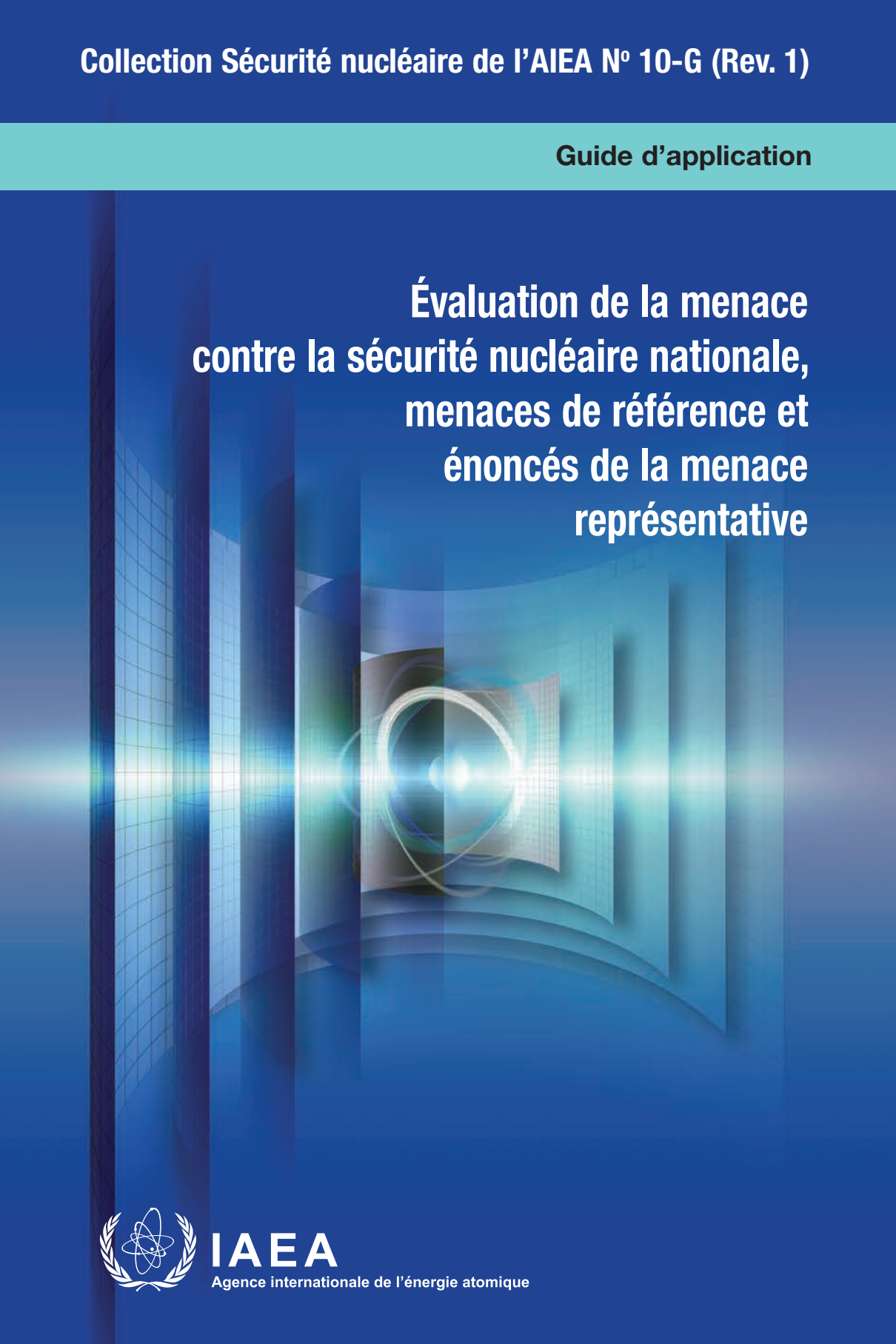
Collection Sécurité nucléaire de l'AIEA Nº 10-G (Rev. 1)

Guide d'application

Évaluation de la menace contre la sécurité nucléaire nationale, menaces de référence et énoncés de la menace représentative



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.

ÉVALUATION DE LA MENACE CONTRE LA SÉCURITÉ NUCLÉAIRE NATIONALE, MENACES DE RÉFÉRENCE ET ÉNONCÉS DE LA MENACE REPRÉSENTATIVE

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 10-G
(Rev. 1)

ÉVALUATION DE LA MENACE CONTRE LA SÉCURITÉ NUCLÉAIRE NATIONALE, MENACES DE RÉFÉRENCE ET ÉNONCÉS DE LA MENACE REPRÉSENTATIVE

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
Novembre 2022
STI/PUB/1926

ÉVALUATION DE LA MENACE CONTRE LA SÉCURITÉ NUCLÉAIRE NATIONALE, MENACES DE RÉFÉRENCE ET ÉNONCÉS DE LA MENACE REPRÉSENTATIVE
AIEA, VIENNE, 2022
STI/PUB/1926
ISBN 978-92-0-240821-0 (imprimé) 978-92-0-240321-5 (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 le cadre de sa mission centrale d'assistance et de coordination internationales concernant la 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 veiller à ce que l'AIEA entretienne et améliore cet ensemble intégré, complet et cohérent de publications de qualité adaptées à l'utilisateur, aux réalités de l'époque et aux besoins en matière de sécurité. L'utilisation adéquate de ces orientations dans le cadre des applications 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 sécurité nucléaire est une responsabilité nationale. Les publications de la collection Sécurité nucléaire de l'AIEA complètent les instruments juridiques internationaux en la matière 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 appliquent dans leur réglementation nationale pour 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 se basent 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 missions d'examen et de services consultatifs, aidant ainsi ces États Membres à appliquer lesdites orientations et facilitant l'échange de données d'expérience et d'idées

utiles. Les informations en retour sur ces missions et services, de même que les enseignements tirés des événements et l'expérience relative à l'utilisation et à 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 cadre 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 DE L'ÉDITEUR

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. L'objectif et les éléments essentiels d'un régime de sécurité nucléaire sont énoncés dans les Fondements de la sécurité nucléaire [1]. Les Recommandations de sécurité nucléaire précisent quels éléments devraient être couverts par un tel régime en ce qui concerne :

a) les matières nucléaires et les installations nucléaires [2] ;
b) les matières radioactives et les installations associées [3] ;
c) les matières nucléaires et autres matières radioactives non soumises à un contrôle réglementaire [4].

