Collection Sécurité nucléaire de l'AIEA nº 42-G

Guide d'application

Sécurité informatique pour la sécurité nucléaire

IAEA
Agence internationale de l'énergie atomique

COLLECTION SÉCURITÉ NUCLÉAIRE DE L'AIEA

Les questions de sécurité nucléaire liées à la prévention, la détection et l'intervention en cas d'actes criminels ou d'actes non autorisés délibérés, mettant en jeu ou visant des matières nucléaires, d'autres matières radioactives, des installations associées ou des activités associées, sont traitées dans la **collection Sécurité nucléaire de l'AIEA**. Ces publications sont conformes aux instruments internationaux relatifs à la sécurité nucléaire, notamment à la Convention sur la protection physique des matières nucléaires telle qu'amendée, à la Convention internationale pour la répression des actes de terrorisme nucléaire, aux résolutions 1373 et 1540 du Conseil de sécurité des Nations Unies et au Code de conduite sur la sûreté et la sécurité des sources radioactives, et elles les complètent.

CATÉGORIES DANS LA COLLECTION SÉCURITÉ NUCLÉAIRE DE L'AIEA

Les publications de la collection Sécurité nucléaire de l'AIEA se répartissent entre les catégories suivantes :

- Les **Fondements de la sécurité nucléaire**, qui portent sur les objectifs et les éléments essentiels d'un régime national de sécurité nucléaire. Ils servent de base à l'élaboration des recommandations en matière de sécurité nucléaire.
- Les **Recommandations en matière de sécurité nucléaire**, qui prévoient des mesures que les États devraient prendre pour établir et maintenir un régime national de sécurité nucléaire efficace conforme aux Fondements de la sécurité nucléaire.
- Les **Guides d'application**, qui fournissent des orientations sur les moyens dont disposent les États Membres pour appliquer les mesures prévues dans les Recommandations en matière de sécurité nucléaire. À ce titre, ils s'intéressent à la mise en application des recommandations relatives à de grands domaines de la sécurité nucléaire.
- Les **Orientations techniques**, qui fournissent des orientations sur des sujets techniques particuliers et complètent les orientations figurant dans les Guides d'application. Elles exposent de manière détaillée comment mettre en œuvre les mesures nécessaires.

RÉDACTION ET EXAMEN

Le Secrétariat de l'AIEA, des experts d'États Membres (qui aident le Secrétariat à rédiger les publications) et le Comité des orientations sur la sécurité nucléaire (NSGC), qui examine et approuve les projets de publications, participent à l'élaboration et à l'examen des publications de la collection Sécurité nucléaire. Selon qu'il convient, des réunions techniques à participation non limitée sont organisées pendant la rédaction afin que des spécialistes d'États Membres et d'organisations internationales concernées puissent examiner le projet de texte et en discuter. En outre, pour faire en sorte que ces projets soient examinés de façon approfondie et largement acceptés au niveau international, le Secrétariat les soumet à tous les États Membres, qui disposent de 120 jours pour les examiner officiellement.

Pour chaque publication, le Secrétariat prépare, et le NSGC approuve, à des étapes successives du processus de préparation et d'examen, ce qui suit :

- un aperçu et un plan de travail décrivant la publication nouvelle ou révisée prévue, son objectif prévu, sa portée et son contenu ;
- un projet de publication à soumettre aux États Membres pour observations pendant la période de consultation de 120 jours ;
- un projet de publication définitif prenant en compte les observations faites par les États Membres.

Le processus d'élaboration et d'examen des publications de la collection Sécurité nucléaire de l'AIEA tient compte des considérations de confidentialité et du fait que la sécurité nucléaire est indissociable des problèmes généraux et particuliers concernant la sécurité nationale.

La prise en compte, dans le contenu technique des publications, des normes de sûreté et des activités de garanties de l'AIEA se rapportant à la sécurité constitue une préoccupation sous-jacente. En particulier, les publications de la collection Sécurité nucléaire qui traitent de domaines dans lesquels il existe des interfaces avec la sûreté, appelées documents d'interface, sont examinées à chaque étape susmentionnée par les Comités des normes de sûreté nucléaire compétents et par le NSGC.

SÉCURITÉ INFORMATIQUE POUR LA SÉCURITÉ NUCLÉAIRE

Les États ci-après sont Membres de l'Agence internationale de l'énergie atomique :

AFGHANISTAN
AFRIQUE DU SUD
ALBANIE
ALGÉRIE
ALLEMAGNE
ANGOLA
ANTIGUA-ET-BARBUDA
ARABIE SAOUDITE
ARGENTINE
ARMÉNIE
AUSTRALIE
AUTRICHE
AZERBAÏDJAN
BAHAMAS
BAHREÏN
BANGLADESH
BARBADE
BÉLARUS
BELGIQUE
BELIZE
BÉNIN
BOLIVIE, ÉTAT PLURINATIONAL DE
BOSNIE-HERZÉGOVINE
BOTSWANA
BRÉSIL
BRUNÉI DARUSSALAM
BULGARIE
BURKINA FASO
BURUNDI
CAMBODGE
CAMEROUN
CANADA
CHILI
CHINE
CHYPRE
COLOMBIE
COMORES
CONGO
CORÉE, RÉPUBLIQUE DE
COSTA RICA
CÔTE D'IVOIRE
CROATIE
CUBA
DANEMARK
DJIBOUTI
DOMINIQUE
ÉGYPTE
EL SALVADOR
ÉMIRATS ARABES UNIS
ÉQUATEUR
ÉRYTHRÉE
ESPAGNE
ESTONIE
ESWATINI
ÉTATS-UNIS D'AMÉRIQUE
ÉTHIOPIE
FÉDÉRATION DE RUSSIE
FIDJI
FINLANDE
FRANCE
GABON
GÉORGIE
GHANA
GRÈCE
GRENADE
GUATEMALA
GUYANA
HAÏTI
HONDURAS
HONGRIE
ÎLES MARSHALL
INDE
INDONÉSIE
IRAN, RÉP. ISLAMIQUE D'
IRAQ
IRLANDE
ISLANDE
ISRAËL
ITALIE
JAMAÏQUE
JAPON
JORDANIE
KAZAKHSTAN
KENYA
KIRGHIZISTAN
KOWEÏT
LESOTHO
LETTONIE
LIBAN
LIBÉRIA
LIBYE
LIECHTENSTEIN
LITUANIE
LUXEMBOURG
MACÉDOINE DU NORD
MADAGASCAR
MALAISIE
MALAWI
MALI
MALTE
MAROC
MAURICE
MAURITANIE
MEXIQUE
MONACO
MONGOLIE
MONTÉNÉGRO
MOZAMBIQUE
MYANMAR
NAMIBIE
NÉPAL
NICARAGUA
NIGER
NIGERIA
NORVÈGE
NOUVELLE-ZÉLANDE
OMAN
OUGANDA
OUZBÉKISTAN
PAKISTAN
PALAOS
PANAMA
PAPOUASIE-NOUVELLE-GUINÉE
PARAGUAY
PAYS-BAS
PÉROU
PHILIPPINES
POLOGNE
PORTUGAL
QATAR
RÉPUBLIQUE ARABE SYRIENNE
RÉPUBLIQUE CENTRAFRICAINE
RÉPUBLIQUE DE MOLDOVA
RÉPUBLIQUE DÉMOCRATIQUE DU CONGO
RÉPUBLIQUE DÉMOCRATIQUE POPULAIRE LAO
RÉPUBLIQUE DOMINICAINE
RÉPUBLIQUE TCHÈQUE
RÉPUBLIQUE-UNIE DE TANZANIE
ROUMANIE
ROYAUME-UNI DE GRANDE-BRETAGNE ET D'IRLANDE DU NORD
RWANDA
SAINTE-LUCIE
SAINT-KITTS-ET-NEVIS
SAINT-MARIN
SAINT-SIÈGE
SAINT-VINCENT-ET-LES-GRENADINES
SAMOA
SÉNÉGAL
SERBIE
SEYCHELLES
SIERRA LEONE
SINGAPOUR
SLOVAQUIE
SLOVÉNIE
SOUDAN
SRI LANKA
SUÈDE
SUISSE
TADJIKISTAN
TCHAD
THAÏLANDE
TOGO
TONGA
TRINITÉ-ET-TOBAGO
TUNISIE
TÜRKİYE
TURKMÉNISTAN
UKRAINE
URUGUAY
VANUATU
VENEZUELA, RÉP. BOLIVARIENNE DU
VIET NAM
YÉMEN
ZAMBIE
ZIMBABWE

Le Statut de l'Agence a été approuvé le 23 octobre 1956 par la Conférence sur le Statut de l'AIEA, tenue au Siège de l'Organisation des Nations Unies, à New York ; il est entré en vigueur le 29 juillet 1957. L'Agence a son Siège à Vienne. Son principal objectif est « de hâter et d'accroître la contribution de l'énergie atomique à la paix, la santé et la prospérité dans le monde entier ».

COLLECTION SÉCURITÉ NUCLÉAIRE DE L'AIEA – Nº 42-G

SÉCURITÉ INFORMATIQUE POUR LA SÉCURITÉ NUCLÉAIRE

GUIDE D'APPLICATION

AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE
VIENNE, 2022

DROIT D'AUTEUR

Unité de la promotion et de la vente
Section d'édition
Agence internationale de l'énergie atomique
Centre international de Vienne
B.P. 100
1400 Vienne (Autriche)
Télécopie : +43 1 26007 22529
Téléphone : +43 1 2600 22417
Courriel : sales.publications@iaea.org
https://www.iaea.org/fr/publications

Imprimé par l'AIEA en Autriche
November 2022
STI/PUB/1918

SÉCURITÉ INFORMATIQUE POUR LA SÉCURITÉ NUCLÉAIRE
AIEA, VIENNE, 2022
STI/PUB/1918
ISBN 978-92-0-239521-3 (imprimé) 978-92-0-239621-0 (pdf)
ISSN 2520-6931

AVANT-PROPOS

de Rafael Mariano Grossi
Directeur général

La collection Sécurité nucléaire de l'AIEA fournit des orientations faisant l'objet d'un consensus international sur tous les aspects de la sécurité nucléaire, afin d'aider les États à honorer leurs responsabilités en la matière. L'AIEA établit et tient à jour ces orientations dans l'exercice de son rôle central d'assistance et de coordination internationales pour les questions de sécurité nucléaire.

Lancée en 2006, la collection Sécurité nucléaire est actualisée en permanence par l'AIEA, en coopération avec des experts des États Membres. En tant que Directeur général, je m'engage à faire en sorte que l'AIEA entretienne et améliore cet ensemble intégré, complet et cohérent de publications de qualité, conviviales et adaptées aux réalités de l'époque et aux besoins en matière de sécurité. La bonne application de ces orientations dans le cadre de l'utilisation de la science et de la technologie nucléaires devrait permettre d'atteindre un niveau élevé de sécurité nucléaire et établir la confiance nécessaire à l'utilisation continue de la technologie nucléaire pour le bien de tous.

La responsabilité de la sécurité nucléaire incombe aux pays. Les publications de la collection Sécurité nucléaire de l'AIEA complètent les instruments juridiques internationaux sur la sécurité nucléaire et servent de référence mondiale pour aider les parties à honorer leurs obligations. Bien qu'elles ne soient pas juridiquement contraignantes pour les États Membres, les orientations sur la sécurité sont largement appliquées. Elles sont devenues une référence indispensable et un dénominateur commun pour la grande majorité des États Membres qui les utilisent dans le cadre de leur réglementation nationale afin d'améliorer la sécurité nucléaire des centrales nucléaires, des réacteurs de recherche et des installations du cycle du combustible ainsi que des applications nucléaires en médecine, dans l'industrie, dans l'agriculture et dans la recherche.

Les orientations de la collection Sécurité nucléaire de l'AIEA sont fondées sur l'expérience pratique des États Membres et font l'objet d'un consensus international. La participation des membres du Comité des orientations sur la sécurité nucléaire et d'autres personnes est particulièrement importante, et je suis reconnaissant à tous ceux qui, par leurs connaissances et leurs compétences, contribuent à l'élaboration de ces orientations.

L'AIEA utilise également les orientations de la collection Sécurité nucléaire lorsqu'elle apporte une assistance aux États Membres dans le cadre de ses missions d'examen et de ses services consultatifs. Cela aide les États Membres à appliquer ces orientations et permet l'échange de données d'expérience et d'idées

utiles. Les informations en retour sur ces missions et services, ainsi que les enseignements tirés des événements et des expériences concernant l'utilisation et l'application des orientations sur la sécurité, sont pris en compte lors de la révision périodique de ces dernières.

Je suis convaincu que les orientations de la collection Sécurité nucléaire de l'AIEA et leur application contribuent de manière inestimable à assurer un niveau élevé de sécurité nucléaire dans le contexte de l'utilisation de la technologie nucléaire. J'encourage tous les États Membres à les promouvoir et à les appliquer et à collaborer avec l'AIEA pour en maintenir la qualité, aujourd'hui comme demain.

NOTE ÉDITORIALE

Les États ne sont pas tenus d'appliquer les orientations publiées dans la collection Sécurité nucléaire de l'AIEA, mais elles peuvent les aider à s'acquitter de leurs obligations en vertu d'instruments juridiques internationaux et assumer leurs responsabilités en matière de sécurité nucléaire au sein de l'État. Les orientations énoncées au conditionnel ont pour but de présenter des bonnes pratiques internationales et de manifester un consensus international selon lequel il est nécessaire pour les États de prendre les mesures recommandées ou des mesures équivalentes.

Les termes relatifs à la sécurité ont le sens donné dans la publication où ils figurent, ou dans les orientations de niveau supérieur que la publication soutient. Autrement, les termes ont le sens qui leur est communément donné.

Un appendice est réputé faire partie intégrante de la publication. Les informations données dans un appendice ont le même statut que le corps du texte. Les annexes ont pour objet de donner des exemples concrets ou des précisions ou explications. Elles ne sont pas considérées comme faisant partie intégrante du texte principal.

Bien que l'exactitude des informations contenues dans la présente publication ait fait l'objet d'un soin particulier, ni l'AIEA ni ses États Membres n'assument une quelconque responsabilité pour les conséquences éventuelles de leur utilisation.

L'emploi d'appellations particulières pour désigner des pays ou des territoires n'implique de la part de l'éditeur, l'AIEA, aucune prise de position quant au statut juridique de ces pays ou territoires, ou de leurs autorités et institutions, ni quant au tracé de leurs frontières.

La mention de noms de sociétés ou de produits particuliers (qu'ils soient ou non signalés comme marques déposées) n'implique aucune intention d'empiéter sur des droits de propriété et ne doit pas être considérée non plus comme valant approbation ou recommandation de la part de l'AIEA.

TABLE DES MATIÈRES

1. INTRODUCTION

GÉNÉRALITÉS

1.1. Les systèmes informatiques jouent un rôle essentiel dans tous les aspects de la sûreté et de la sécurité de l'exploitation des installations et de l'exécution des activités dans lesquelles des matières nucléaires ou d'autres matières radioactives sont utilisées, entreposées ou transportées, y compris le maintien de la protection physique, et dans les mesures qui sont appliquées pour détecter des matières non soumises à un contrôle réglementaire et intervenir en pareille situation. Ces systèmes informatiques doivent donc être protégés contre les actes criminels et les autres actes non autorisés délibérés. À mesure que les techniques progressent, le recours aux systèmes informatiques dans tous les aspects des activités, y compris la sûreté et la sécurité nucléaires, devrait s'accroître.

1.2. Les Fondements de la sécurité nucléaire [1] soulignent l'importance de la sécurité de l'information, notamment de la sécurité informatique, dans le cadre d'un régime de sécurité nucléaire, ainsi que la nécessité de mener des activités pour déterminer les problèmes et les facteurs qui sont susceptibles de nuire à la capacité d'assurer une sécurité nucléaire adéquate, y compris la sécurité informatique, et pour y remédier.

1.3. La sécurité des informations sensibles est un aspect de l'élément essentiel 3 d'un régime de sécurité nucléaire national. Selon la référence [1], « [l]e cadre législatif et réglementaire et les mesures administratives associées [...] [p]révoient la mise en place d'une réglementation et de dispositions pour la protection de la confidentialité des *informations sensibles* et des *ressources d'informations sensibles* ». Assurer la sécurité des informations sensibles et des ressources d'informations sensibles suppose de préserver la confidentialité, l'intégrité et la disponibilité de ces informations et de ces ressources. L'Amendement à la Convention sur la protection physique des matières nucléaires [2] fait de la préservation de la confidentialité des informations son principe fondamental L.

1.4. Selon le paragraphe 4.10 des Recommandations de sécurité nucléaire sur la protection physique des matières nucléaires et des installations nucléaires (INFCIRC/225/Révision 5) [3],

> « [l]es systèmes informatisés utilisés pour la protection physique, la sûreté nucléaire et la comptabilité et le contrôle des matières nucléaires devraient être protégés contre la compromission (cyberattaque, manipulation ou

falsification, par exemple) conformément à l'*évaluation de la menace* ou à la *menace de référence*. »

1.5. Les Recommandations de sécurité nucléaire relatives aux matières radioactives et aux installations associées [4] et sur les matières nucléaires et autres matières radioactives non soumises à un contrôle réglementaire [5] soulignent également la nécessité de prévenir tout accès non autorisé à des informations sensibles et de les préserver de toute compromission. Des propositions d'orientations de catégorie Recommandations, destinées à compléter les recommandations sur la sécurité informatique qui figurent dans les références [3] à [5] jusqu'à ce que ces publications soient révisées, sont présentées dans l'annexe I.

1.6. Lorsque des systèmes informatiques sont utilisés pour traiter, transmettre et stocker des informations sensibles sous forme numérique, la confidentialité, l'intégrité et la disponibilité de ces informations devraient être suffisamment protégées par l'application de mesures de sécurité informatique pendant toute la durée de vie des systèmes concernés. La sécurité informatique comprend les mesures nécessaires pour prévenir, détecter et contrer les cyberattaques commises contre les systèmes informatiques, et pour remettre en état ces systèmes.

1.7. Les menaces contre la sécurité nucléaire savent que les cyberattaques permettent de prendre pour cible des systèmes informatiques afin de commettre des actes malveillants ou de faciliter la commission de tels actes, directement ou conjointement avec des moyens plus classiques comme l'accès physique ou le recours à des initiés. De tels actes peuvent conduire à l'enlèvement non autorisé de matières nucléaires ou d'autres matières radioactives, ou à un sabotage, ce qui peut avoir des conséquences radiologiques inacceptables. Les cyberattaques peuvent également servir à faciliter la commission d'autres actes criminels ou d'autres actes non autorisés délibérés, comme le trafic illicite de matières nucléaires ou d'autres matières radioactives non soumises à un contrôle réglementaire.

1.8. Pour pouvoir faire face à toutes les menaces possibles contre la sécurité nucléaire, un régime de sécurité nucléaire doit prévoir les moyens nécessaires pour lutter contre les menaces qui ont acquis ou peuvent acquérir les compétences requises pour se livrer à des cyberattaques contre des systèmes informatiques. En outre, les menaces contre la sécurité nucléaire qui ne disposent pas de ces compétences peuvent persuader des personnes qui les maîtrisent de les aider (en les payant ou sous la contrainte, par exemple).

1.9. Le maintien d'une sécurité informatique efficace dans les installations où sont manipulées des matières nucléaires ou d'autres matières radioactives et

pour les activités associées comme le transport est un problème important, car la menace est réelle et évolue rapidement. Une grande partie des éléments essentiels du régime de sécurité nucléaire d'un État dépend de systèmes informatiques ou repose sur de tels systèmes ; ces éléments dépendent donc de l'efficacité de la sécurité informatique.

OBJET

1.10. La présente publication a pour objet de donner des orientations sur la conception et la mise en œuvre de la sécurité informatique comme élément à part entière de la sécurité nucléaire.

1.11. Le présent guide d'application est destiné aux décideurs, aux autorités compétentes, aux exploitants, aux expéditeurs, aux transporteurs et aux autres intervenants qui ont des responsabilités dans le domaine de la sécurité et de la sûreté nucléaires.

CHAMP D'APPLICATION

1.12. Les orientations qui figurent dans la présente publication s'appliquent aux aspects de la sécurité nucléaire qui concernent la sécurité informatique et à leur interface avec la sûreté nucléaire et d'autres éléments d'un régime de sécurité nucléaire national, comme la protection physique des matières nucléaires et des installations nucléaires, la sécurité des matières radioactives et des installations et activités associées, la détection des événements de sécurité nucléaire et les interventions lorsque de tels événements se produisent. Elles concernent les systèmes informatiques dont la compromission pourrait porter atteinte à la sécurité nucléaire ou à la sûreté nucléaire.

1.13. La présente publication porte sur les aspects généraux de la sécurité informatique qui s'appliquent à toutes les branches de la sécurité nucléaire, notamment la sécurité des matières nucléaires et des installations nucléaires, des matières radioactives et des installations associées, et des matières nucléaires et autres matières radioactives non soumises à un contrôle réglementaire. On trouvera des orientations plus détaillées sur la sécurité informatique dans les installations nucléaires, y compris des exemples ciblés de mise en œuvre technique de mesures de sécurité informatique et de la gestion des risques liés à la sécurité informatique dans le numéro 33-T de la collection Sécurité nucléaire de l'AIEA, intitulé « Computer Security of Instrumentation and Control Systems at Nuclear

Facilities » [6], et dans le numéro 17-T (Rev. 1) de la même collection, intitulé « Computer Security Techniques for Nuclear Facilities » [7].

1.14. La présente publication prend en compte les orientations relatives à la sécurité de l'information qui figurent dans les Fondements de la sécurité nucléaire [1] et dans les Recommandations de sécurité nucléaire [3–5], mais ne donne pas d'orientations détaillées sur cette question générale. Le numéro 23-G de la collection Sécurité nucléaire de l'AIEA, intitulé « Sécurité de l'information nucléaire » [8], donne des orientations sur la sécurité de l'information nucléaire et sur le recensement et la protection des informations sensibles et des ressources d'informations sensibles.

STRUCTURE

1.15. Après la présente introduction, la section 2 définit les notions et les termes essentiels. La section 3 expose le rôle et les responsabilités de l'État en matière de sécurité informatique dans le cadre du régime de sécurité nucléaire, et la section 4 porte sur le rôle et les responsabilités des entités concernées. La section 5 décrit les activités qui sont menées par l'État afin de mettre en place une stratégie de sécurité informatique pour la sécurité nucléaire et la section 6 présente les activités qui permettent de mettre en œuvre cette stratégie. La section 7 décrit les éléments et les mesures recommandées pour le programme de sécurité informatique (PSI[1]). La section 8 présente les activités qui permettent de maintenir la sécurité informatique. L'appendice contient des considérations techniques importantes sur l'interface avec la sûreté nucléaire.

1.16. L'annexe I contient des propositions d'orientations de catégorie Recommandations sur la sécurité informatique dans le cadre d'un régime de sécurité nucléaire national ; les orientations énoncées dans la présente publication sont compatibles avec ces propositions. Des exemples de mesures d'application possibles figurent dans les annexes II à IV, à l'appui des orientations décrites dans la présente publication. L'annexe II donne un aperçu des profils de cybermenace possibles. L'annexe III contient un exemple d'attribution des responsabilités relatives à la sécurité informatique dans le cadre du régime de

[1] Dans certaines organisations, le programme de sécurité informatique est appelé plan de sécurité informatique.

sécurité nucléaire et l'annexe IV présente un cadre de compétences possible pour la sécurité informatique.

2. NOTIONS ET CONTEXTE

TERMES ESSENTIELS

2.1. Les organismes d'un pays produisent, traitent, manipulent et stockent de nombreux types d'informations différents. Certaines de ces informations, comme les secrets militaires ou les données personnelles des individus, peuvent être jugées suffisamment sensibles pour qu'une protection particulière soit nécessaire. L'État peut instaurer des lois sur la sécurité de l'information qui définissent et classent les informations, et imposent des prescriptions particulières en matière de protection, notamment pour les données numériques et les systèmes informatiques associés. Les informations qui relèvent du régime de sécurité nucléaire de l'État sont soumises à ces prescriptions. Il peut être nécessaire de protéger d'autres informations ou d'assurer une protection supplémentaire pour certains types d'informations dont la compromission pourrait aider un adversaire à commettre un acte malveillant contre une installation ou une activité ou à perpétrer un autre acte non autorisé délibéré où entrent en jeu des matières nucléaires ou d'autres matières radioactives. Une information sensible est une information, sous quelque forme que ce soit, y compris les logiciels, dont la divulgation, la modification, l'altération, la destruction ou le refus d'utilisation non autorisés pourrait compromettre la sécurité nucléaire [1]. La figure 1 représente les ressources d'informations sensibles, les systèmes informatiques et les ressources numériques sensibles (RNS) et les relations qui existent entre ces différentes notions, qui sont définies ci-après.

2.2. Par « ressources d'informations sensibles » on entend [1] tout équipement ou composant utilisé pour entreposer, traiter, contrôler ou transmettre des informations sensibles. De telles informations peuvent être numériques ou stockées sous toute autre forme.

