IAEA BULLETIN
AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE
La publication phare de l'AIEA | Juin 2023 | www.iaea.org/fr/bulletin

LA SÉCURITÉ INFORMATIQUE DANS LE MONDE NUCLÉAIRE

Le Bulletin de l'AIEA
est produit par
le Bureau de l'information
et de la communication (OPIC)
Agence internationale de l'énergie atomique
Centre international de Vienne
B.P. 100, 1400 Vienne (Autriche)
Téléphone : (43-1) 2600-0
iaeabulletin@iaea.org

Direction de la rédaction : Emma Midgley
Conception et production : Ritu Kenn

Le Bulletin de l'AIEA est disponible à l'adresse suivante :
www.iaea.org/fr/bulletin

Couverture :
(Adobestock.com)

Suivez-nous sur :

IAEA

L'Agence internationale de l'énergie atomique (AIEA) a pour mission de prévenir la prolifération des armes nucléaires et d'aider tous les pays – en particulier ceux en développement – à tirer parti de l'utilisation pacifique, sûre et sécurisée de la science et de la technologie nucléaires.

Créée en tant qu'organisme autonome des Nations Unies en 1957, l'AIEA est le seul organisme du système des Nations Unies spécialisé dans les technologies nucléaires. Ses laboratoires spécialisés uniques en leur genre aident au transfert de connaissances et de compétences à ses États Membres dans des domaines comme la santé humaine, l'alimentation, l'eau, l'industrie et l'environnement.

L'AIEA sert aussi de plateforme mondiale pour le renforcement de la sécurité nucléaire. Elle a créé la collection Sécurité nucléaire, dans laquelle sont publiées des orientations sur la sécurité nucléaire faisant l'objet d'un consensus international. Ses travaux visent en outre à réduire le risque que des matières nucléaires et d'autres matières radioactives tombent entre les mains de terroristes ou de criminels, ou que des installations nucléaires soient la cible d'actes malveillants.

Les normes de sûreté de l'AIEA fournissent les principes fondamentaux, les prescriptions et les recommandations pour garantir la sûreté nucléaire et sont l'expression d'un consensus international sur ce qui constitue un niveau élevé de sûreté pour la protection des personnes et de l'environnement contre les effets nocifs des rayonnements ionisants. Elles ont été élaborées pour tous les types d'installations et d'activités nucléaires destinées à des fins pacifiques ainsi que pour les mesures de protection visant à réduire les risques radiologiques existants.

En outre, l'AIEA vérifie au moyen de son système d'inspection que les États Membres respectent l'engagement qu'ils ont pris, au titre du Traité sur la non-prolifération des armes nucléaires et d'autres accords de non-prolifération, de n'utiliser les matières et installations nucléaires qu'à des fins pacifiques.

Le travail de l'AIEA comporte de multiples facettes et fait intervenir un large éventail de partenaires aux niveaux national, régional et international. Les programmes et les budgets de l'AIEA sont établis sur la base des décisions de ses organes directeurs – le Conseil des gouverneurs, qui compte 35 membres, et la Conférence générale, qui réunit tous les États Membres.

L'AIEA a son siège au Centre international de Vienne. Elle a des bureaux locaux et des bureaux de liaison à Genève, à New York, à Tokyo et à Toronto. Elle exploite des laboratoires scientifiques à Monaco, à Seibersdorf et à Vienne. En outre, elle apporte son appui et contribue financièrement au fonctionnement du Centre international Abdus Salam de physique théorique à Trieste (Italie).

Le rôle essentiel de la sécurité informatique dans la sécurité et la sûreté nucléaires

Par Rafael Mariano Grossi, Directeur général de l'AIEA

Le rythme de l'innovation numérique est étourdissant et des technologies telles que l'intelligence artificielle ont fait des progrès qui ont changé la donne même au cours des derniers mois. Ces progrès nous aideront à améliorer les opérations à commande numérique et les technologies d'automatisation dans les installations nucléaires, ce qui pourrait se traduire par une plus grande efficacité opérationnelle, une diminution des coûts de main-d'œuvre et une amélioration de la sûreté et de la sécurité.

Les modèles de réacteurs nucléaires avancés, tels que les petits réacteurs modulaires (PRM) et les microréacteurs, prévoient déjà d'utiliser l'intelligence artificielle et l'apprentissage automatique pour des fonctionnalités innovantes telles que l'automatisation, la surveillance et la maintenance à distance, et les salles de commande partagées. Mais les innovations numériques telles que l'intelligence artificielle et l'apprentissage automatique constituent également une menace. Elles exigent une vigilance constante pour garantir l'intégrité des ressources sensibles et protéger les informations dans les installations nucléaires et radiologiques.

Les barrières et les gardes ont toujours servi à garantir la protection des installations nucléaires contre le sabotage ou les acteurs malveillants mais nous sommes aujourd'hui de plus en plus dépendants des systèmes numériques. Les systèmes de contrôle-commande des installations nucléaires sont utilisés pour des applications essentielles de sûreté et de sécurité. Ils améliorent l'efficacité mais nous devons aussi être particulièrement vigilants pour protéger ces systèmes informatiques. Les pays du monde entier reconnaissent qu'il s'agit d'une priorité.

L'AIEA joue un rôle unique en stimulant la coopération entre les pays et en permettant le partage du savoir-faire technologique et des meilleures pratiques dans l'adoption de technologies en évolution rapide. Parallèlement, nous conseillons les pays sur la manière de minimiser et d'atténuer les vulnérabilités qui pourraient compromettre la sécurité informatique. Ces deux dernières années, nos activités mondiales d'assistance en sécurité informatique ont augmenté de plus d'un quart, avec un accent particulier sur l'appui aux réglementations et inspections nationales en matière de sécurité informatique et les exercices de sécurité informatique.

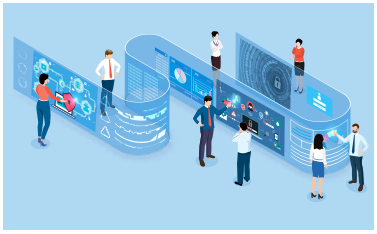
L'AIEA a répondu aux défis de la sécurité nucléaire de ses États Membres par une série d'activités, notamment en fournissant des documents d'orientation et des formations qui leur permettent de mettre en place des programmes nationaux solides de sécurité de l'information et de sécurité informatique. Ces orientations servent également de référence pour évaluer le programme de sécurité informatique et de sécurité de l'information d'un pays dans le cadre d'un service consultatif international sur la protection physique appelé IPPAS.

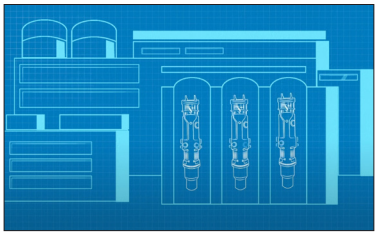
En outre, nous lançons une école pour former des experts à l'élaboration de réglementations de sécurité informatique. Bientôt, de nombreux autres pays pourront accéder aux cours de sécurité informatique de l'AIEA grâce au lancement d'une plateforme d'apprentissage virtuel en ligne.

Parallèlement, l'AIEA appuie les exercices nationaux et régionaux de sécurité informatique qui sensibilisent à la menace des cyberattaques et à leurs incidences potentielles sur la sécurité nucléaire. Nous favorisons la coopération entre les experts internationaux et les décideurs politiques et facilitons la recherche d'accompagnement.

Les activités de l'AIEA en matière de sécurité informatique sont appelées à se développer car les pays, notamment à revenu faible et intermédiaire, se tournent de plus en plus vers la technologie nucléaire pour répondre à leurs priorités, notamment en matière d'énergie propre, de soins contre le cancer, de nutrition et de recherche.

Lors de la Conférence internationale de l'AIEA sur la sécurité informatique dans le monde nucléaire, sur le thème « la sécurité au service la sûreté », nous nous réunirons pour examiner les questions clés, y trouver des solutions et tracer la voie à suivre afin de permettre au secteur nucléaire de tirer le meilleur parti des innovations numériques tout en gardant une longueur d'avance sur ceux qui les utiliseraient pour nuire.





QUESTIONS-RÉPONSES

DANS LE MONDE

INFOS AIEA

Faire face aux menaces contre la sécurité informatique

L'évolution du programme d'assistance de l'AIEA

Par Vasiliki Tafili

Le passage aux sociétés en réseau numérique, où les activités quotidiennes sont interconnectées à l'aide de systèmes informatiques, de l'intelligence artificielle (IA) et des technologies numériques, a un effet considérable sur la sûreté et la sécurité nucléaires. On ne saurait trop insister sur le rôle essentiel des technologies numériques dans le maintien des fonctions de sûreté et de sécurité des installations où sont manipulées des matières nucléaires ou d'autres matières radioactives.

« Les systèmes informatiques et les technologies numériques sont essentiels pour les installations et les activités associées où sont utilisées des matières nucléaires et d'autres matières radioactives », explique Elena Buglova, Directrice de la Division de la sécurité nucléaire de l'AIEA, soulignant que tous les pays doivent mettre en œuvre des programmes de sécurité informatique et améliorer la défense en profondeur de la sécurité nucléaire. « À mesure que la technologie progresse, la protection de la confidentialité, de l'intégrité et de la disponibilité des informations et des biens sensibles exige une vigilance constante pour prévenir et atténuer les risques, ainsi qu'un solide programme de sécurité informatique et sécurité de l'information. »

La nécessité de faire face aux menaces contre la sécurité informatique, aux cyberattaques malveillantes et à toutes les vulnérabilités potentielles que peuvent introduire les technologies numériques, ainsi que l'importance de la sécurité informatique pour la sécurité nucléaire, ont été mentionnées pour la première fois dans une résolution sur la sécurité nucléaire adoptée par la Conférence générale de l'AIEA à sa 55e session ordinaire, en 2011. La Conférence générale y a pris note des efforts de l'AIEA « pour sensibiliser à la menace croissante de cyberattaques et à leur impact potentiel sur la sécurité nucléaire ». La résolution encourageait également l'AIEA à élaborer des documents d'orientation appropriés, à dispenser des cours et à accueillir d'autres réunions d'experts sur la cybersécurité dans les installations nucléaires afin d'aider les pays à se protéger contre les cyberattaques.

« Suite à la résolution de la Conférence générale de 2011, les activités de l'AIEA se sont concentrées sur l'amélioration des capacités de sécurité informatique au niveau des États et des installations », explique Mme Buglova, ajoutant que ces activités ont ensuite été incluses dans les plans de sécurité nucléaire ultérieurs de l'AIEA, notamment les détails de la mise en œuvre actuelle des activités de sécurité informatique de l'AIEA qui sont décrits dans le plan de sécurité nucléaire 2022-2025.

Comment l'AIEA aide-t-elle les pays à développer ou à améliorer leur sécurité informatique ?

La mise en place d'un programme de sécurité informatique solide et actualisé est un élément crucial pour protéger les pays contre les cyberattaques visant tous les types d'infrastructures critiques. L'AIEA a promptement fourni une assistance aux pays à tous les stades de l'élaboration des programmes nationaux de sécurité de l'information et de la sécurité informatique, notamment des documents d'orientation et des formations.

Quatre publications d'orientation de la collection Sécurité nucléaire de l'AIEA et trois publications techniques supplémentaires fournissent des orientations sur la sécurité de l'information et la sécurité informatique. Ces orientations peuvent servir de base à l'élaboration de cadres nationaux de sécurité informatique, notamment de stratégies nationales, ainsi qu'à l'élaboration de réglementations et de formations en matière de sécurité informatique.

Un principe fondamental des orientations de l'AIEA est de préserver les fonctions critiques des installations nucléaires en protégeant les informations et les systèmes informatiques afin de maintenir un environnement sûr et sécurisé à la fois pour les installations et pour les matières. À cette fin, il faut élaborer un programme de sécurité informatique (voir page 6), identifier les fonctions de sécurité nucléaire, utiliser la gestion des risques pour déterminer les conséquences potentielles d'une atteinte à la sécurité, définir le niveau de sécurité informatique requis pour les actifs numériques sensibles et mettre en œuvre une approche graduée et des concepts de défense en profondeur en sécurité informatique. Ces éléments doivent être conçus et mis en œuvre de manière à empêcher toute atteinte et à renforcer la capacité de l'opérateur de détecter les intrusions, d'y répondre et d'atténuer l'impact potentiel des cyberattaques.

À la demande des pays, l'AIEA propose diverses possibilités de formation à des publics variés : autorités compétentes, exploitants, fournisseurs et autres entités qui peuvent avoir des responsabilités dans la mise en œuvre de la sécurité informatique. Ceux-ci peuvent également bénéficier de l'expertise de l'AIEA en matière d'exercices de sécurité informatique dans le cadre du programme de sécurité nucléaire.

De plus, quatre cours en ligne sur la sécurité informatique sont disponibles gratuitement en anglais, arabe, chinois, espagnol, français et russe sur la Cyberplateforme d'apprentissage de l'AIEA pour la formation théorique et pratique en réseau, sur inscription ou via un compte NUCLEUS. Une nouvelle

plateforme de formation innovante et virtuelle sera également bientôt disponible (voir page 12).

