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).

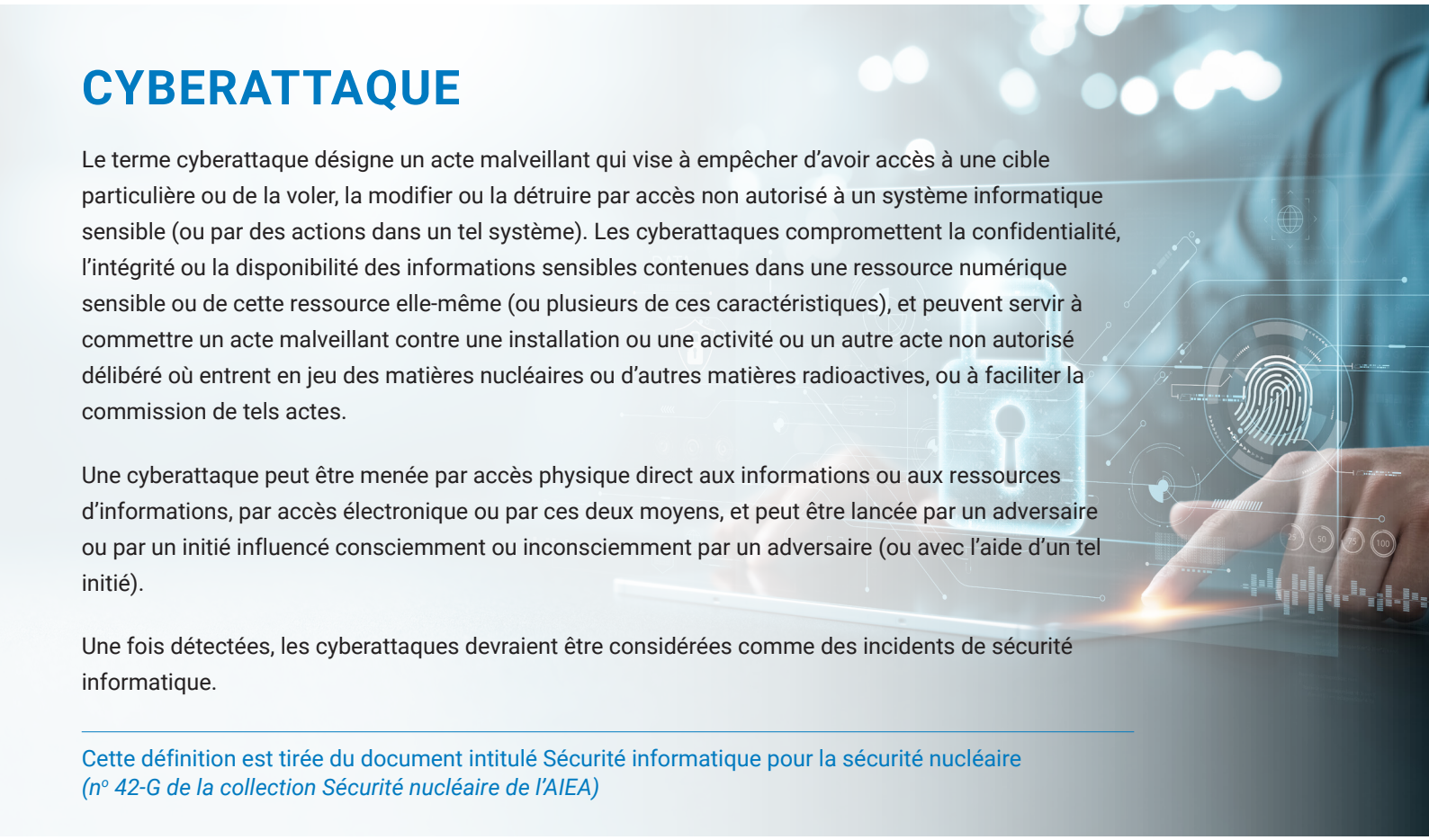
Parallèlement, l'AIEA appuie les exercices nationaux ou régionaux de sécurité informatique dans le cadre de son action de sensibilisation à la menace des cyberattaques et à leurs incidences potentielles sur la sécurité nucléaire. Les exercices comportent différents scénarios où des informations sensibles 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)*