1.2. L'identification et l'évaluation des menaces forment la base de la sélection, de la conception et de la mise en œuvre des mesures de sécurité nucléaire. Pour les matières nucléaires et autres matières radioactives soumises à un contrôle réglementaire et pour les installations et activités associées, les résultats de cette identification et de cette évaluation prennent la forme d'une menace de référence ou d'un énoncé de la menace représentative, qui décrivent les intentions et les capacités des agresseurs potentiels contre lesquels les matières et les installations et activités associées doivent être protégées.

1.3. La présente publication est une révision de la publication n° 10 de la collection Sécurité nucléaire de l'AIEA, intitulée « Élaboration, utilisation et actualisation de la menace de référence »[1]. Elle intègre les éléments nouveaux survenus dans le domaine et s'accorde sur le plan terminologique avec les références [1] à [4], publiées après 2009.

1.4. En outre, la présente publication a une portée plus large que la précédente : elle donne des précisions sur l'utilisation d'une autre approche que la menace de référence, explique comment élaborer des menaces de référence propres à une application et traite plus en détail les menaces impliquant des cyberattaques [5].

---

[1] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Élaboration, utilisation et actualisation de la menace de référence, n° 10 de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2012).

OBJECTIF

1.5. La présente publication décrit les étapes à suivre pour réaliser une évaluation de la menace contre la sécurité nucléaire nationale, en tenant compte des aspects physiques et informatiques, et pour élaborer, utiliser et actualiser les menaces de référence et les énoncés de la menace représentative. Ces étapes sont les suivantes :

a) définir les rôles et les responsabilités de l'État, des autorités compétentes (y compris l'organisme de réglementation[2]) et des exploitants ;
b) identifier et évaluer les menaces touchant la sécurité nucléaire ;
c) élaborer des énoncés de la menace, comme des menaces de référence et des énoncés de la menace représentative, à partir des résultats de l'évaluation de la menace contre la sécurité nucléaire nationale ;
d) utiliser les menaces de référence et/ou les énoncés de la menace représentative pour mettre au point des systèmes et des mesures de sécurité nucléaire ainsi que des prescriptions de sécurité nucléaire ;
e) maintenir la validité de l'évaluation de la menace contre la sécurité nucléaire nationale et du dossier d'évaluation ;
f) maintenir la validité des menaces de référence et des énoncés de la menace représentative.

1.6. La présente publication est destinée aux États, aux autorités compétentes (y compris l'organisme de réglementation), aux organismes d'appui technique et scientifique compétents, aux exploitants d'installations mettant en jeu des matières nucléaires et autres matières radioactives et aux personnes menant des activités connexes, y compris les expéditeurs et les transporteurs.

PORTÉE

1.7. Le concept et la méthode décrits dans la présente publication servent à réaliser une évaluation de la menace contre la sécurité nucléaire nationale, en tenant compte des aspects physiques et informatiques, et à élaborer, à utiliser et à actualiser les menaces de référence et les énoncés de la menace représentative afin de protéger les matières nucléaires et autres matières radioactives soumises à un contrôle réglementaire ainsi que les installations et activités associées.

---

[2] Dans certains États, plusieurs organismes de réglementation sont chargés d'assurer la sécurité nucléaire des matières nucléaires et autres matières radioactives et des installations et activités associées. Au sens de la présente publication, le terme « organisme de réglementation » désigne l'organisme (ou les organismes) compétent(s) dans le contexte donné.

1.8. La présente publication ne couvre pas l'élaboration d'une approche fondée sur les risques, ni la réalisation d'évaluations de la menace et du risque comme fondements de la sécurité nucléaire des matières nucléaires et autres matières radioactives non soumises à un contrôle réglementaire ; des orientations à ce sujet figurent dans la publication n° 24-G de la collection Sécurité nucléaire de l'AIEA, intitulée *Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control* [6].

STRUCTURE

1.9. La section 2 traite de l'évaluation de la menace contre la sécurité nucléaire nationale dans le cadre d'une approche fondée sur les risques. La section 3 présente dans les grandes lignes la procédure à suivre pour réaliser une évaluation de la menace contre la sécurité nucléaire nationale et élaborer, utiliser et maintenir la validité de cette évaluation et du dossier d'évaluation ainsi que des menaces de référence et des énoncés de la menace représentative. La section 4 définit les rôles et les responsabilités des organismes contribuant à l'évaluation de la menace contre la sécurité nucléaire nationale. La section 5 décrit plus en détail la manière de réaliser une évaluation de la menace contre la sécurité nucléaire nationale. La section 6 fait le point sur l'élaboration des menaces de référence et des énoncés de la menace représentative, dont l'utilisation est abordée dans la section 7, et la section 8 donne des orientations pour maintenir la validité de l'évaluation de la menace contre la sécurité nucléaire nationale, du dossier d'évaluation associé et des énoncés de la menace. Enfin, un modèle de menace de référence figure dans l'appendice.

2. ÉVALUATION DE LA MENACE CONTRE LA SÉCURITÉ NUCLÉAIRE NATIONALE ET UTILISATION D'UNE APPROCHE FONDÉE SUR LES RISQUES

2.1. Les conventions internationales et les orientations de la collection Sécurité nucléaire de l'AIEA insistent sur l'importance de l'évaluation de la menace et de l'utilisation d'une approche de la sécurité nucléaire fondée sur les risques. Notamment, le principe fondamental G (Menace) de la Convention sur la protection physique des matières nucléaires amendée [7, 8] et la référence [2]

disposent que « **[la] protection physique dans un État devrait être fondée sur l'évaluation actuelle de la menace faite par l'État** ».