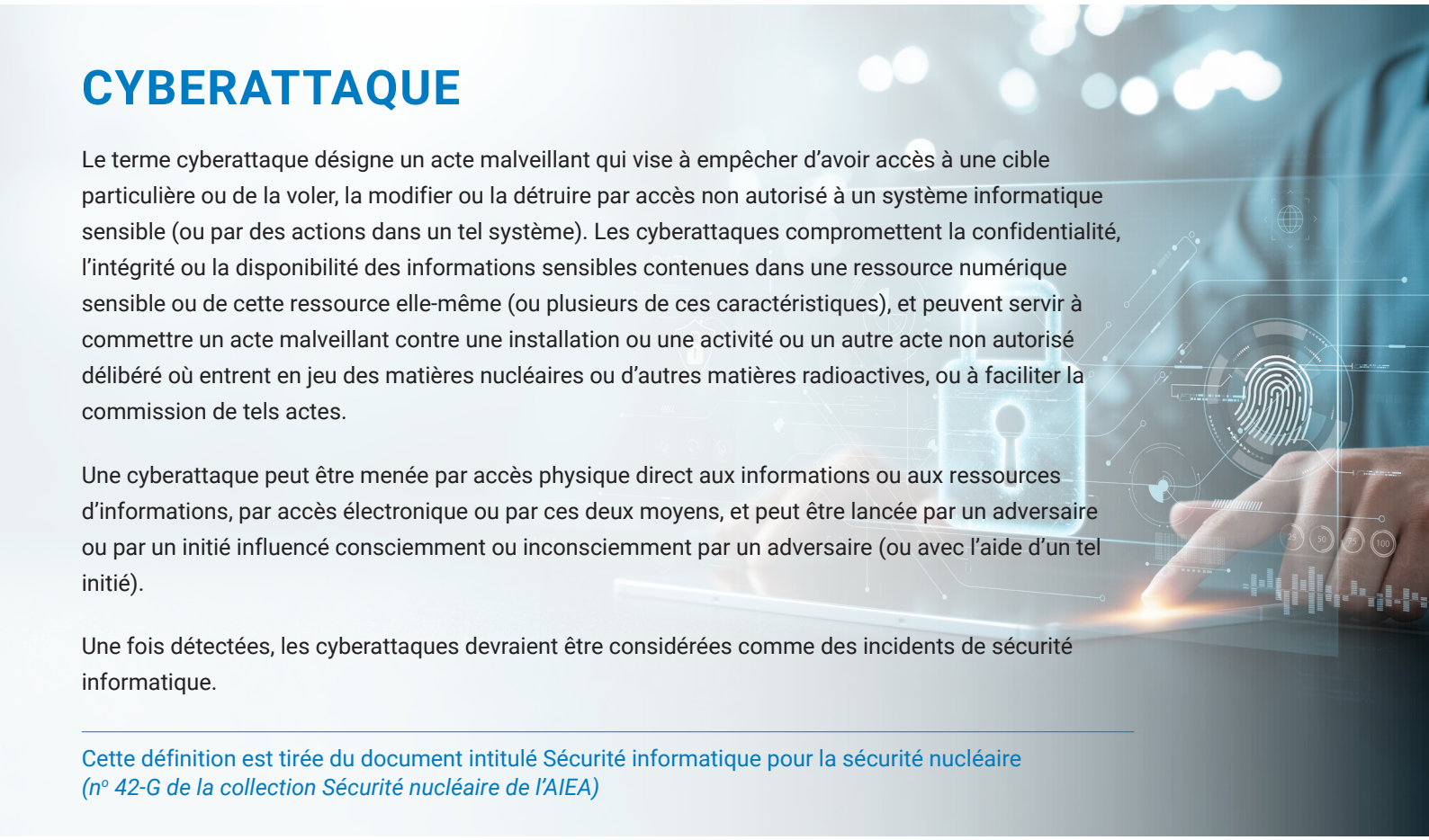
Parallèlement, l'AIEA appuie les exercices nationaux ou régionaux de sécurité informatique dans le cadre de son action de sensibilisation à la menace des cyberattaques et à leurs incidences potentielles sur la sécurité nucléaire. Les exercices comportent différents scénarios où des informations sensibles et des systèmes informatiques sont ciblés directement ou indirectement par une attaque visant à la fois la protection physique et les systèmes électroniques.

La recherche complète les activités de l'AIEA en matière de sécurité informatique, principalement dans le cadre du mécanisme bien établi des projets de recherche coordonnée. Des projets de recherche coordonnée ont été lancés ces dernières années pour faire progresser la recherche mondiale dans le domaine de la sécurité de l'information et de la sécurité informatique et pour mieux se préparer à faire face aux défis et aux risques émergents (voir page 18).

Que nous réserve l'avenir ?

Le programme de sécurité informatique de l'AIEA pour la sécurité nucléaire est en constante évolution. La dépendance des petits réacteurs modulaires et des réacteurs avancés à l'égard des technologies de pointe et du contrôle-commande numérique, les effets attendus de l'IA et l'émergence d'environnements d'apprentissage virtuels font apparaître de nouveaux défis et des domaines où les États auront besoin d'un appui accru.

« Nous assistons à une prise de conscience croissante des implications potentielles ou réelles de la sûreté et de la sécurité nucléaires parmi les pays, les organismes de réglementation, les exploitants et les autres parties prenantes, explique M^me^ Buglova. La croissance importante prévue dans l'utilisation des applications nucléaires pacifiques, en particulier les programmes électronucléaires, nous oblige à considérer la sécurité de l'information et la sécurité informatique comme une partie intégrante de la sécurité nucléaire. »



CYBERATTAQUE

Le terme cyberattaque désigne un acte malveillant qui vise à empêcher d'avoir accès à une cible particulière ou de la voler, la modifier ou la détruire par accès non autorisé à un système informatique sensible (ou par des actions dans un tel système). Les cyberattaques compromettent la confidentialité, l'intégrité ou la disponibilité des informations sensibles contenues dans une ressource numérique sensible ou de cette ressource elle-même (ou plusieurs de ces caractéristiques), et peuvent servir à commettre un acte malveillant contre une installation ou une activité ou un autre acte non autorisé délibéré où entrent en jeu des matières nucléaires ou d'autres matières radioactives, ou à faciliter la commission de tels actes.

Une cyberattaque peut être menée par accès physique direct aux informations ou aux ressources d'informations, par accès électronique ou par ces deux moyens, et peut être lancée par un adversaire ou par un initié influencé consciemment ou inconsciemment par un adversaire (ou avec l'aide d'un tel initié).

Une fois détectées, les cyberattaques devraient être considérées comme des incidents de sécurité informatique.

Cette définition est tirée du document intitulé Sécurité informatique pour la sécurité nucléaire *(n° 42-G de la collection Sécurité nucléaire de l'AIEA)*

Comment élaborer un programme de sécurité informatique

Par Vasiliki Tafili et Trent Nelson

Les installations qui manipulent des matières nucléaires ou d'autres matières radioactives, et qui mènent des activités connexes, sont des infrastructures essentielles qui exigent des niveaux élevés de sûreté et de sécurité. En adoptant une stratégie de sécurité informatique globale et préventive, les organismes peuvent protéger les informations sensibles et systèmes informatiques de ces installations pour éviter qu'ils ne soient compromis. La stratégie que recommande d'adopter l'AIEA suppose que les États établissent des prescriptions pour les stratégies ou politiques nationales, et qu'ils aident à assurer la confidentialité et la protection des informations et des systèmes informatiques sensibles liés à la protection physique, à la sûreté nucléaire ainsi qu'à la comptabilité et au contrôle des matières nucléaires. Ces prescriptions peuvent également prendre la forme de réglementations nationales prévoyant l'élaboration et la mise en œuvre d'un programme de sécurité informatique (PSI)*.

Un PSI est un cadre général qui comprend des éléments clés pour établir un plan efficace de mise en œuvre des politiques et procédures de sécurité informatique qui seront utilisées pendant toute la durée de vie d'une installation nucléaire ou d'une installation contenant des sources radioactives. Il vise à protéger les informations sensibles et les systèmes informatiques indispensables au maintien des fonctions de sûreté et de sécurité contre les cyberattaques afin d'atténuer leurs conséquences.

Stratégie nationale

Toute stratégie de sécurité informatique globale et efficace doit être systématique et intégrer divers éléments, notamment des réglementations, des programmes, des mesures de protection de la sécurité et des capacités de réaction à l'appui des régimes nationaux de sécurité nucléaire.

Réglementation

Une réglementation efficace fournit un cadre juridique pour la protection des systèmes informatiques sensibles et oblige les organismes à mettre en place des PSI et des contrôles appropriés.

Éléments clés du PSI :

Rôles et responsabilités

La définition des rôles et responsabilités des organismes, et l'obligation de rendre compte, sont essentielles pour une gestion efficace, en particulier dans le cas des infrastructures critiques. Il est indispensable de connaître la hiérarchie de l'organisme et de disposer de lignes d'autorité et d'une structure hiérarchique claires pour pouvoir assurer une collaboration et une synergie efficaces et efficientes dans le cadre des PSI.

Gestion des risques, des failles et du respect des règles

La gestion des risques de sécurité informatique consiste à évaluer les failles et effets potentiels des ressources numériques et systèmes informatiques sensibles afin de mettre en place des contrôles de sécurité informatique en suivant une approche graduée pour se défendre contre les cyberattaques. Le niveau des mesures de sécurité appliquées devrait être proportionnel au niveau de risque associé aux informations ou aux systèmes informatiques protégés. En tenant compte des conséquences de la faille ou de la menace, les organismes peuvent déterminer le niveau des mesures de sécurité nécessaires pour atténuer le risque.

Conception et gestion de la sécurité

La conception de la sécurité informatique est un aspect essentiel de la protection contre les cybermenaces. Parmi les grands principes de conception figure l'adoption d'une approche graduée et d'une défense en profondeur, où plusieurs couches de contrôles de sécurité par zone sont appliquées pour prévenir et atténuer les attaques. Les exigences en matière de sécurité doivent également être respectées tout au long du cycle de développement du système, et les organismes tiers doivent suivre des politiques et accords clairs afin de garantir la cohérence et l'efficacité des mesures de sécurité.

Gestion des ressources numériques

Pour que la stratégie de sécurité informatique soit efficace, il convient de suivre une approche systématique, en dressant une liste exhaustive de toutes les fonctions, ressources et de tous les systèmes de l'installation, y compris les ressources numériques sensibles qui sont essentielles à la protection des opérations nucléaires ou à l'utilisation sûre et sécurisée des matières nucléaires et autres matières radioactives. Cette liste doit également couvrir les flux de données et interdépendances importantes pour l'organisation, car ils jouent un rôle dans le contrôle des accès, les sauvegardes et les autres mesures de sécurité visant à protéger ces ressources contre le sabotage ou le vol.

Procédures de sécurité

Les politiques et procédures opérationnelles de sécurité nucléaire permettent à la direction de définir les responsabilités de chacun pour prévenir le vol, le sabotage ou l'utilisation non autorisée de matières et d'installations nucléaires. Avec de telles politiques, l'accès aux informations et aux ressources sensibles est contrôlé de près, et les personnes qui y ont accès sont sélectionnées et formées de manière appropriée.

Gestion du personnel

La fiabilité, la sensibilisation et la formation sont autant de points clés pour la gestion du personnel dans l'industrie nucléaire. Des évaluations de la fiabilité doivent être effectuées pour s'assurer que le personnel est fiable, compétent et n'est pas en situation de conflit d'intérêts qui pourrait compromettre la sûreté ou la sécurité. Il est primordial de toujours disposer d'un personnel qualifié et digne de confiance pour garantir la sûreté et la sécurité nucléaires.

*Pour plus d'informations, voir le document *IAEA Nuclear Security Series No. 17-T (Rev. 1), Computer Security Techniques for Nuclear Facilities*.

Au-delà de la protection physique :

comment le Service consultatif international sur la protection physique (IPPAS) aide à renforcer la sécurité informatique

Par Vasiliki Tafili

Depuis près de 30 ans, le Service consultatif international sur la protection physique (IPPAS) de l'AIEA aide les pays en les conseillant sur la protection physique de tout type d'installation où sont utilisées des matières nucléaires et d'autres matières radioactives, y compris les centrales nucléaires et les unités de radiothérapie d'hôpitaux. Mais en raison des progrès technologiques, les systèmes numériques sont actuellement au cœur du fonctionnement de ces installations, ce qui pose une myriade de nouveaux problèmes de sécurité nucléaire.

Face à la réelle menace de cyberattaques contre les installations, y compris les installations nucléaires, les attributions de l'IPPAS ont été étendues en 2012 pour couvrir la sécurité de l'information et la sécurité informatique aux fins de la protection physique. Depuis lors, un nombre croissant de pays demande ce module dans leur examen IPPAS pour appuyer leur lutte contre les menaces de cybersécurité.

Composante essentielle du programme de sécurité nucléaire de l'AIEA, l'IPPAS est un service consultatif qui examine les pratiques existantes des pays au regard des instruments internationaux pertinents et des orientations de l'AIEA sur la sécurité nucléaire. Il aide les pays qui en font la demande à renforcer leurs régimes, systèmes et mesures nationaux de sécurité nucléaire en les conseillant sur la mise en œuvre des instruments juridiques internationaux.

« Vingt-sept années se sont écoulées depuis la première mission IPPAS. Le service a évolué pour répondre aux problématiques et besoins d'aujourd'hui », explique Heather Looney, cheffe de la Section de la sécurité nucléaire des matières et des installations au sein de la Division de la sécurité nucléaire de l'AIEA. « La protection physique contre le vol, le sabotage ou l'utilisation non autorisée de matières nucléaires et d'autres matières radioactives passe par des mesures de sécurité informatique. Les pays qui invitent une mission IPPAS bénéficient de conseils sur les points à améliorer et la manière d'y parvenir », ajoute-t-elle.

L'IPPAS propose cinq modules : un examen national du régime de sécurité nucléaire pour les matières et installations nucléaires ; un examen des systèmes et mesures de sécurité dans les installations nucléaires ; un examen de la sécurité du transport de matières ; un examen de la sécurité des matières radioactives et des installations et activités associées ; et un examen de la sécurité de l'information et de la sécurité informatique. Depuis la première mision IPPAS en 1996, 97 missions ont eu lieu et 22 pays ont demandé l'inclusion du module sur la sécurité de l'information et la sécurité informatique dans l'examen IPPAS.

