات الكهربائية على أساس طوعيّ، وترحّب اللجنة دائماً بانضمام المزيد من المتطوعين. وتظلّ أوساط خبراء الأمن الحاسوبي في المجال النووي محدودة نسبيًا، حتى على نطاق عالمي. ويتيح الإسهام في عمل اللجنة الدولية للتقنيات الكهربائية فرصةً لبناء المعايير التي يمكن استخدامها عالميًا ودعم الصناعة النووية العالمية.

”بعد أن باتت القضايا العالمية مثل تغيُّر المناخ وأمن الطاقة أكثر إلحاحاً، تتطلع بلدان عدّة إلى اللجوء إلى التكنولوجيا النووية الجديدة والمبتكرة كوسيلة لتوليد طاقة منخفضة الكربون، ما يجعل المعايير أكثر أهميةً للحفاظ على أمان وأمن المرافق النووية.“

— تايغ سميث، اللجنة الدولية للتقنيات النووية



مدوَّنة قواعد السلوك الخاصة بالوكالة الدولية للطاقة الذرية:
20 عاماً من إحراز التقدّم في مجال أمان وأمن المصادر المشعّة

المتحدثون في الفعالية "المساواة بين الجنسين والإدماج، ومدوَّنة قواعد السلوك بشأن أمان المصادر المشعّة وأمنها: 20 عاماً من إحراز التقدّم".
(الصورة: و. فوارزوتا/الوكالة الدولية للطاقة الذرية)

اجتمع أكثر من 270 خبيراً قانونياً وتقنياً من 128 بلداً و4 منظمات دولية في فيينا، النمسا، في أيار/مايو 2023، لاستعراض التقدم المحرَز في مجال أمان وأمن المصادر المشعّة ولمعالجة الجوانب التي يلزم تحسينها.

وتؤدي المصادر المشعة دوراً لا غنى عنه في العديد من المجالات. ففي الطب، هي تساعد في علاج السرطان. وفي الزراعة، تتيح للعلماء تطوير أصناف محاصيل محسَّنة للتكيُّف مع تغيُّر المناخ والتصدّي للأمن الغذائي. وفي الفن وعلم الآثار، تساعد على صَوْن التراث الثقافي الذي لا يُقدَّر بثمن. ولكن يجب التعامل مع هذه المصادر في إطار تدابير الأمان والأمن الملائمة.

ولمساعدة البلدان على التصدّي للمخاطر وحماية الناس والبيئة من التعرُّض العَرَضي للإشعاعات أو الأفعال الإجرامية المتعمَّدة غير المأذون بها التي تنطوي على مصادر مشعّة، وضعت الوكالة مدوَّنة قواعد السلوك بشأن أمان وأمن المصادر المشعّة، والتي وافق عليها مجلس محافظي الوكالة في عام 2003 وتُصادف في هذا العام ذكراها السنوية العشرين.

وقال المدير العام للوكالة رافائيل ماريانو غروسي في الجلسة الافتتاحية للاجتماع المفتوح العضوية للخبراء التقنيين والقانونيين من أجل تبادل المعلومات بخصوص تنفيذ الدول مدوَّنة قواعد السلوك المتعلقة بأمان المصادر المشعة وأمنها: 'مرَّ عشرون عاماً على الموافقة على مدوَّنة قواعد السلوك، ونحن نحرز تقدُّماً مطّرداً في تحسين أمان وأمن المصادر المشعّة في جميع أنحاء العالم'. 'ولكن يجب بذل المزيد من العمل لتحقيق التزام سياسي أكبر ولتعميم أفضل الممارسات العالمية للتصرُّف المستدام والمأمون والآمن بهذه المصادر'.

وكان الاجتماع، الذي عُقد على مدار خمسة أيام، بمثابة منصة للخبراء العالميين لتبادُل المعلومات بشأن ممارسات التنفيذ الوطنية لمدوَّنة قواعد السلوك والوثيقتين الإرشاديتين التكميليتين . وتُعقد هذه الاجتماعات كلّ ثلاث سنوات، ما يمكّن البلدان من تعميم الخبرات، وتبادُل والدروس المستفادة، وتحديد التحديات الراهنة والمستقبلية في تنفيذ المدوَّنة.