2.3. Les systèmes informatiques sont des dispositifs techniques qui produisent, traitent, calculent, communiquent ou stockent des données numériques, y donnent accès ou assurent, fournissent ou contrôlent des services qui utilisent de telles données. Ils peuvent comprendre des ordinateurs de bureau, des ordinateurs portables, des tablettes et d'autres ordinateurs personnels, des smartphones,

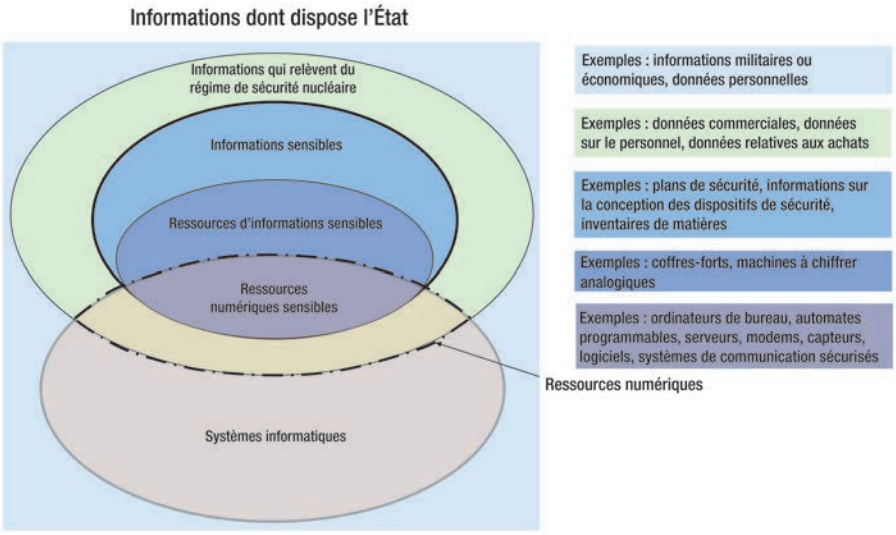

FIG. 1. Informations et systèmes informatiques dans l'État et le régime de sécurité nucléaire.

des ordinateurs centraux, des serveurs, des appareils de contrôle-commande numérique, des automates programmables, des imprimantes, des dispositifs réseau et des composants et des dispositifs embarqués. Ils peuvent aussi comprendre des services virtuels, comme l'informatique en nuage ou les machines virtuelles. Ces systèmes peuvent être constitués d'un composant unique ou de plusieurs ressources numériques.

2.4. Dans un État, les systèmes informatiques remplissent de nombreuses fonctions. Dans le cadre du régime de sécurité nucléaire, certains systèmes informatiques peuvent remplir des fonctions utiles pour les activités et les communications sans être sensibles sur le plan de la sécurité nucléaire. Ils ne sont donc pas concernés par les orientations qui figurent dans la présente publication.

2.5. Les ressources d'informations sensibles doivent être protégées afin qu'il ne soit pas porté atteinte à l'intégrité des informations sensibles qu'elles stockent, traitent, contrôlent ou transmettent. Les méthodes de protection dépendent du type de ressource concerné et de la forme que prennent les informations. La référence [8] porte principalement sur la protection des informations écrites sur papier et des autres informations conservées sous forme imprimée. Les ressources numériques sont les systèmes informatiques (ou les parties de ceux-ci) qui sont associés au régime de sécurité nucléaire d'un État ou qui en relèvent. L'expression « ressources numériques sensibles » (RNS) désigne les ressources d'informations

sensibles qui sont des systèmes informatiques (ou en font partie). Les RNS doivent être protégées par des mesures de sécurité informatique.

2.6. Les RNS sont utilisées dans des systèmes qui remplissent des fonctions de sûreté nucléaire, de sécurité nucléaire et de comptabilité et de contrôle des matières nucléaires, ou qui stockent et traitent des informations sensibles sur ces fonctions. Les RNS, et par conséquent les fonctions essentielles qu'elles remplissent, peuvent être exposées à des cyberattaques et être spécialement prises pour cible par des adversaires. Ce type d'attaque et la compromission d'une RNS peuvent porter atteinte à la sécurité et à la sûreté nucléaires. La compromission d'une RNS peut notamment contribuer ou mener à l'un des résultats suivants :

a) sabotage ayant des conséquences radiologiques inacceptables ou de graves conséquences radiologiques si des zones vitales sont touchées ;
b) enlèvement non autorisé de matières nucléaires ou d'autres matières radioactives ;
c) diminution des capacités à prévenir et détecter les événements de sécurité nucléaire, ainsi qu'à intervenir en pareil cas ;
d) perte ou altération d'informations sensibles, ou impossibilité d'y accéder.

2.7. Selon la situation, il peut être nécessaire de considérer les logiciels comme des informations, comme partie intégrante d'un système informatique ou les deux. Ainsi, en phase de conception, un logiciel peut être une expression de haut niveau d'un algorithme de traitement ; il est alors souhaitable de le considérer comme une information. Sous forme exécutable, un logiciel fait partie intégrante du système informatique associé, qui ne peut fonctionner sans lui, et la plupart des cyberattaques visent à exploiter les vulnérabilités des logiciels.

2.8. La sécurité informatique est une partie de la sécurité de l'information qui porte sur la protection des systèmes informatiques contre toute compromission. Elle s'applique à tous les systèmes interconnectés et à tous les réseaux dont ces systèmes font partie. Dans la présente publication, le terme cybersécurité est considéré comme un synonyme de sécurité informatique et n'est pas employé. Comme l'explique la référence [8], la sécurité informatique est une branche de la sécurité de l'information. Les objectifs, les méthodes et la terminologie de la sécurité de l'information et de la sécurité informatique sont souvent les mêmes.

2.9. Compte tenu de l'interconnectivité des réseaux informatiques et de la circulation de l'information, des mesures de sécurité informatique sont également nécessaires pour protéger les RNS contre les menaces qui utilisent d'autres ressources numériques et d'autres systèmes informatiques. Une approche

multidimensionnelle des mesures de sécurité graduée pour toutes les ressources numériques permet d'assurer une défense en profondeur contre les cyberattaques.

RECENSEMENT DES RESSOURCES NUMÉRIQUES SENSIBLES

2.10. Les détenteurs ou les concepteurs de systèmes informatiques devraient appliquer une procédure systématique pour recenser les fonctions remplies par leurs ressources numériques qui sont nécessaires pour la sécurité et la sûreté nucléaires, toutes les RNS associées et les effets possibles de la compromission d'une RNS sur la sécurité et la sûreté nucléaires. Dans ce cadre, ils devraient être conscients qu'un système informatique dépourvu de RNS peut quand même avoir un effet néfaste sur les RNS d'autres systèmes s'il est compromis ou infecté par un logiciel malveillant[2].

2.11. La sécurité informatique vise à préserver les caractéristiques que sont la confidentialité, l'intégrité et la disponibilité des informations sensibles contenues dans les RNS, et celles des RNS elles-mêmes. Les RNS et leurs informations sensibles contribuent à la bonne exécution des fonctions qui permettent de maintenir le régime de sécurité nucléaire. Selon les informations sensibles que contient une RNS et la fonction système remplie par chaque RNS, il faudrait prendre en considération les besoins de protection pour chacune de ces caractéristiques.

2.12. La première étape d'une procédure systématique devrait consister à recenser les fonctions qui prennent directement en compte un ou plusieurs aspects de la sécurité nucléaire (comme la protection physique, la comptabilité et le contrôle des matières nucléaires ou la gestion des informations sensibles) et de la sûreté nucléaire. Il faudrait ensuite recenser les systèmes informatiques et leurs ressources numériques qui contribuent à l'exécution de ces fonctions.

2.13. Il faudrait alors procéder à une analyse initiale des conséquences de la compromission des ressources numériques de ces systèmes afin de déterminer quelles ressources pourraient altérer les fonctions système nécessaires et porter ainsi atteinte à la sécurité nucléaire si elles étaient compromises par une cyberattaque. Les ressources numériques dont la compromission pourrait avoir des effets néfastes sont les RNS. La notion de RNS est illustrée sur la figure 2.

[2] L'expression « logiciel malveillant » désigne toute forme de code informatique qui est délibérément destiné à commettre un acte malveillant. Un tel logiciel peut par exemple être conçu pour faciliter le vol d'informations sensibles ou compromettre la conception d'un système informatique ou une fonction remplie par un système informatique.

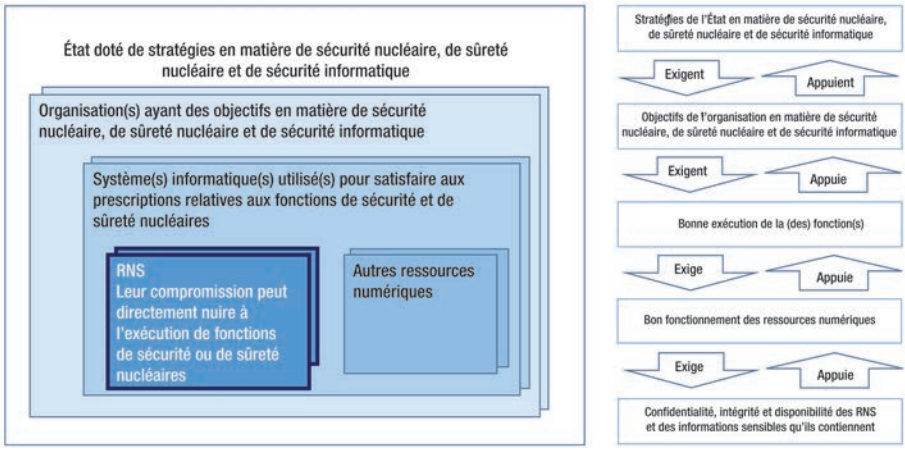

FIG. 2. Diagramme conceptuel d'une ressource numérique sensible (RNS) présente dans un système informatique d'une organisation.

Il faudrait procéder à l'analyse initiale sans tenir compte des mesures de sécurité informatique en vigueur, afin de déterminer quel serait le pire effet possible si les ressources numériques étaient compromises.

2.14. La procédure devrait également prévoir d'examiner les systèmes auxiliaires ou les appareils qui ne jouent pas un rôle direct dans les fonctions de sécurité nucléaire et de sûreté nucléaire afin de déterminer si des cyberattaques contre ces systèmes ou appareils pourraient directement ou indirectement altérer de telles fonctions. Il faudrait également examiner toutes les ressources numériques qui pourraient être connectées temporairement à une RNS afin de déterminer si elles appartiennent à cette catégorie. Ces systèmes sont par exemple les ordinateurs de maintenance et les appareils de mesure numériques.

2.15. Les organisations ont le choix entre plusieurs stratégies différentes pour la gestion des RNS. Elles peuvent les regrouper – par exemple, celles qui font partie du même système ou celles qui sont de nature similaire – et gérer collectivement toutes les RNS d'un même groupe. Un système informatique qui remplit une fonction importante peut donc être considéré comme une RNS unique ou comme un ensemble de RNS. De tels regroupements devraient contribuer à ce que les RNS dont la compromission pourrait avoir des conséquences similaires bénéficient d'un niveau de protection similaire. Une fois que les RNS ont été recensées et classées en fonction des conséquences que pourrait avoir leur compromission, il est possible d'adopter une approche graduée en appliquant le principe de la défense en profondeur.

2.16. Il faudrait définir les prescriptions à respecter pour préserver la confidentialité, l'intégrité et la disponibilité de chaque RNS en évaluant la contribution de chacune d'entre elles à la sécurité et à la sûreté nucléaires et les conséquences possibles de leur dysfonctionnement par suite d'une cyberattaque. À cette fin, il peut être nécessaire de faire appel à un expert en la matière, qui s'inspirera de différents principes et de procédures d'analyse.

2.17. Tant qu'un système informatique n'a pas été évalué pour déterminer s'il s'agit ou non d'une RNS (ou s'il contient des RNS), il devrait être considéré comme « indéterminé ». Par précaution, il faudrait généralement que les mesures de sécurité informatique à respecter pour les ressources indéterminées soient très strictes, car les conséquences possibles d'une cyberattaque sont inconnues. Il faudrait étudier s'il faut interdire ou limiter l'emploi de ces ressources dans le cadre du régime de sécurité nucléaire. Ainsi, l'utilisation d'appareils qui appartiennent au personnel, comme les téléphones portables ou les tablettes, peut être interdite dans les installations nucléaires et la connexion d'un ordinateur tiers à tout système d'une installation nucléaire peut être interdite tant que l'ordinateur concerné n'a pas été examiné en détail. La définition appropriée de la RNS, de son rôle, de ses limites et de ses interfaces, ainsi que du degré admissible de dépendance à l'égard d'autres ressources numériques, sont des aspects essentiels d'une conception sécurisée, qui exigent un avis d'expert fondé sur les principes de la sécurité informatique et de l'ingénierie des systèmes. Ainsi, en modifiant la conception générale d'un système pour transférer une fonctionnalité entre des RNS et d'autres ressources numériques, il est possible de simplifier la définition d'une RNS et les mesures de sécurité informatique correspondantes.

2.18. Si l'on utilise des RNS qui sont mises à disposition dans le cadre de services virtuels ou contractuels, comme l'informatique en nuage, il faudrait faire preuve d'une vigilance particulière, car ce type de services comprend des éléments qui ne sont pas directement sous le contrôle du propriétaire des données. Ainsi, une RNS qui est une application ou un service en nuage repose sur des logiciels et du matériel qui sont sous le contrôle du fournisseur d'informatique en nuage (par exemple pour du stockage en nuage). En pareil cas, il faudrait fixer des conditions contractuelles strictes sur des questions comme le contrôle des accès, la disponibilité, la séparation des données, la destruction des données, les interfaces, les logiciels, le matériel et les procédures d'administration afin que l'application soit correctement protégée contre l'accès et la manipulation non autorisés. Le fait de confier la fourniture de RNS à une autre organisation (autrement dit l'externalisation) ne décharge pas le propriétaire de processus ou l'exploitant de sa responsabilité de protéger les RNS concernées.

2.19. Les RNS peuvent comprendre des composants de systèmes de technologie de l'information et de systèmes de technologie opérationnelle. Pour ces composants, les mesures de sécurité informatique appropriées dépendent du type de système et de sa fonction. Cependant, il existe souvent des interfaces entre les systèmes de technologie de l'information et les systèmes de technologie opérationnelle, et il faudrait que l'ensemble des mesures de sécurité informatique qui sont appliquées pour chaque système tienne compte de ces interfaces.

2.20. Des procédures, généralement appelées « modèles de cycle de vie », sont appliquées pour garantir que les RNS sont conformes aux exigences particulières prévues pour elles. Le modèle de cycle de vie décrit les activités relatives à la mise au point, au fonctionnement, à la maintenance et au retrait d'une RNS, ainsi que les relations qui existent entre ces activités. La sécurité informatique doit être prise en compte à toutes les étapes du cycle de vie d'une RNS. Les installations, les fonctions, les systèmes, les composants, les RNS et les autres ressources numériques peuvent chacun avoir leur propre cycle de vie, qui ont des relations entre eux. Le cycle de vie théorique de la mise au point des systèmes qui a été défini pour les systèmes de contrôle-commande peut servir de référence pour le cycle de vie des systèmes informatiques, notamment les RNS, et devrait être pris en compte pour une installation pendant toute sa durée de vie utile.

CYBERATTAQUE

2.21. 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[3] des informations sensibles contenues dans une RNS ou de la RNS 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. Étroitement liées à cette notion, les attaques non ciblées consistent par exemple à introduire par erreur des programmes malveillants non guidés dans des systèmes informatiques et des réseaux. Ce type d'attaque peut aussi porter atteinte à la sécurité nucléaire.

[3] On suppose que la préservation d'autres caractéristiques, comme l'authentification ou la non-répudiation, fait partie de la protection de la confidentialité, de l'intégrité et de la disponibilité.

2.22. 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.

2.23. Les incidents de sécurité informatique qui sont provoqués par des cyberattaques peuvent être à l'origine d'autres incidents de sécurité informatique et, *in fine*, d'événements de sécurité nucléaire, directement ou dans le cadre d'une série d'agissements malveillants, qui peuvent comprendre d'autres cyberattaques ou un accès physique ou une utilisation non autorisés par des initiés, ou plusieurs de ces moyens (attaque combinée).

LA SÉCURITÉ INFORMATIQUE DANS LES DIFFÉRENTES BRANCHES DE LA SÉCURITÉ NUCLÉAIRE

2.24. Le régime de sécurité nucléaire couvre les trois domaines qui sont traités dans les références [3] à [5], et la sécurité informatique contribue à atteindre les objectifs relatifs à la sécurité nucléaire dans chacun de ces domaines. Le rôle de la sécurité informatique dans chacun d'entre eux est brièvement décrit dans les sections suivantes.

Matières nucléaires et installations nucléaires

2.25. La protection physique des matières nucléaires et des installations nucléaires dépend de l'application de mesures de sécurité destinées à [3] :

a) protéger contre un enlèvement non autorisé ;
b) localiser et récupérer des matières nucléaires manquantes ;
c) protéger contre le sabotage ;
d) atténuer ou réduire le plus possible les incidences d'un sabotage.

2.26. Les systèmes informatiques des installations nucléaires permettent d'assurer des fonctions de contrôle des processus, de sûreté nucléaire, de sécurité nucléaire et de comptabilité et de contrôle des matières nucléaires. Pour chacune de ces fonctions, des RNS qui peuvent être prises pour cible dans le cadre d'une attaque isolée ou lancée conjointement avec une attaque physique (attaque combinée, par exemple) sont utilisées. La sécurité informatique est nécessaire pour protéger ces systèmes informatiques contre les cyberattaques.

Matières radioactives et installations associées

2.27. Les matières radioactives sont utilisées dans le monde entier à des fins très diverses, bien souvent sans que des matières nucléaires entrent en jeu. Des systèmes informatiques sont de plus en plus fréquemment utilisés dans ce cadre pour la sûreté, la sécurité et le fonctionnement. Des mesures de sécurité, y compris des mesures de sécurité informatique, sont nécessaires pour empêcher l'accès non autorisé aux matières radioactives ou l'acquisition de telles matières pour un acte malveillant, ou le sabotage de ces matières et des installations associées.

2.28. Le cadre législatif et réglementaire devrait tenir compte du fait que le registre national des sources radioactives ou des matières radioactives contient généralement des informations sensibles qui doivent être protégées. Dans ce domaine, la sécurité informatique est nécessaire pour préserver la confidentialité, l'intégrité et la disponibilité des informations sensibles et des ressources d'informations sensibles, et notamment des RNS, pour contribuer par exemple à préserver la confidentialité et l'intégrité des registres de sources, ainsi que la disponibilité des données nécessaires pour intervenir en cas d'incident.

Matières nucléaires et autres matières radioactives non soumises à un contrôle réglementaire

2.29. Les matières non soumises à un contrôle réglementaire sont des matières nucléaires ou d'autres matières radioactives qui sont présentes en quantité suffisante pour être placées sous contrôle réglementaire, mais qui ne sont pas contrôlées, soit parce que le contrôle a été défaillant pour une raison quelconque, soit parce qu'il n'a jamais eu lieu. La sécurité des matières nucléaires et des autres matières radioactives non soumises à un contrôle réglementaire est assurée grâce à l'action coordonnée des autorités compétentes, qui exercent les fonctions qui leur sont attribuées : prévention et détection des événements de sécurité nucléaire et intervention si un tel événement se produit. De nombreux systèmes qui sont utilisés pour remplir ces fonctions sont des RNS ou bénéficient de l'appui de RNS.

2.30. La sécurité informatique est nécessaire dans ce domaine, notamment pour préserver la confidentialité des informations sensibles, l'intégrité des systèmes de détection, la confidentialité, l'intégrité et la disponibilité des systèmes de transmission de données, ainsi que la disponibilité des dispositifs d'appui en cas d'intervention, comme les télécommunications ou la criminalistique nucléaire.

MENACES, VULNÉRABILITÉS ET MESURES DE SÉCURITÉ INFORMATIQUE

Menaces

2.31. Une menace est une personne ou un groupe de personnes ayant la motivation, l'intention et la capacité de commettre un acte malveillant. Tout individu qui commet ou tente de commettre un acte malveillant est un adversaire.

2.32. La connaissance des menaces et des risques associés à de possibles cyberattaques est indispensable pour l'élaboration de mesures de sécurité informatique dans le cadre de la sécurité nucléaire. Il s'agit notamment de savoir quels pourraient être la motivation, les intentions, les moyens et les tactiques d'une menace contre la sécurité nucléaire lors de la préparation et du lancement d'une cyberattaque. L'annexe II donne quelques exemples des caractéristiques générales des menaces contre la sécurité nucléaire qui pourraient mener des cyberattaques.

Vulnérabilités

2.33. Les vulnérabilités d'un système informatique ou d'un réseau informatique sont les caractéristiques opérationnelles qui exposent le système concerné à un risque d'exploitation ou à une menace donnée. Ces failles peuvent être de nature administrative, physique ou technique. En exploitant des vulnérabilités, un adversaire peut accéder sans autorisation à une RNS ou la contrôler. Les conséquences de l'exploitation d'une vulnérabilité d'une RNS peuvent aller de négligeable à élevé en fonction du risque qu'elles puissent perturber l'utilisation de la RNS et sa fonction.

2.34. Le matériel et les logiciels des systèmes informatiques sont de plus en plus complexes, et le nombre de systèmes informatiques et leur degré d'interconnectivité augmentent continuellement. Cette complexité rend plus difficile le maintien de la connaissance complète des systèmes, et donc le maintien des compétences requises pour la gestion de la sécurité. Le nombre de vulnérabilités d'un système dépend de la complexité de celui-ci. Un système ne devrait donc pas être plus complexe que ne l'exige la fonction qui lui est assignée.

2.35. L'exploitation de vulnérabilités découvertes récemment permet la réussite de nombreuses cyberattaques. Ainsi, une « attaque du jour zéro » est une situation dans laquelle un adversaire exploite une vulnérabilité que le défenseur ne connaît pas. En outre, du fait de l'évolution rapide des nouvelles technologies informatiques, la nature des vulnérabilités peut changer et des catégories

complètement nouvelles de vulnérabilités peuvent apparaître seulement après que ces technologies ont été adoptées et utilisées concrètement.

2.36. Vu la complexité de certains systèmes informatiques et la possibilité qu'ils présentent des vulnérabilités cachées, les mesures de sécurité informatique en vigueur peuvent être insuffisantes pour réduire le risque à un niveau satisfaisant pour une utilisation dans certaines applications de sécurité et de sûreté nucléaires. Lorsque ces mesures ne permettent pas de réduire le risque à un niveau satisfaisant, il faudrait envisager d'autres méthodes (conception ou répartition des fonctions différentes, par exemple).

Approche graduée et défense en profondeur pour la sécurité informatique

2.37. Les mesures de sécurité informatique peuvent être de nature technique, physique ou administrative, ou appartenir à plusieurs de ces catégories. Un ensemble de mesures de contrôle devrait être adopté à l'aide d'une approche fondée sur les risques qui repose sur une approche graduée et sur la défense en profondeur afin d'assurer une sécurité informatique satisfaisante. Les mesures de sécurité informatique particulières qui sont mises en œuvre peuvent être une combinaison de certaines mesures prescrites dans des orientations de haut niveau ou dans des prescriptions édictées par l'État, et d'autres mesures définies par un exploitant dans le cadre de sa propre procédure fondée sur les risques.

2.38. Les niveaux de sécurité informatique permettent de connaître l'ampleur et la rigueur des mécanismes de sécurité jugés nécessaires pour différentes RNS. Selon une approche graduée, il faudra une série de mesures de protection différentes pour chaque niveau afin de satisfaire aux prescriptions de sécurité du niveau concerné. Des prescriptions plus rigoureuses sont appliquées pour les RNS les plus critiques. Ce concept est illustré sur la figure 3.

2.39. Un des moyens concrets de mise en œuvre d'une approche graduée consiste à regrouper les systèmes informatiques et les RNS associées en zones de sécurité informatique, des mesures de sécurité informatique graduées étant appliquées pour chaque zone en fonction des exigences de protection (c'est-à-dire du niveau de sécurité). Des niveaux de sécurité informatique sont ensuite attribués à chaque zone en fonction des effets possibles d'une cyberattaque sur les fonctions, les systèmes et les RNS de la zone concernée.

2.40. Le recours aux niveaux de sécurité informatique, qui sont présentés sur la figure 3, est une approche graduée qui suppose de définir des exigences de sécurité informatique proportionnées aux conséquences possibles d'une

cyberattaque réussie. Les considérations suivantes peuvent guider l'application de cette méthode :

a) Des exigences plus contraignantes sont appliquées pour les RNS dont la compromission peut avoir les conséquences les plus graves, notamment les événements de sécurité nucléaire les plus importants.
b) Des exigences de faible niveau sont appliquées pour les systèmes informatiques qui remplissent des fonctions de sécurité nucléaire, mais qui ne sont pas considérés comme des RNS.
c) Des exigences générales sont appliquées pour tous les niveaux de sécurité et tous les systèmes informatiques qui remplissent des fonctions qui ont un rapport avec la sécurité nucléaire, et peuvent prendre la forme de mesures de sécurité informatique identiques à celles qui sont mises en œuvre pour les systèmes informatiques d'autres zones.