2.2. Dans la référence [1], l'élément essentiel 9 est décrit comme suit :

> « Un *régime de sécurité nucléaire* fait appel à des approches fondées sur les risques, y compris dans l'allocation des ressources aux *systèmes de sécurité nucléaire* et aux *mesures de sécurité nucléaire*, et dans la conduite des activités relatives à la sécurité nucléaire, approches qui sont elles-mêmes basées sur une *approche graduée* et sur la *défense en profondeur* prenant en compte :
>
> a) l'évaluation actuelle par l'État des *menaces contre la sécurité nucléaire*, tant internes qu'externes ;
> b) l'attractivité et la vulnérabilité relatives des *cibles* identifiées face aux *menaces contre la sécurité nucléaire* ;
> c) les caractéristiques des *matières nucléaires*, *d'autres matières radioactives* et des *installations* et *activités associées* ;
> d) les conséquences néfastes potentielles des actes criminels ou des actes non autorisés délibérés mettant en jeu ou visant des *matières nucléaires*, *d'autres matières radioactives*, des *installations associées*, des *activités associées*, des *informations sensibles ou des ressources d'informations sensibles*, et des autres actes que l'État considère comme nuisant à la sécurité nucléaire. »

2.3. En outre, le paragraphe 3.10 de la référence [2] dispose ce qui suit :

> « L'État devrait définir — à partir de l'*évaluation de la menace* ou de la *menace de référence* — des prescriptions pour la protection physique des *matières nucléaires* en cours d'utilisation, d'entreposage et de *transport* ainsi que pour les *installations nucléaires*, en fonction des conséquences qui pourraient résulter d'un *enlèvement non autorisé* ou d'un *sabotage*. »

De plus, les paragraphes 3.17 et 3.18 de la référence [3] précisent que :

> « L'État devrait évaluer la *menace* nationale concernant les *matières radioactives*, les *installations associées* et les *activités associées*. Il devrait réexaminer périodiquement cette *menace* et évaluer les incidences de tout changement de la *menace* sur la conception ou l'actualisation du *régime de sécurité nucléaire*... L'*organisme de réglementation* devrait utiliser les résultats de l'*évaluation de la menace* comme base commune pour définir

les prescriptions de sécurité pour les *matières radioactives* et en réévaluer périodiquement l'adéquation. »

2.4. Les parties suivantes abordent plus en détail plusieurs questions liées à l'évaluation de la menace contre la sécurité nucléaire nationale dans le cadre d'une approche fondée sur les risques, aux agresseurs et à leurs attributs et caractéristiques et à la sécurité de l'information.

APPROCHE FONDÉE SUR LES RISQUES ET ÉNONCÉS DE LA MENACE

2.5. L'élément essentiel 9 d'un régime de sécurité nucléaire [1] consiste en l'utilisation d'approches fondées sur les risques, y compris dans l'allocation des ressources aux systèmes de sécurité nucléaire et aux mesures de sécurité nucléaire et dans la conduite des activités relatives à la sécurité nucléaire, approches qui sont elles-mêmes basées sur une approche graduée et sur la défense en profondeur. La menace, l'attractivité et la vulnérabilité des cibles potentielles et les conséquences potentielles d'actes malveillants devraient être prises en considération lors de l'adoption d'une approche fondée sur les risques.

2.6. Le paragraphe 3.41 de la référence [2] dispose que « [l]'État devrait veiller à ce que son *régime de protection physique* soit à même de définir le risque d'un *enlèvement non autorisé* et d'un *sabotage* et de le maintenir à des niveaux acceptables grâce à une gestion du risque ». La menace et les conséquences potentielles d'actes malveillants devraient être réévaluées périodiquement et des systèmes et des mesures de sécurité nucléaire appropriés devraient être mis en place pour prévenir les actes malveillants ou réduire la possibilité que de tels actes soient commis.

2.7. L'évaluation de la menace contre la sécurité nucléaire nationale est une analyse des menaces existantes relatives à la sécurité nucléaire, notamment des menaces contre la sécurité physique et informatique, effectuée au moyen d'informations provenant de sources mondiales, régionales et nationales, qui doit permettre de déterminer les attributs et les caractéristiques des agresseurs potentiels.

2.8. Les résultats de cette évaluation, consignés dans le dossier d'évaluation, servent à établir des énoncés de la menace. Ceux-ci décrivent les attributs et les caractéristiques des agresseurs potentiels crédibles contre lesquels les activités et les installations associées aux matières nucléaires et autres matières radioactives doivent être protégées.

2.9. L'évaluation de la menace existante contre la sécurité nucléaire, exposée dans les énoncés de la menace tels que les menaces de référence et les énoncés de la menace représentative, facilite l'application d'une approche de la sécurité nucléaire fondée sur les risques et appuie la gestion du risque dans les différentes installations et activités. Les énoncés de la menace peuvent aider à concevoir et à évaluer des systèmes et des mesures de sécurité nucléaire tenant compte des conséquences potentielles d'un acte malveillant.

2.10. Les États peuvent choisir d'élaborer des énoncés de la menace sous la forme soit de menaces de référence, soit d'énoncés de la menace représentative, ou utiliser les deux en appliquant une approche réglementaire adaptée[3] à chaque type d'installation et d'activité. Les énoncés de la menace représentative peuvent servir à élaborer des prescriptions réglementaires pour un sous-ensemble particulier de matières ou d'installations de moindre risque à protéger, tandis que les menaces de référence peuvent être utilisées pour mettre en œuvre des prescriptions réglementaires privilégiant une approche basée sur les résultats pour protéger une installation ou une activité spécifique à plus haut risque. Par exemple, une autorité compétente pourrait utiliser un énoncé de la menace représentative pour établir des prescriptions réglementaires pour la protection des sources radioactives de catégorie 1 en cours d'utilisation et d'entreposage, et un exploitant pourrait utiliser une menace de référence pour concevoir et évaluer un système de sécurité nucléaire visant à protéger une source radioactive de catégorie 1 spécifique contre différents scénarios d'attaque conformément aux prescriptions basées sur les résultats établies.

2.11. En fonction des résultats de l'évaluation de la menace contre la sécurité nucléaire nationale, les États peuvent décider d'établir des énoncés de la menace représentative différents pour différentes catégories de matières nucléaires et autres matières radioactives et différents types d'installations et d'activités (p. ex. sources radioactives de catégorie 1, irradiateurs, transport de matières radioactives), pour différents objectifs d'agresseurs (p. ex. vol, sabotage) et pour les biens risquant particulièrement d'être la cible de cyberattaques (p. ex. informations sensibles ou systèmes informatiques relatifs à la sûreté nucléaire, à la sécurité nucléaire, à la comptabilité et au contrôle des matières nucléaires ou à l'intervention d'urgence).

2.12. De même, sur la base de l'évaluation de la menace contre la sécurité nucléaire nationale, les États peuvent choisir d'élaborer des menaces de référence

---

[3] Les approches réglementaires basées sur les prescriptions et sur les résultats sont décrites plus en détail dans les références [2, 3, 8, 9].

différentes pour les matières utilisées dans des installations ou des activités précises présentant des risques plus élevés (p. ex. réacteurs de recherche, transport du combustible nucléaire usé). Ces menaces de référence devraient tenir compte des caractéristiques des installations ou activités (p. ex. conception, emplacement), des considérations politiques (p. ex. le degré de prudence nécessaire pour maintenir la confiance du public) et des capacités et des ressources de l'État et de l'exploitant.