Que doit attendre un pays de l'examen de la sécurité de l'information et de la sécurité informatique ?

L'équipe IPPAS, composée d'experts internationaux en sécurité nucléaire, commence par examiner la manière dont les politiques nationales concernant les programmes de sécurité de l'information et de sécurité informatique ont été mises en place et gérées. Elle examine ensuite le cadre législatif et réglementaire en comparant les procédures et pratiques en place dans le pays avec les obligations spécifiées dans la Convention sur la protection physique des matières nucléaires et son amendement de 2005, et avec les orientations fournies dans les publications pertinentes de la collection Sécurité nucléaire de l'AIEA. Elle peut ainsi déterminer si le pays dispose des politiques et procédures nécessaires pour garantir un niveau de sécurité informatique suffisant dans les installations nucléaires et radiologiques critiques.

Au niveau de l'installation, l'examen de sécurité informatique porte sur la gestion de la sécurité informatique, le programme de sécurité informatique (voir page 6), le contrôle des accès, l'architecture de sécurité informatique défensive, ainsi que la détection des incidents de sécurité informatique et les mesures pour y faire face. L'équipe peut également évaluer des domaines transversaux tels que la gestion des risques, les approches graduées, la culture de sécurité nucléaire et la gestion des ressources humaines.

Le Japon a accueilli une mission IPPAS en 2015, puis sa mission de suivi en 2018. « Il a été très utile pour le Japon d'examiner l'état actuel des mesures de sécurité informatique et de tenir compte des suggestions d'amélioration formulées par l'équipe », estime Hiroyuki Sugawara, Directeur chargé de la sécurité nucléaire internationale à la Division de la sécurité nucléaire de l'Autorité de réglementation nucléaire japonaise (ARN). « Pour donner suite aux conclusions de l'IPPAS, nous avons décidé de renforcer les mesures de sécurité informatique et d'augmenter le nombre d'inspecteurs spécialisés dans ce domaine. L'ARN a également commencé à tenir compte des menaces de sécurité informatique dans ses évaluations nationales des menaces et à exiger que les titulaires de licence prennent des mesures de sécurité informatique efficaces et améliorent le contenu de leurs plans de sécurité informatique en y ajoutant des contre-mesures contre les cyberattaques. »

Depuis 1996, le Service consultatif international de l'AIEA sur la protection physique (IPPAS) aide les pays à trouver des solutions pour renforcer la protection des matières et installations nucléaires. (Photo : AIEA)

En France, à la suite d'une mission IPPAS en 2018, une plus grande place a été faite à la sécurité informatique dans le cadre national de sécurité nucléaire. « La mission IPPAS a nécessité un engagement fort des diverses parties prenantes, et donné l'occasion à la France de consolider son régime de sécurité nucléaire et de stimuler sa mise en œuvre », explique Frédéric Boën, chef de projet de sécurité informatique au Ministère de la transition énergétique, Direction de la défense et de la sécurité, Bureau de la sécurité nucléaire. « Le personnel de sécurité informatique a été renforcé et des lignes directrices réglementaires ont été établies conformément aux normes internationales et aux orientations de l'AIEA sur la sécurité nucléaire. »

L'AIEA gère depuis 2016 la base de données des bonnes pratiques de l'IPPAS pour partager les conclusions de ces missions avec la communauté internationale de la sécurité nucléaire et améliorer ainsi les résultats de l'aide offerte par l'AIEA aux pays du monde entier. « L'alimentation de cette base de données et le partage de ces exemples font que les missions IPPAS ont des retombées hors du pays hôte dans toute la communauté internationale de sécurité nucléaire, et démultiplient l'incidence de l'aide que l'AIEA propose à ses États Membres », explique M^{me} Looney.

La majorité des bonnes pratiques nationales concerne la gestion de la sécurité nucléaire, pierre angulaire de la sécurité et de la coordination informatiques. En outre, les États Membres ont accès, par l'intermédiaire de leurs points de contact désignés, à 40 bonnes pratiques de sécurité informatique, applicables tant au niveau des États que des installations.

L'AIEA continue d'aider les pays à renforcer leur régime national de sécurité nucléaire et la demande de missions IPPAS pour 2023 et 2024 reste élevée.

L'AIEA aide des pays africains à élaborer une réglementation de sécurité informatique

Par Andrea Rahandini

La demande d'isotopes radioactifs en Afrique devrait augmenter dans les années à venir car de plus en plus de pays intensifient leur utilisation pacifique de la technologie nucléaire. L'augmentation du nombre de cas de cancer a entraîné une augmentation de la demande en radiothérapie, en radiologie et en médecine nucléaire. L'utilisation des applications nucléaires a augmenté dans les domaines de l'industrie, de l'agriculture et de la science. La demande de production de radio-isotopes dans les réacteurs de recherche a donc aussi augmenté. Ces réacteurs essentiels fonctionnent à l'aide de systèmes informatiques potentiellement vulnérables à des cyberattaques. Comme les centrales nucléaires, il leur faut des plans de protection pour prévenir les attaques malveillantes éventuelles, les atténuer et y faire face. La protection de tous les types d'installations nucléaires contre l'éventualité de telles attaques est un élément clé de l'utilisation sûre et sécurisée de la technologie nucléaire en Afrique.

Pour contrer ces menaces, de nombreux pays d'Afrique s'inspirent de l'Égypte, du Ghana et du Nigéria, qui possèdent et exploitent chacun un réacteur de recherche nucléaire. Avec l'aide de l'AIEA, ces trois pays élaborent et renforcent leur réglementation de sécurité informatique et mettent en œuvre des programmes afin de bien sécuriser leurs installations contre les actes informatiques malveillants qui pourraient nuire à leur sécurité et à leur sûreté nucléaires.

« La sécurité informatique continue de devenir de plus en plus importante à mesure que les technologies numériques et les systèmes informatiques sont intégrés dans la sûreté et la sécurité nucléaires des installations où se trouvent des matières nucléaires et autres matières radioactives et dans leurs aspects opérationnels », explique Trent Nelson, responsable de la sécurité de l'information et de la sécurité informatique à la Division de la sécurité nucléaire de l'AIEA. « L'AIEA travaille avec les pays d'Afrique pour élaborer, examiner et améliorer les réglementations de sécurité informatique. »

En Égypte, l'AIEA collabore avec l'Autorité égyptienne de réglementation nucléaire et radiologique (ENRRA) pour examiner la réglementation de sécurité informatique existante et combler les lacunes éventuelles des aspects réglementaires. En 2022, un cours national a été organisé pour constituer les capacités nationales nécessaires pour mener des inspections de sécurité informatique dans les installations nucléaires. Utilisant les orientations sur la sécurité nucléaire de l'AIEA et les techniques dont disposent les inspecteurs, le cours a permis aux participants d'acquérir les connaissances et l'expertise pratique nécessaires pour mieux évaluer l'efficacité de la sécurité informatique dans les installations nucléaires et radiologiques.

Nadia M. Nawwar, ingénieure informatique à l'installation de production de radio-isotopes de l'Autorité égyptienne de l'énergie atomique (EAEA), était l'une des 22 participantes. « Je sais maintenant comment l'organisme de réglementation effectue les inspections de sécurité informatique et quelles dispositions de sécurité informatique l'exploitant doit mettre en place », dit-elle. « Depuis que nous avons participé au cours, nous sommes en mesure d'examiner et de valider plus efficacement les éléments de réglementation de sécurité informatique. Le cours nous a aidés à élaborer et à mettre en œuvre un programme de sécurité informatique afin de protéger les informations sensibles de l'installation et les actifs numériques sensibles vulnérables aux cyberattaques. »

Au Ghana, l'AIEA a mené une mission d'expertise en avril 2023 pour évaluer la réglementation nationale actuelle de sécurité informatique et le programme d'inspection de l'Autorité ghanéenne de réglementation nucléaire (GNRA).

« La mise au point de la sécurité informatique au Ghana a posé plusieurs difficultés, notamment l'absence de connaissances techniques locales en la matière, la conciliation des questions juridiques et du savoir-faire technique et les modalités de gestion des ressources nécessaires », indique Nelson Kodzotse Agbemava, chef d'équipe à la section cybersécurité nucléaire de la GNRA. « Au cours de l'élaboration de la réglementation, un examen par des experts de l'AIEA et d'autres pays a été sollicité pour garantir une approche globale et systématique de la sécurité informatique. »

De même, l'AIEA a mené une mission d'experts au Nigéria en octobre 2022. « La nécessité d'un cadre législatif et réglementaire efficace de sécurité informatique a été reconnue en 2019 lors de l'examen du Plan intégré d'appui en matière de sécurité nucléaire (INSSP) par l'AIEA dans le pays », explique Ethel Ofoegbu, responsable de la réglementation à l'Autorité nigériane de réglementation nucléaire (NNRA). « En conséquence, l'AIEA a évalué la réglementation nationale en matière de sécurité informatique, identifié les lacunes et fourni

L'AIEA lancera son école d'élaboration des éléments de réglementation de sécurité informatique en août 2023, dans le but d'aider les pays à élaborer leur réglementation nationale de sécurité informatique.

les conseils nécessaires. Cet examen a notamment donné lieu à l'élaboration d'un projet de réglementation nigériane sur la sécurité informatique pour les installations et activités nucléaires et radiologiques. » Actuellement, le Nigéria examine le projet de réglementation et prévoit un cours sur les inspections dans le domaine informatique.

Face à l'augmentation du nombre de demandes d'assistance des pays, l'AIEA élabore un document technique pour les aider à établir les éléments clés de la réglementation de sécurité informatique. L'AIEA se tient également prête à aider de nombreux autres pays à élaborer une réglementation de sécurité informatique dès que l'école d'élaboration des éléments de réglementation de sécurité informatique de l'AIEA sera lancée en août 2023. L'école permettra à l'AIEA d'aider simultanément plusieurs pays à élaborer leur réglementation nationale de sécurité informatique. Après le premier atelier en août, les sessions suivantes seront organisées deux fois par an dans toutes les régions. Ensemble, les participants auront l'occasion d'élaborer leurs stratégies nationales de sécurité informatique, fondement réglementaire d'un programme de sécurité informatique solide.

L'innovation dans la formation virtuelle à la sécurité informatique pour les installations nucléaires et radiologiques

Par Anjarika Strohal

L'omniprésence actuelle et les progrès constants des technologies numériques sont en train de changer rapidement et profondément nos modes de vie. Les infrastructures critiques d'aujourd'hui, dont l'électronucléaire et d'autres utilisations pacifiques de la technologie nucléaire, comptent largement sur les technologies numériques pour assurer leur exploitation harmonieuse et fiable. Les promesses des nouvelles technologies en évolution rapide, telles que l'intelligence artificielle, pour ce qui est de résoudre des problèmes et améliorer les opérations contrôlées par des systèmes numériques seront probablement utiles à l'amélioration des applications nucléaires. Elles sont donc maintenant utilisées et prises en compte dans les modèles de réacteurs avancés.

Malheureusement, ces technologies numériques aux nombreux avantages peuvent également introduire de nombreuses vulnérabilités encore inconnues, en raison de la menace toujours présente de cyberintrusions ou de cyberattaques malveillantes contre des installations nucléaires, qui pourraient exploiter ces mêmes technologies.

Le nombre et l'ampleur des cyberattaques de plus en plus sophistiquées ont généré dans l'industrie nucléaire une demande urgente de formation à la sécurité informatique pour les installations nucléaires et radiologiques. Pour contribuer à répondre à cette demande, l'AIEA a conçu une série de cours sur des sujets allant des bases de la sécurité informatique aux applications plus avancées destinées aux systèmes de contrôle-commande.

À l'occasion de ces cours sur mesure, pointus et complexes qui mettent l'accent sur l'apprentissage par l'expérience, l'AIEA a réalisé qu'il fallait une plateforme en ligne simple permettant de normaliser le programme et d'en favoriser une utilisation plus large et plus universelle par les organismes de formation - sans assistance en présentiel de l'AIEA. Les restrictions de voyage liées à la pandémie de COVID-19 et l'utilisation généralisée des technologies virtuelles souligné encore ce besoin et accéléré la mise en place de la plateforme.

L'outil de formation virtuelle, appelé « Learners », vise à fournir des cours sur la sécurité informatique adaptés et attrayants à la communauté nucléaire, en présentant du matériel didactique et l'expérience d'exercices pratiques effectués dans un environnement virtuel. Il suffit de disposer d'un ordinateur et d'une connexion internet fiable pour accéder à tout le matériel didactique. « La nouvelle plateforme devrait jouer un rôle clé dans l'amélioration de la sensibilisation et de la formation

Sécurité informatique –
formation et autres activités

à la sécurité informatique pour la sécurité nucléaire, dans le renforcement de la communauté d'experts et dans l'amélioration de la sûreté et de la sécurité des installations nucléaires et de celles associées aux matières radioactives », explique Elena Buglova, directrice de la Division de la sécurité nucléaire de l'AIEA.

À partir de juin 2023, l'AIEA mettra la plateforme Learners à disposition du monde entier afin de renforcer la sécurité informatique dans les installations nucléaires, ainsi que dans les installations et activités mettant en jeu des sources radioactives.

L'Institut autrichien de technologie (AIT) - un centre collaborateur de l'AIEA en matière de sécurité de l'information et de sécurité informatique pour la sécurité nucléaire - s'est associé à l'AIEA pour créer la plateforme Learners.