2.41. Des mesures de sécurité informatique sont également nécessaires pour les systèmes informatiques qui ne sont pas considérés comme des RNS. Compte tenu de l'interconnectivité des réseaux informatiques et de la circulation de l'information, une approche multidimensionnelle des exigences de sécurité informatique graduées pour tous ces systèmes est requise pour assurer une défense en profondeur contre les cyberattaques. Dans l'exemple présenté plus haut, les systèmes informatiques qui se trouvent dans une zone où les exigences sont de niveau 4 ou 5 ne seront probablement pas classés comme RNS, mais des mesures de protection s'appliqueront aux systèmes de ces zones pour offrir des couches de protection contre l'intrusion et la compromission des RNS situées dans les zones où le niveau est plus élevé.

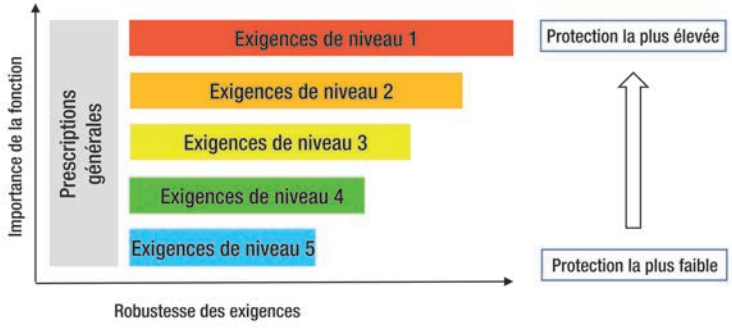

FIG. 3. L'approche graduée, illustrée par la notion de niveau de sécurité informatique.

2.42. En matière de sécurité informatique, la défense en profondeur consiste à mettre en place plusieurs couches défensives de mesures de sécurité informatique qui devraient être neutralisées ou contournées pour qu'une cyberattaque puisse progresser et porter atteinte à une RNS. L'association adéquate de mesures de sécurité informatique qui sont complémentaires ou se chevauchent permet d'assurer une défense en profondeur. Celle-ci est obtenue non seulement par la mise en place de plusieurs couches défensives, mais aussi par l'application de mesures de sécurité informatique qui permettent de prévenir et détecter une attaque contre une RNS et de protéger celle-ci, d'intervenir, d'atténuer les conséquences de l'attaque et de faciliter la remise en état de la ressource. Par exemple, si la prévention échoue (violation d'une règle qui interdit l'utilisation de supports de stockage amovibles, par exemple) ou si les mécanismes de protection sont contournés (par un nouveau virus qui n'est pas reconnu comme une cyberattaque, par exemple), il existe encore des mécanismes permettant de détecter toute altération non autorisée d'une RNS touchée et d'intervenir.

2.43. Pour qu'une défense en profondeur soit efficace, il faudrait également que, grâce à la conception, aucune défaillance unique d'une mesure de sécurité informatique d'une couche ne puisse rendre plus d'une couche inactive ou inefficace. L'exploitation d'une vulnérabilité critique d'un dispositif de protection fréquemment déployé peut par exemple permettre de contourner plusieurs couches de défense si la défense en profondeur ne prévoit pas différents dispositifs, différentes configurations ou d'autres mesures différentes. Il faudrait gérer la diversité des mesures de sécurité informatique de manière à parvenir à un équilibre entre la défense en profondeur mise en place et la complexité du système.

2.44. La défense en profondeur peut être assurée pour la conception d'un système composé de zones dont les niveaux de sécurité informatique diffèrent et qui sont souvent représentées sous forme d'anneaux concentriques. Un des principes généraux à respecter est qu'il ne devrait y avoir de connexions directes qu'entre des zones de sécurité informatique adjacentes.

2.45. Il est également possible de contribuer à l'efficacité de la défense en profondeur en veillant à ce que différentes parties de l'organisme exploitant aient des attributions complémentaires en matière de sécurité informatique, avec une réelle séparation des tâches, de telle sorte que toute erreur commise par une personne puisse être détectée par une autre personne et corrigée.

2.46. Le recensement des menaces et des vulnérabilités et l'évaluation du risque permettent d'établir un cadre fondé sur le risque pour l'élaboration de mesures de sécurité proportionnées. Dans ce contexte, le risque est l'éventualité que

des menaces contre la sécurité nucléaire qui exploitent des vulnérabilités aient des effets néfastes sur des RNS, et donc sur la sécurité et la sûreté nucléaires. Il dépend par conséquent de la probabilité d'une attaque et de la gravité de ses conséquences. La relation entre ces termes est illustrée sur la figure 4 et peut être expliquée comme suit dans le contexte de la sécurité informatique :

a) Dans le cadre du régime de sécurité nucléaire, les détenteurs de systèmes informatiques s'attachent à éviter les événements de sécurité nucléaire et donc à réduire au minimum les risques que des incidents de sécurité informatique pouvant contribuer à déclencher des événements de sécurité nucléaire se produisent.
b) Les menaces contre la sécurité nucléaire peuvent souhaiter déclencher des événements de sécurité nucléaire et prendre des RNS pour cible afin de les compromettre ou de les saboter.
c) Les menaces contre la sécurité nucléaire peuvent donc se lancer dans une activité qui consiste à exploiter des vulnérabilités, ce qui pose des risques liés à la sécurité informatique pour les RNS ; si ces risques se matérialisent, des événements de sécurité nucléaire peuvent se produire.
d) Les détenteurs des systèmes imposent des mesures de sécurité informatique pour réduire les risques liés à la sécurité informatique qui pèsent sur les RNS.
e) Lorsque des mesures de sécurité informatique appropriées sont définies, la probabilité que certains incidents de sécurité informatique se produisent peut être étudiée dans le cadre d'une approche fondée sur les risques. Il est possible de réduire les risques en éliminant la menace, en imposant des mesures de sécurité informatique visant à diminuer la probabilité qu'une attaque provoque un incident de sécurité informatique, ou en limitant ou en atténuant les conséquences d'un tel incident.
f) Le recensement et la gestion des risques devraient être des processus continus, qui tiennent compte de l'évolution des facteurs de risque.

Responsabilités relatives à la sécurité informatique dans un régime de sécurité nucléaire

2.47. Dans le cadre d'un régime de sécurité nucléaire, de nombreuses organisations utilisent des systèmes informatiques pour des fonctions comme le traitement de l'information, la sécurité nucléaire, la sûreté nucléaire ou la comptabilité et le contrôle des matières nucléaires.

2.48. La protection des informations sensibles qui sont stockées dans de tels systèmes et des RNS associées incombe à chacune de ces organisations.

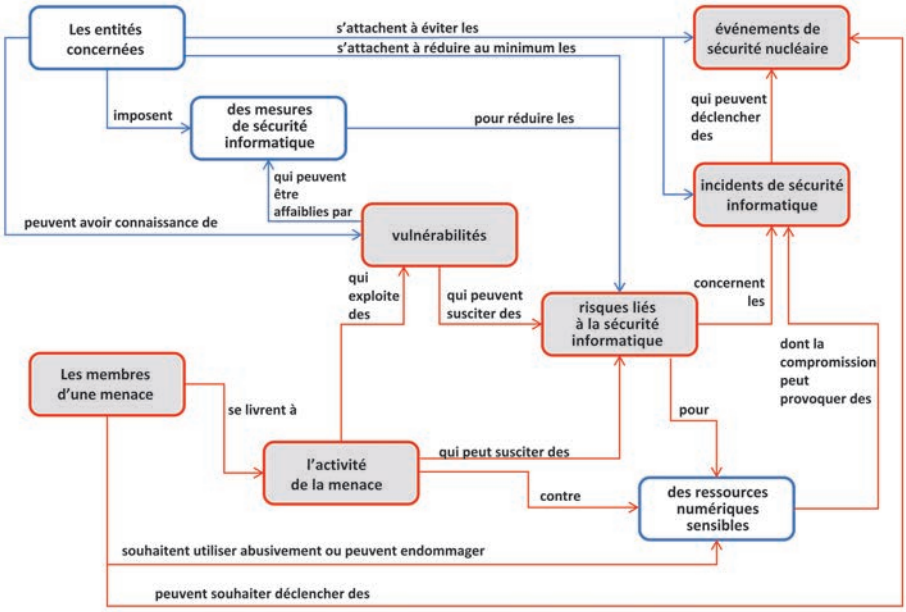

FIG. 4. Approche fondée sur les risques pour les mesures de sécurité informatique (adapté de la norme ISO/IEC 27005:2018) [9].

2.49. Les organisations qui peuvent avoir des responsabilités relatives à la sécurité informatique dans le cadre d'un régime de sécurité nucléaire sont représentées sur la figure 5. Il s'agit notamment des autorités compétentes[4] et des exploitants[5], qui se voient confier de telles responsabilités conformément aux prescriptions juridiques et réglementaires nationales dans le cadre du régime de sécurité nucléaire.

[4] Les autorités compétentes comprennent aussi les services de police, les services de secours, les services de protection des frontières et les forces armées qui jouent un rôle dans la protection des installations et des activités, dans la détection des incidents où entrent en jeu des matières nucléaires ou d'autres matières radioactives non soumises à un contrôle réglementaire et dans les interventions qui ont lieu si un tel événement se produit.

[5] Dans la présente publication, le terme « exploitants » désigne l'ensemble des entités qui sont titulaires d'une licence dans le cadre d'un régime de sécurité nucléaire, notamment les exploitants d'installations où entrent en jeu des matières nucléaires ou d'autres matières radioactives, ceux qui mènent des activités connexes, les expéditeurs et les transporteurs.

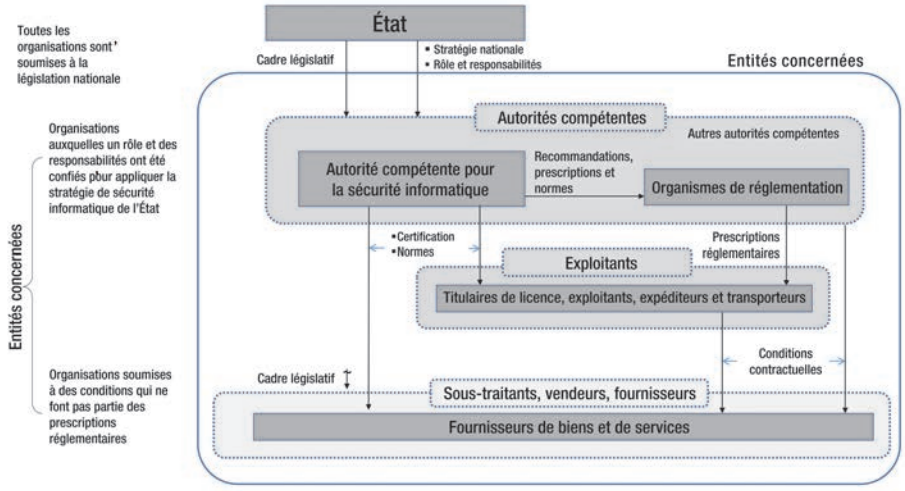

FIG. 5. Organisations ayant des responsabilités relatives à la sécurité informatique dans le cadre d'un régime de sécurité nucléaire.

2.50. L'État peut avoir une (des) autorité(s) compétente(s) désignée(s) pour la sécurité informatique, qui peut (peuvent) être distincte(s) des autorités compétentes ayant des responsabilités dans le domaine de la sécurité nucléaire. En outre, les autorités compétentes peuvent être soumises à des prescriptions de sécurité informatique imposées par des prescriptions juridiques nationales et par des normes qui ne font pas partie du régime de sécurité nucléaire.

2.51. Les vendeurs, les sous-traitants et les fournisseurs sont les organisations qui fournissent des biens et des services aux autorités compétentes et aux exploitants, mais dont les responsabilités relatives à la sécurité informatique (protection des informations sensibles et des RNS associées, par exemple) peuvent découler de conditions fixées dans les contrats qu'ils ont conclus avec les autorités compétentes et les exploitants, et non de prescriptions juridiques et réglementaires nationales.

2.52. Le rôle et les responsabilités de l'État, des autorités compétentes, des exploitants, des vendeurs, des sous-traitants et des fournisseurs en matière de sécurité informatique sont présentés en détail dans les sections 3 et 4.

COMPÉTENCES ET MOYENS EN SÉCURITÉ INFORMATIQUE

2.53. Une sécurité informatique efficace et robuste est mise en place, maintenue et pérennisée par un personnel compétent et habilité, l'encadrement étant efficace et la direction bien informée et active. Chaque organisation qui est soumise au régime de sécurité nucléaire devrait acquérir et maintenir des compétences et des moyens dans le domaine de la sécurité informatique, en fonction de ses responsabilités et de son rôle particuliers.

3. RÔLE ET RESPONSABILITÉS DE L'ÉTAT

3.1. Dans le cadre de son régime de sécurité nucléaire, l'État devrait élaborer et pérenniser une stratégie nationale de sécurité informatique (appelée « la stratégie » dans la suite de la présente publication). Il devrait désigner une autorité compétente, à laquelle l'élaboration de la stratégie incomberait en premier lieu.

CONSIDÉRATIONS D'ORDRE LÉGISLATIF ET RÉGLEMENTAIRE

3.2. L'État devrait veiller à ce que la sécurité informatique soit dûment prise en compte par une législation et une réglementation qui s'appliquent au régime de sécurité nucléaire et sont compatibles avec celui-ci. Il devrait intégrer dans sa législation nationale des prescriptions appropriées pour la sécurité informatique, de sorte que celle-ci soit correctement assurée dans le cadre de la sécurité nucléaire.

3.3. L'État devrait veiller à ce que sa législation incrimine les cyberattaques contre les systèmes informatiques qui relèvent du régime de sécurité nucléaire. En matière de sécurité informatique, des dispositions législatives particulières peuvent être nécessaires pour tenir compte des spécificités de certaines infractions et des modes opératoires employés pour mener une cyberattaque.

3.4. L'État devrait veiller à ce que le cadre législatif ou réglementaire prévoie des sanctions si un acte non autorisé criminel ou délibéré qui est commis contre une RNS peut compromettre la sécurité nucléaire.

3.5. L'État devrait examiner d'autres législations et des instruments juridiques internationaux (conventions, par exemple) pour faciliter l'élaboration des

dispositions relatives à la sécurité informatique et leur mise en œuvre pour la sécurité nucléaire. Ces textes peuvent notamment être les suivants :

a) lois sur les délits informatiques ;
b) lois sur le terrorisme ;
c) lois sur la protection des infrastructures nationales critiques ;
d) lois qui imposent de communiquer des informations ;
e) lois relatives au respect de la vie privée et au traitement des données personnelles ;
f) instruments internationaux (conventions, par exemple) applicables à la cybercriminalité.

3.6. L'État devrait réexaminer et actualiser son cadre législatif et réglementaire régulièrement afin d'y intégrer des dispositions concernant les cybermenaces et les vulnérabilités nouvelles ou émergentes.

3.7. L'État devrait désigner une autorité compétente principale pour la sécurité informatique[6], qui serait chargée de surveiller l'application de la législation et de la réglementation relatives à la sécurité informatique et de les faire respecter dans le cadre du régime de sécurité nucléaire (cette autorité est appelée « autorité compétente pour la sécurité informatique » dans la suite de la présente publication).

3.8. En matière de sécurité informatique, l'État peut décider de mettre en place un cadre législatif et réglementaire qui ne se limite pas au régime de sécurité nucléaire, et le champ d'application de certaines lois et de certains règlements peut aller au-delà du régime de sécurité nucléaire. L'autorité compétente pour la sécurité informatique devrait alors s'assurer que le cadre est suffisant pour la sécurité nucléaire et, s'il ne l'est pas, l'État devrait élargir ce cadre par toutes les prescriptions nécessaires de manière cohérente par rapport au régime de sécurité nucléaire.

3.9. L'État devrait veiller à ce que les autorités compétentes disposent de moyens financiers, humains et techniques suffisants pour exercer les responsabilités qui concernent l'interprétation et l'exécution satisfaisantes de leurs obligations

[6] Un État peut confier cette responsabilité à différentes autorités dans des contextes différents. Ainsi, l'autorité compétente qui est chargée de la sécurité informatique dans les installations nucléaires et celle qui est responsable de la sécurité informatique dans le milieu médical ou pour la surveillance aux frontières ne sont pas nécessairement les mêmes. Dans la présente publication, l'expression « autorité compétente » est employée pour désigner toute autorité de ce type qui a une responsabilité dans un contexte particulier.

juridiques relatives à la sécurité informatique dans le cadre du régime de sécurité nucléaire national.

AUTORITÉ COMPÉTENTE POUR LA SÉCURITÉ INFORMATIQUE DANS LE CADRE DU RÉGIME DE SÉCURITÉ NUCLÉAIRE

3.10. Selon les modalités d'organisation retenues par l'État, l'autorité compétente pour la sécurité informatique dans le cadre du régime de sécurité nucléaire peut être ou non l'organisme de réglementation de la sécurité nucléaire. De même, les responsabilités relatives à la sécurité informatique dans l'État peuvent être réparties entre plusieurs organisations, mais l'État devrait confier la responsabilité de la sécurité informatique à une seule autorité compétente pour chaque branche du régime de sécurité nucléaire. Ainsi, l'autorité compétente pour la sécurité informatique dans les centrales nucléaires et celle qui est compétente pour la sécurité informatique dans le cadre de la surveillance aux frontières ne sont pas nécessairement les mêmes.

3.11. Lorsqu'il existe plusieurs autorités compétentes pour la sécurité informatique dans le cadre du régime de sécurité nucléaire, ou lorsque l'autorité concernée n'est pas l'autorité compétente pour la sécurité nucléaire, l'État devrait créer et pérenniser un organisme ou un mécanisme de coordination approprié afin que la responsabilité relative à chaque aspect de la sécurité nucléaire soit clairement définie pour toutes les autorités compétentes.

3.12. L'État devrait recenser toutes les autorités compétentes[7] et tous les exploitants qui ont un rôle et des responsabilités en matière de sécurité informatique dans le cadre du régime de sécurité nucléaire, et s'assurer que l'autorité compétente pour la sécurité informatique dans ce cadre exerce un contrôle sur chacune des organisations répertoriées.

3.13. L'État devrait imposer aux autorités compétentes et aux exploitants recensés d'élaborer et d'appliquer des PSI conformément à la stratégie.

3.14. L'État devrait définir les responsabilités relatives à la sécurité informatique et les assigner à toutes les entités qui relèvent du régime de sécurité nucléaire.

---

[7] Les autorités compétentes à prendre en compte comprennent, s'il y a lieu, tous les organismes ou mécanismes de coordination, les forces de l'ordre, les douanes et la police des frontières, les services de renseignement et de sécurité, les services de santé et les agences de l'environnement.

3.15. L'annexe III contient un exemple de liste de responsabilités relatives à la sécurité nucléaire à partir de laquelle des responsabilités pour la sécurité informatique peuvent être déduites, en fonction de la nature du régime de sécurité nucléaire d'un État et de ses RNS.

3.16. Dans certains cas, des organisations qui fournissent un appui ne relèvent pas des organismes de réglementation de l'État, mais jouent un rôle essentiel dans la réalisation des objectifs relatifs à la sécurité nucléaire en matière de sécurité informatique. Pour ce type d'organisation, les responsabilités et les exigences de sécurité informatique peuvent être définies dans des contrats, comme pour les contrats qui sont conclus avec les vendeurs, les sous-traitants et les fournisseurs. L'État peut imposer des prescriptions de sécurité informatique (qui concernent par exemple la conception, le fonctionnement et la formation du personnel) pour certains systèmes informatiques et à des vendeurs, des sous-traitants et des fournisseurs qui sont soumis au régime de sécurité nucléaire, conformément à la stratégie.

INTERFACES AVEC D'AUTRES DOMAINES

3.17. L'État devrait veiller à ce que les interfaces entre la sécurité informatique et d'autres domaines fonctionnent correctement. À cette fin, une action de l'État qui ne concerne pas la sécurité informatique peut être nécessaire (imposer des prescriptions dans les autres domaines, par exemple).

3.18. L'État devrait veiller à ce que la stratégie définisse les interfaces entre la sécurité informatique et tous les autres domaines concernés afin que les différentes autorités compétentes et les exploitants connaissent leur rôle et leurs responsabilités en la matière.

Sûreté nucléaire

3.19. La sécurité et la sûreté nucléaires ont toutes deux pour but de protéger les personnes, les biens, la société et l'environnement. Les mesures de sécurité et de sûreté doivent être conçues et appliquées de manière intégrée afin de créer une synergie entre ces deux domaines et de façon telle que les mesures de sécurité ne compromettent pas la sûreté et que les mesures de sûreté ne compromettent pas la sécurité [1].

3.20. La sécurité informatique joue un rôle important dans l'interface entre la sécurité nucléaire et la sûreté nucléaire, surtout au vu du recours grandissant

aux systèmes informatiques dans tous les aspects de l'exploitation des installations nucléaires.

3.21. L'État devrait prendre en compte la réglementation relative à la sécurité nucléaire et à la sûreté nucléaire lorsqu'il élabore la réglementation pour la sécurité informatique et devrait veiller à ce que ces réglementations soit appliquées de manière cohérente.

3.22. La bonne exécution d'une fonction de sûreté nucléaire qui repose sur un système informatique ou pour laquelle un tel système fournit un appui dépend de l'intégrité et de la disponibilité des informations correspondantes (y compris les logiciels), et parfois du maintien de la confidentialité de ces informations. La sécurité informatique devrait donc faire partie intégrante des processus de gestion du cycle de vie des systèmes informatiques qui sont utilisés pour la sûreté nucléaire, afin que les prescriptions de sécurité informatique et de sûreté nucléaire soient prises en considération conjointement.

3.23. Il devrait y avoir une relation cohérente et rationnelle entre les classes de sûreté et les niveaux de sécurité informatique qui sont attribués aux ressources numériques, afin qu'une ressource numérique appartenant à une certaine classe de sûreté soit correctement protégée sur le plan de la sécurité informatique, mais il n'y a pas nécessairement d'équivalence simple entre les classes de sûreté et les niveaux de sécurité informatique. En outre, certaines ressources numériques qui ne sont pas formellement classées de sûreté peuvent cependant être non négligeables pour la sûreté du point de vue de la sécurité, et donc être des RNS. Le choix du niveau de sécurité informatique approprié dépend de la fonction système et des ressources numériques particulières qui sont utilisées dans le système et par l'organisation. Ce choix ne peut se faire qu'avec des compétences et des moyens appropriés, à l'aide d'un avis fondé sur des principes reconnus.

3.24. L'application des mesures de sécurité informatique ne devrait pas nuire à la performance, à l'efficacité, à la fiabilité et à l'exécution des fonctions de sûreté nucléaire.

3.25. L'appendice présente d'autres points que l'État peut prendre en considération lorsqu'il analyse les interfaces avec la sûreté nucléaire.

Protection physique

3.26. Les systèmes de protection physique, par exemple les systèmes qui assurent un contrôle des accès physiques, la surveillance de la sécurité, la détection

d'incidents de sécurité et des fonctions d'alarme et d'intervention, utilisent souvent des systèmes informatiques. La compromission malveillante de ces systèmes informatiques (c'est-à-dire la compromission de la confidentialité, de l'intégrité ou de la disponibilité des informations qu'ils contiennent) peut dégrader le fonctionnement d'un système de protection physique et faciliter des actions physiques commises en vue d'un enlèvement non autorisé de matières ou d'un sabotage. La sécurité informatique devrait faire partie intégrante des processus de gestion du cycle de vie des systèmes informatiques qui sont utilisés pour les fonctions ou les systèmes de protection physique.

3.27. Les systèmes de protection physique, par exemple ceux qui assurent un contrôle des accès physiques, peuvent aussi jouer un rôle utile pour la sécurité informatique, et leur utilisation devrait être envisagée pour la protection des systèmes informatiques.

3.28. Certains États peuvent considérer que la sécurité informatique fait partie de la protection physique, telle qu'elle est décrite dans la référence [3]. Dans la présente publication, la sécurité informatique est traitée comme un domaine indépendant, distinct de la protection physique, afin de faire apparaître et de souligner les différences entre les deux sujets. La nature de l'interface avec la protection physique dépend de la situation propre à chaque État.

3.29. L'application des mesures de sécurité informatique ne devrait pas nuire à la performance, à l'efficacité, à la fiabilité et à l'exécution des fonctions des systèmes de protection physique.

Fonctions relatives aux technologies de l'information et aux technologies opérationnelles

3.30. Les responsabilités relatives à la gestion et à la sécurité des systèmes de technologie de l'information et des technologies opérationnelles (notamment les systèmes de contrôle industriel et de contrôle-commande) sont souvent réparties entre plusieurs départements au sein d'une organisation. Des relations et une collaboration efficaces entre ces départements sont indispensables pour que la sécurité soit sans faille. Lors de cyberattaques, des systèmes de technologie de l'information ont été utilisés à la fois pour la reconnaissance et comme moyen d'attaque contre des technologies opérationnelles.

3.31. Les procédures, la terminologie et l'évaluation du risque peuvent ne pas être identiques pour les personnes qui sont responsables des systèmes de technologie de l'information et pour celles qui s'occupent des technologies opérationnelles.

Une collaboration efficace entre ces personnes est indispensable pour éviter les malentendus et une application incohérente des mesures de sécurité informatique.