2.13. Certaines menaces mises en évidence lors de l'évaluation de la menace contre la sécurité nucléaire nationale peuvent ne pas être prises en compte dans les menaces de référence ou les énoncés de la menace représentative car considérées hors dimensionnement. La protection contre ces menaces doit être examinée dans le plan d'intervention spécialisé de l'État, même si le système de sécurité nucléaire de l'exploitant assure naturellement une certaine protection à cet égard, et l'intervention de l'État doit être coordonnée avec le plan d'intervention d'urgence de l'exploitant. Bien qu'il appartienne à l'État d'élaborer des mesures pour contrer ces menaces, l'exploitant peut jouer un rôle en l'aidant à assurer la protection face à elles ou à en atténuer les conséquences.

2.14. Les décisions relatives aux risques contre la sécurité nucléaire sont prises sur la base des menaces existantes intéressant un État, de la possibilité que des menaces nouvelles et émergentes se fassent jour et des décisions concernant la recherche d'un juste milieu entre la prudence d'une part et les coûts et incidences opérationnelles d'autre part. Les menaces internationales et régionales, les facteurs politiques et financiers, la perception du risque par le public et les enseignements tirés des précédentes évaluations de la menace contre la sécurité nucléaire pourraient également être prises en compte.

AGRESSEURS POTENTIELS ET LEURS ATTRIBUTS ET CARACTÉRISTIQUES

2.15. Les agresseurs potentiels peuvent être des terroristes, d'autres criminels ou des extrémistes qui cherchent à acquérir et à utiliser des matières nucléaires ou d'autres matières radioactives pour fabriquer des dispositifs nucléaires explosifs, des engins à dispersion de radioactivité ou des dispositifs d'irradiation. Ils peuvent également chercher à saboter les installations dans lesquelles des matières nucléaires ou d'autres matières radioactives sont utilisées ou entreposées ou à entraver le transport de ces matières.

2.16. Les agresseurs potentiels sont caractérisés par leurs motivations, leurs intentions et leurs capacités. Leurs motivations peuvent être d'ordre financier, politique ou idéologique ou résulter d'un mécontentement ou de pressions, par exemple. Leurs intentions peuvent comprendre la possession non autorisée de matières nucléaires ou d'autres matières radioactives, l'acquisition d'informations ou de ressources d'informations sensibles, l'endommagement par le sabotage ou l'embarras public de l'exploitant d'une installation ou d'une activité ou de l'État. Leurs capacités dépendent de caractéristiques telles que le nombre de personnes impliquées, le niveau d'organisation et de coordination et l'implication ou non d'initiés. Elles comprennent également les aptitudes, les moyens et les compétences pertinentes des personnes et du groupe, notamment les tactiques, les armes, les explosifs, les moyens de transport, les outils physiques et informatiques, la connaissance des vulnérabilités des logiciels et le niveau d'accès à une installation ou à ses systèmes informatiques.

2.17. Les agresseurs peuvent être des initiés [9], c'est-à-dire des personnes bénéficiant d'un accès autorisé à des installations ou des activités associées ou à des informations ou des ressources d'informations sensibles, qui pourraient 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. Des agresseurs peuvent chercher à obtenir un accès autorisé à une installation (p. ex. à s'y faire engager en tant qu'employés ou contractants) pour en tirer parti par la suite, devenant ainsi des initiés, ou le personnel d'une installation peut développer l'intention de commettre ou de faciliter des actes malveillants et devenir ainsi une menace interne.

2.18. Il convient de tenir compte de la possibilité de collusion entre des initiés et des agresseurs externes. Un initié pourrait par exemple commettre un acte non autorisé, physiquement ou par des moyens informatiques, pour aider un agresseur externe à commettre un acte malveillant.

2.19. Les États devraient envisager le risque d'actes malveillants impliquant un accès physique à l'installation ou à l'activité mais aussi d'actes mettant en jeu une cyberattaque. Les systèmes informatiques relatifs à la sûreté nucléaire (notamment les systèmes de contrôle-commande), à la comptabilité et au contrôle des matières nucléaires, à la sécurité nucléaire et à l'intervention d'urgence (notamment les systèmes de communication et d'alarme) pourraient être la cible d'une telle attaque. Les agresseurs pourraient aussi combiner une attaque physique à une attaque contre un système informatique, par exemple falsifier électroniquement

les droits d'accès pour s'introduire de force dans l'installation à des fins de sabotage ou de vol de matières.

2.20. Il importe de réfléchir à la possibilité qu'aussi bien des initiés que des agresseurs externes commettent des actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des informations dans des systèmes informatiques. De tels actes pourraient être facilités soit par des initiés, soit par des agresseurs externes lançant une cyberattaque depuis l'extérieur. Le risque que des logiciels malveillants soient introduits dans des systèmes informatiques via la chaîne d'approvisionnement devrait également être pris en considération.

2.21. En outre, il convient de tenir compte du risque d'attaques menées à l'aide de dispositifs pilotés à distance, comme des drones, des missiles ou des armes à énergie dirigée.

CONSIDÉRATIONS RELATIVES À LA SÉCURITÉ DE L'INFORMATION

2.22. Toutes les informations crédibles sur les menaces, notamment celles émanant des services de renseignement nationaux et les autres informations sensibles, devraient être prises en considération lors de l'élaboration et de l'actualisation des énoncés de la menace. Certaines de ces informations et nombre de leurs sources doivent être protégées. Les menaces de référence et les énoncés de la menace représentative utilisés pour concevoir et évaluer des systèmes de sécurité nucléaire devraient être protégés en tant qu'informations sensibles, c'est-à-dire des informations, sous quelque forme que ce soit, y compris un logiciel, dont la divulgation, la modification, l'altération, la destruction ou le refus d'utilisation non autorisés pourrait compromettre la sécurité nucléaire.

2.23. Des orientations détaillées sur la protection des informations sensibles relatives à la sécurité nucléaire figurent dans la publication n° 23-G de la collection Sécurité nucléaire de l'AIEA, intitulée « Sécurité de l'information nucléaire » [10].