وعلى مدار الأسبوع، خاض المشاركون في مواضيع متنوعة، شملت تطوُّر الأمان والأمن النوويين، والجوانب القانونية، والتعاون الدولي، والتطوير في المستقبل وتأثير مدوَّنة قواعد السلوك. وتناولت المناقشاتُ التحدّيات والأولويات المتعلقة بإنشاء الإطار الرقابي الملائم لأمان وأمن المصادر المشعة، وإدارة دورة حياتها، ولوائح الاستيراد والتصدير الخاصة بها، وكيف ينبغي التصرُّف في هذه المصادر عندما يُعلن عنها أنها مهمَلة. والأهم من ذلك، أتاح الاجتماع للمشاركين الفرصة لتعميم النُّهج الخاصة بهم لتنفيذ أحكام مدوَّنة قواعد السلوك بشكل فعّال.

إرشادات أساسية لمستقبل مأمون وآمن

أكد الرئيس المشارِك للاجتماع، رمزي جمال، نائب الرئيس التنفيذي ورئيس العمليات الرقابية في هيئة الأمان النووي الكندية، في كلمته في الفعالية الافتتاحية على أن تنفيذ مدوَّنة قواعد السلوك مسألة ضرورية لضمان حماية البيئة والجمهور والعاملين. "الهدف الذي ننشده هو ضمان مجمل أمان وأمن المصادر المشعّة خلال دورة حياتها الكاملة لتجنُّب التعرض العَرَضي للإشعاعات والحؤول دون استخدام المصادر المشعّة بنيّة خبيثة. وهذا جهد جارٍ قائم على التعاون".

وخاطبت أيضاً تيريزا كلارك، وهي نائبة مدير شعبة في اللجنة التنظيمية النووية الأمريكية، الحاضرين كرئيسةٍ مشارِكة، في معرض تقديم جلسة خاصة عن تاريخ المدوَّنة قائلةً: "عند التفكير في هذه السنوات العشرين والاحتفال بها، أردنا تحقيق فهم مشترك لخلفية المدوَّنة من المنظور القانوني والتقني، حتى نتمكن من تعميم الخبرات، وأفضل الممارسات، والتعلُّم من بعضنا البعض، لتحسين تنفيذ المدوَّنة على مستوى العالم".

وتوضح مدوَّنة قواعد السلوك كيف يمكن للبلدان ضمان أمان وأمن المصادر المشعّة من إنتاجها الأولي ووصولاً إلى التخلص النهائي منها. وهي تتضمّن اعتباراتٍ دولية وتقدّم توصياتٍ بشأن إعداد ومواءَمة وتنفيذ السياسات والقوانين واللوائح الوطنية، وكذلك بشأن التعاون فيما بين البلدان. وعلى الرغم من أنها صكٌ غير ملزم قانوناً، فقد أعربت 146 دولة عن دعمها السياسي لتنفيذ أحكام المدوَّنة منذ موافقة مجلس المحافظين عليها في عام 2003.

وتُستكمل مدوَّنة قواعد السلوك بوثيقتين إرشاديتين. وتتناول الإرشادات بشأن استيراد المصادر المشعّة وتصديرها الأدوار والمسؤوليات في ضمان استيراد المصادر المشعة وتصديرها بطريقة مأمونة وآمنة. توفّر الإرشادات بشأن التصرُّف في المصادر المشعَّة المهمَلة إرشاداتٍ بشأن التصرُّف في المصادر المهمَلة، إذ تحدّد خيارات التصرُّف فيها في نهاية عمرها مثل إعادة تدويرها وإعادة استخدامها، والخَزْن الطويل الأجل لها والتخلُّص منها، وإعادتها إلى المورّد. كما تشجّع هذه الإرشادات على وَضْع سياسة واستراتيجية وطنية لإدارة المصادر المهمَلة.