Services de renseignement

3.32. L'État devrait veiller à ce que les services de renseignement apportent un appui approprié pour contribuer à effectuer une évaluation nationale de la menace précise et actualisée, qui tient compte du risque de cyberattaque contre le régime de sécurité nucléaire, ou pour tenir à jour cette évaluation. S'il y a lieu, il faudrait mettre en place des protocoles et des procédures pour faciliter les transferts d'informations sur les cybermenaces aux entités concernées qui sont soumises au régime de sécurité nucléaire afin d'assurer une sécurité informatique adéquate face à des menaces évolutives.

3.33. L'État devrait veiller à ce que les services de renseignement connaissent le rôle de la sécurité informatique dans le régime de sécurité nucléaire, et notamment les types de RNS qui peuvent exister et leur importance.

Organismes d'intervention

3.34. L'État devrait veiller à ce que des systèmes et des mesures de sécurité nucléaire soient mis en place par toutes les autorités compétentes et par tous les exploitants afin de détecter et d'évaluer les incidents de sécurité informatique qui ont ou sont susceptibles d'avoir des conséquences générales pour la sécurité nucléaire, et à ce que les autorités compétentes concernées soient prévenues si un tel incident se produit, afin qu'une intervention appropriée puisse être déclenchée.

3.35. Les plans d'intervention spécialisés devraient prévoir des instructions concernant les interventions face à une cyberattaque ou à une attaque combinée.

Aide et coopération internationales (y compris les échanges d'informations)

3.36. Les États sont encouragés à coopérer les uns avec les autres et avec les organisations internationales, s'il y a lieu, afin de protéger les RNS et les informations sensibles correspondantes et de détecter les menaces de cyberattaque, surtout les menaces vraisemblables de sabotage de matières nucléaires ou d'une installation nucléaire (par exemple en appliquant le paragraphe 3 de l'article 5 de la Convention sur la protection physique des matières nucléaires, telle qu'amendée [2]). Il est possible d'instaurer la confiance et d'améliorer la sécurité informatique par l'échange et l'analyse rapides d'informations sur

les vulnérabilités, les menaces et les incidents de sécurité informatique. La confidentialité de ces informations devrait être dûment préservée.

3.37. L'État devrait mettre en place des mécanismes d'échanges d'informations sécurisés et contrôlés afin de coordonner toute intervention faisant suite à une cyberattaque contre le régime de sécurité nucléaire national. La coopération et l'assistance internationales sont souhaitables afin de faciliter les enquêtes sur les cyberattaques et les poursuites contre leurs auteurs.

3.38. L'État est encouragé à avoir régulièrement recours à des services de conseil ou d'évaluation afin d'évaluer la stratégie, les PSI et leur application dans le cadre du régime de sécurité nucléaire.

4. RÔLE ET RESPONSABILITÉS DES AUTORITÉS COMPÉTENTES ET DES EXPLOITANTS

4.1. Dans un régime de sécurité nucléaire, la sécurité informatique est une question transversale pour les autorités compétentes et les exploitants. Ces organisations ont une certaine responsabilité dans la protection des RNS.

4.2. Les autorités compétentes et les exploitants sont à la fois producteurs et utilisateurs d'informations sensibles, qui, souvent, sont traitées par des RNS placées sous leur contrôle, sont stockées sur de telles RNS ou en font partie intégrante. Les autorités compétentes et les exploitants devraient mettre en œuvre des mesures de sécurité informatique afin de protéger les RNS et les informations sensibles correspondantes.

4.3. Les autorités compétentes et les exploitants devraient déterminer quelles sont leurs RNS, caractériser celles-ci en fonction de l'effet possible de leur compromission sur la sécurité et la sûreté nucléaires, et définir dans leur PSI le niveau des mesures de sécurité informatique qui est nécessaire pour chacune de ces RNS.

4.4. Les autorités compétentes et les exploitants devraient mettre en œuvre des mesures de sécurité informatique afin de préserver la confidentialité, l'intégrité et

la disponibilité des RNS et des informations qu'elles contiennent. Les mesures de sécurité informatique devraient par exemple avoir les caractéristiques suivantes :

a) Elles devraient être conçues pour empêcher tout accès non autorisé aux RNS par des personnes, des processus ou des appareils (selon une approche graduée).
b) Elles devraient garantir que des données ou un programme malveillants ne peuvent être introduits dans des RNS.
c) Elles devraient être prises en compte dans les dispositions relatives à la gestion de la chaîne d'approvisionnement.

4.5. Les autorités compétentes et les exploitants devraient appliquer une procédure formelle afin de s'assurer que seuls les membres du personnel jugés compétents et dignes de confiance sont autorisés à mener des activités qui touchent la sécurité informatique.

4.6. Les autorités compétentes et les exploitants ne devraient autoriser les membres du personnel non habilités à mener de telles activités que dans des cas exceptionnels et seulement lorsque des mesures de sécurité solides sont en place pour prévenir et détecter les actes non autorisés.

4.7. Les autorités compétentes et les exploitants devraient évaluer et gérer les interfaces entre la sécurité nucléaire et la sûreté nucléaire qui concernent la sécurité informatique [4] de telle manière que les mesures de sécurité et les mesures de sûreté n'aient pas d'incidence négative les unes sur les autres et qu'elles se renforcent mutuellement dans la mesure du possible.

4.8. Chaque autorité compétente et chaque exploitant devrait gérer un PSI qui décrit de quelle manière l'entité concernée assurera une sécurité informatique satisfaisante conformément aux prescriptions édictées par l'État et par son autorité compétente pour la sécurité informatique. Si plusieurs organisations utilisent les mêmes RNS ou sont interdépendantes en la matière, toutes les responsabilités partagées et tous les liens de dépendance devraient figurer dans leur PSI.

4.9. Les autorités compétentes et les exploitants devraient régulièrement évaluer leurs mesures de sécurité informatique afin de s'assurer qu'elles sont conformes aux prescriptions réglementaires. La périodicité de ces évaluations devrait être fixée de manière à pouvoir tenir rapidement compte de tout changement concernant la menace ou d'autres facteurs qui influent sur le risque. Les évaluations peuvent comprendre des audits, des examens, des tests de performance et des exercices, selon le cas. Les autorités compétentes et les exploitants devraient également

mener des autoévaluations lorsque des systèmes informatiques sont modifiés afin d'étudier si les changements effectués peuvent créer des vulnérabilités ou de nouvelles RNS.

RECOURS À DES VENDEURS, DES SOUS-TRAITANTS ET DES FOURNISSEURS

4.10. Les autorités compétentes et les exploitants devraient imposer des obligations contractuelles aux vendeurs, aux sous-traitants et aux fournisseurs afin qu'ils mettent en œuvre des mesures de sécurité informatique adaptées au rôle qu'ils jouent. Les contrats devraient mentionner les mesures de sécurité informatique qui doivent être prises pour qu'aucune activité d'une partie ne permette de lancer une cyberattaque contre l'autre partie et que les informations sensibles détenues par les parties soient convenablement protégées.

4.11. Les autorités compétentes et les exploitants, ainsi que leurs vendeurs, leurs sous-traitants et leurs fournisseurs, devraient gérer des protocoles et des procédures pour pouvoir communiquer rapidement des informations sur les incidents de sécurité informatique.

AUTORITÉ COMPÉTENTE POUR LA SÉCURITÉ INFORMATIQUE

4.12. L'autorité compétente pour la sécurité informatique devrait établir des prescriptions, des normes et des recommandations de sécurité informatique adaptées pour chaque autorité compétente et pour chaque exploitant à l'aide d'une approche graduée tenant compte des risques.

4.13. L'autorité compétente pour la sécurité informatique devrait veiller à ce que ces prescriptions tiennent compte de la stratégie, des exigences relatives à l'exploitation et à la sécurité que l'autorité compétente ou l'exploitant concernés doivent respecter et de leurs capacités et compétences avérées.

4.14. L'autorité compétente pour la sécurité informatique devrait utiliser une approche fondée sur les risques [1], qui repose sur une approche graduée et sur la défense en profondeur, afin d'assurer une sécurité informatique satisfaisante.

4.15. Chaque autorité compétente devrait veiller à ce que toutes les opérations qui sont effectuées pendant le cycle de vie des RNS dont elle est responsable

(conception, déploiement, maintenance et retrait, par exemple) soient convenablement contrôlées, suivies et consignées.

4.16. À l'aide d'évaluations régulières, chaque autorité compétente devrait vérifier que sa réglementation relative à la sécurité informatique est continuellement respectée et devrait si nécessaire veiller à ce que des mesures correctives soient prises.

4.17. L'autorité compétente pour la sécurité informatique peut imposer aux autorités compétentes ou aux exploitants de mettre en œuvre des mesures de sécurité informatique particulières, élaborées à l'aide de l'évaluation du risque qu'elle a effectuée (elle adopte alors une approche normative). Sinon, elle peut définir des prescriptions fondées sur les résultats pour la sécurité informatique, ce qui permet aux autorités compétentes ou aux exploitants d'utiliser une approche fondée sur les risques pour établir des mesures de sécurité informatique appropriées. L'autorité compétente pour la sécurité informatique peut aussi mixer les deux approches.

4.18. Les critères qui président au choix d'une approche normative ou d'une approche fondée sur les résultats (ou d'une association adéquate de ces deux approches) dépendent du cadre législatif et de la structure organisationnelle de l'État, ainsi que de plusieurs autres facteurs, notamment :

a) la compétence de l'exploitant concernant l'interprétation des prescriptions fondées sur les résultats et la conception, l'installation et l'évaluation d'un système de sécurité nucléaire efficace ;
b) le nombre et la diversité des installations et des exploitants qui seront soumis à la réglementation, et la mesure dans laquelle les prescriptions normatives peuvent réduire la marge de manœuvre de l'exploitant pour l'élaboration de mesures appropriées ;
c) la gravité des conséquences possibles des actes malveillants qu'il faut empêcher ou contre lesquels il faut assurer une protection [10].

L'approche normative

4.19. Dans le cas de l'approche normative, l'autorité compétente pour la sécurité informatique élabore les mesures de sécurité informatique particulières qu'elle juge nécessaires pour atteindre les objectifs de sécurité informatique qui lui ont été fixés.

4.20. Parmi les avantages de l'approche normative, on peut citer la simplicité de mise en œuvre par l'autorité compétente pour la sécurité informatique et par l'autorité compétente ou l'exploitant concernés, le fait qu'il n'est pas nécessaire de communiquer des informations sensibles et la facilité à mener des inspections et des évaluations. Cette approche peut être particulièrement appropriée lorsque la menace et les conséquences possibles sont faibles. Elle peut aussi être la plus pertinente lorsqu'il n'est pas possible de conduire une évaluation détaillée de la menace ou d'établir une menace de référence.

4.21. En revanche, l'approche normative manque parfois de souplesse dans des circonstances particulières. De surcroît, si cette approche est adoptée, l'autorité compétente concernée n'est pas tenue de s'assurer que les mesures de sécurité informatique mises en œuvre sont suffisantes. La responsabilité de la prévention des risques incombe en premier lieu à l'autorité compétente pour la sécurité informatique, car c'est elle qui définit précisément les mesures de sécurité informatique nécessaires pour faire face à la menace de cyberattaque. L'autorité compétente ou l'exploitant concernés sont uniquement tenus d'appliquer les mesures de sécurité informatique prescrites.

L'approche fondée sur les résultats

4.22. Dans le cas de l'approche fondée sur les résultats, l'autorité compétente pour la sécurité informatique définit les objectifs de sécurité informatique et impose aux autorités compétentes ou aux exploitants d'établir et d'appliquer des mesures de sécurité informatique qui permettent d'atteindre ces objectifs, grâce à un certain niveau de protection contre les cyberattaques et à des interventions spécialisées.

4.23. L'approche fondée sur les résultats laisse une certaine latitude aux autorités compétentes ou aux exploitants pour proposer une combinaison de mesures de sécurité informatique propre à une organisation particulière. L'adéquation de ces mesures est ensuite appréciée par rapport à l'évaluation de la menace ou à la menace de référence afin de vérifier que les mesures fondées sur les résultats satisfont aux objectifs. L'approche fondée sur les résultats présente notamment l'avantage de tenir compte du fait qu'une sécurité informatique efficace peut être obtenue par de nombreuses combinaisons de mesures de sécurité informatique et que les organisations et les conditions d'exploitation peuvent être différentes.

4.24. L'approche fondée sur les résultats suppose que l'autorité compétente pour la sécurité informatique et les autorités compétentes ou les exploitants disposent de compétences et de moyens suffisants dans le domaine de la sécurité informatique pour établir des prescriptions et mettre en œuvre des mesures de

sécurité informatique. Elle suppose également parfois que l'État communique aux autorités compétentes et aux exploitants des informations sensibles contenues dans l'évaluation de la menace ou dans la menace de référence.

L'approche mixte

4.25. L'approche mixte intègre des éléments de l'approche normative et de l'approche fondée sur les résultats. Il existe de nombreuses variantes de cette approche, dont voici deux exemples :

a) L'État peut exiger l'application d'une approche fondée sur les résultats lorsque les conséquences possibles sont graves ou très graves, tout en autorisant l'adoption d'une approche normative lorsque les conséquences possibles sont limitées ou très limitées ;
b) L'État peut imposer un ensemble de prescriptions normatives pour certains aspects de la sécurité informatique (comme la protection des informations sensibles) et prévoir des mesures de sécurité informatique supplémentaires, adoptées pour prendre en compte tous les autres aspects et déterminées à l'aide de l'approche fondée sur les résultats.

4.26. Le principal avantage de l'approche mixte est sa souplesse. Les inconvénients de cette approche sont semblables à ceux de l'approche fondée sur les résultats et de l'approche normative et dépendent de la manière dont elle est utilisée. Une approche mixte bien menée peut toutefois aboutir à un équilibre satisfaisant et limiter les inconvénients des deux autres approches.

ORGANISME DE RÉGLEMENTATION

4.27. L'organisme de réglementation[8] de la sécurité nucléaire devrait établir des prescriptions réglementaires pour les mesures de sécurité informatique afin de protéger les RNS et les informations sensibles correspondantes. Par voie de

[8] Il peut y avoir plusieurs organismes de réglementation dans un État, chacun ayant des responsabilités relatives à la sécurité nucléaire dans différents domaines. Ainsi, l'organisme de réglementation qui est chargé de la sécurité nucléaire dans les installations nucléaires peut ne pas être le même que celui qui est responsable de la sécurité nucléaire dans les secteurs où des sources radioactives sont utilisées. Dans la présente publication, l'expression « organisme de réglementation » est employée pour désigner tout organisme de ce type qui a une responsabilité dans un contexte particulier. L'organisme de réglementation de la sécurité nucléaire peut également être l'autorité compétente pour la sécurité informatique, auquel cas les orientations qui figurent dans la précédente sous-section s'appliquent aussi à cet organisme.

réglementation, il devrait veiller à ce que les entités concernées exercent leurs responsabilités relatives à la sécurité informatique conformément aux prescriptions réglementaires.

4.28. L'organisme de réglementation devrait veiller à ce que sa réglementation soit suffisamment souple pour être adaptable à la nature et à la situation évolutives des systèmes informatiques, des cyberattaques et des mesures de sécurité informatique.

4.29. Il est souhaitable que l'organisme de réglementation publie un guide sur sa réglementation relative à la sécurité informatique afin d'aider les entités concernées à l'appliquer. L'organisme de réglementation devrait réexaminer ce guide périodiquement afin de s'assurer qu'il tient dûment compte de la cybermenace et présente correctement l'objet de la réglementation.

4.30. L'organisme de réglementation devrait veiller à ce que la sécurité informatique soit prise en considération pour l'évaluation et la procédure de délivrance des licences ou d'autres procédures qui sont appliquées pour la délivrance d'autorisations.

4.31. L'organisme de réglementation devrait s'assurer que chaque exploitant a mis en place un PSI qui décrit les mesures de sécurité informatique adoptées.

4.32. L'organisme de réglementation devrait vérifier que les prescriptions réglementaires et les conditions de licence qui concernent la sécurité informatique sont continuellement respectées en procédant régulièrement à des inspections et, si nécessaire, en lançant des actions coercitives afin que des mesures correctives soient rapidement prises.

5. MISE EN PLACE DE LA STRATÉGIE DE SÉCURITÉ INFORMATIQUE

STRATÉGIE DE SÉCURITÉ INFORMATIQUE POUR LE RÉGIME DE SÉCURITÉ NUCLÉAIRE

5.1. La stratégie[9] fixe les grands objectifs du régime de sécurité nucléaire national qui concernent la sécurité informatique et qui doivent être pris en compte dans des documents de catégorie inférieure, lesquels serviront à mettre en œuvre la stratégie. La stratégie doit être applicable, réalisable et vérifiable.

5.2. Les points suivants devraient figurer dans la stratégie :

a) manière dont l'évaluation de la menace est effectuée, y compris le recensement des scénarios de cyberattaque possibles ;
b) manière dont les objectifs de sécurité nucléaire sont fixés ;
c) manière dont les compétences et les niveaux de capacité en sécurité informatique peuvent être définis ;
d) attribution à toutes les autorités compétentes et à tous les exploitants (et éventuellement aux vendeurs, aux sous-traitants et aux fournisseurs) de rôles et de responsabilités en matière de sécurité informatique ;
e) définition et création de nouvelles organisations ou adaptation des rôles relatifs à la sécurité informatique pour des organisations existantes en cas de déficit de capacités ;
f) démarches à suivre pour la mise en place, l'intégration et la coordination des activités de sécurité informatique qui sont menées par les autorités compétentes et les exploitants ;
g) mesures propres à maintenir des moyens dans le domaine de la sécurité informatique pour le régime de sécurité nucléaire.

5.3. Les sections 5 à 8 contiennent des orientations supplémentaires sur ces questions, qui doivent être traitées dans la stratégie.

[9] L'État peut décider de faire figurer certaines informations sensibles en appendice à la stratégie afin de limiter plus facilement la diffusion de ces informations.

5.4. La présente section décrit les activités préparatoires que l'État et son autorité compétente pour la sécurité informatique devraient mener pour mettre en place la stratégie, et notamment :

a) Procéder à une évaluation de la menace ;
b) Évaluer les conséquences d'une cyberattaque contre des RNS pour la sécurité nucléaire ;
c) Déterminer s'il convient d'adopter l'approche normative, l'approche fondée sur les résultats ou l'approche mixte pour réglementer la sécurité informatique ;
d) Définir un cadre pour les moyens et les compétences en sécurité informatique ;
e) Intégrer et coordonner les activités de sécurité informatique qui sont menées par les autorités compétentes et les exploitants.

ÉVALUATION DE LA CYBERMENACE QUI PÈSE SUR LE RÉGIME DE SÉCURITÉ NUCLÉAIRE

5.5. L'État devrait tenir à jour une évaluation des menaces qui pèsent sur son régime de sécurité nucléaire [1, 5]. Ces informations peuvent servir à élaborer un énoncé national de la menace ou à définir une menace de référence.

5.6. L'évaluation de la menace ou la menace de référence qui sont établies par l'État devraient prévoir que des adversaires peuvent lancer des cyberattaques, y compris à l'aide d'initiés, et des attaques combinées.

5.7. Une cyberattaque permet à un adversaire d'entreprendre un acte malveillant alors qu'il ne se trouve pas sur le site visé, ni même sur le territoire de l'État où ce site est installé. Pour son évaluation, l'État devrait donc tenir compte des menaces internationales.

5.8. L'État devrait veiller à ce que l'évaluation de la menace relative aux cyberattaques (évaluation de la cybermenace) soit régulièrement mise à jour. Il faudrait fixer la fréquence d'examen de l'évaluation de la menace en tenant compte de l'évolution rapide des techniques, des progrès des systèmes informatiques, des vulnérabilités découvertes récemment et de la nature évolutive des cyberattaques possibles et des approches correspondantes de la sécurité informatique.

5.9. L'État devrait veiller à ce que les changements qui sont apportés à l'évaluation de la menace et qui concernent les cyberattaques soient communiqués

aux autorités compétentes et aux exploitants concernés dans les meilleurs délais et en toute sécurité.

5.10. L'État devrait prendre toutes les mesures raisonnables pour tenir compte de la nature évolutive de la cybermenace et pour favoriser l'adoption de mesures de sécurité informatique qui tiennent compte à l'avance des changements ou qui s'y adaptent facilement, et qui restent donc efficaces.

5.11. En dehors des services de renseignement nationaux, d'autres autorités compétentes, des exploitants, des vendeurs, des sous-traitants et des fournisseurs peuvent détenir des informations qui peuvent être utiles pour l'évaluation de la menace.

5.12. L'État peut définir des protocoles pour l'échange sécurisé d'informations sur la menace, y compris pour des communications directes entre organisations.

5.13. Les autorités compétentes et les exploitants ne peuvent être tenus de se protéger contre tous les niveaux de menace. Au-dessus d'un certain niveau de menace, l'État est tenu d'intervenir à l'appui de l'autorité compétente ou de l'exploitant concernés (figure 6). Pour les autorités compétentes et les exploitants qui utilisent une menace de référence, on parle alors souvent d'« événement allant au-delà de la menace de référence ».

5.14. L'État devrait veiller à ce que l'évaluation de la menace ou la menace de référence pour la sécurité informatique contiennent suffisamment de détails pour les évaluations ultérieures du risque, lesquelles permettent d'assurer une sécurité informatique satisfaisante et efficace pour l'ensemble du régime de sécurité nucléaire national.

5.15. Par l'intermédiaire de l'autorité compétente pour la sécurité informatique, l'État devrait définir des critères, des procédures et des moyens pour toute intervention qui fait suite à une cyberattaque contre des autorités compétentes ou des exploitants, ou leurs vendeurs, leurs sous-traitants ou leurs fournisseurs. Ces procédures devraient prévoir des protocoles permettant une communication sécurisée avec l'organisme d'intervention.

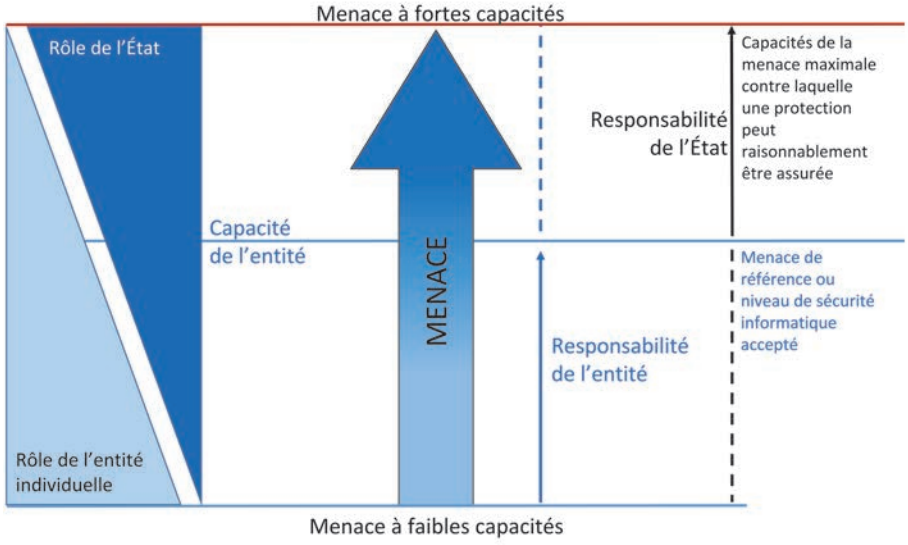

FIG. 6. Rôle et responsabilités concernant la protection contre les menaces.

DÉSIGNATION D'UNE AUTORITÉ COMPÉTENTE POUR L'ÉVALUATION DE LA CYBERMENACE

5.16. L'État devrait veiller à ce qu'une évaluation de la menace de cyberattaque soit effectuée régulièrement et au moment opportun. Il devrait confier cette mission à une autorité compétente qui a un savoir-faire utile pour la définition et l'évaluation de la cybermenace. L'autorité compétente pour l'évaluation de la cybermenace et l'autorité compétente pour la sécurité informatique ne sont pas nécessairement les mêmes.

5.17. Lorsqu'elle exerce ses fonctions, l'autorité compétente pour l'évaluation de la cybermenace devrait consulter toutes les autorités compétentes et tous les exploitants qui, selon l'État, ont un rôle et des responsabilités concernant les évaluations de la cybermenace et qui ont des compétences et des moyens, et coopérer avec eux dans le cadre d'une procédure officielle d'évaluation de la cybermenace. L'autorité compétente devrait piloter la coordination et le regroupement de ces différentes contributions à l'évaluation des menaces de cyberattaque.

5.18. L'autorité compétente pour l'évaluation de la cybermenace devrait être chargée de s'assurer que cette évaluation contienne suffisamment de détails pour les évaluations ultérieures du risque, qui serviront à mettre en œuvre convenablement et efficacement des mesures de sécurité informatique pour l'ensemble du régime de sécurité nucléaire national.

ÉVALUATION DES CONSÉQUENCES DU DYSFONCTIONNEMENT DES RNS

5.19. Pour chaque autorité compétente concernée et pour chaque exploitant concerné, l'autorité compétente pour la sécurité informatique devrait déterminer la gravité des conséquences possibles des cyberattaques qu'ils sont tenus d'empêcher par des mesures de sécurité informatique efficaces.