3. VUE D'ENSEMBLE DE LA PROCÉDURE D'ÉLABORATION, D'UTILISATION ET DE MAINTIEN DE LA VALIDITÉ DE L'ÉVALUATION DE LA MENACE CONTRE LA SÉCURITÉ NUCLÉAIRE NATIONALE, DU DOSSIER ASSOCIÉ, DES MENACES DE RÉFÉRENCE ET DES ÉNONCÉS DE LA MENACE REPRÉSENTATIVE

3.1. La procédure d'élaboration, d'utilisation et de maintien de la validité de l'évaluation de la menace contre la sécurité nucléaire nationale, du dossier associé, des menaces de référence et des énoncés de la menace représentative est présentée dans la figure 1. Elle comporte cinq étapes :

1) définition des rôles et des responsabilités ;
2) réalisation de l'évaluation de la menace contre la sécurité nucléaire nationale et constitution du dossier d'évaluation ;
3) élaboration des menaces de référence et/ou des énoncés de la menace représentative ;
4) utilisation des menaces de référence et/ou des énoncés de la menace représentative dans le cadre réglementaire ;
5) maintien de la validité de l'évaluation de la menace contre la sécurité nucléaire nationale, des menaces de référence et/ou des énoncés de la menace représentative.

3.2. À l'étape 1, l'État devrait définir les rôles et responsabilités pertinents de l'organisme de réglementation et des autres autorités compétentes, ainsi que des exploitants, conformément à son cadre juridique et réglementaire.

3.3. À l'étape 2 — réalisation de l'évaluation de la menace contre la sécurité nucléaire nationale — l'autorité chargée de l'évaluation et les autres autorités compétentes devraient rassembler des renseignements et d'autres informations sur les menaces, notamment des données en libre accès et des informations issues d'anciens événements de sécurité nucléaire et d'événements de sécurité liés à des activités non nucléaires. Elles devraient analyser ces informations et estimer quel intérêt elles pourraient avoir pour la sécurité nucléaire. Elles devraient aussi évaluer la crédibilité des informations et écarter celles jugées non crédibles. À partir des informations restantes, elles devraient identifier les agresseurs potentiels, définir leurs attributs et caractéristiques et caractériser le risque d'agression. Elles devraient également déterminer si les capacités spécifiques des agresseurs

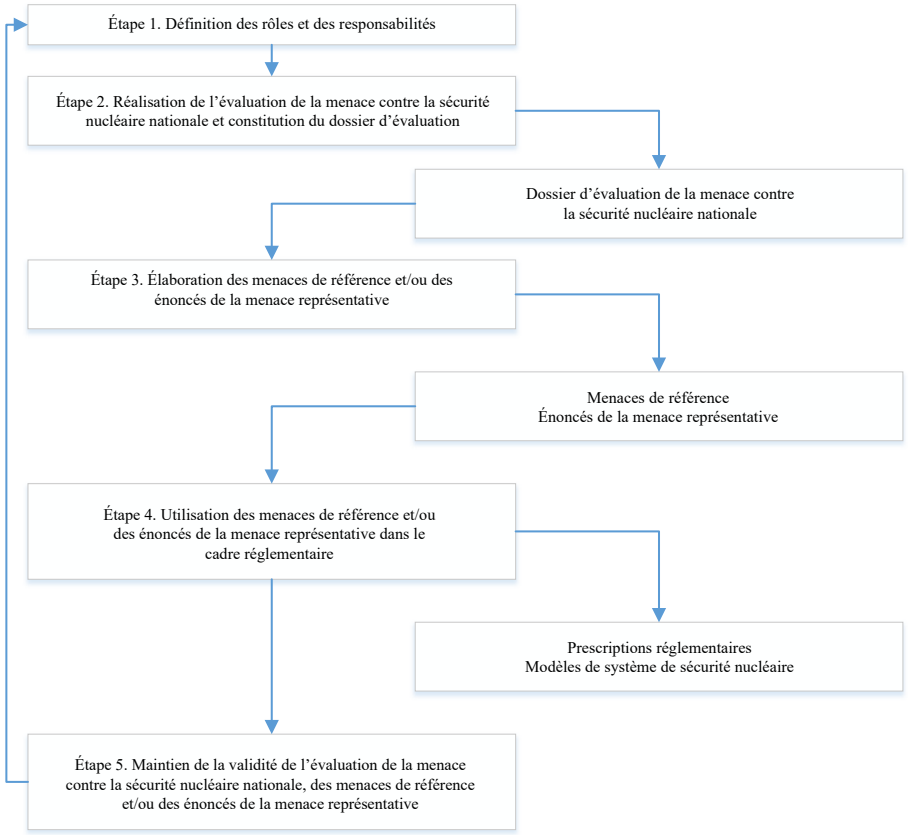


FIG. 1. Procédure d'élaboration, d'utilisation et de maintien de la validité de l'évaluation de la menace contre la sécurité nucléaire nationale, du dossier associé, des menaces de référence et des énoncés de la menace représentative.

pourraient leur permettre d'atteindre des cibles potentielles. Les résultats de ces travaux devraient être consignés dans le dossier d'évaluation de la menace contre la sécurité nucléaire nationale.

3.4. À l'étape 3, l'autorité chargée de l'élaboration des énoncés de la menace devrait, en accord avec les autres autorités compétentes, le cas échéant, utiliser les résultats de l'évaluation de la menace contre la sécurité nucléaire nationale pour élaborer des menaces de référence propres à une matière, à une installation ou à une activité et/ou des énoncés de la menace représentative applicables à différents types et différentes catégories de matières nucléaires, d'autres matières radioactives et d'installations et activités associées.

3.5. Les mesures prises par l'organisme de réglementation à l'étape 4 dépendront de l'approche réglementaire suivie :

a) Dans le cas d'une approche basée sur les résultats, l'organisme de réglementation devrait transmettre les menaces de référence aux exploitants concernés, qui devraient alors élaborer des scénarios d'attaque propres à leur installation et, à partir de ces scénarios, concevoir des systèmes de sécurité nucléaire permettant de contrer les menaces de référence et d'atteindre les objectifs de sécurité nucléaire définis dans le cadre juridique national.
b) Dans le cas d'une approche basée sur les prescriptions, l'organisme de réglementation devrait élaborer des prescriptions réglementaires fondées sur les énoncés de la menace représentative et les objectifs de sécurité nucléaire définis dans le cadre juridique national, et veiller à ce que les exploitants mettent en œuvre des systèmes et des mesures de sécurité nucléaire conformes à ces prescriptions.
c) Dans le cas d'une approche combinée, l'organisme de réglementation devrait intégrer des éléments de l'approche basée sur les résultats et de l'approche basée sur les prescriptions.