واختتمت الرئيسة المشارِكة عايدة أحمد الشحّي، مديرة إدارة الأمان الإشعاعي في الهيئة الاتحادية للرقابة النووية في الإمارات العربية المتحدة، قائلةً: "تجلب مدوَّنة قواعد السلوك ووثيقتاها الإرشاديتان فوائد ملموسةً للأمان الإشعاعي والأمن النووي على المستويَيْن الوطني والدولي، ما يمكّن من الاستفادة الكاملة من المصادر المشعّة من أجل مستقبل مستدام".

وتعمل الوكالة وتتعاون بشكل وثيق مع البلدان لضمان التصرُّف المنسَّق والمأمون والآمن بشأن المصادر المشعّة. وهي تدعم البلدان في تنفيذ مبادئ المدوَّنة وتقدّم مساعدة واسعة النطاق في إعداد استراتيجيات وخطط عمل لتنفيذ المدوَّنة؛ وتحسين نُظم الترخيص والتفتيش والإنفاذ والتصرُّف؛ وتعزيز قدرة الهيئات التنظيمية الوطنية بما يتماشى مع معايير الأمان الصادرة عن الوكالة، وإرشادات الأمن النووي، وأفضل الممارسات الدولية.

تعزيز التنوع والإدماج في المجال النووي

على هامش الاجتماع، استضافت هيئة الأمان النووي الكندية فعالية جانبية بعنوان "المساواة بين الجنسين والإدماج، ومدوَّنة قواعد السلوك بشأن أمان المصادر المشعّة وأمنها: 20 عاماً من إحراز التقدّم". وجمعَت الفعالية 120 مشاركاً لمناقشة سُبل تشجيع وتعزيز مشاركة المرأة في المجال النووي – بما في ذلك في مجال الأمان والأمن النوويين– وتوفير فرص متكافئة لجميع الأفراد، بغض النظر عن نوع الجنس.

وقالت رومينا فيلشي، الرئيسة والرئيسة التنفيذية لهيئة الأمان النووي الكندية: "يُسهم وجود التمثيل المتنوع على الطاولة في زيادة المواقف المتقصية، الأمر الذي يؤدي بدوره إلى ثقافة أمان أكثر متانةً في المنظمة. فالمساواة بين الجنسين ليست قضية نسائية فحسب ولكنها قضية مجتمعية يتعيّن على الجميع معالجتها"، مضيفةً أن الطلب المتزايد على الموارد البشرية يحتّم علينا ضمان إتاحة فرص أكبر للنساء في المجال النووي.

وخلال الفعالية، قالت ليدي إيفرار، نائبة المدير العام ورئيسة إدارة الأمان والأمن النوويين في الوكالة: "يُعتمد الأمان والأمن النوويان على مواقف متقصية وقائمة على التعلُّم، والانفتاح على التعقيبات البنّاءة، والقدرة على الجمع بين وجهات النظر المختلفة، وحشد الخبرات المختلفة. ويُعَدُّ التنوع، بما في ذلك التنوع الجنساني، رصيداً حقيقياً في هذا الصدد. ونحن أكثر قوةً وأكثر كفاءةً عندما نتبنى التنوع ونشجع موظفينا على التعبير عن آرائهم".

وقالت مارغريت دوون، نائبة المدير العام ورئيسة إدارة الشؤون الإدارية في الوكالة، إنّ "تعزيز مشاركة النساء والأشخاص من خلفيات متنوعة في القطاعات ذات الصلة بالطاقة النووية مسألة حيوية لأي منظمة". وسلّطت الضوءَ على مبادرات الوكالة بشأن تحسين المساواة بين الجنسين، بما في ذلك برنامج المنح الدراسية ماري سكلودوفسكا-كوري وبرنامج ليزا مايتنر، بهدف جلب المزيد من النساء إلى المجال النووي.