« L'environnement d'apprentissage virtuel améliore considérablement les capacités opérationnelles et stratégiques en appuyant divers objectifs de formation », fait observer Helmut Leopold, chef du Centre pour la sûreté et la sécurité numériques à l'AIT. « En simulant des environnements réels, la plateforme permet aux apprenants d'acquérir des compétences pratiques et une expérience essentielles pour une gestion efficace de la sécurité nucléaire ».

Apprendre à renforcer la sécurité informatique

La plateforme Learners de l'AIEA est accessible sur demande pour renforcer la formation en sécurité nucléaire. Conçue pour être conviviale, elle s'adresse à un public international et offre une assistance multilingue. Elle propose notamment des exercices guidés, un retour d'information immédiat, l'intégration de présentations et un appui multi-écrans. Ces caractéristiques la rendent adaptable et accessible aux organismes de formation et aux utilisateurs directs.

Conçue comme un outil d'élaboration, de mise à disposition et d'utilisation d'environnements interactifs simulés, la plateforme Learners a été élaborée à l'aide de technologies à source ouverte. Des modules supplémentaires sur la normalisation des plateformes informatiques et l'approvisionnement en infrastructures et en logiciels facilitent le partage et l'échange de connaissances avec les formateurs de l'AIEA et d'autres organismes qui comptent utiliser la plateforme.

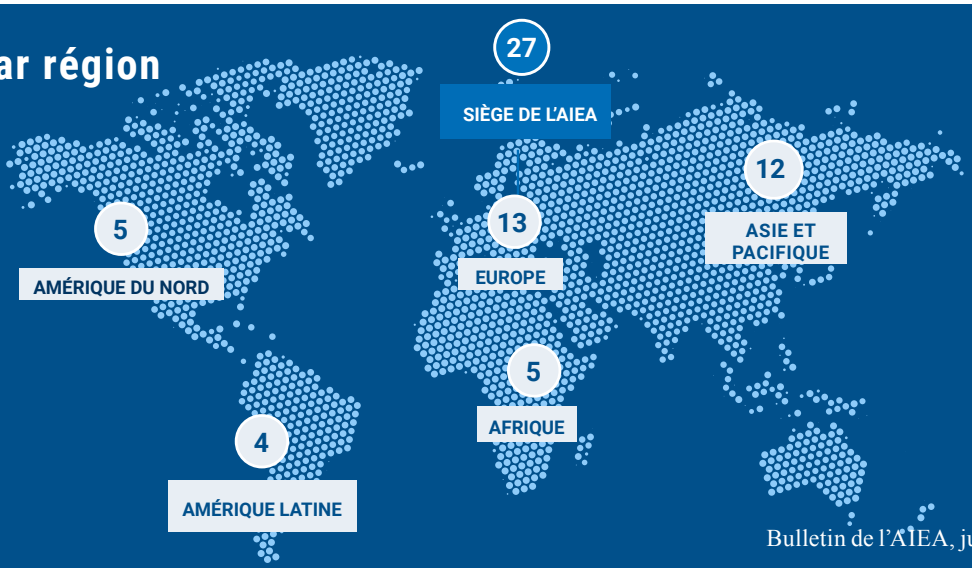
Douze exercices pratiques ont été créés et organisés en six domaines thématiques sur la base des orientations sur la sécurité nucléaire de l'AIEA concernant la sécurité informatique. « En utilisant des environnements virtualisés représentatifs d'installations réelles, la plateforme Learners renforce l'acquisition de compétences pratiques et favorise un accès plus équitable aux connaissances et aux compétences », ajoute M^me^ Buglova.

La plateforme Learners est l'une des facettes du travail que l'AIEA fait pour sensibiliser, renforcer la coopération et fournir aux États l'appui nécessaire face aux menaces croissantes liées à la cybersécurité dans le secteur nucléaire. Plus de 120 pays ont bénéficié d'activités de renforcement des capacités au cours des cinq dernières années. En outre, un soutien adapté sous la forme de missions d'experts, de cours nationaux, régionaux et internationaux, de réunions techniques et de webinaires a favorisé une collaboration active, la mise en commun des connaissances et le développement des compétences. Enfin, l'AIEA aide les pays à organiser des exercices de cybersécurité à grande échelle.

Un centre de formation pratique et de démonstration

Pour l'avenir, il est crucial de poursuivre les investissements dans de telles initiatives de renforcement des capacités afin de disposer des normes de sécurité nucléaire les plus élevées dans le monde entier. Le Centre de formation et de démonstration en matière de sécurité nucléaire (NSTDC) de l'AIEA, établissement à la pointe de la technologie qui ouvrira ses portes au second semestre 2023, contribuera à renforcer les capacités des pays à lutter contre le terrorisme nucléaire au moyen d'expériences de formation pratique. Les cours innovants proposés au NSTDC comprendront des sujets liés à la sécurité informatique et des scénarios de cyberattaques qui pourraient viser des installations nucléaires ou des installations et activités mettant en jeu des sources radioactives.

Événements par région



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

Par Mitchell Hewes

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

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

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

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

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

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

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

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

Défis à relever

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

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

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

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

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

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

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

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

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

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

Sécurité nucléaire : des exercices de sécurité informatique pour se préparer à répondre aux cyberattaques

Par Emma Midgley

Historiquement, la protection des matières nucléaires contre les attaques malveillantes était assurée dans les installations nucléaires par des moyens de protection physique tels que des armes, des gardes et des barrières. Aujourd'hui encore, ces moyens sont utilisés pour ériger des forteresses autour des installations nucléaires, empêchant le vol de matières nucléaires ou d'autres matières radioactives, le sabotage ou l'accès non autorisé aux systèmes de contrôle. Cependant, ces dernières décennies, dans un monde de plus en plus informatisé, la menace de cyberattaques a grandi. Tous les pays, même ceux qui ont les programmes électronucléaires et de recherche les plus avancés, peuvent être vulnérables à une attaque. Il est devenu nécessaire d'élaborer des cadres nationaux de sécurité informatique face aux cybermenaces visant les installations nucléaires. Par des exercices à grande échelle, l'AIEA aide les pays à améliorer leur protection contre les cyberattaques et leurs stratégies de détection et d'intervention face aux cyberattaques contre les installations nucléaires.

L'AIEA a conçu des exercices de sécurité informatique pour les centrales nucléaires et les installations radiologiques, qui ont été effectués au niveau national dans le monde entier. Ces exercices permettent aux pays de s'entraîner et de se préparer à faire face au pire scénario : une atteinte à la cybersécurité dans une installation nucléaire. Les scénarios théoriques peuvent mettre en évidence les faiblesses des politiques, procédures et processus, ainsi que les lacunes à combler par des techniques d'atténuation, le renforcement des capacités ou des changements organisationnels. En plus d'aider les États à exécuter des exercices à grande échelle pour tester la sécurité informatique de leurs installations nucléaires, les orientations sur la sécurité nucléaire de l'AIEA concernant la sécurité informatique constituent également une ressource essentielle permettant aux pays de mettre en place d'importantes mesures de sécurité informatique pour détecter et prévenir les cyberattaques, et y faire face.

« Il est essentiel d'élaborer des politiques, de définir les rôles et les responsabilités et d'établir des procédures détaillées pour faire face aux incidents de sécurité informatique avant qu'ils ne se produisent », souligne Trent Nelson, responsable de la sécurité de l'information et de la sécurité informatique au sein de la Division de la sécurité nucléaire de l'AIEA. « C'est là que l'AIEA peut apporter son aide à bien des égards : exercices, conseils, mise en commun des meilleures pratiques et procédures pour garantir une communication efficace et une protection solide de la sécurité. »

Les facteurs qui rendent les installations nucléaires vulnérables aux cyberattaques sont notamment le personnel, la complexité de la chaîne d'approvisionnement et le partage des informations sensibles entre les nombreuses parties prenantes qui utilisent les systèmes informatiques appuyant les fonctions nucléaires.

« Prenons l'exemple d'une attaque où la compromission d'un fournisseur et la falsification d'une commande de travail amèneraient un technicien de confiance disposant d'un accès autorisé à effectuer une action subtilement incorrecte », poursuit Trent Nelson. « Ce n'est qu'un des moyens que des acteurs malveillants pourraient utiliser pour contourner les systèmes de sécurité. »

Un élément important pour réduire les incidences potentielles de toute cyberattaque est la sensibilisation des parties prenantes et la communication efficace entre elles, car n'importe quel groupe ou membre d'un groupe peut être la cible d'acteurs malveillants. Quatre acteurs principaux interviennent dans la défense des installations nucléaires : l'organisme de réglementation, l'exploitant de l'installation, les organismes d'appui technique [équipes d'intervention en cas d'incident de sécurité informatique (CSIRT), centres opérationnels de sécurité informatique] et les organisations tierces, telles que les fournisseurs et les organismes d'appui. Les exercices sont un bon moyen de tester les communications, la transmission de rapports et les notifications entre les parties prenantes et de vérifier et valider la sûreté et la sécurité des structures organisationnelles.

Un élément important pour réduire les incidences potentielles de toute cyberattaque est la sensibilisation des parties prenantes et la communication efficace entre elles

L'idéal serait que les systèmes de sécurité informatique des installations nucléaires soient impénétrables mais la nature évolutive des acteurs malveillants et la faillibilité humaine font qu'il est pratiquement impossible de prédire comment se passera la prochaine attaque de grande envergure. Il est donc essentiel de détecter rapidement les attaques. Lors d'un récent exercice en Slovénie, une simulation de cyberattaque a permis de vérifier et de valider les capacités de détection et défense contre les cyberattaques.

« La sécurité informatique n'est pas un projet ni un processus mais un cheminement sans fin qui nécessite des efforts, une attention et un entraînement constants », explique Samo Tomažič, chef de la division de la cybersécurité de l'Administration slovène de sûreté nucléaire. « Des exercices tels que celui effectué en Slovénie permettent à toutes les entités concernées du secteur nucléaire d'évaluer la solidité de leurs plans d'intervention en cas de cyberattaque réussie. »

En cas d'incident grave de sécurité informatique, qui pourrait donner lieu à un événement de sûreté ou de sécurité nucléaire, une CSIRT devrait intervenir en plus des parties prenantes habituelles à une installation nucléaire. Un tel incident pourrait entraîner par exemple la violation des politiques ou des procédures de sécurité, des répercussions sur des actifs ou des systèmes numériques sensibles, ou encore la perte d'informations sensibles et du contrôle de fonctions essentielles à la sûreté nucléaire.

Dans ce cas, dès qu'un incident de sécurité informatique ou une compromission de celle-ci sont décelés, la CSIRT travaille avec les parties prenantes de l'installation pour enquêter sur l'incident, recueillir des données criminalistiques, analyser les faits et les lieux, et aider à contenir et à annihiler l'intrusion pour que les exploitants puissent remettre l'installation nucléaire en service. À la fin de l'intervention, des preuves informatiques judiciaires sont réunies pour aider toute enquête criminelle sur l'attaque et assurer un partage efficace des informations afin de renforcer les mesures de sécurité informatique dans l'installation nucléaire pour l'avenir.

Lors de l'exercice en Slovénie, la détection des cyberattaques était essentielle pour répondre à la simulation d'incident et pour tester et valider les procédures d'intervention. Ces exercices permettent de tester la relation entre la sûreté, la sécurité et la préparation des interventions d'urgence, et de renforcer les régimes de sécurité nucléaire en déterminant leurs faiblesses potentielles et en procédant aux changements nécessaires pour mieux les préparer aux éventuelles menaces de cybersécurité. Ils permettent également de tester les voies nationales et internationales de notification et de transmission de rapports. D'une manière générale, la conduite régulière d'exercices de sécurité informatique est un aspect important du maintien de la sécurité des installations nucléaires.

Améliorer les techniques de détection des anomalies de sécurité informatique au moyen des projets de recherche coordonnée

Par Rodney Busquim e Silva et Andrea Rahandini

La détection d'anomalies dans l'exploitation des systèmes informatiques qui contrôlent les fonctions critiques de sûreté et de sécurité nécessite de vastes compétences, et les mesures nécessaires doivent être testées, analysées et modifiées afin d'en garantir la robustesse.

« La détection des anomalies joue un rôle important dans l'évaluation rapide des menaces qui pourraient viser les systèmes informatiques des installations nucléaires et radiologiques », fait observer Scott Purvis, chef de la Section de la gestion de l'information à la Division de la sécurité nucléaire de l'AIEA. « D'ordinaire, les techniques de détection des anomalies reposent sur des applications d'intelligence artificielle telles que l'apprentissage automatique, les méthodes fondées sur les statistiques, les connaissances ou d'autres technologies », explique-t-il. Ces technologies sont utilisées pour déceler les écarts par rapport aux communications réseau ou mesures de processus prévues, qui peuvent être le premier signe d'un contournement des défenses d'un système informatique par un intrus, et peuvent ainsi détecter les cyberattaques en temps réel.

Elles sont importantes parce qu'un malfaiteur très habile peut introduire des logiciels malveillants qui compromettent les fonctions de sûreté ou de sécurité d'un système informatique en falsifiant les données provenant des capteurs et les indicateurs envoyés à un exploitant. L'exploitant peut donc ignorer qu'une activité malveillante est en train de se produire et réagira d'abord en fonction de ce qui est affiché dans la salle de commande, ce qui peut l'induire en erreur et lui faire prendre des mesures inappropriées. Seule la détection automatique des moindres anomalies dues à une telle cyberattaque permettra à un exploitant d'être correctement informé.

Pour agir dans ce domaine de travail important et relever d'autres défis de sécurité informatique, l'AIEA a lancé en 2016 un projet de recherche coordonnée (PRC) spécifique.