3.6. À l'étape 5, les autorités compétentes devraient réexaminer l'évaluation de la menace contre la sécurité nucléaire nationale et le dossier associé, ainsi que les menaces de référence et les énoncés de la menace représentative, et les réviser si nécessaire. Une révision devrait être entreprise selon un cycle défini, en cas d'évolution de la menace et/ou afin d'intégrer les enseignements tirés d'un événement de sécurité nucléaire. En cas de menaces nouvelles ou émergentes exigeant un réexamen immédiat, les autorités compétentes devraient, en collaboration avec les exploitants, prendre les mesures nécessaires pour gérer ces menaces, si besoin en dehors du cadre des menaces de référence ou des énoncés de la menace représentative existants en attendant que ceux-ci soient révisés. Cette procédure devrait être intégrée dans le régime de sécurité nucléaire de l'État.

3.7. Ces étapes sont décrites plus en détail dans les sections 4 à 8, qui énoncent également des orientations pratiques à l'intention des États, des autorités compétentes et des exploitants.

4. RÔLES ET RESPONSABILITÉS

4.1. L'État, les autorités compétentes (y compris l'organisme de réglementation) et les exploitants ont des rôles et des responsabilités concernant l'évaluation de la menace contre la sécurité nucléaire nationale et l'élaboration de menaces de référence et/ou d'énoncés de la menace représentative. Ces rôles et responsabilités devraient être clairement définis avant le début de la réalisation de l'évaluation de la menace contre la sécurité nucléaire nationale.

ÉTAT

4.2. L'État est chargé de désigner, de coordonner et de superviser les autorités compétentes qui dirigeront les travaux suivants ou y participeront :

a) réalisation d'une évaluation de la menace contre la sécurité nucléaire nationale et maintien de sa validité et de celle du dossier associé ;
b) élaboration et maintien de la validité des menaces de référence et/ou des énoncés de la menace représentative ;
c) utilisation des menaces de référence et/ou des énoncés de la menace représentative[4].

4.3. Un événement de sécurité nucléaire peut entraîner une situation d'urgence nucléaire ou radiologique. Le paragraphe 4.22 de la publication n° GSR Part 7 de la collection Normes de sûreté de l'AIEA, intitulée « Préparation et conduite des interventions en cas de situation d'urgence nucléaire ou radiologique » [11], dispose que le « gouvernement veille à ce que l'évaluation des dangers tienne compte des résultats des évaluations de la menace faites aux fins de la sécurité nucléaire ».

AUTORITÉS COMPÉTENTES

4.4. Toutes les autorités compétentes concernées devraient participer à l'évaluation de la menace contre la sécurité nucléaire nationale afin qu'un maximum de menaces crédibles soient identifiées et prises en compte dans l'évaluation.

---

[4] L'État peut charger différentes autorités compétentes de diriger les différents processus ; cependant, les rôles et responsabilités de chacune doivent être clairement définis et un mécanisme destiné à assurer leur coordination doit être bien établi et mis en œuvre.

4.5. Il est possible que plusieurs entités nationales, comme les services de renseignements (y compris les services de sécurité), les ministères de l'intérieur et des affaires étrangères, les centres de sécurité informatique, les forces de l'ordre, les forces armées, l'organisme de réglementation en matière de sécurité nucléaire et d'autres organismes compétents, possèdent des compétences pertinentes pour l'identification et l'évaluation des menaces crédibles. Ces entités peuvent disposer de personnels familiarisés avec les processus de collecte et d'analyse des informations et capables d'émettre les jugements nécessaires. Elles peuvent également avoir accès à des sources d'information particulières, notamment avoir des contacts dans d'autres États ou des organisations régionales ou internationales.

4.6. Les autorités compétentes peuvent notamment avoir les responsabilités suivantes :

a) rassembler et regrouper des informations sur les menaces potentielles ;
b) analyser les informations disponibles sur les menaces pour en confirmer la crédibilité ;
c) échanger des informations pertinentes sur les menaces avec les autres autorités compétentes ;
d) déterminer le sous-ensemble de menaces crédibles pertinent pour la sécurité nucléaire, en coordination avec les autres autorités compétentes ;
e) coopérer à l'évaluation de la menace, identifier les agresseurs potentiels et établir le dossier d'évaluation de la menace contre la sécurité nucléaire nationale ;
f) élaborer des menaces de référence et/ou des énoncés de la menace représentative à partir des résultats de l'évaluation de la menace contre la sécurité nucléaire nationale ;
g) maintenir la validité de l'évaluation de la menace contre la sécurité nucléaire nationale et du dossier associé, ainsi que des menaces de référence et des énoncés de la menace représentative ;
h) transmettre le dossier d'évaluation de la menace contre la sécurité nucléaire nationale, selon qu'il convient, aux organismes d'intervention d'urgence compétents[5] ;
i) tenir compte de l'évaluation de la menace contre la sécurité nucléaire nationale dans l'évaluation des dangers [12] ;
j) prendre en considération les aspects liés à la sécurité de l'information.

[5] L'intervention en matière de sécurité nucléaire désignant l'intervention menée en cas d'événement de sécurité nucléaire, le terme « organisme d'intervention d'urgence » est utilisé dans la présente publication pour éviter toute erreur d'interprétation. Il est utilisé au sens du terme « organisme d'intervention » tel que défini dans la publication nº GSR Part 7 [11].

4.7. Certaines autorités compétentes (comme les forces de l'ordre nationales et locales, les forces armées, les autorités chargées du contrôle des frontières et les autorités douanières) ont des responsabilités beaucoup plus vastes dans un État. Elles peuvent notamment être chargées d'assurer la protection contre les menaces liées à la sécurité nucléaire, individuellement ou de manière collaborative, ou de prêter appui à l'exploitant lors d'un événement de sécurité nucléaire. Ces autorités devraient participer à l'élaboration des menaces de référence et/ou des énoncés de la menace représentative et des prescriptions réglementaires ou être consultées à cet égard.

4.8. L'organisme de réglementation en matière de sécurité nucléaire, agissant en collaboration avec d'autres autorités compétentes s'il convient, est chargé des tâches suivantes :

a) élaborer des prescriptions à l'intention des exploitants en s'appuyant sur les énoncés de la menace représentative et/ou transmettre aux exploitants les menaces de référence et les prescriptions basées sur les résultats qui doivent servir à l'élaboration de scénarios d'attaque et à la conception de systèmes et de mesures de sécurité nucléaire ;
b) veiller à ce que les exploitants examinent comme il convient les dispositifs de sécurité et d'urgence et les révisent si nécessaire, en tenant compte des scénarios d'attaque et des résultats des évaluations de la menace.