وقدّم كريستر فيكتورسون، المدير العام للهيئة الاتحادية للرقابة النووية في الإمارات، وجهة نظره في هذا الشأن قائلاً: "ركّزت الهيئة الاتحادية للرقابة النووية أنشطتها على تعزيز المساواة بين الجنسين. ويُعدُّ التزام القيادة ودعمها مسألة حيوية، بما في ذلك الدراسات الاستقصائية بشأن كيفية تحسين الشمولية والمعاملة العادلة لجميع الموظفين. ومن المهم بالقدر نفسه أن يكون هناك إطار مناسب وتنفيذ فعال وشامل".

– بقلم أرتيم فلاسوف

البلدان الناطقة باللغة العربية تناقش خطط الأمن النووي

تقاسَم المشاركون في اجتماع إقليمي عُقد مؤخراً في تونس تجاربهم في مجال إعداد وتنفيذ الخطط المتكاملة لدعم الأمن النووي
الصورة: ز. حسن/الوكالة الدولية للطاقة الذرية والهيئة العربية للطاقة الذرية)

اجتمعت البلدان الأعضاء في الشبكة العربية للهيئات الرقابية مؤخراً في تونس لتبادُل أفضل الممارسات، والتحديات القائمة، والفرص السانحة المتعلقة بتنفيذ أنشطة الأمن النووي في إطار الخطط المتكاملة لدعم الأمن النووي الخاصّة بكلّ منها. وأبرزَ الاجتماع أهمية النُّهج الإقليمية لتحسين القدرات التنظيمية والتشغيلية - وهي نُهج متأصّلة في برنامج الأمن النووي التابع للوكالة الدولية للطاقة الذرية.

وقالت إيلينا بوغلوفا، مديرة شعبة الأمن النووي في الوكالة: "إنّ تناوُل الأمن النووي من منظور إقليمي يحسّن التعاون الدولي وييسّر تنفيذ برنامج الأمن النووي التابع للوكالة". وتابعت قائلةً: "ومن شأن التعاون مع الشبكات الإقليمية مثل الشبكة العربية للهيئات الرقابية أن يعزّز فعالية آلية دعم الخطة المتكاملة لدعم الأمن النووي، ما يخلق فرصاً لتحديد ومناقشة الاحتياجات والتحديات المشتركة فيما بين البلدان المتقاربة جغرافيًا أو البلدان الناطقة باللغة نفسها".

وفي الاجتماع، قدّم 28 مشاركاً من 14 بلداً معلوماتٍ عن تنفيذ الخطط الوطنية المتكاملة لدعم الأمن النووي لديهم. وشملت مجالات التركيز الخاصة الأنشطة المتعلقة بالأطر التشريعية والتنظيمية للأمن النووي؛ وتقييمات التهديدات والمخاطر الوطنية؛ ونُظم الحماية المادية؛ والكشف عن الأعمال الإجرامية وغير المأذون بها المنطوية على مواد نووية أو مواد مشعّة أخرى غير خاضعة للتحكم الرقابي؛ والتصدّي لأحداث الأمن النووي المنطوية على مواد غير خاضعة للتحكم الرقابي؛ واستدامة نُظم الأمن النووي الوطنية.

ويُعَدُّ لبنان حاليًا أحد البلدان التي تستخدم الخطة المتكاملة لدعم الأمن النووي كآليةٍ لتعزيز البنية الأساسية الوطنية للأمن النووي. وقال حسن بساط، رئيس القسم المسؤول عن الترخيص والتفتيش والتنظيم في الهيئة اللبنانية للطاقة الذرية: "أتاحت لنا حلقة العمل مشارَكة تجربتنا الوطنية في تنفيذ الخطة المتكاملة لدعم الأمن النووي ومناقشة تحديات الأمن النووي في بلداننا وكذلك السُّبل الممكنة لمعالجتها". "كانت المحصّلة الأكثر أهميةً هي تحديد مجالات الأولوية المشتركة للخطة المتكاملة لدعم الأمن النووي التي هي بحاجة إلى مزيد من التحسين فيما بين الدول الأعضاء في الشبكة العربية للهيئات الرقابية".