La recherche-développement dans le cadre des PRC constitue un élément indispensable des activités de l'AIEA dans le domaine de la sécurité informatique pour la sécurité nucléaire. Ces projets génèrent un ensemble de résultats de recherche et de conclusions exploitables qui complètent les efforts constants de l'AIEA pour renforcer les capacités des pays en matière de prévention et de détection des incidents de sécurité informatique susceptibles de compromettre directement ou indirectement la sûreté et la sécurité des installations nucléaires et radiologiques, d'intervention face à tels incidents et de relèvement après leur survenance.

« Les adversaires sont de plus en plus ingénieux et leurs cybercapacités rendent de plus en plus difficile la mise au point d'outils de détection d'anomalies », indique Scott Purvis. « La mise au point de techniques de détection des anomalies nécessite l'accès à un réseau réaliste et physiquement cohérent et aux données sur les processus de l'installation afin d'entraîner et de tester les modèles de détection ».

Scénario de cyberattaque pour renforcer les capacités

Le PRC de 2016, intitulé « Amélioration de l'analyse des incidents de sécurité informatique dans les installations nucléaires », a produit des résultats notables, permettant notamment des travaux de recherche plus poussés sur des outils et des techniques ciblés, qui n'avaient pu être effectués jusqu'alors sans risquer d'exposer des informations sensibles d'installations nucléaires et radiologiques.

Composée de chercheurs de 13 pays et de 17 organisations, l'équipe du PRC a créé une installation fictive appelée « centrale nucléaire d'Asherah », et un simulateur (ANS) de l'installation a été mis au point par l'Université de São Paulo. Ensemble, les chercheurs ont élaboré des scénarios réalistes de cyberattaques d'une installation nucléaire. Ces scénarios de cyberattaque ont permis de tester et d'évaluer l'efficacité des mesures de sécurité informatique ainsi que les conséquences potentielles de la compromission d'un actif numérique pour l'exploitation de l'installation. En outre, l'équipe a travaillé à la collecte et à l'analyse de données et à la mise au point et à l'essai de techniques de détection des cyberattaques.

« Nous avons mis au point et utilisé l'ANS pour générer un ensemble de données afin d'entraîner nos modèles d'apprentissage automatique et d'en évaluer l'efficience. Le PRC de l'AIEA a réuni des partenaires internationaux pour effectuer des recherches et produire de nouvelles connaissances dans ce domaine, indique Ricardo Marques, professeur à l'École polytechnique de l'Université de São Paulo (Brésil). La coopération entre les participants au PRC a été essentielle pour la validation du travail accompli ».

En outre, les résultats du PRC ont été mis à profit pour la formation théorique et pratique continue de nombreux étudiants de troisième cycle et de chercheurs dans diverses disciplines, renforçant ainsi la recherche et les efforts déployés pour améliorer constamment la sécurité informatique dans les installations nucléaires et radiologiques.

L'Université de São Paulo a mis au point un simulateur à partir d'une installation fictive appelée « centrale nucléaire d'Asherah ».
(Photo : AIEA)

« J'ai effectué une partie des recherches de mon doctorat à l'aide de l'ANS et son interface homme-machine mise au point dans le cadre du PRC de l'AIEA, qui permet à l'utilisateur d'observer le simulateur et de communiquer avec lui », explique Si Wen, doctorante de l'Université de Tsinghua (Chine). « J'ai effectué des recherches sur les techniques de détection des anomalies et l'ANS était essentiel à la production des données nécessaires à l'entraînement et à l'évaluation d'un algorithme de détection mis au point pour les centrales nucléaires. Sans la collaboration entre tous les instituts participants et sans les outils mis au point par l'équipe du PRC, je n'aurais pas pu effectuer mes recherches doctorales sur la cybersécurité des systèmes informatiques des centrales nucléaires », ajoute-t-elle.

Les résultats du PRC — l'ANS, les outils et les orientations — sont accessibles aux instituts de recherche intéressés du monde entier. Ils peuvent être obtenus en soumettant à l'AIEA, par l'intermédiaire de l'autorité nationale compétente, un formulaire de demande disponible sur le Portail d'information sur la sécurité nucléaire de l'AIEA (NUSEC).

Plus récemment, en 2023, l'AIEA a lancé un nouveau PRC intitulé « Amélioration de la sécurité informatique des systèmes de détection des rayonnements » pour étudier les méthodologies et les techniques permettant d'améliorer la sécurité informatique du matériel de détection des rayonnements. Les projets de recherche prévus dans le cadre de ce nouveau PRC, auquel participent 12 organisations (laboratoires nationaux, universités et instituts de recherche nationaux) de 11 pays, porteront sur l'utilisation des technologies numériques émergentes, telles que l'informatique en nuage, et permettront de continuer à étudier et à mettre au point des techniques innovantes de détection des anomalies.

Sécuriser les technologies numériques de la prochaine génération de réacteurs nucléaires

Par Joanne Liou

Toutes les innovations sont porteuses d'avantages susceptibles de transformer les industries mais comportent aussi des risques. Dans le domaine nucléaire, les réacteurs nucléaires avancés, notamment les petits réacteurs modulaires (PRM), intègrent des technologies innovantes, en particulier des technologies numériques qui apportent des solutions inédites.

Les PRM suscitent un intérêt croissant. Ces réacteurs réacteurs nucléaires avancés ont une capacité électronucléaire limitée – habituellement jusqu'à 300 MWe par tranche, soit environ un tiers de la capacité de production des réacteurs nucléaires de puissance traditionnels. Pour autant, l'utilisation d'une technologie numérique de pointe dans ces nouveaux réacteurs pose de nouveaux défis en termes de sûreté et de sécurité nucléaires. À travers le monde, on compte plus de 80 modèles et concepts de PRM à différents stades de développement.

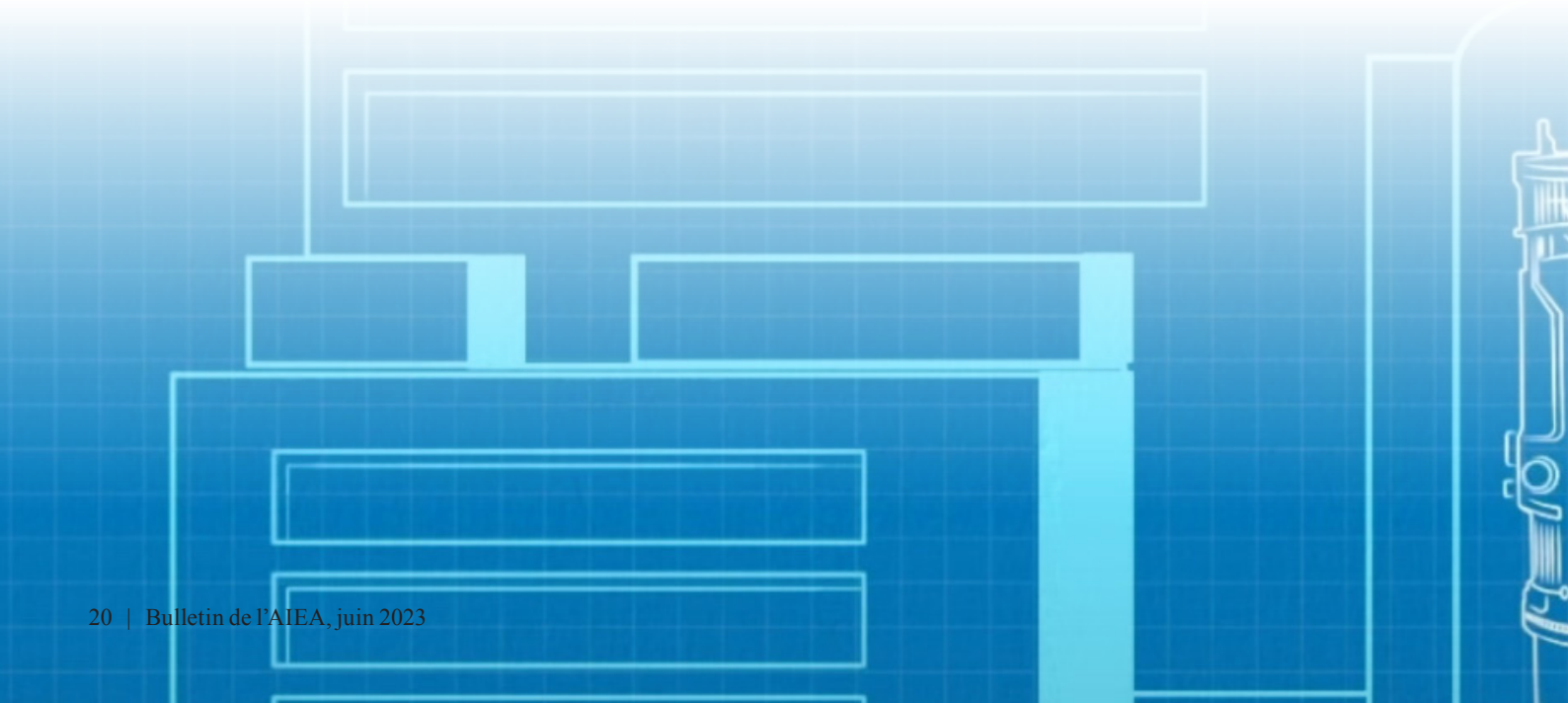
« L'un des défis du déploiement des PRM est d'accélérer la mise au point de leur technologie et de démontrer leur niveau de préparation tout en respectant les normes de sûreté et de sécurité nucléaires », fait observer Rodney Busquim e Silva, responsable de la sécurité de la technologie de l'information à l'AIEA. « Il faut donc mieux concevoir les solutions de commande-contrôle numériques et de sécurité informatique et les maintenir tout au long du cycle de vie du PRM ».

Solutions et défis informatiques

Les modèles innovants de PRM reposent sur des systèmes de contrôle-commande numériques qui leur confèrent des caractéristiques novatrices. Le nombre croissant de technologies numériques nécessaires à l'automatisation, au contrôle et à la maintenance à distance, et à d'autres caractéristiques nouvelles, montre qu'il faut disposer de solutions informatiques.

Certains PRM sont conçus pour être déployés dans des zones isolées et avec peu de personnel sur place, ce qui peut nécessiter une surveillance à distance constante et fiable. Compte tenu de la conception des systèmes de contrôle-commande numériques, l'application de mesures de sécurité informatique devrait être une condition préalable à une communication sécurisée entre le site du PRM et un centre de soutien. « La nécessité d'échanger des informations peut ouvrir des brèches susceptibles d'être exploitées par les cybercriminels et impose donc de prendre des mesures de cybersécurité solides pour protéger l'infrastructure de communication », indique Mike St. John-Green, expert en cybersécurité informatique basé au Royaume-Uni. « La confidentialité, la disponibilité et l'intégrité des informations doivent être protégées pour les opérations à distance afin de garantir un fonctionnement sûr et fiable des PRM et des infrastructures connexes ».

L'intelligence artificielle (IA) et l'apprentissage automatique (AA) appuient également l'exploitation des PRM. L'IA fait référence aux technologies qui produisent des systèmes capables de suivre des problèmes complexes, tandis que les technologies d'AA apprennent à accomplir une tâche particulière à partir de données. En combinant des simulations numériques d'installations nucléaires et des systèmes de surveillance et de contrôle avec des systèmes d'IA, l'industrie nucléaire cherche à optimiser des fonctions complexes, ce qui pourrait accroître l'efficacité opérationnelle. Ces avantages comportent toutefois un risque de cyberattaques. Par exemple, les algorithmes logiciels de l'IA et de l'AA reposent sur des bases de données qui pourraient être manipulées et ainsi entraîner une prise de décision erronée de l'IA.



« Ces systèmes peuvent par exemple, par injection de code, être alimentés intentionnellement avec des données corrompues, au cours du processus de développement, de la livraison ou de l'installation du logiciel. Le défi global est de savoir comment assurer une transparence suffisante des algorithmes d'IA/AA. L'utilisation acceptable de l'IA/AA doit être clairement définie et liée à des niveaux de risque acceptables », fait observer Si Wen, doctorant à l'Université de Tsinghua (Chine).

La sécurité dès la conception

Les experts s'accordent à dire que la sécurité informatique des installations nucléaires doit être prise en compte dès le commencement. Cette approche proactive, dite planification de la sécurité dès la conception, s'appuie sur les meilleures pratiques et les enseignements tirés. Elle répond au principe d'« intégration dans la conception » qui s'applique également à la sûreté, aux garanties et au déclassement nucléaires.

La sécurité informatique dès la conception vise à réduire les risques de sécurité à la source par une approche qui envisage systématiquement et de manière cohérente la sécurité à toutes les étapes de la durée de vie de l'installation ou du processus.