5.20. La gravité de ces conséquences devrait être évaluée à l'aide des caractéristiques et des attributs des RNS. Les autorités compétentes et les exploitants devraient étudier la gravité des conséquences indépendamment de toute probabilité et des types de cyberattaques qui pourraient conduire à ces conséquences.

5.21. La figure 7 montre les différents niveaux de gravité pour plusieurs types d'événements de sécurité nucléaire qui se rattachent aux branches de la sécurité nucléaire traitées dans les références [3] à [5]. L'autorité compétente pour la sécurité informatique devrait déterminer la gravité des conséquences et évaluer l'efficacité des mesures de sécurité informatique pour la prévention ou l'atténuation de ces conséquences.

5.22. L'autorité compétente pour la sécurité informatique peut déterminer, en coopération avec les autres autorités compétentes concernées, le niveau de protection à exiger à chaque niveau en fonction de la gravité des conséquences.

5.23. La mise en place d'une sécurité informatique efficace exige un éventail de compétences et des niveaux de capacité adaptés au rôle et aux responsabilités de chaque autorité compétente, de chaque exploitant, de chaque vendeur, de chaque sous-traitant et de chaque fournisseur. Lorsque des décisions et des mesures fondées sur un avis doivent être prises, le niveau de capacité sera nécessairement plus élevé. Pour que la sécurité informatique soit efficace, il faut définir ces compétences et ces niveaux de capacité pour chaque autorité compétente, pour chaque exploitant, pour chaque vendeur, pour chaque sous-traitant et pour chaque fournisseur, et obtenir l'assurance qu'ils sont maintenus et utilisés.

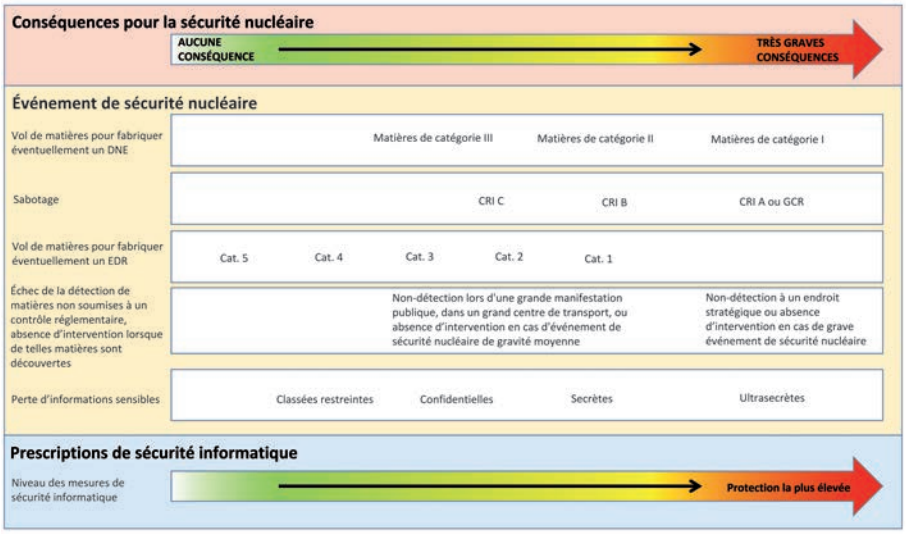

FIG. 7. Gravité des conséquences pour différents types d'événements de sécurité nucléaire (les niveaux de gravité sont indépendants et la gravité devrait être évaluée séparément pour chaque conséquence). GCR : graves conséquences radiologiques ; DNE : dispositif nucléaire explosif ; EDR : engin à dispersion de radioactivité ; CRI : conséquences radiologiques inacceptables.

5.24. L'autorité compétente pour la sécurité informatique devrait établir un cadre de compétences et de niveaux de capacité pour la sécurité informatique. On en trouvera un exemple dans l'annexe IV.

5.25. Le cadre devrait garantir que les compétences et les niveaux de capacité en sécurité informatique prescrits pour chaque autorité compétente, chaque exploitant, chaque vendeur, chaque sous-traitant et chaque fournisseur conviennent au regard de leurs responsabilités respectives en matière de sécurité informatique. Des orientations supplémentaires sur la définition des rôles, le développement et le maintien des compétences dans les organisations et le renforcement des capacités pour les organisations et les personnes figurent dans d'autres publications de la collection Sécurité nucléaire de l'AIEA [3, 11].

MÉTHODE D'ÉVALUATION DU RISQUE EMPLOYÉE POUR DÉTERMINER LES MESURES DE SÉCURITÉ INFORMATIQUE À APPLIQUER

5.26. Les mesures de sécurité informatique devraient être établies à l'aide d'une approche fondée sur les risques. L'autorité compétente pour la sécurité informatique devrait définir une méthode ou une série de méthodes d'évaluation du risque, en application desquelles les organisations responsables doivent :

a) déterminer si chaque système informatique existant remplit une fonction utile pour le régime de sécurité nucléaire ;
b) déterminer si chaque ressource numérique existante est une RNS ;
c) mener une analyse des risques pour la sécurité informatique afin de déterminer le niveau des mesures de sécurité informatique exigé pour chaque RNS ou autre ressource numérique, selon le principe qui est illustré sur la figure 3.

5.27. La méthode devrait tenir compte des éléments suivants :

a) toute législation ou réglementation applicable ;
b) importance des fonctions remplies par la RNS, y compris l'importance de la protection de la confidentialité, de l'intégrité et de la disponibilité de la RNS et des informations sensibles qu'elle contient, pour la sécurité et la sûreté nucléaires (c'est-à-dire la classe de sûreté de la RNS) ;
c) évaluation des conséquences des cyberattaques qui seraient lancées contre la RNS ;
d) contexte dans lequel la RNS est utilisée ;
e) identification et évaluation des menaces qui peuvent s'attaquer aux autorités compétentes et aux exploitants, à leurs vendeurs, à leurs sous-traitants et à leurs fournisseurs, ainsi qu'à la RNS, selon l'évaluation nationale de la menace, la menace de référence ou l'énoncé de la menace ;
f) intérêt de la RNS pour les menaces contre la sécurité nucléaire ;
g) vulnérabilités intrinsèques de la RNS.

5.28. L'autorité compétente pour la sécurité informatique peut modifier les résultats de l'évaluation du risque en fonction des conséquences possibles d'une compromission de la RNS, surtout si cette compromission a l'un quelconque des effets suivants :

a) la fonction de la RNS devient indéterminée ;

b) la RNS se comporte de manière inattendue ou effectue des actions inattendues ;
c) la RNS tombe en panne ;
d) la RNS fonctionne comme prévu (c'est-à-dire qu'elle est tolérante aux pannes).

5.29. L'évaluation du risque devrait prendre en compte les aspects de la sécurité dans leur ensemble, afin d'analyser les attaques combinées, dans le cadre desquelles des cyberattaques contre la protection physique (avec l'aide de membres du personnel, en particulier des initiés) et la sécurité informatique peuvent être lancées. Ceux qui mènent cette évaluation devraient donc pouvoir entrer en contact avec les personnes ayant toutes les compétences voulues, par exemple dans le domaine de la protection physique et de la sécurité informatique pour la sécurité et la sûreté nucléaires.

6. MISE EN ŒUVRE DE LA STRATÉGIE DE SÉCURITÉ INFORMATIQUE

6.1. La présente section décrit les responsabilités qui incombent à l'autorité compétente pour la sécurité informatique lorsqu'elle confie un rôle et des responsabilités aux autorités compétentes et aux exploitants en la matière.

6.2. Le rôle et les responsabilités en question devraient être consignés dans la stratégie ou dans des documents connexes.

6.3. L'autorité compétente pour la sécurité informatique peut établir des prescriptions sous forme de normes, de prescriptions réglementaires par l'intermédiaire d'un organisme de réglementation ou de conditions contractuelles pour les vendeurs, les sous-traitants ou les fournisseurs, et peut élaborer des documents d'orientation pour expliquer comment ces prescriptions devraient être respectées.

ATTRIBUTION DES RESPONSABILITÉS EN MATIÈRE DE SÉCURITÉ INFORMATIQUE

6.4. L'autorité compétente pour la sécurité informatique devrait veiller à ce que toutes les autorités compétentes et tous les exploitants qui utilisent des RNS soient

responsables au premier chef de la sécurité informatique de ces RNS et de toutes les autres ressources numériques qu'ils détiennent et dont la compromission pourrait porter atteinte à la sécurité nucléaire ou à la sûreté nucléaire.

6.5. L'autorité compétente pour la sécurité informatique devrait veiller à ce que toutes les autorités compétentes, tous les exploitants, tous les vendeurs, tous les sous-traitants et tous les fournisseurs qui interviennent au cours du cycle de vie des RNS se voient confier des responsabilités adéquates concernant la sécurité informatique de ces RNS.

6.6. L'autorité compétente pour la sécurité informatique devrait veiller à ce qu'il y ait un partage approprié des responsabilités entre l'État d'une part et les autorités compétentes et les exploitants d'autre part, afin que les risques induits par les menaces contre la sécurité nucléaire qui ont le plus de moyens soient maintenus à un niveau suffisamment bas.

6.7. L'autorité compétente pour la sécurité informatique devrait veiller à ce que les autorités compétentes et les exploitants concernés prévoient de s'occuper de la sécurité informatique pendant la détection de tout incident de sécurité informatique et l'intervention qui en résulte.

RELATIONS ENTRE LES AUTORITÉS COMPÉTENTES ET LES EXPLOITANTS

6.8. L'autorité compétente pour la sécurité informatique devrait prévoir une coordination des responsabilités relatives à la sécurité informatique entre les autorités compétentes et les exploitants qui relèvent du régime de sécurité nucléaire et ceux qui n'y sont pas soumis. Des autorités nationales chargées de la sécurité informatique peuvent par exemple ne pas être concernées par le régime de sécurité nucléaire, ce qui exige une coordination avec les autorités soumises à ce régime.

6.9. L'autorité compétente pour la sécurité informatique devrait établir des canaux de communication clairs entre les autorités compétentes, les exploitants et, s'il y a lieu, l'organisme ou le mécanisme de coordination mentionné au paragraphe 3.11.

6.10. L'autorité compétente pour la sécurité informatique devrait veiller à ce qu'il y ait un mécanisme de coopération, de coordination, d'échange d'informations et, s'il y a lieu, d'intégration des activités relatives à la sécurité informatique pour les autorités compétentes et les exploitants.

6.11. Lorsqu'elle confie des responsabilités relatives à la sécurité informatique aux autorités compétentes et aux exploitants, l'autorité compétente pour la sécurité informatique devrait trouver un juste équilibre entre deux exigences contradictoires, à savoir la nécessité d'assurer une défense en profondeur et l'utilisation efficace et efficiente des moyens disponibles dans le cadre du régime de sécurité nucléaire national, en tenant compte des points suivants :

a) L'indépendance contribue à assurer une défense en profondeur, car, si des choix indépendants sont faits en matière de conception et d'exploitation, il est moins probable qu'une défaillance de cause commune ou de mode commun se produise. On entend par indépendance l'indépendance fonctionnelle et financière à l'égard des organisations soumises à la réglementation et d'autres organismes concernés par l'utilisation de matières nucléaires ou d'autres matières radioactives. L'autorité compétente pour la sécurité informatique devrait s'assurer que les compétences et les niveaux de capacité des autorités compétentes et des exploitants sont suffisants pour qu'ils puissent prendre des décisions sur la sécurité informatique de manière autonome.
b) La mise en commun des moyens peut contribuer à une utilisation plus efficace et plus efficiente des ressources. Une autorité compétente ou un exploitant peut par exemple faire appel à une autre autorité compétente dans des domaines spécialisés de la criminalistique numérique, étant donné que cette compétence est rarement demandée. En pareil cas, un accord entre les entités concernées devrait fixer un délai de réponse pour la fourniture d'un appui à la suite d'une demande. L'autorité compétente pour la sécurité informatique devrait vérifier que des dispositions appropriées ont été prises pour qu'un appui efficace et rapide soit fourni si des autorités compétentes ou des exploitants ont besoin de l'aide d'autres autorités compétentes.

6.12. Lorsqu'elle cherche à trouver un équilibre entre l'indépendance et l'interdépendance des autorités compétentes et des exploitants, l'autorité compétente pour la sécurité informatique devrait tenir compte des moyens nécessaires pour assurer une protection contre les attaques combinées et intervenir si une telle attaque est lancée. Ces moyens peuvent être une combinaison de mesures de sécurité informatique et d'autres mesures de sécurité nucléaire (action des forces d'intervention chargées de la protection physique, par exemple) qui peuvent être mises en œuvre par d'autres autorités compétentes.

6.13. L'attribution des responsabilités et les compétences et les niveaux de capacité peuvent montrer qu'il faut créer de nouvelles organisations ou modifier des organisations existantes.

COMPÉTENCES ET MOYENS EN SÉCURITÉ INFORMATIQUE

6.14. L'autorité compétente pour la sécurité informatique devrait imposer aux autorités compétentes et aux exploitants d'analyser leurs objectifs de sécurité informatique afin de dresser une liste complète des compétences dont ils ont besoin. Elle peut décider de mener cette analyse elle-même, surtout lorsque l'autorité compétente ou l'exploitant concernés applique essentiellement des mesures de sécurité définies par l'autorité compétente pour la sécurité informatique.

6.15. L'autorité compétente pour la sécurité informatique devrait imposer aux autorités compétentes et aux exploitants de prouver qu'ils disposent des compétences nécessaires à des niveaux de capacité suffisants pour s'acquitter des responsabilités qui leur ont été conférées en matière de sécurité informatique. L'annexe III présente des responsabilités généralement attribuées aux autorités compétentes et l'annexe IV donne un exemple de cadre de compétences et de niveaux de capacité.

6.16. L'autorité compétente pour la sécurité informatique devrait imposer aux autorités compétentes et aux exploitants de prouver que toutes les personnes ayant des responsabilités en matière de sécurité informatique sont habilitées et convenablement formées, ont des connaissances techniques et des compétences suffisantes pour exercer leurs fonctions et connaissent bien le risque lié aux cyberattaques.

6.17. L'autorité compétente pour la sécurité informatique devrait imposer aux autorités compétentes et aux exploitants de mettre en œuvre des programmes de formation continue qui permettent de développer et de maintenir les compétences nécessaires à l'exercice de leurs responsabilités relatives à la sécurité informatique.

6.18. L'autorité compétente pour la sécurité informatique devrait encourager les autorités compétentes et les exploitants à évaluer leur propre niveau de capacité pour les compétences qui intéressent l'exercice de leurs responsabilités, afin de favoriser le développement et l'évolution de leurs compétences.

6.19. L'autorité compétente pour la sécurité informatique devrait mener des activités d'assurance afin d'évaluer la formation et les connaissances techniques du personnel des autorités compétentes et des exploitants dans le domaine de la sécurité informatique. Elle devrait imposer à chaque autorité compétente et à chaque exploitant de prouver qu'il maintient continuellement ses compétences et ses niveaux de capacité en sécurité informatique à la mesure des responsabilités qui lui ont été conférées dans ce domaine.

INTERVENTION EN CAS D'INCIDENT DE SÉCURITÉ INFORMATIQUE

6.20. L'autorité compétente pour la sécurité informatique devrait imposer aux autorités compétentes et aux exploitants d'élaborer, de mettre en œuvre et de tester des procédures de sécurité informatique visant à prévenir et à détecter les incidents de sécurité informatique et à intervenir lorsqu'un tel incident se produit.

6.21. L'autorité compétente pour la sécurité informatique devrait donner aux autorités compétentes et aux exploitants des orientations sur les caractéristiques des incidents qui peuvent constituer des incidents de sécurité informatique. Ces derniers peuvent aussi être des événements de sécurité nucléaire, comme le vol d'informations sensibles ou la perturbation de fonctions de sécurité nucléaire ou de sûreté nucléaire. En outre, des cyberattaques peuvent être lancées dans le cadre d'attaques combinées. La détection de cyberattaques discrètes ou secrètes peut donner des indications à l'avance sur les intentions possibles d'un adversaire.

6.22. L'autorité compétente pour la sécurité informatique devrait veiller à ce que les autorités compétentes, les exploitants et les organismes d'intervention concernés disposent de moyens d'intervention appropriés pour faire face aux incidents de sécurité informatique, et à ce que ces organisations exposent dans leur PSI les circonstances dans lesquelles ces moyens seront mobilisés.

6.23. L'autorité compétente pour la sécurité informatique devrait définir des prescriptions afin que les incidents de sécurité informatique soient signalés sans délai à l'organisme de réglementation de la sécurité nucléaire ou aux autres autorités compétentes concernées.

6.24. L'autorité compétente pour la sécurité informatique devrait veiller à ce qu'une autorité compétente ou un exploitant ayant des capacités suffisamment avancées (il a par exemple des compétences en criminalité de la sécurité informatique) procède à l'analyse technique de tous les incidents de sécurité informatique où une RNS entre en jeu.

EXERCICES

6.25. L'autorité compétente pour la sécurité informatique devrait veiller à ce que des exercices de sécurité nucléaire comportant une partie sécurité informatique soient organisés afin d'évaluer la capacité de l'État à intervenir en cas d'incident de sécurité informatique, notamment en cas d'attaque combinée.

6.26. L'autorité compétente pour la sécurité informatique devrait s'assurer que les autorités compétentes et les exploitants organisent régulièrement des exercices de sécurité informatique en vue d'entraîner les participants et de vérifier la pertinence de leur PSI, y compris du plan d'intervention spécialisé. S'il y a lieu, ces exercices devraient être regroupés avec d'autres exercices de sécurité nucléaire et devraient périodiquement être organisés conjointement avec des exercices d'intervention d'urgence.

ACTIVITÉS D'ASSURANCE

6.27. L'autorité compétente pour la sécurité informatique devrait mener des activités d'assurance afin que la sécurité informatique soit réellement maintenue dans l'ensemble du régime de sécurité nucléaire national, et vérifier que les mesures de sécurité informatique mises en œuvre apportent une protection qui est conséquente à l'évaluation de la menace et au risque que l'État a jugé acceptable.

6.28. L'autorité compétente pour la sécurité informatique devrait régulièrement et officiellement donner l'assurance à l'État que les autorités compétentes et les exploitants disposent de compétences et de niveaux de capacité suffisants en sécurité informatique.

Qualification de sécurité des pièces et des services

6.29. Les autorités compétentes, les exploitants et leurs vendeurs, leurs sous-traitants et leurs fournisseurs doivent être assurés que les appareils, les pièces et les services obtenus sont protégés par des mesures de sécurité informatique afin d'empêcher l'introduction de vulnérabilités, y compris l'introduction directe de logiciels malveillants ou la mise en place de portes d'entrée pour des cyberattaques.

6.30. Les autorités compétentes et les exploitants devraient s'assurer que leurs vendeurs, leurs sous-traitants et leurs fournisseurs qui interviennent pour les RNS dont ils sont responsables respectent les prescriptions de sécurité informatique applicables (développement logiciel sécurisé, par exemple) afin de réduire au minimum les vulnérabilités des RNS et d'empêcher l'utilisation de la chaîne d'approvisionnement comme porte d'entrée pour une cyberattaque. Il s'agit notamment d'examiner les méthodes, les procédures et les appareils qui sont utilisés par les vendeurs, les sous-traitants et les fournisseurs.

6.31. Dans les cahiers des charges qui concernent les RNS et les services correspondants, l'autorité compétente pour la sécurité informatique peut imposer

aux autorités compétentes, aux exploitants, aux vendeurs, aux sous-traitants et aux fournisseurs d'appliquer certaines normes nationales ou internationales. Ces normes devraient porter sur toutes les étapes du cycle de vie d'une RNS.

6.32. L'autorité compétente pour la sécurité informatique peut confier à un organisme d'accréditation le soin de garantir que les vendeurs, les sous-traitants et les fournisseurs qui conçoivent et fournissent des RNS et apportent un appui pour leur utilisation appliquent les pratiques de sécurité informatique prescrites.

6.33. Les autorités compétentes et les exploitants sont encouragés à procéder si nécessaire à des contrôles d'assurance, par exemple des essais de réception en usine et des inspections ou des audits de sécurité informatique (conformément aux conditions contractuelles), chez les vendeurs, les sous-traitants et les fournisseurs.

COOPÉRATION ET ASSISTANCE INTERNATIONALES

6.34. L'autorité compétente pour la sécurité informatique devrait veiller à ce que les relations nécessaires aient été établies avec ses homologues d'autres États et avec des organismes internationaux afin de pouvoir au besoin organiser la coopération et l'assistance internationales efficacement pour renforcer la sécurité informatique dans le cadre des régimes de sécurité nucléaire. Elle devrait prendre en compte ces relations à la lumière des responsabilités, des moyens et des compétences de toutes les organisations concernées.

7. ÉLABORATION D'UN PROGRAMME DE SÉCURITÉ INFORMATIQUE

7.1. La présente section contient des recommandations de mesures et d'éléments pour le PSI de chaque organisation. La figure 8 donne un exemple de cadre pour le PSI, y compris les documents connexes et les documents auxiliaires.

CONTENU D'UN PROGRAMME DE SÉCURITÉ INFORMATIQUE

7.2. Le PSI de chaque autorité compétente et de chaque exploitant définit la mission de l'organisation concernée pour la mise en œuvre de la stratégie sous forme de responsabilités, de procédures et de rôles au sein de l'organisation. Il

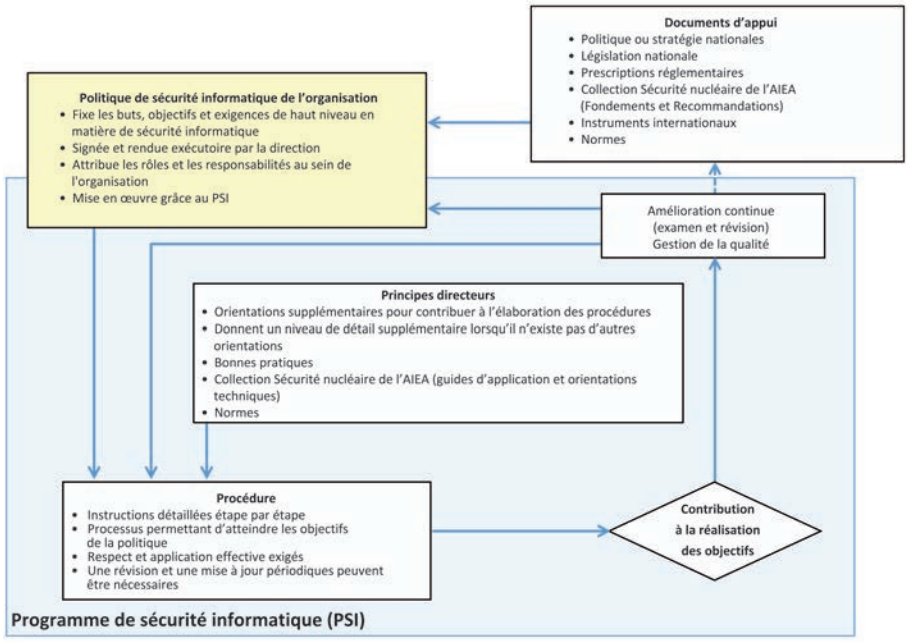

FIG. 8. Caractéristiques générales d'un programme de sécurité informatique classique.

décrit aussi les moyens par lesquels l'autorité compétente ou l'exploitant compte atteindre les objectifs de sécurité nucléaire ou mettre en œuvre les mesures de sécurité informatique prévues par la législation, la réglementation, les normes et les orientations publiées par l'organisme de réglementation dont il relève et par l'autorité compétente pour la sécurité informatique.

7.3. L'autorité compétente pour la sécurité informatique devrait veiller à ce que chaque autorité compétente et chaque exploitant élabore et gère un PSI conformément aux orientations qui figurent dans la présente section. Le PSI devrait être établi dans le cadre du plan de sécurité général du site et faire partie du système de gestion de chaque organisation.

7.4. L'autorité compétente pour la sécurité informatique devrait veiller à ce que la sécurité informatique soit présentée comme un aspect essentiel de la culture de sécurité nucléaire et devrait favoriser une recherche d'amélioration continue grâce à l'adhésion explicite de la direction de chaque autorité compétente et de chaque exploitant.

7.5. Le PSI devrait présenter la sécurité informatique au sein de l'organisation sous l'angle de la sensibilité aux vulnérabilités, des mesures de protection, de l'analyse des conséquences et des mesures d'atténuation, afin de déterminer et de maîtriser le risque acceptable résultant d'une cyberattaque, et de faciliter le retour à des conditions de fonctionnement sûres.