وحاليًا، حصل 19 من أصل 22 عضواً في الشبكة العربية للهيئات الرقابية على خطة

متكاملة معتمدة لدعم الأمن النووي. وعالميًا، وافق 92 بلداً على خطط متكاملة لدعم الأمن النووي.

وقالت السيدة شيماء خالد جناحي، رئيسة وحدة التحليل الفيزيائي، إدارة الوقاية من الإشعاع، المجلس الأعلى للبيئة في البحرين: "على المستوى الإقليمي، نتشارك الحدود، فضلاً عن تحديات محدِّدة". "لقد مكَّنت حلقة العمل من تقاسُم الخبرات والمعارف التي نأمل أن تتبعها إجراءات متينة لتحسين وتعزيز الأمن النووي في المنطقة".

واستضافت الهيئة العربية للطاقة الذرية الاجتماع وتلقّى دعماً ماليًا من الاتحاد الأوروبي.

آلية دعم الخطة المتكاملة لدعم الأمن النووي

تساعد الوكالة البلدانَ، بناء على طلبها، على إعداد خطة متكاملة لدعم الأمن النووي، والتي توفّر الإطار لنهج منتظم وشامل لتحديد احتياجات الأمن النووي الوطنية وترتيب أولوياتها ووَضْع خطة لتنفيذ تحسينات الأمن النووي على المستوى الوطني. تُستكمل عملية إعداد الخطة المتكاملة لدعم الأمن النووي بأداة التقييم الذاتي الطوعي المتاحة للبلدان المهتمة من خلال البوابة الإلكترونية للمعلومات المتعلقة بالأمن النووي (NUSEC).

وتمكّن الخطة المتكاملة لدعم الأمن النووي وخطة التنفيذ المرتبطة بها البلدانَ من تلبية احتياجاتها الأكثر إلحاحاً، وتحديد المجالات التي يمكن معالجتها على المستوى الوطني وغيرها من المجالات حيث ثمة حاجة إلى طلب المساعدة من المجتمع الدولي.

وبمجرد تحديد احتياجات كلّ بلد، يمكن للوكالة أن تبدأ في بناء أُسس المساعدة المستهدَفة، مثل تلك التي تقدّمها الخدمة الاستشارية الدولية المعنية بالحماية المادية والخدمة الاستشارية الدولية الخاصة بالأمن النووي التابعتان للوكالة.

التعاون بين الوكالة الدولية للطاقة الذرية-الشبكة العربية للهيئات الرقابية

الشبكة العربية للهيئات الرقابية هي شبكة إقليمية تأسّست في عام 2010 في إطار الشبكة العالمية المعنيّة بالأمان والأمن النوويين التابعة للوكالة. وتعمل الشبكة العربية للهيئات الرقابية على تحسين وتعزيز ومواءمة الوقاية من الإشعاعات وأُطر البنية الأساسية الرقابية للأمان والأمن النوويين في البلدان المشاركة فيها، وهي بمثابة محفَل لتقاسم وتبادُل الخبرات والممارسات الرقابية.

– بقلم فاسيليكي تافيلي

منشورات الوكالة الدولية للطاقة الذرية

مجاناً على الموقع الإلكتروني

التنزيل هنا

www.iaea.org/books

لطلب كتاب، يرجى الكتابة إلى:

sales.publications@iaea.org

التنزيل

أمن المعلومات النووية

ومنشورات أخرى صادرة عن

الوكالة الدولية للطاقة الذرية عن

الأمن الحاسوبي في العالم النووي

www.iaea.org/bulletin/64-2

طالعوا هذا العدد وسائر أعداد مجلة الوكالة عبر الرابط:

www.iaea.org/ar/bulletin

للحصول على مزيد من المعلومات عن الوكالة وعملها، زوروا موقعنا الشبكي

www.iaea.org

أو تابعونا على

ISSN 1819-1800 23-01968A