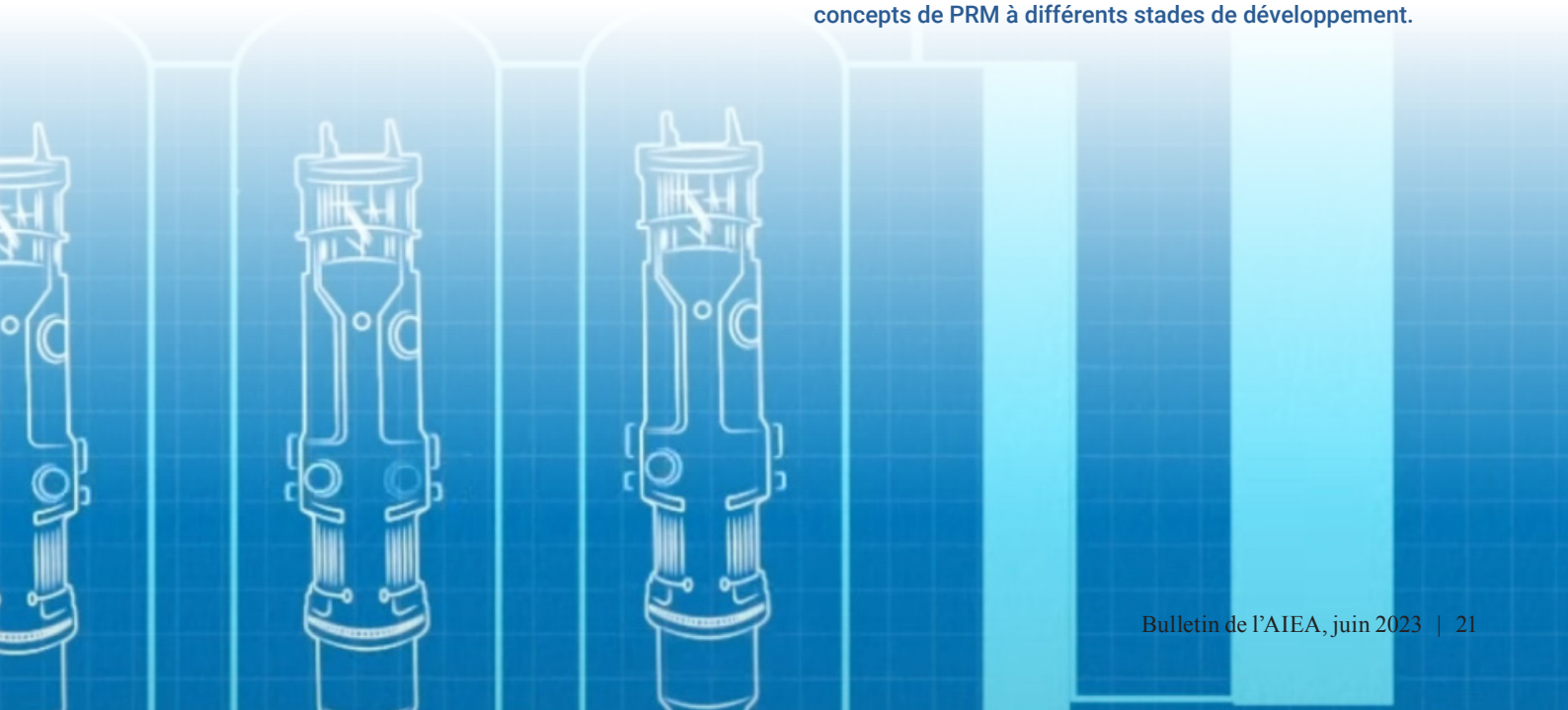
« Les mesures de sécurité informatique doivent être prises en compte et appliquées tout au long du cycle de vie des PRM, dès leur conception, pendant leur exploitation et jusqu'à leur déclassement », souligne M. Busquim e Silva. « Lorsque la sécurité, y compris la cybersécurité, est intégrée à la conception dès le départ, les concepteurs des installations peuvent faire des choix qui les rendront plus sûres, plus efficaces et moins coûteuses. »

Rôle de l'AIEA

L'AIEA met en relation des experts d'organisations nucléaires et autres, qui examinent les questions de sécurité informatique liées aux caractéristiques technologiques et opérationnelles des PRM et décèlent les difficultés en la matière. Par exemple, en février 2022, l'AIEA a organisé une réunion technique sur les systèmes de contrôle-commande et la sécurité informatique pour les PRM afin d'encourager la coopération et de faciliter l'échange d'informations entre experts internationaux. Les participants ont convenu de la nécessité d'harmoniser les approches et les réglementations nationales afin de rendre le marché international des PRM viable. « Les solutions de contrôle-commande concernant les PRM standardisés ouvrent un tout nouveau champ technique. L'automatisation toujours plus poussée nécessaire aux nouveaux modes d'exploitation et l'utilisation généralisée des systèmes numériques exigent des mesures de sécurité informatique et des solutions d'ingénierie dès la conception afin de garantir une exploitation sûre et sécurisée des centrales », déclare Jorge Casanova, qui a participé à la réunion en tant que représentant de l'Autorité argentine de réglementation nucléaire.

En mars 2023, l'AIEA a également organisé un atelier pour approfondir la réflexion sur le développement des capacités techniques liées à la sécurité informatique et aux systèmes de contrôle-commande pour les PRM. En outre, l'AIEA envisage de lancer un projet de recherche coordonnée sur le sujet en 2024.

À travers le monde, on compte plus de 80 modèles et concepts de PRM à différents stades de développement.



Renforcer la sécurité informatique pour la sûreté et la sécurité nucléaires

Par Lydie Evrard

Directrice générale adjointe et Cheffe du Département de la sûreté et de la sécurité nucléaires de l'AIEA

La sûreté nucléaire et la sécurité nucléaire partagent le même objectif et la même vision : protéger les personnes, les sociétés et l'environnement contre les effets nocifs potentiels des rayonnements ionisants. Bien que les activités concernant la sûreté nucléaire et la sécurité nucléaire soient différentes, il est essentiel d'établir une approche bien coordonnée de la gestion de leur interface. Il est important de veiller à ce que les mesures pertinentes soient mises en œuvre de manière à tirer parti des possibilités d'amélioration mutuelle, sans compromettre ni la sûreté, ni la sécurité.

On sait que dans les installations nucléaires et radiologiques, des systèmes et des mesures de sécurité physique sont nécessaires pour protéger le matériel, les systèmes et les dispositifs – généralement destinés à assurer la sûreté nucléaire – contre un acte délibéré de sabotage qui pourrait entraîner un rejet aux conséquences radiologiques. En règle générale, dans les anciens modèles et applications, les systèmes de sûreté ne devaient être protégés que par des mesures de protection physique. Cependant, les évolutions technologiques omniprésentes et sans cesse plus poussées de nos jours confèrent aux systèmes numériques un rôle croissant dans l'efficacité des opérations des installations nucléaires et radiologiques, en particulier ceux qui sont responsables d'importantes fonctions des installations, tels que les systèmes de contrôle-commande, notamment ceux utilisés pour la sûreté et la sécurité.

La sécurité de ces systèmes exige une vigilance rigoureuse afin de détecter les vulnérabilités et d'empêcher tout accès non autorisé aux systèmes de contrôle numérique qui pourrait compromettre les fonctions de sûreté ou de sécurité. À cet égard, la sécurité informatique devient de plus en plus importante pour l'interaction entre la sûreté et la sécurité, et elle est prise en compte dans d'autres domaines clés, notamment l'infrastructure réglementaire, les dispositions techniques de la conception et de la construction des installations nucléaires, les contrôles d'accès aux installations nucléaires, la catégorisation des sources radioactives, la gestion des sources radioactives et des matières radioactives, y compris le combustible usé et les déchets radioactifs, la détection et la récupération des sources non contrôlées, ainsi que les plans d'intervention d'urgence et de secours.

Au niveau national, les décideurs politiques doivent tenir compte de la sécurité nucléaire et de la sûreté nucléaire lors de l'élaboration de la réglementation sur la sécurité informatique. L'attribution claire

des responsabilités, le leadership et la gestion des risques sont le fondement de l'interface de sûreté et de sécurité et jouent un rôle tout aussi important dans la mise en œuvre de mesures de sécurité informatique efficaces. En même temps, la sécurité informatique est par nature un défi mondial.

Dans ce contexte, l'importance de la coopération internationale et le rôle central de l'AIEA sont largement reconnus. L'interface entre la sûreté nucléaire et la sécurité nucléaire est soulignée dans les normes de sûreté de l'AIEA et les orientations de l'AIEA sur la sécurité nucléaire. Depuis dix ans environ, l'AIEA conçoit et propose aux pays un ensemble complet d'assistance dans le domaine technique de la sécurité de l'information et de la sécurité informatique, les aidant à prendre des mesures efficaces contre les cyberattaques qui pourraient avoir une incidence sur la sécurité nucléaire. En outre, l'AIEA appuie la mise en place de synergies entre les systèmes et les mesures de sûreté nucléaire et de sécurité nucléaire afin que les mesures prises dans les deux domaines se complètent au lieu de se nuire.

À l'avenir, les progrès technologiques renforceront encore l'importance d'une sécurité informatique solide pour la sûreté et la sécurité nucléaires aux niveaux des États et des installations. Les technologies en évolution rapide telles que l'intelligence artificielle sont prometteuses pour ce qui est de résoudre certains problèmes et d'améliorer les opérations contrôlées numériquement. Dans le même temps, elles posent de nouveaux défis qui doivent être relevés. De même, les technologies sans fil et d'automatisation sont envisagées et utilisées aujourd'hui dans la conception de réacteurs nucléaires avancés tels que les petits réacteurs modulaires et les microréacteurs. Face à l'évolution constante et rapide des cybermenaces, l'appui de l'AIEA face aux besoins des États Membres en matière de renforcement de la sécurité informatique pour la sûreté et la sécurité nucléaires nécessite de se tenir activement au fait de toutes les nouvelles possibilités et de tous les défis de ces nouvelles technologies afin de proposer les normes, les meilleures pratiques, les formations et les orientations les plus efficaces. Le Département de la sûreté nucléaire de l'AIEA s'y emploie constamment.

Lutter contre les menaces dans un monde de plus en plus numérisé

Par Wolfgang Picot

En mai 2022, l'Institut autrichien de technologie (AIT) est devenu le premier centre collaborateur de l'Agence internationale de l'énergie atomique (AIEA) en matière de sécurité de l'information et de sécurité informatique pour la sécurité nucléaire. L'AIT appuie les cours et les exercices régionaux et internationaux sur la sécurité informatique pour les installations et activités nucléaires, élabore des modules de démonstration technique pour sensibiliser aux cybermenaces et contribue à l'élaboration de matériel de formation pour le Centre de formation et de démonstration en matière de sécurité nucléaire à Seibersdorf.

Pour mieux comprendre cette coopération, nous nous sommes entretenus avec Helmut Leopold, directeur du Centre pour la sûreté et la sécurité numériques de l'AIT.

Quels sont les risques et les menaces qui se font jour dans le domaine de la sécurité informatique en général ?

Aujourd'hui, de nombreux appareils numériques modernes sont construits en vue de réseaux plus étendus. Nombre d'entre eux ont besoin d'un accès à internet pour fonctionner. Le développement de chaque logiciel comporte toujours un risque d'erreurs pouvant conduire à des vulnérabilités. Des interfaces mal protégées et des utilisateurs irresponsables augmentent le nombre de menaces de sécurité pour l'exploitation des systèmes de technologie de l'information (TI).

Les attaquants exploitent les vulnérabilités des systèmes numériques pour y accéder. Les méthodes et outils des attaques évoluent avec les processus d'innovation numérique. Des logiciels pour pirates informatiques sont maintenant facilement disponibles sur internet, ce qui rend les attaques plus faciles même pour les moins doués d'entre eux. Nous sommes confrontés à un écosystème de cyberattaques diversifié mû par le crime organisé, l'espionnage économique et industriel et le cyberterrorisme.

Ainsi, aujourd'hui, un large spectre de cyberattaques menace les utilisateurs, les entreprises et les autorités, et peut toucher l'infrastructure numérique d'États entiers en même temps que des campagnes de désinformation ciblées, ébranlant les bases de nos sociétés.

Le secteur nucléaire est-il confronté aux mêmes dangers ?

Les entreprises et les particuliers utilisent des technologies de l'information (TI) qui sont avant tout basées sur les données et la communication. En revanche, les installations de production et les infrastructures essentielles utilisent des technologies dites d'exploitation qui surveillent et contrôlent les comportements et les résultats de processus de production définis. Les technologies d'exploitation sont traditionnellement beaucoup moins interconnectées que les TI. Cependant, avec les progrès technologiques, les deux domaines ont convergé, et les logiciels et dispositifs des technologies d'exploitation sont de plus en plus connectés à des réseaux plus vastes.

Cette évolution pose problème, car la sensibilisation à la cybersécurité est moins répandue dans le domaine des technologies d'exploitation que dans celui des TI.

Par conséquent, ces nouvelles menaces pour la sécurité des TI deviennent pertinentes pour les technologies d'exploitation utilisées pour la production industrielle et les infrastructures essentielles. Il en va de même pour le secteur nucléaire, qui avait traditionnellement une approche conservatrice et maintenait des systèmes de contrôle isolés.

Commet agit l'AIT pour renforcer la cybersécurité dans le domaine de la sécurité nucléaire ?

Le programme de recherche de l'AIT étudie l'incidence des scénarios de menace en évolution sur les systèmes des technologies d'exploitation et vise à mettre au point un savoir-faire et de nouvelles solutions pour accroître la résilience des infrastructures essentielles face aux cyberattaques. Ces travaux servent à élaborer de nouvelles normes de sécurité mondiales, des procédures de certification pour les éléments essentiels des systèmes et des nouvelles architectures de systèmes afin d'intégrer de solides mesures de cybersécurité dans les systèmes des technologies d'exploitation dès le début de leur conception.

L'AIT propose également une formation complète pour préparer aux attaques de cybersécurité. Dans des simulations complexes de systèmes de TI « virtualisés », les utilisateurs, les développeurs de systèmes, le personnel d'exploitation et les représentants des gouvernements réagissent à des scénarios réalistes de cyberattaque. Ces simulations sont essentielles pour garantir la résilience des systèmes de TI et des technologies d'exploitation et leur capacité à lutter efficacement contre les cybermenaces.

Quels sont les avantages de l'environnement d'apprentissage virtuel mis au point par l'AIT et l'AIEA ?

L'expérience pratique est le mode d'apprentissage le plus efficace. L'AIT et l'AIEA ont mis au point une simulation qui permet de créer des « jumeaux numériques » d'infrastructures numériques essentielles existantes et qui forme également à des scénarios d'application très réalistes.