EXPLOITANTS

4.9. Les exploitants devraient mettre en œuvre des systèmes et des mesures de sécurité nucléaire permettant d'atteindre au moins un des objectifs suivants :

a) satisfaire aux prescriptions réglementaires, y compris les prescriptions pertinentes élaborées à partir de l'énoncé de la menace représentative ;
b) assurer une protection contre une série de scénarios d'attaque propres à une installation ou à une activité, scénarios élaborés sur la base de la menace de référence.

4.10. Dans certains cas, la répartition des responsabilités en matière de sécurité nucléaire entre les exploitants et les autorités compétentes peut être influencée par le fait que les exploitants sachent quelles incidences des mesures de sécurité nucléaire données auraient sur les plans financier et opérationnel et sur la sûreté. Le point de vue des exploitants, formel ou informel, devrait être pris en considération lors de l'élaboration des menaces de référence, des énoncés

de la menace représentative et des prescriptions réglementaires. En particulier, les exploitants devraient :

a) donner leur avis sur les menaces contre la sécurité nucléaire d'une installation et d'une activité données qui devraient être prises en compte dans les menaces de référence et/ou les énoncés de la menace représentative ;
b) donner à l'organisme de réglementation, si nécessaire et demandé dans le cadre juridique et réglementaire, des informations en retour sur les incidences qu'auraient, sur les plans financier et opérationnel et sur la sécurité et la sûreté, d'éventuelles décisions touchant aux menaces de référence, aux énoncés de la menace représentative et/ou aux prescriptions réglementaires ;
c) donner des informations complémentaires, déduites des attaques physiques, des cyberattaques et des attaques combinées qui ont pu se produire, sur les scénarios d'attaque et les attributs et caractéristiques des agresseurs, si nécessaire et demandé dans le cadre juridique et réglementaire.

5. RÉALISATION D'UNE ÉVALUATION DE LA MENACE CONTRE LA SÉCURITÉ NUCLÉAIRE NATIONALE

5.1. L'évaluation de la menace contre la sécurité nucléaire nationale a pour objet de fournir une analyse des menaces crédibles, avec une description des motivations, des intentions et des capacités des agresseurs potentiels. Elle n'a pas vocation à décrire des scénarios d'attaque spécifiques.

5.2. Une description des menaces potentielles suffisamment ciblée et détaillée peut être utilisée pour déterminer le niveau de protection suffisant et adéquat pour les matières nucléaires et autres matières radioactives ainsi que les installations et activités associées. Elle constitue une base sur laquelle un système de sécurité nucléaire peut être conçu efficacement.

5.3. Dans le cadre de l'évaluation de la menace contre la sécurité nucléaire nationale, des informations sur les menaces existantes et les menaces potentielles crédibles sont recueillies et analysées et des informations sur les attributs et caractéristiques des agresseurs potentiels sont rassemblées et regroupées. L'évaluation aboutit à une description détaillée des menaces liées

à la sécurité nucléaire : le dossier d'évaluation de la menace contre la sécurité nucléaire nationale. Tous les organismes compétents dans divers domaines d'expertise et de responsabilité devraient collaborer étroitement à la collecte et à l'analyse de ces informations. Il importe également que ces organismes entretiennent de bonnes relations de travail pour garantir l'efficacité de l'évaluation. Les documents relatifs à la réalisation de l'évaluation devraient être conservés afin de faciliter le réexamen et la révision périodiques nécessaires au maintien de la validité de l'évaluation.

5.4. Les rôles et responsabilités liés à la réalisation ou à la supervision des tâches détaillées dans les parties suivantes sont décrits à la section 4.

APPORTS : COLLECTE D'INFORMATIONS PERTINENTES SUR LES MENACES

5.5. La première étape de la réalisation d'une évaluation de la menace contre la sécurité nucléaire nationale consiste à rassembler et à regrouper des informations exhaustives sur tous les agresseurs potentiels, leurs motivations, leurs intentions et leurs capacités. Ces informations, sensibles ou non, devraient renseigner à la fois sur les capacités physiques et sur les capacités informatiques, sur les agresseurs externes et sur les initiés.

5.6. Les sources d'information possibles devraient être identifiées et les informations pertinentes collectées. La sensibilité de ces informations devrait être prise en considération pour garantir l'application de mesures de sécurité adéquates pour les informations comme pour leurs sources. Un mécanisme devrait être établi, s'il n'y en a pas déjà un, pour faciliter l'échange d'informations sur les menaces entre tous les organismes participant à l'évaluation de la menace et pour assurer la sécurité des informations sensibles. Des accords écrits peuvent être nécessaires pour définir les modalités d'échange des informations relatives aux menaces.

5.7. Les services de renseignement et d'autres sources d'informations sur les menaces pourraient fournir des informations suffisantes pour concevoir un système de sécurité nucléaire. Toutefois, en raison des limites des renseignements et de la nature évolutive des menaces, les systèmes de sécurité nucléaire conçus pour contrer uniquement les menaces connues au moment de la conception pourraient ne pas être efficaces contre les menaces futures.

5.8. L'évaluation de la menace contre la sécurité nucléaire nationale ne devrait pas s'appuyer sur une seule source. C'est en utilisant des renseignements et des informations de plusieurs sources, regroupées en un ensemble cohérent, que l'on obtiendra l'évaluation de la menace contre la sécurité nucléaire nationale la plus complète, la plus fiable et la plus solide. Toutes les sources crédibles et pertinentes de renseignements et d'informations sur les menaces, tant nationales qu'internationales, devraient être prises en compte au stade de la collecte de données.

5.9. Les informations et les renseignements devraient notamment provenir, selon le cas, des services de renseignement (notamment les services de sécurité), des services de sécurité informatique et de sécurité de l'information, des forces de l'ordre, de l'Organisation internationale de police criminelle, de l'organisme de réglementation en matière de sécurité nucléaire et des autres autorités compétentes, des autorités chargées du contrôle des frontières, des autorités douanières, des forces armées, des expéditeurs et des transporteurs, des rapports officiels gouvernementaux, des rapports des exploitants sur les incidents, des bases de données gérées par des organisations internationales et d'autres sources librement accessibles.