7.6. Le PSI devrait au moins contenir les éléments suivants :

a) Organisation et responsabilités :
   i) organigrammes ;
   ii) personnes responsables et responsabilités en matière de communication d'informations ;
   iii) sanctions et mesures correctives ;
   iv) procédure périodique d'examen et d'approbation ;
   v) interfaces avec d'autres programmes.
b) Gestion des ressources numériques :
   i) liste de tous les systèmes informatiques ;
   ii) liste de toutes les applications des systèmes informatiques ;
   iii) flux de données et schémas des réseaux, où figurent toutes les connexions à des systèmes informatiques externes ;
   iv) gestion de la configuration (matériel, microprogrammes, applications logicielles, état des appareils et configurations correspondantes) ;
   v) classification des ressources numériques et recensement des RNS, y compris le degré d'importance de ces ressources (c'est-à-dire leur contribution aux fonctions de sécurité nucléaire, de sûreté nucléaire et de comptabilité et de contrôle des matières nucléaires).
c) Évaluation des risques, de la vulnérabilité et du respect des règles :
   i) périodicité de l'examen et de la réévaluation du PSI ;
   ii) autoévaluation (comprenant des tests actifs et des tests passifs) ;
   iii) réévaluation périodique et corrective des risques et méthode employée à cette fin ;
   iv) procédures de contrôle et détection et correction des défauts ;
   v) contrôle du respect de la législation et de la réglementation.
d) Conception de la sécurité des systèmes :
   i) principes fondamentaux d'architecture et de conception ;
   ii) approches fondamentales de la conception de la sécurité (niveaux et zones de sécurité, par exemple) ;
   iii) élaboration des prescriptions de sécurité informatique pour les vendeurs, les sous-traitants et les fournisseurs ;
   iv) sécurité tout au long du cycle de vie.

e) Procédures de sécurité pour l'exploitation :
   i) contrôle des accès ;
   ii) sécurité des données ;
   iii) sécurité des communications ;
   iv) sécurité de la plateforme et des applications (durcissement, gestion des correctifs et protection contre les logiciels malveillants, par exemple) ;
   v) surveillance du système (y compris la journalisation) ;
   vi) maintien de la sécurité informatique ;
   vii) gestion des incidents ;
   viii) continuité des opérations et reprise après sinistre ;
   ix) sauvegarde du système.
f) Gestion du personnel :
   i) habilitation (enquêtes de sécurité sur le personnel) ;
   ii) sensibilisation et formation ;
   iii) qualification du personnel ;
   iv) cessation d'emploi ou transfert de personnel.

7.7. Le PSI devrait faire partie intégrante du système de gestion de l'organisation et devrait être coordonné avec les autres éléments de ce système. Il peut être divisé en sections portant sur des niveaux de sécurité différents afin qu'il soit plus facile à utiliser de manière efficace et conformément à la règle du « besoin d'en connaître » et aux exigences de confidentialité.

7.8. Le PSI devrait être examiné régulièrement et actualisé pour tenir compte des nouvelles connaissances qui concernent ou non le cadre du régime de sécurité nucléaire, et notamment des aspects suivants :

a) nouvelles technologies qui peuvent être utilisées à des fins de cyberattaque ou pour se protéger contre les cyberattaques ;
b) nouvelles caractéristiques, notamment les changements de tactiques, de techniques et de procédures connus ;
c) nouveaux types d'incidents de sécurité informatique ou d'événements de sécurité nucléaire.

7.9. Le PSI devrait prévoir des exercices réguliers afin d'entraîner les participants et de vérifier la pertinence du PSI, y compris pour ce qui est du plan d'intervention spécialisé. S'il y a lieu, ces exercices devraient faire partie d'autres exercices de sécurité et devraient périodiquement être organisés conjointement avec des exercices d'intervention d'urgence.

ÉVALUATION DU RISQUE AU NIVEAU D'UNE ORGANISATION

7.10. En fonction des moyens dont disposent les autorités compétentes ou les exploitants et des effets néfastes possibles des cyberattaques sur les RNS dont ils sont responsables, le PSI peut décrire une méthode que l'organisation utilisera pour procéder à des évaluations locales du risque qui pèse sur ses systèmes informatiques en tenant compte des menaces locales.

7.11. Les objectifs de ces évaluations sont les suivants :

a) identifier et comprendre le risque et les facteurs de risque ;
b) servir de référence pour le recensement des systèmes informatiques et des RNS ;
c) servir de référence pour faciliter l'analyse de l'évolution des RNS, des autres ressources numériques, de la menace, des répercussions possibles sur la sécurité informatique et des conséquences qui en résultent pour la sécurité nucléaire ;
d) contribuer à vérifier le bien-fondé de prescriptions de haut niveau.

7.12. L'organisation peut évaluer le risque pour l'organisation elle-même ou pour un système particulier.

7.13. Pour ces évaluations du risque, il faudrait partir de l'énoncé national de la menace ou de la menace de référence et tenir compte d'autres sources d'information existantes sur les cybermenaces.

7.14. L'évaluation du risque devrait prendre en considération les conséquences néfastes de la compromission ou du dysfonctionnement de chaque système informatique pour la sécurité nucléaire ou la sûreté nucléaire afin de déterminer quelles sont les RNS.

7.15. Si les résultats de l'évaluation du risque s'écartent sensiblement de ce que l'autorité compétente pour la sécurité informatique a supposé, les autorités compétentes ou les exploitants devraient régler le problème dans les meilleurs délais. Ces écarts peuvent notamment s'expliquer par une évolution de la situation locale sur le plan de la menace ou par des changements de matériel qui créent de nouvelles vulnérabilités.

7.16. L'évaluation du risque devrait porter sur tous les aspects de la sécurité nucléaire collectivement, notamment par exemple la protection physique, la protection contre les menaces internes et la sécurité informatique, afin de pouvoir

évaluer le risque que font peser les attaques combinées. Elle devrait donc être menée avec la contribution de spécialistes de chacun de ces domaines.

MESURES DE SÉCURITÉ INFORMATIQUE

7.17. Le PSI définit des mesures de sécurité informatique qui permettent d'assurer des fonctions de prévention, de détection, de retardement, d'intervention et d'atténuation, et de garantir que des actes non malveillants ne provoqueront pas une dégradation de la sécurité informatique qui augmenterait la sensibilité aux cyberattaques.

7.18. Les mesures de sécurité informatique particulières qui peuvent être appliquées sont de trois types différents :

a) Mesures de contrôle technique : solutions matérielles ou logicielles permettant d'assurer une protection contre les intrusions ou les autres actes malveillants dirigés contre des RNS, de les détecter, d'en atténuer les conséquences et de procéder à la remise en état. Il faudrait tenir compte des avantages des mesures de contrôle technique, surtout le fait qu'elles permettent une action protectrice continue et automatique, lorsque l'efficacité des différents types de mesures est évaluée.
b) Mesures de contrôle physique : barrières physiques destinées à protéger les RNS contre les dommages matériels et les accès physiques non autorisés. Les mesures de contrôle physique sont notamment les gardiens et des barrières comme les verrous, les clôtures, les grilles, les cages, les dispositifs antifraude et les salles d'isolement.
c) Mesures de contrôle administratif : règles, procédures et pratiques conçues pour protéger les RNS par un contrôle des agissements du personnel. Les mesures de contrôle administratif comprennent des mesures opérationnelles et des mesures de gestion, et sont généralement de nature directive, car elles énoncent ce que les salariés et le personnel des organisations tierces devraient et ne devraient pas faire, mais comprennent aussi des mesures visant à influer sur les comportements, comme le fait de promouvoir une solide culture de sécurité.

RECOURS À UNE APPROCHE GRADUÉE POUR DÉTERMINER LES MESURES DE SÉCURITÉ INFORMATIQUE À APPLIQUER

7.19. Les mesures de sécurité informatique qui figurent dans le PSI devraient être déterminées à l'aide d'une approche graduée, selon laquelle les mesures de sécurité sont appliquées en proportion des conséquences éventuelles d'une cyberattaque. Un des moyens concrets de mise en œuvre d'une approche graduée consiste à regrouper les systèmes informatiques qui assurent des fonctions de sécurité nucléaire en zones, des mesures de sécurité informatique graduées étant appliquées pour chaque zone. Pour mettre en œuvre ce type de mesures, on définit généralement des niveaux de sécurité informatique (voir par. 2.41 à 2.46).

7.20. Le PSI devrait prévoir une méthode écrite, comme celle qui figure dans la section 2, pour la détermination du niveau de sécurité informatique approprié pour chaque ressource numérique, notamment pour les RNS, si l'autorité compétente pour la sécurité informatique l'exige. Par exemple, certaines autorités compétentes ou certains exploitants peuvent être tenus de mettre en œuvre des mesures de sécurité informatique obligatoires, au lieu de définir par eux-mêmes le niveau de sécurité à appliquer aux systèmes informatiques, aux ressources numériques et aux RNS.

7.21. La méthode employée pour déterminer les niveaux de sécurité informatique devait être soumise à l'approbation de l'autorité compétente pour la sécurité informatique.

CONCEPTION DES MESURES DE SÉCURITÉ INFORMATIQUE

7.22. Le PSI devrait contribuer à ce que les mesures de sécurité informatique soient autant que possible appliquées dès la conception des systèmes informatiques. Les mesures de sécurité informatique sont généralement beaucoup plus faciles à mettre en œuvre et plus efficaces lorsqu'elles sont prises en compte durant la conception que lorsqu'elles sont ajoutées a posteriori.

7.23. Les prescriptions de sécurité nucléaire et les prescriptions de sûreté nucléaire devraient être prises en compte durant la conception des systèmes informatiques.

DÉFENSE EN PROFONDEUR POUR LES MESURES DE SÉCURITÉ INFORMATIQUE

7.24. La notion de défense en profondeur est essentielle pour la sécurité nucléaire. Le PSI devrait définir comment la défense en profondeur s'applique aux mesures de sécurité informatique. Pour ce faire, il existe différents moyens, notamment :

a) Appliquer des mesures de sécurité informatique diverses et indépendantes et exiger que leur conception, leur fonctionnement et leur maintenance soient indépendants. Cette démarche permet par exemple de garantir qu'une seule vulnérabilité ne permet pas à un adversaire de contourner directement plusieurs couches de défense en profondeur.
b) Séparer les fonctions des membres du personnel ou des équipes qui ont un accès privilégié à des RNS. Il faudrait notamment envisager de séparer les fonctions de conception, de mise en œuvre et d'administration des mesures de sécurité informatique de celles qui concernent l'exploitation de l'installation ou le déroulement de l'activité.

GESTION DES VENDEURS, DES SOUS-TRAITANTS ET DES FOURNISSEURS

7.25. Les autorités compétentes ou les exploitants peuvent faire appel à des vendeurs, à des sous-traitants ou à des fournisseurs pour se procurer des biens ou des services pour lesquels les vendeurs, les sous-traitants ou les fournisseurs auront nécessairement accès à des informations sensibles et à des RNS. En pareil cas, une convention, par exemple une licence ou le contrat de fourniture des biens et services, devrait contenir des exigences appropriées en matière de sécurité informatique.

7.26. Lorsqu'ils rédigent ce type de licence ou de contrat, les autorités compétentes et les exploitants devraient envisager d'y ajouter des clauses pour tenir compte du fait que les vendeurs, les sous-traitants et les fournisseurs peuvent détenir des informations uniques et exclusives (concernant par exemple les vulnérabilités qui peuvent devenir visibles après la fin du contrat initial) et qu'ils devront peut-être les communiquer aux autorités compétentes et aux exploitants.

7.27. Les autorités compétentes et les exploitants devraient définir des exigences de sécurité informatique particulières pour les vendeurs, les sous-traitants et les fournisseurs dans leur PSI. Ces exigences peuvent concerner aussi bien le travail sur site que le travail hors site.

7.28. Les autorités compétentes et les exploitants devraient veiller à ce que les vendeurs, les sous-traitants et les fournisseurs mettent en œuvre des mesures de sécurité informatique pour la mise au point et la livraison des produits et des services qu'ils fournissent.

7.29. Les autorités compétentes et les exploitants peuvent fixer des exigences particulières pour la sécurité informatique dans le cadre des contrats. Ces exigences peuvent notamment être les suivantes :

a) interdiction de communiquer des informations sensibles et certaines autres informations ;
b) exigences concernant la protection des informations sensibles, notamment concernant la conservation ou la destruction de ces informations ;
c) limites fixées pour l'accès autorisé aux systèmes informatiques et les activités qui peuvent être menées sur ces systèmes ;
d) activités interdites ;
e) sanctions en cas de non-respect des exigences de sécurité informatique imposées ;
f) restrictions relatives à l'accès à distance ;
g) exigences concernant les tests sur les services et les produits qui sont livrés dans le cadre du contrat.

7.30. Les autorités compétentes et les exploitants peuvent envisager d'imposer aux vendeurs, aux sous-traitants et aux fournisseurs de prouver qu'ils respectent les conditions contractuelles relatives à la sécurité informatique.

7.31. Les autorités compétentes et les exploitants devraient imposer aux vendeurs, aux sous-traitants et aux fournisseurs de signaler dans les meilleurs délais les incidents de sécurité informatique, y compris les menaces potentielles et les vulnérabilités qui peuvent porter atteinte à la sécurité nucléaire. Les obligations et les protocoles de signalement devraient figurer dans les contrats.

7.32. Le recours à des vendeurs, à des sous-traitants et à des fournisseurs peut entraîner un transfert ou un partage des risques. Ce transfert ou ce partage des risques peut être soumis à l'accord de l'organisme de réglementation de la sécurité nucléaire ou de l'autorité compétente pour la sécurité informatique. Cependant, la responsabilité de la sécurité nucléaire, y compris pour la sécurité informatique, ne peut être transférée à des vendeurs, à des sous-traitants ou à des fournisseurs.

8. MAINTIEN DE LA SÉCURITÉ INFORMATIQUE

8.1. La présente section décrit les mesures et les éléments recommandés pour le maintien de la sécurité informatique dans le cadre d'un régime de sécurité nucléaire. Ces mesures et ces éléments devraient figurer dans le PSI.

8.2. Les autorités compétentes et les exploitants devraient disposer de programmes de mise en valeur des ressources humaines appropriés afin de pouvoir maintenir les compétences et le niveau de capacité nécessaires pour s'acquitter des responsabilités qui leur ont été conférées en matière de sécurité informatique.

8.3. Les autorités compétentes et les exploitants devraient mettre en place des processus pour l'utilisation des meilleures pratiques et des enseignements tirés de l'expérience [1], surtout des incidents de sécurité informatique et, lorsque cela est possible, de l'expérience d'autres autorités compétentes, d'autres exploitants, d'autres secteurs concernés et de leurs homologues dans d'autres États.

8.4. Les autorités compétentes et les exploitants devraient intégrer la sécurité informatique à leur programme de pérennisation et y contribuer en y consacrant des moyens suffisants. Les programmes de pérennisation devraient porter sur les aspects pertinents des compétences et des niveaux de capacité nécessaires pour la mise au point, l'exploitation, la maintenance et le démantèlement ou le retrait des RNS et des autres ressources numériques.

CULTURE DE SÉCURITÉ

8.5. Développer, favoriser et maintenir une solide culture de sécurité nucléaire est un élément essentiel d'un régime de sécurité nucléaire [1]. Dans le domaine de la sécurité informatique, les personnes et les processus jouent souvent un rôle fondamental dans la protection des systèmes informatiques, et l'erreur humaine est l'un des facteurs qui contribuent le plus à provoquer des incidents de sécurité informatique. La culture de sécurité nucléaire devrait aider les salariés à détecter et à signaler les comportements inhabituels des systèmes informatiques ou des personnes qui les utilisent, et à signaler les erreurs humaines qui peuvent porter atteinte à la sécurité informatique.

8.6. La sécurité informatique devrait être présentée comme un aspect essentiel de la culture de sécurité nucléaire grâce à l'adhésion explicite de la direction et à

des actions de sensibilisation et de formation. Le PSI devrait prévoir des activités qui renforcent la culture de sécurité nucléaire.

8.7. Dans le cadre d'une véritable culture de sécurité nucléaire, toutes les organisations devraient veiller à ce que leurs salariés et leurs sous-traitants connaissent parfaitement leurs responsabilités en matière de sécurité informatique et aient pleinement conscience de l'importance de ces responsabilités, surtout en ce qui concerne la sécurité et la sûreté nucléaires. Les salariés et les sous-traitants devraient suivre une formation théorique et pratique en sécurité informatique qui soit adaptée à leur rôle et à leurs responsabilités.

FORMATION

8.8. Les autorités compétentes et les exploitants devraient mettre en place des programmes de formation en sécurité informatique pour tous les salariés et tous les sous-traitants. Ces programmes doivent tenir compte de la stratégie et viser à développer et à maintenir leurs compétences et leurs niveaux de capacité.

8.9. Les programmes de formation devraient comprendre des activités de sensibilisation et de développement des connaissances et des compétences.

8.10. Les thèmes recommandés pour mieux faire connaître la sécurité informatique et pour former les personnes sont notamment les suivants :

a) connaissance des types de cybermenaces et des techniques d'attaque correspondantes ;
b) connaissance de l'ingénierie sociale et conseils pour lutter contre cette pratique ;
c) détection des cyberattaques et intervention en cas de cyberattaque ;
d) responsabilités des personnes en matière de sécurité informatique et sanctions en cas de non-respect des règles ;
e) conséquences possibles des cyberattaques sur la sécurité et la sûreté nucléaires ;
f) bonnes pratiques de sécurité informatique ;
g) utilisation des appareils portatifs et des supports amovibles ;
h) utilisation des médias sociaux ;
i) modifications du niveau ou de la nature de la cybermenace ou du risque.

8.11. Le personnel chargé de la maintenance, de l'exploitation et de la conception des systèmes nucléaires devrait connaître les risques que les cyberattaques

altérant des fonctions de contrôle-commande font peser sur la sécurité et la sûreté nucléaires.

8.12. Le personnel chargé de la maintenance, de l'exploitation et de la conception des systèmes de protection physique devrait connaître les effets possibles des cyberattaques sur les fonctions de ces systèmes.

8.13. Il faudrait communiquer les modifications des règles et des procédures de sécurité à tous les salariés et à tous les sous-traitants concernés le plus rapidement possible.

8.14. Il conviendrait d'organiser des formations techniques spécialisées et adaptées aux fonctions qu'ils exercent pour les salariés et les sous-traitants qui ont des responsabilités administratives et techniques dans le domaine de la sécurité informatique (personnel d'appui en technologies de l'information, personnel chargé du contrôle-commande, administrateurs des systèmes de sécurité et personnel de maintenance du matériel technique, par exemple).

8.15. Les programmes de formation devraient définir les exigences de formation auxquelles sont soumis les vendeurs, les sous-traitants et les fournisseurs pour les travaux à réaliser sur site et hors site.

8.16. La direction devrait périodiquement suivre des formations et assister à des réunions de sensibilisation sur la cybermenace et la gestion du risque.

8.17. Les autorités compétentes et les exploitants devraient fréquemment examiner et mettre à jour leurs programmes de formation pour tenir compte du caractère évolutif de la sécurité informatique, et notamment de l'évolution de la cybermenace et des techniques de cyberattaque.

8.18. Les autorités compétentes et les exploitants devraient désigner des responsables de l'appui aux programmes de formation et du maintien de ces programmes et leur allouer des moyens suffisants.

8.19. Il faudrait conserver une trace écrite des formations structurées suivies par tous les salariés et tous les sous-traitants.

8.20. Les activités de formation et de sensibilisation sur la sécurité de l'information et la sécurité informatique sont souvent regroupées. L'annexe III de la référence [8] contient un exemple de programme de sensibilisation à la sécurité de l'information, qui peut être adapté pour prendre en compte la sécurité informatique.

PLANS D'INTERVENTION SPÉCIALISÉS ET INTERVENTIONS

8.21. Le PSI devrait décrire les mesures de sécurité informatique qui sont prises pour détecter les incidents de sécurité informatique, intervenir si un tel incident se produit et en atténuer les conséquences.

8.22. Le PSI devrait mentionner les analyses et les actions appropriées qui permettent de déterminer la cause, les effets immédiats et les conséquences possibles d'un incident de sécurité informatique. Ces éléments ne sont pas toujours directement visibles, mais doivent être déterminés le plus tôt possible.

8.23. Dans le cadre de l'analyse d'un incident de sécurité informatique, il faudrait envisager la possibilité que l'incident soit une activité précurseur ou une activité de reconnaissance pour une future attaque.

8.24. Le PSI devrait contenir des plans d'intervention spécialisés afin de pouvoir intervenir en cas de cyberattaque. Ces plans devraient tenir compte de la possibilité qu'une attaque de l'intérieur ou une attaque combinée soit lancée. Ils devraient définir les types particuliers d'incidents de sécurité informatique et les interventions requises lorsque ces types d'incidents se produisent.

8.25. Lorsqu'un incident de sécurité informatique est également un événement de sécurité nucléaire, le plan d'intervention spécialisé applicable devrait être déclenché. Le PSI et les plans d'intervention spécialisés correspondants devraient énumérer les actions à mener immédiatement lorsque la sûreté nucléaire est compromise (en pareil cas, des plans d'urgence peuvent aussi être déclenchés, mais ils n'entrent pas dans le cadre de la présente publication).

8.26. Le PSI devrait décrire les conditions dans lesquelles des moyens supplémentaires sont mobilisés et le rôle de ces moyens en cas d'intervention à la suite d'un incident de sécurité informatique.

8.27. Dans le cadre de l'analyse d'un incident de sécurité informatique, une équipe multidisciplinaire peut être amenée à étudier les conséquences d'un incident pour la sécurité et la sûreté nucléaires.

ACTIVITÉS D'ASSURANCE EN SÉCURITÉ INFORMATIQUE

8.28. Les autorités compétentes et les exploitants devraient vérifier que leur système de gestion dispose de moyens efficaces permettant d'assurer que les

prescriptions de sécurité informatique sont respectées, y compris dans le cadre de la chaîne d'approvisionnement.

8.29. Les autorités compétentes et les exploitants (sauf ceux qui appliquent uniquement des mesures de sécurité informatique imposées par l'organisme de réglementation ou l'autorité compétente pour la sécurité informatique) devraient donner l'assurance à l'autorité compétente pour la sécurité informatique que les moyens alloués à la sécurité informatique sont adaptés et proportionnés au niveau de la menace qui est décrite dans l'évaluation de la menace.

8.30. Les autorités compétentes et les exploitants devraient s'assurer que les inspections ou les évaluations destinées à contrôler le respect des prescriptions de sécurité nucléaire comprennent une évaluation des mesures de sécurité informatique.

Appendice

CONSIDÉRATIONS RELATIVES À L'INTERFACE AVEC LA SÛRETÉ NUCLÉAIRE POUR LA SÉCURITÉ INFORMATIQUE DANS LES INSTALLATIONS

A.1. Le sabotage d'une installation peut compromettre sa sûreté nucléaire ou sa disponibilité en cas de cyberattaque contre des systèmes qui sont importants pour la sûreté de l'installation et qui utilisent des systèmes informatiques, reposent sur de tels systèmes ou fonctionnent grâce à leur appui. De telles attaques peuvent provoquer des défaillances ou des dysfonctionnements de systèmes importants pour la sûreté qui ne pourraient se produire si ces systèmes étaient en état de marche ou en état de défaillance connu.

A.2. Des actes malveillants peuvent porter atteinte à un seul système (ou élément) ou être la cause commune du comportement indésirable de plusieurs systèmes (ou éléments). Lors de la conception de l'installation, il faudrait veiller à ce que des actes malveillants ne puissent pas provoquer la défaillance de plusieurs niveaux de défense en profondeur pour la sûreté ou les contourner.

A.3. La sécurité informatique vise à réduire le risque que des adversaires puissent commettre des actes de sabotage à l'aide de cyberattaques qui pourraient compromettre la sécurité, la sûreté ou la disponibilité de l'installation. La sécurité informatique joue un rôle dans tous les niveaux de défense en profondeur pour la sûreté, telle que cette notion est décrite dans la référence [12], et doit donc s'appliquer aux fonctions, aux systèmes et au matériel à tous les niveaux.

A.4. Dans le domaine de la sécurité informatique, l'interface entre la sûreté et la sécurité comprend plusieurs éléments importants pour la sécurité et la sûreté nucléaires. Il s'agit notamment des systèmes, des procédures et du personnel. Les mesures de sécurité remplissent souvent des fonctions utiles pour la sécurité nucléaire (et vice versa), et il faudrait tenir compte des possibilités de tenir compte de ces fonctions complémentaires lors de l'élaboration des mesures de sécurité informatique.

A.5. Un dispositif qui permet de contrôler automatiquement la validité, l'authenticité et l'intégrité des données reçues avant qu'elles ne soient utilisées par une fonction de sûreté est un exemple de mesure de sûreté qui peut aussi avoir un intérêt pour la sécurité. La maintenance ou la modification du dispositif peut dégrader les fonctions de sûreté ou de sécurité si les exécutants ignorent qu'il y a

plusieurs fonctions (interdépendances). Il faudrait donc décrire les fonctions de sûreté et de sécurité remplies par ce type de dispositif dans la documentation relative aux systèmes et aux composants.

A.6. La stratégie de sûreté peut également nuire à la sécurité (et vice versa). Ainsi, la conception à des fins de sûreté suppose souvent de répartir les fonctions entre différents éléments ou différents systèmes afin d'isoler les effets d'une défaillance, et de prévoir des systèmes redondants et divers afin qu'une défaillance unique ne compromette pas des fonctions importantes. Ce type de stratégie peut entraîner une hausse du nombre d'éléments du système qui sont importants pour la sûreté, ce qui accroît la complexité et peut conduire à une augmentation du nombre de cibles possibles pour une cyberattaque. Les mesures de sécurité et de sûreté devraient donc toujours être prises en considération pour détecter et résoudre les conflits.