Dans cet environnement virtuel, les utilisateurs des secteurs public et privé peuvent évaluer et tester l'efficacité des mécanismes de protection et des processus opérationnels.

L'expérience tirée de cet environnement d'apprentissage virtuel contribue à la mise en place de capacités défensives durables dans les organisations publiques et privées.

Outre la formation virtuelle, comment les travaux et l'expertise de l'AIT en sécurité informatique font-ils progresser la sécurité nucléaire ?

Nous pouvons contribuer à la défense contre les attaquants, par exemple en mettant au point des logiciels pour surveiller les périphériques de périmètre qui relient généralement les réseaux internes des organisations à internet. Les attaquants se servent souvent de ces systèmes comme porte d'entrée avant de faire des dégâts.

Nous mettons à profit notre expérience de la détection des anomalies pour entraîner des logiciels d'analyse qui surveillent ces périphériques de périmètre généralement utilisés dans un type particulier d'installation nucléaire.

Un tel logiciel peut déclencher une alarme ou prendre des contre-mesures si un périphérique se comporte de manière anormale. Ainsi, les exploitants peuvent rapidement détecter et bloquer les cyberattaques avant qu'elles ne causent des dommages importants.

Il y a un an l'AIT a été désigné premier centre collaborateur de l'AIEA dans le domaine de la sécurité informatique pour la sécurité nucléaire et reste aujourd'hui le seul centre de ce type. Qu'est-ce que cela implique pour le travail de l'AIT ?

Nous sommes extrêmement fiers d'avoir été désignés centre collaborateur et nous continuons à appuyer l'organisation d'un cours régional sur la sécurité informatique pour les systèmes d'instrumentation et de contrôle dans le secteur nucléaire. Le cours a été organisé deux fois en 2022 et a utilisé certains résultats de notre entreprise commune pour élaborer une plateforme de formation virtuel.

Nous avons également participé à des activités sur la sécurité informatique dans le cadre de la mise au point de petits réacteurs modulaires.

En ce moment, nous aidons l'AIEA à préparer la conférence internationale de 2023 sur la sécurité informatique dans le monde nucléaire : la sécurité pour la sûreté, où nous ferons des démonstrations de notre plateforme de formation virtuelle, présiderons des tables rondes et présenterons des documents sur nos recherches dans le secteur, et plus encore.

Comment l'AIT participe-t-il au Centre de formation et de démonstration en matière de sécurité nucléaire ?

Nous avons travaillé en étroite collaboration avec nos collègues de l'AIEA pour mettre au point des modules de formation, des démonstrations et des exercices pour ce centre. Nous intégrons des modules de sécurité informatique aux cours sur la protection physique des matières nucléaires et des autres matières radioactives, et sur la détection et l'intervention au cas où des matières nucléaires et d'autres matières radioactives échappent au contrôle réglementaire. Ce fonctionnement vise à renforcer l'idée que la sécurité informatique est une partie intégrante et indissociable de la sécurité nucléaire.

Comment la collaboration internationale protège le monde contre les cybermenaces

Tighe Smith est le coordonnateur du Groupe de travail A9 du Sous-comité 45A de la CEI. Il a été nommé par un comité pour diriger le groupe de travail A9, qui s'occupe de la cybersécurité à la Commission électrotechnique internationale (CEI).

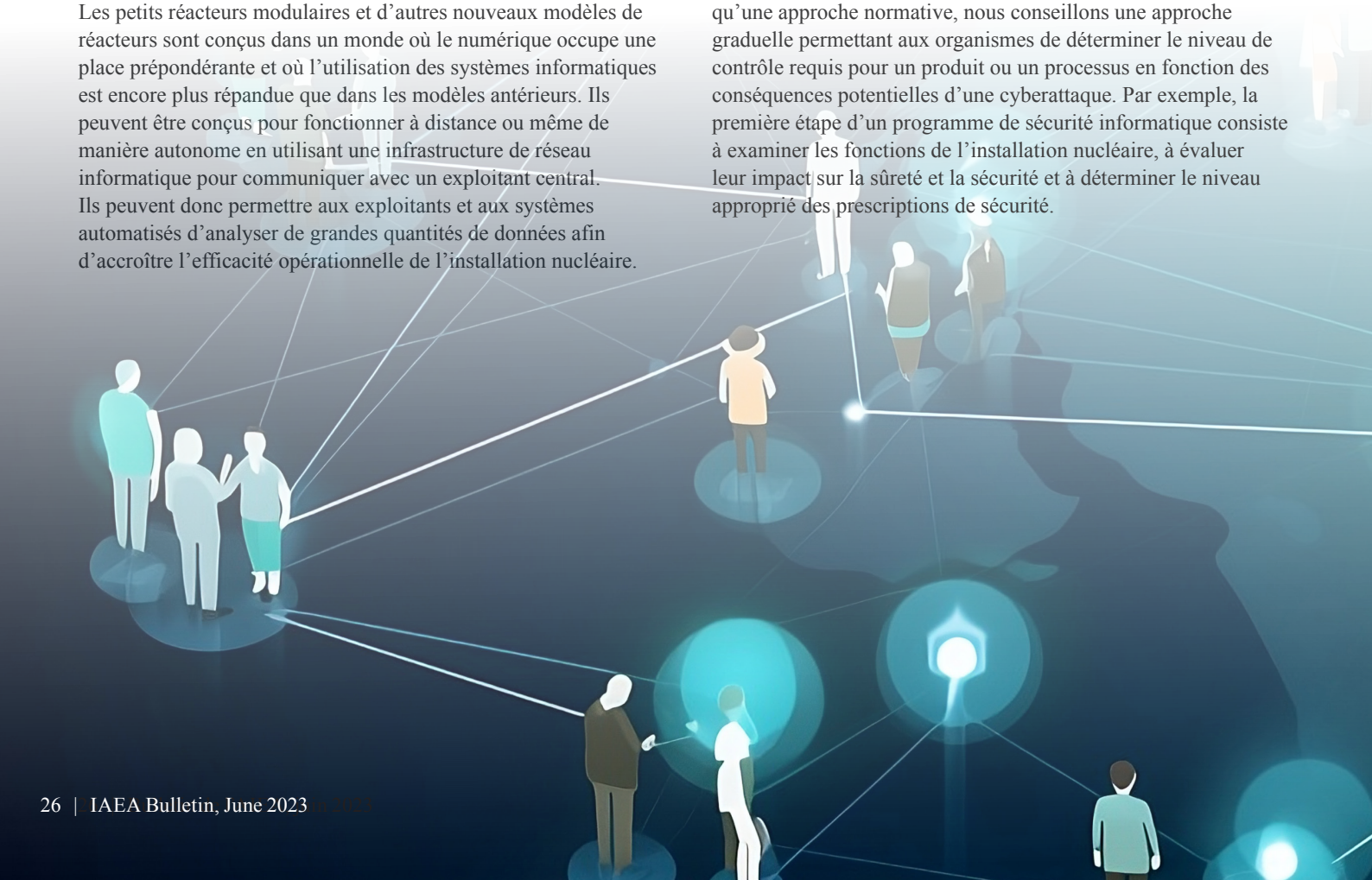
La CEI est une organisation mondiale à but non lucratif qui élabore des normes internationales pour la conception, la construction et l'exploitation du matériel électrique, notamment celui utilisé dans les centrales nucléaires. Fondée en 1906, la CEI rassemble plus de 170 pays et a déjà publié 10 000 normes internationales.

L'industrie nucléaire fait face à un défi important pour maintenir la sécurité informatique en raison de l'utilisation généralisée d'appareils numériques. Cette tendance se voit dans la vie de tous les jours, où réfrigérateurs, éclairage et autres appareils intelligents contrôlés à distance via l'informatique en nuage sont devenus courants. De nombreux systèmes des installations nucléaires qui n'avaient auparavant aucun composant numérique en sont maintenant dotés. La puissance de calcul, la reprogrammabilité et la capacité d'interconnexion de ces systèmes fournissent une efficacité inégalée à l'appui des opérations, de la sûreté nucléaire et de la sécurité nucléaire.

Les petits réacteurs modulaires et d'autres nouveaux modèles de réacteurs sont conçus dans un monde où le numérique occupe une place prépondérante et où l'utilisation des systèmes informatiques est encore plus répandue que dans les modèles antérieurs. Ils peuvent être conçus pour fonctionner à distance ou même de manière autonome en utilisant une infrastructure de réseau informatique pour communiquer avec un exploitant central. Ils peuvent donc permettre aux exploitants et aux systèmes automatisés d'analyser de grandes quantités de données afin d'accroître l'efficacité opérationnelle de l'installation nucléaire.

Cependant, cette modernisation numérique de l'industrie nucléaire suscite des défis supplémentaires car, sans une sécurité informatique adéquate, des points faibles ou des vulnérabilités pourraient être exploités par des acteurs malveillants dans le cadre d'une attaque contre l'une de ces installations.

Pour relever les défis de l'évolution rapide de la technologie numérique dans les installations nucléaires et répondre à la nécessité d'appuyer l'harmonisation entre les pays et les installations, la CEI a adopté une approche fondée sur les conséquences et les risques, alignée sur les orientations concernant la sécurité de l'information et la sécurité informatique de la collection Sécurité nucléaire de l'AIEA (NSS). Plutôt qu'une approche normative, nous conseillons une approche graduelle permettant aux organismes de déterminer le niveau de contrôle requis pour un produit ou un processus en fonction des conséquences potentielles d'une cyberattaque. Par exemple, la première étape d'un programme de sécurité informatique consiste à examiner les fonctions de l'installation nucléaire, à évaluer leur impact sur la sûreté et la sécurité et à déterminer le niveau approprié des prescriptions de sécurité.



Prévention, détection et atténuation

Comme il est difficile de prévoir l'évolution future des cyberattaques, la CEI a travaillé en étroite collaboration avec l'AIEA et élaboré des normes recommandant que les programmes de sécurité informatique dans les installations nucléaires mettent l'accent sur la détection, l'intervention et le relèvement, ainsi que la prévention. Même si certains éléments d'une cyberattaque réussissent, des mécanismes doivent être mis en place pour rétablir et assurer la bonne exécution des fonctions nécessaires pour garantir que la sûreté et la sécurité ne sont pas compromises.

Avec la numérisation rapide de notre monde et la croissance de l'intelligence artificielle et de l'apprentissage automatique, la sécurité informatique des installations nucléaires peut paraître une tâche colossale. La collaboration internationale est cruciale pour continuer à exploiter ces installations de manière sûre et sécurisée malgré ces défis. Depuis plus d'un demi-siècle, l'AIEA, la communauté internationale et l'industrie nucléaire collaborent à la normalisation pour promouvoir la sûreté et la sécurité de la technologie nucléaire pacifique. Les enjeux mondiaux tels que les changements climatiques et la sécurité énergétique devenant de plus en plus pressants, de nombreux pays se tournent vers des technologies nucléaires nouvelles et innovantes pour produire de l'énergie bas carbone, ce qui rend la normalisation encore plus importante pour maintenir la sûreté et la sécurité des installations nucléaires.

Collaboration dans le monde nucléaire

L'AIEA et la CEI apportent une contribution essentielle aux efforts internationaux visant à établir des normes pour la sécurité de l'information et la sécurité informatique dans les installations nucléaires. L'AIEA élabore des orientations dans la collection Sécurité nucléaire sur la base d'un consensus international, établissant les concepts et les normes de la sécurité de l'information et de sécurité informatique, éléments fondamentaux de la réalisation des objectifs de sécurité nucléaire. La collection Sécurité nucléaire fournit des conseils sur l'organisation des ressources de l'État et la préparation des réglementations industrielles et des concepts de mise en œuvre d'une approche cybernétique dans les installations nucléaires.

En tant qu'organisation internationale de normalisation qui promeut les meilleures pratiques et le partage des connaissances, la CEI travaille en étroite collaboration avec l'AIEA. Dans le cadre du mémorandum d'accord entre la CEI et l'AIEA, les scientifiques et les experts qui travaillent avec la CEI élaborent des normes et des rapports techniques sur la mise en œuvre des orientations de l'AIEA au moyen de prescriptions programmatiques et techniques spécifiques. Ces prescriptions peuvent être mises à profit dans la conception et le développement des systèmes numériques actuels et futurs qui peuvent être certifiés par rapport à des modèles réglementaires conformes aux orientations de l'AIEA. Des experts détenant l'expérience de l'industrie nucléaire dans l'application des normes de la CEI peuvent alors concourir à l'élaboration des futures orientations de l'AIEA.

Les scientifiques et les experts contribuent aux travaux de la CEI à titre volontaire et de nouveaux collaborateurs sont toujours les bienvenus. La communauté des experts en sécurité informatique dans le domaine nucléaire est relativement réduite, même à l'échelle mondiale. Contribuer au travail de la CEI permet d'élaborer des normes qui peuvent être utilisées dans le monde entier et de soutenir l'industrie nucléaire du monde entier.

Code de conduite de l'AIEA

20 ans de progrès en matière de sûreté et de sécurité des sources radioactives

Les intervenants de la manifestation parallèle « Équité femmes-hommes et inclusion, et le Code de conduite sur la sûreté et la sécurité des sources radioactives : 20 ans de progrès ». (Photo : W. Wawrzuta/AIEA)

Plus de 270 experts juridiques et techniques de 128 pays et de 4 organisations internationales se sont réunis à Vienne (Autriche) en mai 2023 pour examiner les progrès réalisés en matière de sûreté et de sécurité des sources radioactives et pour se pencher sur les domaines où des améliorations sont nécessaires.