A.7. La pertinence d'une mesure de sécurité informatique donnée dépend de considérations qui concernent à la fois la sécurité et la sûreté. La conception d'une telle mesure exige donc des compétences dans les deux domaines. Les mesures de sécurité informatique comprennent des mesures techniques, physiques et administratives, et toutes les mesures doivent agir en synergie. Une telle approche peut par exemple exiger que certaines fonctions de sécurité (comme le recueil des données de contrôle ou le déclenchement des alarmes de sécurité) soient remplies par des systèmes qui peuvent surveiller les systèmes de contrôle-commande, mais pas influer sur leur fonctionnement, ou que des examens de sécurité actifs ne puissent être effectués que lorsque les systèmes de contrôle-commande ne sont pas connectés au réseau. Des exceptions à une telle approche peuvent être autorisées, mais elles devraient être analysées et justifiées au cas par cas.

A.8. Le risque acceptable pour une installation sera probablement le même si la cause de la situation est un événement de sûreté ou un événement de sécurité. L'approche commune à adopter peut être résumée comme suit :

a) Le principe de la défense en profondeur (c'est-à-dire l'utilisation de plusieurs couches de protection) s'applique à la sûreté et à la sécurité.
b) On cherche à prévenir tout événement initiateur, à détecter précocement toute situation anormale et à intervenir rapidement afin d'éviter que la situation ne se détériore.
c) La conception prévoit une atténuation des conséquences, au cas où les actions précédentes échoueraient.

d) Une planification approfondie des interventions d'urgence a été mise en place pour tenir compte des situations où la prévention, la détection et l'atténuation des conséquences ont échoué.

A.9. La relation entre la sécurité informatique et la sûreté exige une coordination efficace, notamment pour une classification et une gestion des ressources tenant compte des considérations de sécurité et de sûreté. Cette coordination peut être rendue plus difficile par le recours grandissant aux logiciels et aux réseaux dans les systèmes informatiques et par leur évolution rapide pour cette raison, de sorte que la conception et le mode opératoire des mesures de sécurité informatique évoluent eux aussi rapidement. Ce phénomène pose un problème lorsque les analyses de la sûreté reposent sur des prévisions précises de futurs comportements déterministes. Cette analyse peut être rendue encore plus délicate par l'incertitude relative à l'efficacité des mesures de sécurité informatique, de sorte qu'elle peut être incapable de prévoir avec exactitude le comportement futur d'un système en cas d'événement initiateur (par exemple lorsqu'un système est la cible de cyberattaques).

A.10. L'application de mesures de sécurité informatique à des systèmes existants impose souvent de revoir l'analyse de la sûreté qui a déjà été menée. En général, des mesures de sécurité informatique intégrées permettent de maîtriser ou de modifier d'une autre manière le comportement d'un système important pour la sûreté, par rapport à des mesures distinctes ou indépendantes.

RÉFÉRENCES

[1] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Objectif et éléments essentiels du régime de sécurité nucléaire d'un État, n° 20 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2014).

[2] Convention sur la protection physique des matières nucléaires, INFCIRC/274/Rev.1, AIEA, Vienne (1980) ; Amendement de la Convention sur la protection physique des matières nucléaires, INFCIRC/274/Rev.1/Mod.1, AIEA, Vienne (2016).

[3] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Recommandations de sécurité nucléaire sur la protection physique des matières nucléaires et des installations nucléaires, INFCIRC/225/Révision 5, n° 13 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2011).

[4] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Recommandations de sécurité nucléaire relatives aux matières radioactives et aux installations associées, n° 14 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2011).

[5] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, INSTITUT INTERRÉGIONAL DE RECHERCHE DES NATIONS UNIES SUR LA CRIMINALITÉ ET LA JUSTICE, OFFICE DES NATIONS UNIES CONTRE LA DROGUE ET LE CRIME, OFFICE EUROPÉEN DE POLICE, ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE, ORGANISATION INTERNATIONALE DE POLICE CRIMINELLE-INTERPOL, ORGANISATION MONDIALE DES DOUANES, Recommandations de sécurité nucléaire sur les matières nucléaires et autres matières radioactives non soumises à un contrôle réglementaire, n° 15 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2011).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev. 1), IAEA, Vienna (en préparation).

[8] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Sécurité de l'information nucléaire, n° 23-G de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2017).

[9] ORGANISATION INTERNATIONALE DE NORMALISATION, Technologies de l'information — Techniques de sécurité — Gestion des risques en sécurité de l'information, ISO/CEI 27005:2008, ISO, Genève (2008).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements, IAEA Nuclear Security Series No. 10-G (Rev. 1), IAEA, Vienna (2021).

[11] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Culture de sécurité nucléaire, n° 7 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2009).

[12] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Sûreté des centrales nucléaires : conception, n° SSR-2/1 (Rev. 1) de la collection Normes de sûreté de l'AIEA, AIEA, Vienne (2017).

Annexe I

PROPOSITIONS D'ORIENTATIONS DE CATÉGORIE RECOMMANDATIONS SUR LA SÉCURITÉ INFORMATIQUE DANS LE CADRE D'UN RÉGIME DE SÉCURITÉ NUCLÉAIRE NATIONAL

I-1. Les « ÉLÉMENTS D'UN RÉGIME DE SÉCURITÉ NUCLÉAIRE NATIONAL POUR LA SÉCURITÉ INFORMATIQUE » qui figurent dans la présente annexe ont été élaborés par des experts de plus de 20 États Membres pour compléter les Recommandations existantes publiées dans la collection Sécurité nucléaire de l'AIEA [I-1] à [I-3] et constituent des propositions d'orientations de catégorie Recommandations sur la conception, la mise en œuvre et le maintien de la sécurité informatique dans le cadre du régime de sécurité nucléaire d'un État. Les États peuvent décider de considérer ce texte comme des orientations de catégorie Recommandations. Les orientations qui figurent dans la partie principale de la présente publication sont compatibles avec les propositions d'orientations de catégorie Recommandations que contient la présente annexe.

GÉNÉRALITÉS

I-2. L'objet des Recommandations [I-1] à [I-3] qui ont été publiées dans la collection Sécurité nucléaire de l'AIEA est de donner des orientations aux États et à leurs autorités compétentes sur la manière de développer ou de renforcer, de mettre en place et de maintenir un régime de sécurité nucléaire national efficace afin d'assurer la sécurité des matières nucléaires, des installations nucléaires, des matières radioactives et des installations associées, et des matières nucléaires et autres matières radioactives non soumises à un contrôle réglementaire.

I-3. Les Recommandations publiées présentent les bonnes pratiques que les États Membres devraient adopter pour la mise en œuvre des Fondements de la sécurité nucléaire [I-4]. Ces Fondements énoncent qu'il incombe aux États de veiller à ce que les informations sensibles et les ressources d'informations sensibles soient protégées face aux menaces contre la sécurité nucléaire.

I-4. Une attaque contre la sécurité nucléaire peut prendre pour cible des informations sensibles ou des ressources d'informations sensibles afin de porter atteinte à des fonctions système de sécurité nucléaire ou de sûreté nucléaire. Elle peut être un acte de sabotage isolé ou entrer dans le cadre d'une attaque combinée contre une installation, qui peut associer une cyberattaque et une attaque physique,

ou contre une organisation afin d'avoir un accès non autorisé à des matières. La sécurité informatique fait donc partie intégrante du régime de sécurité nucléaire d'un État et est nécessaire pour que l'État puisse atteindre ses objectifs.

I-5. Les ressources numériques sensibles sont les ressources d'informations sensibles qui sont des systèmes informatiques et dont la compromission pourrait porter atteinte à la sécurité nucléaire. Elles nécessitent donc l'application de mesures de sécurité informatique.

I-6. Les mesures de sécurité informatique visent à maintenir la confidentialité, l'intégrité et la disponibilité des informations sensibles contenues dans les ressources numériques sensibles, ainsi que des ressources elles-mêmes.

I-7. Les publications existantes de catégorie Recommandations ne contiennent pas suffisamment d'orientations sur les mesures de sécurité informatique à appliquer pour protéger les ressources numériques sensibles.

OBJET

I-8. La présente annexe contient des propositions d'orientations sur la sécurité informatique pour la mise en œuvre des éléments essentiels des Fondements de la sécurité nucléaire [I-4] lorsqu'ils ne sont pas suffisamment traités dans les Recommandations [I-1] à [I-3]. Ces orientations ne visent en aucune manière à modifier les Recommandations existantes.

I-9. La présente annexe est destinée à être utilisée par les États, les autorités compétentes, les exploitants[1], les fournisseurs, les vendeurs, les sous-traitants, les spécialistes de la sécurité nucléaire et les spécialistes de la sûreté nucléaire.

CHAMP D'APPLICATION

I-10. Les présentes orientations s'appliquent aux aspects de la sécurité nucléaire qui concernent la sécurité informatique.

I-11. Les présentes orientations portent sur les aspects généraux de la sécurité informatique qui s'appliquent à tous les domaines de la sécurité nucléaire,

[1] Dans ce contexte, le terme « exploitants » désigne les titulaires de licence, les expéditeurs et les transporteurs.

notamment la sécurité des matières nucléaires et des installations nucléaires [I-1], des matières radioactives et des installations associées [I-2], et des matières nucléaires et autres matières radioactives non soumises à un contrôle réglementaire [I-3]. Il faudrait les mettre en œuvre en adoptant une approche graduée.

ÉLÉMENTS D'UN RÉGIME DE SÉCURITÉ NUCLÉAIRE NATIONAL POUR LA SÉCURITÉ INFORMATIQUE

Responsabilité de l'État

I-12. L'État devrait élaborer une stratégie de sécurité informatique[2] à l'appui de son régime de sécurité nucléaire.

Attribution des responsabilités en matière de sécurité informatique

I-13. L'État devrait désigner des autorités compétentes et leur confier la responsabilité de l'élaboration et de la mise en œuvre du cadre législatif et réglementaire pour la sécurité informatique, à l'appui du régime de sécurité nucléaire. L'autorité compétente pour la sécurité informatique et l'autorité compétente (ou les autorités compétentes) pour d'autres aspects de la sécurité nucléaire ne sont pas nécessairement les mêmes.

I-14. En matière de sécurité informatique, l'État devrait veiller à ce que les fonctions, les rôles et les autres attributions soient définis et étroitement coordonnés entre toutes les autorités compétentes concernées par la sécurité nucléaire et en leur sein.

Cadre législatif et réglementaire

I-15. L'État devrait veiller à ce que le cadre législatif et réglementaire comprenne des prescriptions de sécurité nucléaire pour la prévention et la détection des actes non autorisés qui sont commis contre des systèmes informatiques et qui peuvent porter atteinte à la sécurité nucléaire, et pour les interventions en pareil cas. Ces prescriptions devraient être utilisées pour l'évaluation de la menace qui est effectuée par l'État.

---

[2] Cette stratégie peut être propre au régime de sécurité nucléaire ou plus générale, comme la stratégie applicable à la protection des infrastructures critiques. Au lieu de stratégie, certains États parlent de « politique ».

I-16. L'État devrait mettre en place une procédure d'inspection et de coercition pour contrôler le respect des prescriptions de sécurité informatique qui font partie du cadre législatif et réglementaire.

I-17. L'État devrait veiller à ce que le cadre législatif et réglementaire prévoie des sanctions si un acte non autorisé qui est commis contre un système informatique peut porter atteinte à la sécurité nucléaire.

Autorités compétentes

I-18. Les autorités compétentes devraient veiller à ce que les exploitants élaborent et appliquent une politique de sécurité informatique et les programmes de sécurité informatique correspondants conformément aux prescriptions nationales relatives à la sécurité nucléaire.

I-19. Les autorités compétentes devraient veiller à ce que la sécurité informatique soit prise en considération pour l'évaluation et la procédure de délivrance des licences ou d'autres procédures qui sont appliquées pour la délivrance d'autorisations.

I-20. Les autorités compétentes devraient vérifier que les prescriptions de sécurité informatique sont continuellement respectées par l'exploitant en procédant régulièrement à des inspections et, si nécessaire, en ayant recours à la coercition afin que des mesures correctives soient prises.

Responsabilité des exploitants

I-21. Les exploitants devraient déterminer quelles sont les ressources numériques sensibles et les caractériser en fonction des conséquences possibles de leur compromission pour la sécurité nucléaire.

I-22. Les exploitants devraient définir des mesures de sécurité informatique appropriées[3] et veiller à ce que ces mesures soient mises en œuvre afin de protéger les ressources numériques sensibles contre la compromission pendant tout leur cycle de vie (dans toute la mesure du possible) conformément aux principes de l'approche graduée et de la défense en profondeur.

---

[3] Les mesures de sécurité peuvent être des mesures de contrôle physique, technique ou administratif.

I-23. Les exploitants devraient faire de la sécurité informatique un principe de conception pour les ressources numériques sensibles et leur utilisation, y compris pour la protection contre les accès non autorisés (par des personnes, des processus ou des appareils) et les logiciels malveillants.

I-24. Les exploitants devraient évaluer et gérer les mesures de sécurité informatique de telle manière qu'elles ne portent pas atteinte à la protection physique, à la sûreté nucléaire et aux activités de comptabilité et de contrôle des matières nucléaires.

I-25. Les exploitants devraient mener des activités d'assurance afin de vérifier que les mesures de sécurité informatique adoptées respectent les prescriptions de sécurité informatique.

I-26. Les exploitants devraient veiller à ce que les mesures de sécurité informatique soient prises en compte dans les dispositions qu'ils ont prises concernant la gestion de la chaîne d'approvisionnement nucléaire afin de réduire au minimum les vulnérabilités des systèmes informatiques et d'empêcher l'utilisation de la chaîne d'approvisionnement comme porte d'entrée pour une cyberattaque.

I-27. Les organismes publics, notamment les autorités compétentes, devraient suivre les recommandations qui figurent aux paragraphes I-21 à I-26 pour la protection des ressources numériques sensibles dont ils ont la responsabilité.

Coopération et assistance internationales

I-28. La coopération et l'assistance internationales devraient notamment porter sur des questions de sécurité informatique qui intéressent la sécurité nucléaire.

Identification et évaluation des menaces

I-29. L'évaluation de la menace effectuée par l'État[4] (et la menace de référence, s'il y a lieu) devrait envisager que des adversaires potentiels utilisent des moyens informatiques, y compris avec l'aide d'initiés et en lançant des attaques combinées. L'évaluation de la menace devrait être réexaminée et actualisée pour tenir compte de l'évolution de la cybermenace et devrait être dûment diffusée dans les meilleurs délais.

[4] Également appelée « évaluation nationale de la menace ».

I-30. Lorsque la menace de référence ou l'évaluation de la menace pour une cyberattaque est distincte de la menace de référence ou de l'évaluation de la menace pour une attaque physique, l'État devrait veiller à ce que l'évaluation de la menace (et la menace de référence, s'il y a lieu) soit élaborée de manière coordonnée.

Interface entre sûreté et sécurité

I-31. L'interface entre la sûreté et la sécurité, y compris la sécurité informatique, devrait être gérée de telle manière que ces domaines n'aient pas d'incidence négative l'un sur l'autre et qu'ils se renforcent mutuellement dans la mesure du possible.

Maintien de la sécurité informatique

I-32. La sécurité informatique devrait être traitée de manière intégrée et coordonnée dans le cadre du système de gestion de chaque autorité compétente et de chaque exploitant.

I-33. La sécurité informatique devrait être présentée comme un aspect essentiel de la culture de sécurité nucléaire.

I-34. La sécurité informatique devrait être intégrée aux programmes de pérennisation des autorités compétentes et des exploitants et devrait bénéficier de moyens suffisants.

Planification, préparation et intervention en cas d'incident de sécurité informatique

I-35. L'État devrait s'assurer que les autorités compétentes, les exploitants et les autres parties concernées disposent de plans d'intervention spécialisés et de moyens d'intervention d'urgence pour faire face convenablement aux incidents de sécurité informatique qui peuvent porter atteinte à la sécurité nucléaire.

I-36. L'État devrait s'assurer que les autorités compétentes, les exploitants et les autres parties concernées effectuent régulièrement des exercices afin d'évaluer la pertinence des parties des plans d'intervention qui portent sur la sécurité informatique.

I-37. Le régime de sécurité nucléaire national devrait prévoir des prescriptions concernant le signalement sans délai des incidents de sécurité informatique à l'autorité compétente (ou aux autorités compétentes).

RÉFÉRENCES POUR L'ANNEXE I

[I-1] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Recommandations de sécurité nucléaire sur la protection physique des matières nucléaires et des installations nucléaires (INFCIRC/225/Révision 5), nº 13 de la collection Sécurité nucléaire de l'AIEA , AIEA, Vienne (2011).

[I-2] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Recommandations de sécurité nucléaire relatives aux matières radioactives et aux installations associées, nº 14 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2011).

[I-3] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, INSTITUT INTERRÉGIONAL DE RECHERCHE DES NATIONS UNIES SUR LA CRIMINALITÉ ET LA JUSTICE, OFFICE DES NATIONS UNIES CONTRE LA DROGUE ET LE CRIME, OFFICE EUROPÉEN DE POLICE, ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE, ORGANISATION INTERNATIONALE DE POLICE CRIMINELLE-INTERPOL, ORGANISATION MONDIALE DES DOUANES, Recommandations de sécurité nucléaire sur les matières nucléaires et autres matières radioactives non soumises à un contrôle réglementaire, nº 15 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2011).

[I-4] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Objectif et éléments essentiels du régime de sécurité nucléaire d'un État, nº 20 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2014).

Annexe II

PROFILS DE CYBERMENACE

II-1. Il est important de comprendre la cybermenace pour pouvoir élaborer et mettre en œuvre des mesures de protection. La cybermenace diffère de la menace physique contre les matières nucléaires, les autres matières radioactives et les installations et activités associées. Elle n'est pas limitée par la proximité avec le lieu concerné, par le nombre d'assaillants ou par le périmètre de l'installation prise pour cible. La connaissance des caractéristiques de la cybermenace et des scénarios d'attaque possibles est précieuse pour les mesures de prévention et d'intervention. Les adversaires, leurs outils, leurs tactiques et leurs cibles sont des éléments dynamiques, et il faut constamment s'attacher à évaluer la menace actuelle.

II-2. Les tendances prédominantes sont notamment les suivantes [II-1], [II-2] :

a) nombre croissant d'adversaires ayant les moyens de lancer des cyberattaques ;
b) nombre croissant d'individus et de groupes qui proposent la « cybercriminalité en tant que service », ce qui facilite la tâche aux adversaires qui ne disposaient pas auparavant des compétences nécessaires ;
c) complexité grandissante des techniques utilisées pour les cyberattaques, ce qui rend la détection et les interventions plus difficiles ;
d) usage constant de l'ingénierie sociale dans le cadre des cyberattaques, et notamment des techniques du « hameçonnage ciblé » et du « point d'eau » ;
e) les adversaires s'attachent de plus en plus à détecter et à exploiter les vulnérabilités des systèmes de contrôle industriel ;
f) multiplication des logiciels rançonneurs ;
g) difficulté constante à protéger la chaîne d'approvisionnement contre les cyberattaques.

II-3. Au minimum, l'autorité compétente pour l'évaluation de la cybermenace, l'autorité compétente pour la sécurité informatique et les exploitants qui participent à l'évaluation de la menace doivent prendre en considération les attributs et les caractéristiques qui sont énumérés dans la section suivante pour chaque menace interne ou externe identifiée. La caractérisation de la cybermenace est délicate, car il est difficile de savoir qui sont les assaillants et les attaques peuvent être anonymes. Il peut néanmoins être utile d'établir des profils de menace.

ATTRIBUTS ET CARACTÉRISTIQUES DE LA CYBERMENACE

II-4. Les caractéristiques et attributs suivants de la cybermenace peuvent être utiles pour établir des profils de menace :

a) motivation : politique, financière, idéologique ou personnelle ;
b) intentions : saboter des matières radioactives ou une installation radiologique, voler des matières radioactives ou nucléaires, semer la panique dans la population et provoquer des perturbations sociales, créer une instabilité politique, faire de nombreux morts et blessés, voler des informations sensibles ;
c) compétences : aptitude à utiliser des systèmes informatiques et des systèmes de commande automatisés pour appuyer directement des attaques physiques, pour recueillir des renseignements, pour lancer des cyberattaques et pour collecter des fonds ;
d) connaissances : cibles, plans et procédures de site, mesures de sécurité, mesures de sûreté et procédures de radioprotection, activités, utilisation possible des matières nucléaires ou d'autres matières radioactives ;
e) financement : source, montant et disponibilité ;
f) tactiques : tendre un piège ou recourir à la ruse ou à la force.

DESCRIPTION GÉNÉRALE DE LA CYBERMENACE

II-5. Les catégories de menaces peuvent être établies de différentes manières. Les catégories suivantes sont présentées à titre d'exemple (certaines peuvent se chevaucher).

II-6. Menace interne : la menace interne est l'une des attaques contre lesquelles il est le plus difficile de se défendre. Le terme « initié » désigne toute personne bénéficiant d'un accès autorisé à des installations associées ou des activités associées ou à des informations sensibles ou des ressources d'informations sensibles, qui pourrait commettre un acte criminel ou des actes non autorisés délibérés mettant en jeu ou visant des matières nucléaires, d'autres matières radioactives, des installations ou activités associées, ou d'autres actes que l'État considère comme nuisant à la sécurité nucléaire, ou en faciliter la commission [II-3]. L'initié est une personne à qui l'on fait confiance, qui a suivi une formation sur les systèmes internes et qui, pour une raison quelconque, utilise son accès et ses connaissances de manière compromettante et potentiellement malveillante. Les raisons qui poussent une personne à devenir un initié sont très diverses, et cette catégorie comprend aussi bien des salariés mécontents que

des agents infiltrés. L'initié involontaire constitue un cas particulier. Un initié involontaire est un initié n'ayant ni l'intention ni la motivation de commettre un acte malveillant qui est exploité à son insu par un adversaire [II-3].

II-7. Extrémiste : le terme « extrémisme » s'applique aux groupes dont l'expression politique ou sociale sort de la norme (c'est un activisme qui se manifeste par des comportements inacceptables). Des extrémistes peuvent commettre un acte individuel ou peuvent se coordonner vaguement avec des individus ayant le même état d'esprit pour lancer une cyberattaque contre une certaine cible. Ces groupements ne sont pas toujours étroitement contrôlés par un personnage central et n'appliquent pas toujours des règles d'engagement précises.

II-8. Pirate amateur : l'expression « pirates amateurs » désigne les individus ou les groupes qui sont motivés par la célébrité ou la notoriété, plutôt que par le désir d'infliger des dommages ou par l'appât du gain. Les compromissions provoquées par les pirates amateurs peuvent être non ciblées (c'est-à-dire que l'installation nucléaire n'était pas spécifiquement visée) et peuvent au contraire s'expliquer par un environnement hostile. Un système de commande d'une installation nucléaire peut par exemple être infecté par un virus ordinaire à cause d'une gestion défaillante des appareils portatifs et des supports amovibles.

II-9. Groupe criminel organisé : des groupes criminels organisés ont élaboré des cyberattaques très complexes et très ciblées contre plusieurs secteurs d'activité. L'objectif est le gain monétaire, qui peut être obtenu directement par le vol d'argent ou indirectement par la vente de données volées ou d'informations sur une compromission à d'autres menaces.

II-10. État-nation : les États-nations constituent souvent une menace dotée de solides compétences et très persistante. Les motivations et les objectifs des attaques correspondantes se limitent normalement à la collecte d'informations, et les attaques sont souvent soumises à des règles d'engagement structurées.

II-11. Terroriste : jusqu'à présent, les cyberattaques attribuées à des terroristes ont le plus souvent pris la forme d'actions simples comme le bombardement de la messagerie d'ennemis idéologiques, les attaques par déni de service ou la défiguration de sites web, mais les terroristes pourraient acquérir de plus en plus de compétences techniques pour lancer des attaques basées sur le réseau. Les terroristes pourraient disposer de ces compétences en interne ou faire appel à des pirates [I-4]. Ils peuvent prendre pour cible et tenter de saboter des infrastructures critiques, par exemple des centrales nucléaires, mais leur objectif peut aussi consister à s'emparer de matières nucléaires et d'autres matières radioactives.

CARACTÉRISTIQUES DES ATTAQUES

II-12. Il importe également de connaître les caractéristiques des attaques afin d'élaborer des mesures de dissuasion, de prévention, de détection, d'atténuation et d'intervention. Plusieurs types d'attaques sont décrits dans les sections suivantes (les catégories ne s'excluent pas mutuellement).

Attaque non ciblée

II-13. Bon nombre des menaces décrites plus haut sont susceptibles de lancer des attaques contre des cibles de sécurité nucléaire précises. Cependant, des attaques non ciblées peuvent également se produire : des programmes malveillants non guidés peuvent par exemple être introduits par erreur dans des systèmes informatiques et des réseaux et porter ainsi atteinte à la sécurité nucléaire. Un système de commande d'une installation nucléaire peut notamment être infecté par un virus ordinaire à cause d'une gestion défaillante des dispositifs mobiles.

Attaques persistantes

II-14. Une cyberattaque peut être lancée pour obtenir des effets immédiats ou peut s'inscrire dans une campagne de longue durée contre une installation ou une organisation. Une attaque persistante peut commencer par la compromission d'un système informatique et se poursuivre par une longue campagne de collecte d'informations. Le résultat peut être un événement ayant de réelles conséquences ou l'objectif de l'attaque peut être uniquement de s'infiltrer pour une activité future.

Attaques combinées

II-15. Les attaques combinées sont des actes coordonnés qui se composent d'une cyberattaque et d'un acte physique. Une cyberattaque peut par exemple compromettre un système de contrôle de l'accès physique pour permettre à des personnes non autorisées de pénétrer physiquement dans une zone.

TABLEAUX DES PROFILS DE MENACE

II-16. Les tableaux II-1 et II-2 présentent un ensemble possible de profils d'assaillants. Le tableau II-1 porte sur les menaces internes (voir aussi la référence [II-3]) et le tableau II-2 recense les menaces externes possibles. Ces tableaux décrivent les grands types d'assaillants, les ressources dont ils disposent, la durée

des attaques, les outils qu'ils sont susceptibles d'utiliser et leurs motivations. Les profils doivent être adaptés à chaque situation.

RÉFÉRENCES POUR L'ANNEXE II

[II-1] AUSTRALIAN CYBER SECURITY CENTRE, ACSC 2015 Threat Report (2015), www.cyber.gov.au/sites/default/files/2020-04/ACSC_Threat_Report_2015.pdf

[II-2] GEORGIA INSTITUTE OF TECHNOLOGY, Emerging Cyber Threats Report 2016 (2015), https://iisp.gatech.edu/sites/default/files/documents/threats_report_2016.pdf

[II-3] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Mesures de prévention et de protection contre les menaces internes, nº 8-G (Rev. 1) de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2020).

[II-4] CONGRESSIONAL RESEARCH SERVICE, Terrorist Use of the Internet: Information Operations in Cyberspace (2011), www.hsdl.org/?view&did=8233

TABLEAU II-1. MENACES INTERNES

Menace	Ressources (compétences, connaissances, accès, financement)	Durée	Tactiques	Motivation	Intentions
Agent infiltré	Facilite l'« ingénierie sociale » Accès au système à un certain niveau Documentation et connaissances spécialisées à disposition concernant le système	Variable, mais l'assaillant ne peut généralement pas y consacrer de longues heures en dehors de ses activités de travail normales	Accès existant, connaissance de la programmation et de l'architecture du système Connaissance possible de mots de passe existants Possibilité d'introduire des portes dérobées ou des chevaux de Troie spécialement mis au point Appui spécialisé externe possible Peut être contrôlé par un responsable externe	Politique, financière, idéologique	Vol d'informations internes, de secrets industriels, de données personnelles Sabotage

TABLEAU II-1. MENACES INTERNES (suite)

Menace	Ressources (compétences, connaissances, accès, financement)	Durée	Tactiques	Motivation	Intentions
Initié agissant sous la contrainte	Accès au système à un certain niveau Documentation et connaissances spécialisées à disposition concernant le système	Variable, mais l'assaillant ne peut généralement pas y consacrer de longues heures en dehors de ses activités de travail normales	Accès existant, connaissance de la programmation et de l'architecture du système Connaissance possible de mots de passe existants Possibilité d'introduire des portes dérobées ou des chevaux de Troie spécialement mis au point Appui spécialisé externe possible Contrôlé par un responsable externe	Personnelle	Vol d'informations internes, de secrets industriels, de données personnelles Sabotage
Initié involontaire	Accès au système dans le cadre des activités de travail normales		Donne involontairement un accès interne à un adversaire	Aucune motivation requise	

TABLEAU II-1. MENACES INTERNES (suite)

Menace	Ressources (compétences, connaissances, accès, financement)	Durée	Tactiques	Motivation	Intentions
Salarié ou utilisateur du système mécontents (plusieurs types)					
Actuellement en poste – utilisateurs d'ordinateurs non spécialisés	Ressources moyennes/importantes Accès au système à un certain niveau Documentation et connaissances spécialisées à disposition sur certains systèmes administratifs et opérationnels	Variable, mais l'assaillant ne peut généralement pas y consacrer de longues heures (n'est pas nécessairement compétent pour tout)	Accès existant, connaissance de la programmation et de l'architecture du système Connaissance possible de mots de passe existants Aptitude à introduire des outils ou scripts « amateurs » (parfois plus élaborés s'il dispose de compétences informatiques particulières)	Personnelle, financière	Vengeance, dégâts, chaos Vol d'informations internes Nuire à l'employeur ou à un autre salarié Dégrader l'image de marque ou la confiance

TABLEAU II-1. MENACES INTERNES (suite)

Menace	Ressources (compétences, connaissances, accès, financement)	Durée	Tactiques	Motivation	Intentions
Actuellement en poste – utilisateurs d'ordinateurs spécialisés, administrateurs, développeurs, etc...	Large accès informatique et grandes compétences en informatique Accès à distance possible	Très longue		Personnelle, financière	
Actuellement sous contrat – tiers	Accès local ou à distance, et peut-être un rôle d'appui	Variable	Introduction de composants altérés dans des maillons de la chaîne d'approvisionnement Infiltration par des dispositifs mobiles ou des connexions à distance	Personnelle, financière	

TABLEAU II-1. MENACES INTERNES (suite)

Menace	Ressources (compétences, connaissances, accès, financement)	Durée	Tactiques	Motivation	Intentions
Anciens salarié ou utilisateur mécontents	Ressources limitées s'il ne collabore pas avec un groupe plus large Possède peut-être encore des documents sur le système Peut se servir d'un ancien accès non contrôlé Liens possibles avec des membres du personnel de l'installation	Variable et dépend du groupe avec lequel l'assaillant coopère	Connaissance possible de mots de passe existants L'assaillant peut se servir d'un ancien accès non contrôlé Il peut avoir créé des portes dérobées dans le système lorsqu'il était encore en poste « Ingénierie sociale »	Personnelle	Vengeance, dégâts, chaos Vol d'informations internes Nuire à l'employeur ou à un autre salarié Dégrader l'image de marque ou la confiance

TABLEAU II-2. MENACES EXTERNES

Menace	Ressources (compétences, connaissances, accès, financement)	Durée	Tactiques	Motivation	Intentions
Attaque non ciblée	Compétences diverses	Variable	Pas de cible précise, utilise généralement des processus informatiques habituels et exploite des vulnérabilités, y compris l'ingénierie sociale	Personnelle – divertissement, statut	Célébrité, attention des médias Compromission d'une cible fortuite
Extrémiste	Compétences diverses, mais généralement limitées Peu de connaissances du système en dehors des informations publiquement disponibles	Peut être soumis à des contraintes de temps, car ses activités peuvent concerner des événements actuels ou récents	Activités de piratage individuelles ou en petit groupe Envoi d'outils à des groupements plus grands	Résolu à obtenir un effet politique	Attention des médias Mettre publiquement dans une situation embarrassante

TABLEAU II-2. MENACES EXTERNES (suite)

Menace	Ressources (compétences, connaissances, accès, financement)	Durée	Tactiques	Motivation	Intentions
Pirate amateur	Compétences diverses, mais généralement limitées Peu de connaissances du système en dehors des informations publiquement disponibles	Très longue, l'assaillant n'est pas très patient	Scripts et outils généralement disponibles Mise au point d'outils possible	Personnelle – divertissement, statut	Compromission d'une cible fortuite Exploitation des vulnérabilités les plus simples
Groupe criminel organisé	Ressources importantes Recours à des compétences spécialisées	Variable, mais courte la plupart du temps	Scripts, outils « maison » L'assaillant peut engager un pirate contre rémunération Il peut engager un ancien salarié ou un salarié actuellement en fonctions « Ingénierie sociale »	Chantage Extorsion (de fonds) Exploitation des craintes du secteur sur le plan financier et de l'image Vente d'informations (techniques, internes ou personnelles)	Vol de matières Vol d'informations sensibles Vente d'informations ou d'un accès

TABLEAU II-2. MENACES EXTERNES (suite)

Menace	Ressources (compétences, connaissances, accès, financement)	Durée	Tactiques	Motivation	Intentions
État-nation	Ressources et compétences importantes Activités de collecte de renseignements Formation sur le système ou expérience concrète du système possibles Équipes d'experts spécialisés	Variable, mais peut lancer des attaques de longue durée	Outils complexes L'assaillant peut engager un ancien salarié ou un salarié actuellement en fonctions « Ingénierie sociale »	Politique Collecte de renseignements Création de points d'accès pour des actions ultérieures	Vol de technologies Reconnaissance pour de futures attaques Sabotage

TABLEAU II-2. MENACES EXTERNES (suite)

Menace	Ressources (compétences, connaissances, accès, financement)	Durée	Tactiques	Motivation	Intentions
Terroriste	Compétences diverses Formation sur le système ou expérience concrète du système possibles Recours possible à un agent infiltré Peut disposer de fonds importants Compétences grandissantes	Très longue, l'assaillant est très patient	Scripts, outils « maison » L'assaillant peut engager un pirate contre rémunération Il peut engager un ancien salarié ou un salarié actuellement en fonctions « Ingénierie sociale »	Collecte de renseignements Création de points d'accès pour des actions ultérieures Chaos Vengeance Toucher l'opinion publique (peur)	Appui à des attaques combinées Reconnaissance pour de futures attaques Sabotage Vol de matières

Annexe III

ATTRIBUTION DES RESPONSABILITÉS RELATIVES À LA SÉCURITÉ INFORMATIQUE

III-1. Le tableau III-1 présente un exemple type d'attribution de responsabilités aux autorités compétentes. Il peut être utile de créer un tableau de responsabilités habituelles en sécurité informatique qui corresponde à ces responsabilités types en sécurité nucléaire.

TABLEAU III-1. EXEMPLE TYPE DE RESPONSABILITÉS RELATIVES À LA SÉCURITÉ INFORMATIQUE DANS UN RÉGIME DE SÉCURITÉ NUCLÉAIRE

Type d'entité	Responsabilités en matière de sécurité nucléaire
Organisme de réglementation	Instaurer un régime de contrôle réglementaire des matières radioactives, des installations associées et des activités associées qui rend des personnes autorisées responsables au premier chef de la sécurité nucléaire Créer un système de catégorisation axée sur la sécurité Créer et tenir à jour un registre national des matières radioactives Participer à l'évaluation nationale de la menace Définir et utiliser la menace de référence, élaborer et utiliser un autre énoncé de la menace ou utiliser une autre menace définie afin d'établir une réglementation en matière de sécurité Appliquer la procédure d'autorisation (d'octroi de licence), y compris l'examen et l'évaluation des systèmes de sécurité et des mesures de gestion de la sécurité Établir des prescriptions réglementaires et fournir des directives en matière de sécurité, notamment des prescriptions touchant la protection de l'information Gérer l'interface entre la sûreté et la sécurité Conduire des inspections de sécurité Prendre des mesures coercitives en cas de non-respect des prescriptions applicables Alimenter des bases de données régionales et internationales et participer à d'autres activités de coopération

TABLEAU III-1. EXEMPLE TYPE DE RESPONSABILITÉS RELATIVES À LA SÉCURITÉ INFORMATIQUE DANS UN RÉGIME DE SÉCURITÉ NUCLÉAIRE (suite)

Type d'entité	Responsabilités en matière de sécurité nucléaire
	Encourager et promouvoir une solide culture de sécurité nucléaire Participer à la planification, à la préparation et à la conduite des interventions en cas d'événement de sécurité nucléaire, y compris dans le cadre d'exercices Administrer les processus d'autorisation et de contrôle des importations et des exportations de matières radioactives Notifier aux exploitants toute menace spécifique ou accrue Examiner et évaluer la conception du système de sécurité (dans le cadre de la procédure d'autorisation)
Forces de l'ordre	Intervenir pour interrompre un acte malveillant (accès non autorisé, enlèvement non autorisé, sabotage) Participer à la planification, à la préparation et à la conduite des interventions en cas d'événement de sécurité nucléaire, y compris dans le cadre d'exercices Participer à l'évaluation nationale de la menace Identifier des menaces spécifiques ou accrues Vérifier les antécédents à des fins d'habilitation Détecter les événements de sécurité nucléaire et enquêter à leur sujet
Douanes et police des frontières	Participer à l'évaluation nationale de la menace Identifier des menaces spécifiques ou accrues Contrôler les importations et les exportations et détecter les cas de non-respect des prescriptions applicables Communiquer avec l'organisme de réglementation en ce qui concerne l'inventaire national des matières radioactives
Services de renseignement et de sécurité	Évaluation nationale directe de la menace Identifier des menaces spécifiques ou accrues
Agence nationale chargée des interventions d'urgence	Coordonner la planification, la préparation et les interventions en cas d'événement de sécurité nucléaire
Organismes de défense civile, services de santé et agences de l'environnement	Participer à la planification, à la préparation et aux interventions en cas d'événement de sécurité nucléaire

TABLEAU III-1. EXEMPLE TYPE DE RESPONSABILITÉS RELATIVES À LA SÉCURITÉ INFORMATIQUE DANS UN RÉGIME DE SÉCURITÉ NUCLÉAIRE (suite)

Type d'entité	Responsabilités en matière de sécurité nucléaire
Ministère de la justice et parquet	Infliger des sanctions aux auteurs d'actes malveillants
Ministère des affaires étrangères	Participer à la coopération régionale et internationale

Annexe IV

EXEMPLE DE CADRE DE COMPÉTENCES ET DE NIVEAUX DE CAPACITÉ POUR LA SÉCURITÉ INFORMATIQUE

IV-1. La mise en place d'un cadre de compétences et de niveaux de capacité contribue de manière déterminante à ce que les organisations et les personnes soient et restent compétentes dans l'exercice de leur rôle et de leurs responsabilités en matière de sécurité informatique.

IV-2. La présente annexe illustre ce que l'on entend par cadre de compétences et niveaux de capacité. Elle ne vise pas à donner des orientations suffisantes pour pouvoir élaborer un tel cadre.

IV-3. Pour chaque organisation ou individu, le cadre recense les compétences nécessaires pour des aspects particuliers de la sécurité informatique. Ces aspects peuvent par exemple être les suivants :

a) gestion (capacités, stratégie, gestion de crise, gouvernance, organisation) ;
b) intervention en cas d'incident (informatique judiciaire, lutte informatique défensive) ;
c) cadre législatif et réglementaire (droit pénal, réglementation) ;
d) sécurité et gestion de l'information (cryptographie, cryptage, stockage) ;
e) achats (contrats, chaîne d'approvisionnement) ;
f) activités d'assurance (tests, accréditation, gestion de la configuration) ;
g) architecture de sécurité informatique ;
h) coordination et assistance internationales.

Les normes internationales ISO 27002 [IV–1] (pour les systèmes de gestion de la sécurité de l'information) et CEI 63096 [IV–2] (norme ISO 27002 appliquée aux centrales nucléaires) contiennent également des listes de domaines de contrôle qui peuvent être adaptées pour être utilisées comme domaines de compétences.

IV-4. Le cadre énumère les capacités et les connaissances particulières en sécurité informatique qui sont nécessaires pour chaque compétence, en s'appuyant sur l'évaluation de la menace concernant les cyberattaques, sur la connaissance de la nature des systèmes informatiques qui sont utilisés dans le cadre du régime de sécurité nucléaire et sur la connaissance des vulnérabilités de ces systèmes.

IV-5. Les organisations et les individus ne présentent pas tous le même niveau de maturité concernant les compétences en sécurité informatique. Le cadre classe le niveau de capacité dans chaque compétence à l'aide d'une échelle qui compte au moins trois niveaux. Cette méthode permet de mettre en œuvre une approche graduée. Exemple de classement de la maturité, de la plus faible à la plus grande :

a) Basique (débutant) : présente un comportement automatique et fondé sur les règles, qui est très limité et inflexible.
b) Intermédiaire (professionnel) : agit consciemment pour respecter des objectifs et des plans à long terme dans le cadre d'une politique constante.
c) Poussée (expert) : comprend intuitivement la situation, est capable de s'occuper immédiatement des aspects essentiels.

IV-6. Des niveaux de capacité plus élevés sont nécessaires pour assurer une protection contre les menaces à fortes capacités ou pour prévenir de graves conséquences radiologiques. On considère par exemple que des autorités compétentes et des exploitants qui entreposent, transportent ou utilisent des matières nucléaires de catégorie I ou II, ou qui exploitent des installations ou exercent des activités pouvant avoir de graves conséquences radiologiques, gèrent des conséquences graves ou très graves.

IV-7. Le cadre garantit que les organisations et les individus qui sont chargés de la conception des mesures de sécurité informatique ont de grandes compétences dans le domaine concerné.

IV-8. Certaines organisations exigent que ces capacités soient continuellement présentes sur le site, tandis que d'autres comptent sur l'aide d'autres organisations.

IV-9. Le cadre décrit en détail le profil habituel des activités qu'une autorité compétente, un exploitant ou un tiers peut être autorisé à exercer. Ainsi, une autorité compétente ou un exploitant ayant les compétences nécessaires à un niveau poussé peut jouer un rôle moteur dans les activités d'évaluation nationale de la menace qui concernent la sécurité informatique. En revanche, une autorité compétente ou un exploitant qui a des compétences de niveau basique ne peut jouer qu'un rôle d'appui pour l'évaluation nationale de la menace. Ces différences sont présentées dans le tableau IV-1.

TABLEAU IV-1. CLASSEMENT DES ACTIVITÉS EN FONCTION DU NIVEAU DE COMPÉTENCE

Type d'activité	Parties prenantes de niveau basique	Parties prenantes de niveau intermédiaire (activités supplémentaires par rapport au niveau basique)	Parties prenantes de niveau poussé (activités supplémentaires par rapport au niveau intermédiaire)
Activités qui concernent la connaissance de la situation sur le plan de la menace	A une connaissance de base des agissements de la menace (comme les attaques par hameçonnage)	Comprend les conséquences des menaces contre la sécurité informatique pour sa propre situation	Surveille constamment et de manière proactive des menaces contre la sécurité informatique qui évoluent rapidement
Activités relatives aux évaluations de la menace et à l'élaboration de scénarios	Contribution sur demande (donne par exemple des détails concrets sur la manière dont les choses se déroulent réellement sur le lieu de travail)	Participe à l'évaluation nationale de la menace Élabore des scénarios pour un site particulier à partir de l'évaluation de la menace lorsque les conséquences possibles sont moyennes, faibles ou très faibles	Rôle moteur dans les activités d'évaluation nationale de la menace Élabore des scénarios pour un site particulier lorsque les conséquences possibles sont graves ou très graves Évalue les scénarios élaborés par des parties prenantes de niveau intermédiaire

RÉFÉRENCES POUR L'ANNEXE IV

[IV-1] ORGANISATION INTERNATIONALE DE NORMALISATION, Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information, ISO/IEC 27002:2013, ISO, Genève (2013).

[IV-2] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation, Control and Electrical Power Systems — Security Controls, IEC 63096:2020, IEC, Geneva (2020).

GLOSSAIRE

attaque combinée. Acte malveillant consistant dans le lancement coordonné d'une cyberattaque et d'une attaque physique.

cyberattaque. Acte malveillant destiné à empêcher d'avoir accès à une cible particulière ou à la voler, la modifier ou la détruire par accès non autorisé à un système informatique sensible (ou par des actions dans un tel système).

incident de sécurité informatique. Incident qui nuit ou peut nuire à la confidentialité, à l'intégrité, ou à la disponibilité d'un système informatique (y compris les données qu'il contient), ou qui constitue une violation des règles de sécurité ou présente un risque imminent de violation de ces règles.

information sensible. Information, sous quelque forme que ce soit, y compris les logiciels, dont la divulgation, la modification, l'altération, la destruction, ou le refus d'utilisation non autorisés pourrait compromettre la sécurité nucléaire.

mesures de sécurité informatique. Mesures destinées à prévenir, détecter ou retarder, contrer et atténuer les conséquences d'actes malveillants ou d'autres actes qui pourraient compromettre la sécurité informatique.

niveau de sécurité informatique. Degré de protection requis pour répondre aux besoins de sécurité informatique concernant une fonction relative à la sécurité nucléaire, à la sûreté nucléaire, à la comptabilité et au contrôle des matières nucléaires ou à la gestion des informations sensibles.

programme de sécurité informatique (PSI). Plan appliqué pour mettre en œuvre la stratégie de sécurité informatique, où sont définis les rôles, les responsabilités et les procédures au sein d'un organisme. Il décrit précisément les moyens d'atteindre les objectifs de sécurité informatique et fait partie du plan général de sécurité (ou s'y rattache).

ressources d'informations sensibles. Tout équipement ou composant utilisé pour entreposer, traiter, contrôler ou transmettre des informations sensibles. Les ressources d'informations sensibles comprennent les systèmes de contrôle, les réseaux, les systèmes d'information et tout autre support électronique ou physique.

ressources numériques sensibles (RNS). Ressources d'informations sensibles qui sont des systèmes informatiques (ou en font partie).

sécurité de l'information. Protection de la confidentialité, de l'intégrité et de la disponibilité des informations.

sécurité informatique. Partie de la sécurité de l'information qui concerne la protection des systèmes informatiques contre toute compromission.

systèmes informatiques. Dispositifs techniques qui produisent, traitent, calculent, communiquent ou stockent des données numériques, y donnent accès, ou assurent, fournissent ou contrôlent des services qui utilisent de telles données.

ⓘ Ces systèmes peuvent être physiques ou virtuels. Ils peuvent comprendre des ordinateurs de bureau, des ordinateurs portables, des tablettes et d'autres ordinateurs personnels, des smartphones, des ordinateurs centraux, des serveurs, des ordinateurs virtuels, des logiciels, des bases de données, des supports amovibles, des appareils de contrôle-commande numérique, des automates programmables, des imprimantes, des dispositifs réseau et des composants et des dispositifs embarqués.

zone de sécurité informatique. Ensemble de systèmes ayant des limites physiques ou logiques communes – et défini si nécessaire à l'aide de critères supplémentaires – auquel est attribué un seul niveau de sécurité informatique afin de simplifier la gestion, la communication et l'application des mesures de sécurité informatique.

IAEA
Agence internationale de l'énergie atomique

Nº 26

OÙ COMMANDER ?

Vous pouvez vous procurer les publications de l'AIEA disponibles à la vente chez nos dépositaires ci-dessous ou dans les grandes librairies.

Les publications non destinées à la vente doivent être commandées directement à l'AIEA. Les coordonnées figurent à la fin de la liste ci-dessous.

AMÉRIQUE DU NORD

Bernan / Rowman & Littlefield
15250 NBN Way, Blue Ridge Summit, PA 17214 (États-Unis d'Amérique)
Téléphone : +1 800 462 6420 • Télécopie : +1 800 338 4550
Courriel : orders@rowman.com • Site web : www.rowman.com/bernan

Renouf Publishing Co. Ltd
22-1010 Polytek Street, Ottawa, ON K1J 9J1 (Canada)
Téléphone : +1 613 745 2665 • Télécopie : +1 613 745 7660
Courriel : order@renoufbooks.com • Site web : www.renoufbooks.com

RESTE DU MONDE

Veuillez-vous adresser à votre libraire préféré ou à notre principal distributeur :

Eurospan Group
Gray's Inn House
127 Clerkenwell Road
London EC1R 5DB
(Royaume-Uni)

Commandes commerciales et renseignements :
Téléphone : +44 (0) 176 760 4972 • Télécopie : +44 (0) 176 760 1640
Courriel : eurospan@turpin-distribution.com

Commandes individuelles :
www.eurospanbookstore.com/iaea

Pour plus d'informations :
Téléphone : +44 (0) 207 240 0856 • Télécopie : +44 (0) 207 379 0609
Courriel : info@eurospangroup.com • Site web : www.eurospangroup.com

Les commandes de publications destinées ou non à la vente peuvent être adressées directement à :

Unité de la promotion et de la vente
Agence internationale de l'énergie atomique
Centre international de Vienne, B.P. 100, 1400 Vienne (Autriche)
Téléphone : +43 1 2600 22529 ou 22530 • Télécopie : +43 1 26007 22529
Courriel : sales.publications@iaea.org • Site web : https://www.iaea.org/fr/publications

Cette publication donne des orientations sur la conception et la mise en œuvre de la sécurité informatique comme élément essentiel de la sécurité nucléaire. Elle porte sur les aspects de la sécurité nucléaire qui concernent la sécurité informatique et à leur interface avec la sûreté nucléaire et d'autres éléments d'un régime de sécurité nucléaire national, notamment la sécurité des matières nucléaires et des installations nucléaires, des matières radioactives et des installations associées, et des matières nucléaires ou d'autres matières radioactives non soumises à un contrôle réglementaire. Elle aborde notamment les thèmes suivants : systèmes informatiques dont la compromission pourrait porter atteinte à la sécurité nucléaire ou à la sûreté nucléaire ; rôle et responsabilités de l'État et des autres entités concernées en matière de sécurité informatique dans le cadre du régime de sécurité nucléaire ; activités qui sont menées par l'État afin de mettre en place et d'appliquer une stratégie de sécurité informatique pour la sécurité nucléaire ; éléments des programmes de sécurité informatique ; activités qui permettent de maintenir la sécurité informatique dans le cadre du régime de sécurité nucléaire.

AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE
VIENNE