Les sources radioactives sont indispensables dans de nombreux domaines. En médecine, elles aident à traiter le cancer. En agriculture, elles permettent aux scientifiques d'élaborer des variétés de cultures améliorées face au changement climatique pour assurer la sécurité alimentaire. En art et en archéologie, elles contribuent à la préservation d'un patrimoine culturel inestimable. Mais ces sources doivent être manipulées selon des mesures de sûreté et de sécurité appropriées.

Pour aider les pays à faire face aux risques et à protéger les populations et l'environnement contre une exposition accidentelle aux rayonnements ou contre des actes intentionnels non autorisés mettant en jeu des sources radioactives, l'AIEA a élaboré le Code de conduite sur la sûreté et la sécurité des sources radioactives, qui a été approuvé en 2003 par le Conseil des gouverneurs de l'AIEA et marque cette année son 20e anniversaire.

« Vingt ans se sont écoulés depuis l'approbation du Code de conduite et nous faisons des progrès constants dans l'amélioration de la sûreté et de la sécurité des sources radioactives dans le monde », a déclaré Rafael Mariano Grossi, Directeur général de l'AIEA, lors de la séance d'ouverture de la réunion à participation non limitée d'experts techniques et juridiques consacrée au partage d'informations concernant l'application par les États du Code de conduite sur la sûreté et la sécurité des sources radioactives. « Cependant, reste du travail à faire pour parvenir à un engagement politique encore plus fort et pour partager les meilleures pratiques mondiales de gestion durable, sûre et sécurisée de ces sources ».

Pendant cinq jours, des experts internationaux ont pu échanger des informations sur les pratiques nationales d'application du Code de conduite et de ses deux documents d'orientation complémentaires. Tous les trois ans, ces réunions permettent aux pays de partager leurs expériences, d'échanger les enseignements tirés et de déterminer les enjeux actuels et futurs de l'application du Code.

Tout au long de la semaine, les participants ont approfondi divers sujets, notamment l'évolution de la sûreté et de la sécurité nucléaires, les aspects juridiques, la coopération internationale, l'évolution future et l'incidence du Code de conduite. Les discussions ont porté sur les difficultés et les priorités de la mise en place d'un cadre réglementaire approprié pour la sûreté et la sécurité des sources radioactives, de la gestion de leur cycle de vie, de la réglementation des importations et des exportations et de la gestion des sources retirées du service. On soulignera que la réunion a permis aux participants de partager leurs approches respectives de l'application effective des dispositions du Code de conduite.

Des orientations essentielles pour un avenir sûr et sécurisé

S'exprimant lors de l'événement d'ouverture, le coprésident de la réunion, Ramzi Jammal, premier vice-président et chef de la réglementation des opérations

à la Commission canadienne de sûreté nucléaire (CCSN), a souligné que l'application du Code de conduite est primordiale pour assurer la protection de l'environnement, du public et des travailleurs. « Notre objectif ultime est d'assurer la sûreté et la sécurité globales des sources radioactives tout au long de leur cycle de vie afin d'éviter toute exposition accidentelle aux rayonnements et d'empêcher qu'elles ne soient utilisées à des fins malveillantes. C'est un effort collaboratif constant. »

En présentant une session spéciale sur l'histoire du Code, Theresa Clark, Directrice adjointe de division à la Commission de la réglementation nucléaire des États-Unis, s'est également adressée aux participants en tant que coprésidente : « En réfléchissant à ces vingt ans et en les célébrant, nous voulions parvenir à une compréhension commune de l'origine du Code d'un point de vue juridique et technique, afin de partager nos expériences et nos meilleures pratiques et d'apprendre les uns des autres pour améliorer l'application du Code dans le monde ».

Le Code de conduite explique comment les pays peuvent garantir la sûreté et la sécurité des sources radioactives depuis leur production initiale jusqu'à leur stockage définitif. Il contient des considérations internationales et des recommandations sur l'élaboration, l'harmonisation et la mise en œuvre des politiques, lois et réglementations nationales, ainsi que sur la coopération entre les pays. Bien qu'il s'agisse d'un instrument juridiquement non contraignant, 146 États ont exprimé leur soutien politique à l'application de ses dispositions depuis son approbation par le Conseil des gouverneurs en 2003.

Deux documents d'orientation complètent le Code de conduite. Les Orientations pour l'importation et l'exportation de sources radioactives traitent des rôles et des responsabilités en matière d'importation et d'exportation sûres et sécurisées de sources radioactives. Les Orientations sur la gestion des sources radioactives retirées du service fournissent des explications sur la gestion des sources retirées du service, décrivant les possibilités de gestion de fin de vie telles que le recyclage et la réutilisation, l'entreposage à long-terme, le stockage définitif et le retour au fournisseur. Elles encouragent également la mise en place d'une politique et d'une stratégie nationales de gestion des sources retirées du service.

« Le Code de conduite et ses Orientations apportent des avantages concrets à la sûreté radiologique et à la sécurité nucléaire nationales et internationales, permettant de tirer pleinement parti des sources radioactives pour un avenir durable », a conclu la coprésidente Aayda Ahmed Al Shehhi, Directrice de la Sûreté radiologique à l'Autorité fédérale de réglementation nucléaire des Émirats arabes unis (AFRN).

L'AIEA travaille en étroite coopération avec les pays pour assurer la gestion harmonisée, sûre et sécurisée des sources radioactives. Elle les aide à appliquer les principes du Code et leur fournit une assistance étendue dans l'élaboration de stratégies et de plans d'action pour l'application du Code, l'amélioration des systèmes d'autorisation, d'inspection, de coercition et de gestion, et le renforcement des capacités des organismes nationaux de réglementation conformément à ses normes de sûreté, à ses orientations sur la sécurité nucléaire et aux meilleures pratiques internationales.

Renforcer la diversité et l'inclusion dans le domaine nucléaire

En marge de la rencontre, un événement parallèle intitulé « Équité femmes-hommes et inclusion, et le Code de conduite sur la sûreté et la sécurité des sources radioactives : 20 ans de progrès », a été organisé par la CCSN. Il a réuni 120 participants qui ont examiné les moyens de promouvoir et de renforcer la participation des femmes dans le domaine nucléaire, notamment en sûreté et sécurité nucléaires, et d'offrir des chances égales à toutes les personnes, quel que soit leur sexe.

« Une représentation diversifiée à la table des discussions contribue à une augmentation des attitudes de questionnement, ce qui renforce la culture de sûreté dans l'organisation. L'équité femmes-hommes ne concerne pas seulement les femmes, c'est une question de société qui doit être abordée par tous », a déclaré Rumina Velshi, Présidente et directrice générale de la CCSN, ajoutant qu'en raison de la demande croissante en ressources humaines, il faut absolument donner aux femmes davantage de possibilités dans le domaine nucléaire.

« La sûreté et la sécurité nucléaires reposent sur un questionnement et une ouverture à l'apprentissage et aux observations constructives, et sur la capacité de combiner différents points de vue et de mobiliser différentes compétences spécialisées. La diversité, et notamment une meilleure répartition femmes-hommes, est un véritable atout à cet égard. Nous sommes plus forts et plus efficaces lorsque nous accueillons la diversité et encourageons notre personnel à exprimer son opinion », a déclaré Lydie Evrard, Directrice générale adjointe de l'AIEA et Cheffe du Département de la sûreté et de la sécurité nucléaires, pendant l'événement.

Margaret Doane, Directrice générale adjointe de l'AIEA et Cheffe du Département de la gestion, a déclaré que « le renforcement de la participation des femmes et des personnes d'origines diverses dans les secteurs liés au nucléaire est vital pour toute organisation ». Elle a souligné les initiatives de l'AIEA visant à améliorer l'égalité femmes-hommes, notamment le programme de bourses Marie Skłodowska-Curie et le programme Lise Meitner, qui visent à amener davantage de femmes dans le domaine nucléaire.

Christer Viktorsson, Directeur général de l'AFRN, a fait part de son point de vue sur le sujet : « L'AFRN a des mesures ciblées pour promouvoir l'égalité femmes-hommes. La volonté et le soutien des dirigeants sont essentiels, notamment pour effectuer des enquêtes sur les possibilités d'amélioration de l'inclusivité et du traitement équitable de l'ensemble du personnel. Il est tout aussi important de disposer d'un cadre approprié et d'une mise en œuvre efficace qui soient inclusifs. »

— Artem Vlasov

Les pays arabophones examinent les plans sur la sécurité nucléaire

Participants à une réunion régionale tenue récemment en Tunisie échangeant leurs expériences de l'élaboration et de la mise en œuvre d'un INSSP. (Photo : Z. Hassan/AIEA et AAEA)

Les pays membres du Réseau arabe des organismes de réglementation nucléaire (ANNuR) se sont réunis récemment en Tunisie pour discuter ensemble des meilleures pratiques, des défis et des possibilités concernant la mise en œuvre d'activités de sécurité nucléaire dans le cadre de leurs plans intégrés d'appui en matière de sécurité nucléaire (INSSP) respectifs. La réunion a souligné l'importance des approches régionales pour améliorer les capacités réglementaires et opérationnelles, approches inhérentes au programme de sécurité nucléaire de l'AIEA.

« Envisager la sécurité nucléaire d'un point de vue régional permet d'améliorer la coopération internationale et de faciliter la mise en œuvre du programme de sécurité nucléaire de l'AIEA », explique Elena Buglova, directrice de la Division de la sécurité nucléaire de l'AIEA. « La coopération avec des réseaux régionaux comme ANNuR renforce encore l'efficacité du mécanisme d'appui de l'INSSP, créant des possibilités de définir les enjeux communs et de les examiner entre pays géographiquement proches ou partageant la même langue ».

Lors de la réunion, 28 participants de 14 pays ont fourni des informations sur la mise en œuvre de leurs INSSP nationaux. Les domaines abordés ont été notamment les activités liées aux cadres législatifs et réglementaires de sécurité nucléaire, l'évaluation nationale des menaces et des risques, les régimes de protection physique, la détection des actes criminels ou non autorisés mettant en jeu des matières nucléaires ou d'autres matières radioactives non soumises à un contrôle réglementaire, l'intervention en cas d'événements de sécurité nucléaire mettant en jeu ces matières, et le maintien des régimes nationaux de sécurité nucléaire.

Le Liban est actuellement l'un des pays qui utilisent l'INSSP comme mécanisme pour renforcer son infrastructure nationale de sécurité nucléaire. « L'atelier nous a permis de partager notre expérience nationale de mise en œuvre de l'INSSP et d'examiner les défis de la sécurité nucléaire dans nos pays ainsi que des moyens possibles de les relever », dit Hassan Basat, chef de section responsable de l'autorisation, de l'inspection et de la réglementation à la Commission libanaise de l'énergie atomique. « Le résultat le plus important a été l'identification des domaines prioritaires communs de l'INSSP qui doivent être renforcés par les membres de l'ANNuR ».

Actuellement, 19 des 22 membres de l'ANNuR ont un INSSP approuvé. Au

niveau mondial, 92 pays ont des INSSP approuvés.

« Au niveau régional, nous avons en commun des frontières et des défis spécifiques », indique Shaima Khalid AlJanahi, cheffe de l'unité d'analyse physique de la Direction de la radioprotection du Conseil suprême de l'environnement de Bahreïn. « L'atelier a permis la mise en commun d'expériences et de connaissances qui, nous l'espérons, sera suivie d'actions résolues visant à améliorer et à renforcer la sécurité nucléaire dans la région ».

La réunion était organisée par l'Agence arabe de l'énergie atomique (AAEA) avec l'appui financier de l'Union européenne.

Le mécanisme de soutien de l'INSSP

L'AIEA aide les pays qui en font la demande à élaborer un INSSP, cadre d'une approche systématique et globale d'identification et de hiérarchisation des besoins nationaux en matière de sécurité nucléaire afin d'établir un plan de mise en œuvre des améliorations de la sécurité nucléaire au niveau national. Le processus de l'INSSP est complété par un outil d'auto-évaluation volontaire mis à la disposition des pays intéressés sur le Portail d'information sur la sécurité nucléaire (NUSEC).

L'INSSP et son plan de mise en œuvre permettent aux pays de faire face à leurs besoins les plus urgents et d'identifier les questions qui peuvent être résolues au niveau national et celles pour lesquelles il faut une aide de la communauté internationale.

Une fois que les besoins de chaque pays ont été identifiés, l'AIEA peut commencer à jeter les bases d'une assistance ciblée, telle que celle fournie par les missions du Service consultatif international sur la protection physique (IPPAS) et du Service consultatif international sur la sécurité nucléaire (INSServ).

Coopération entre l'AIEA et l'ANNuR

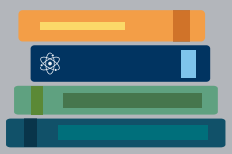
L'ANNuR est un réseau régional créé en 2010 dans le cadre du Réseau mondial de sûreté et de sécurité nucléaires (GNSSN) de l'AIEA. L'ANNuR favorise, améliore, renforce et harmonise les infrastructures réglementaires de radioprotection et de sûreté et sécurité nucléaires dans les pays participants, et sert de cadre de mise en commun et d'échange de données d'expérience et de pratiques réglementaires.

— Vasiliki Tafili

Publications de l'AIEA gratuites en ligne

télécharger ici

www.iaea.org/books



Pour commander un livre, écrivez à
sales.publications@iaea.org

TÉLÉCHARGER

Sécurité de l'information nucléaire

et d'autres publications de l'AIEA sur
la sécurité informatique dans le monde nucléaire

www.iaea.org/bulletin/64-2

Vous pouvez lire cette publication et d'autres numéros du Bulletin de l'AIEA en ligne à l'adresse www.iaea.org/fr/bulletin

Pour de plus amples informations sur l'AIEA et les travaux qu'elle mène, rendez-vous sur le site www.iaea.org/fr

ou suivez-nous sur

ISSN 0251-4044 23-01968F