5.10. Les organismes d'appui technique et scientifique, les entités commerciales et les bases de données en libre accès pourraient être utilisées pour obtenir des informations complémentaires sur les menaces potentielles, en particulier celles contre la sécurité informatique. Les exploitants pourraient aussi avoir des informations sur ces menaces et sur leurs attributs et caractéristiques.

5.11. Les informations pertinentes sur les attributs et les caractéristiques des menaces potentielles contre d'autres types d'infrastructures critiques devraient être prises en considération, ces menaces pouvant être semblables à celles contre la sécurité nucléaire.

5.12. Des informations devraient être recueillies concernant les événements de sécurité nucléaire récents et anciens (y compris ceux touchant la sécurité informatique), le cas échéant.

5.13. La collecte d'informations devrait permettre d'identifier tous les types de menaces pertinents, notamment :

a) les menaces à l'échelle mondiale, nationale et locale ;
b) les attaques physiques, les cyberattaques et les attaques combinées ;

c) les menaces internes, les agresseurs externes et les menaces résultant de la collusion entre des initiés et des agresseurs externes.

5.14. Les capacités des agresseurs crédibles, même non démontrées, devraient être prises en compte. De même, il convient de tenir compte des agresseurs potentiels tenaces planifiant des attaques en plusieurs étapes sur de longues périodes, des possibles évolutions technologiques, de la fréquence potentielle des attaques et du risque d'attaque sur la chaîne d'approvisionnement (p. ex. de matériel et/ou de logiciels modifiés compromis avant la livraison).

ANALYSE DES INFORMATIONS PERTINENTES SUR LES MENACES

5.15. Une fois les informations pertinentes sur les menaces rassemblées, il convient de les regrouper à l'aide d'outils de gestion de l'information afin de les indexer et de les trier. Le fait de classer efficacement l'ensemble des renseignements et des informations obtenus permet de garantir que toutes les données nécessaires à l'analyse sont disponibles. Les informations devraient ensuite être analysées en vue de déterminer et de consigner les motivations, les intentions et les capacités crédibles des agresseurs potentiels en matière de sécurité nucléaire.

5.16. De l'exhaustivité des informations rassemblées et de la justesse de l'analyse dépendront le degré de confiance pouvant être accordé aux menaces de référence et aux énoncés de la menace représentative élaborés par après.

5.17. La collecte et l'analyse des informations sont souvent itératives. Dans bien des cas, l'analyse fait ressortir le besoin d'informations supplémentaires ou révèle des menaces jusque-là inconnues ou émergentes à propos desquelles des informations sont nécessaires. Cette analyse suppose d'une part de dresser un état des connaissances sur la base des informations disponibles et d'autre part d'estimer comment les attributs et les caractéristiques des agresseurs pourraient évoluer à l'avenir.

5.18. Au cours de l'analyse, il convient d'évaluer la crédibilité des informations utilisées dans l'évaluation de la menace contre la sécurité nucléaire nationale. La fiabilité et l'expertise technique de la source d'information devraient généralement être prises en compte à cet égard. Les forces de l'ordre et les services de renseignement, y compris les services de sécurité, devraient indiquer quel degré de confiance peut selon eux être accordé aux informations qu'ils fournissent. Les informations en libre accès faciles à obtenir (p. ex. sur les médias ou les réseaux sociaux) peuvent être utiles, mais leur exactitude

doit être vérifiée minutieusement. Le degré de confiance dans une information devrait influencer la décision d'utiliser cette information ultérieurement. À ce stade, certains éléments pourraient être mis de côté car jugés non pertinents pour l'analyse et de nouvelles lacunes dans les informations pourraient être repérées (p. ex. comme suite à l'élimination d'informations jugées trop peu crédibles).

5.19. Aux fins de l'évaluation de la menace contre la sécurité nucléaire nationale, il convient de tenir compte au minimum des attributs et caractéristiques énumérés ci-dessous, et ce pour chaque menace identifiée (bien qu'il puisse ne pas y avoir de données disponibles sur certains de ces attributs et caractéristiques pour certaines menaces) :

a) les motivations des agresseurs, qui peuvent être politiques, financières, idéologiques et/ou personnelles (p. ex. fruit d'un mécontentement ou de pressions), entre autres ;
b) la ténacité des agresseurs ;
c) la détermination des agresseurs, notamment leur niveau d'aversion au risque et leur disposition à risquer leur vie ;
d) les capacités démontrées des agresseurs, y compris la caractérisation des événements de sécurité nucléaire passés ;
e) les intentions des agresseurs, comme le sabotage de matériel ou d'une installation, l'enlèvement non autorisé de matières nucléaires ou d'autres matières radioactives ou le vol d'informations sensibles ;
f) le nombre d'agresseurs, notamment d'attaquants, de coordonnateurs et d'auxiliaires, dans un groupe ;
g) le type et le nombre d'armes à la disposition des agresseurs ;
h) le type et la quantité d'explosifs à la disposition des agresseurs, qu'il s'agisse de dispositifs acquis ou improvisés, et la sophistication des mécanismes de déclenchement ;
i) les outils à la disposition des agresseurs, notamment le matériel mécanique, thermique ou électromagnétique, le matériel à commande manuelle ou électronique et le matériel de communication ;
j) les moyens de transport à la disposition des agresseurs, notamment le type (public, privé) et le mode (terrestre, maritime, aérien) de transport et le type et le nombre de véhicules ;
k) les modes d'accès probables aux cibles, à la fois physiques et informatiques ;
l) l'influence sur les opérations et/ou le personnel ;
m) les tactiques potentielles des agresseurs, comme la furtivité, la tromperie, la force, les activités de reconnaissance ou l'ingénierie sociale ;

n) les compétences de planification des agresseurs, p. ex. la capacité de prévoir une diversion ou de coordonner plusieurs attaques menées simultanément par de plus petits groupes ;
o) les compétences pratiques, les connaissances et l'expérience des agresseurs, notamment les compétences liées à l'ingénierie, à l'utilisation d'explosifs, aux produits chimiques et aux communications et l'expérience militaire ou paramilitaire ;
p) l'accès à des compétences dans les domaines de l'informatique et de la sécurité informatique, notamment la connaissance des systèmes de contrôle, des mesures de sécurité informatique, de la rétro-ingénierie et des tests de vulnérabilité, de l'ingénierie des protocoles de communication, de l'ingénierie sociale, de l'obfuscation des sources, de la redirection des attributions, de la surveillance des réseaux et de la manipulation du trafic ;
q) la possession de connaissance ou l'accès à des informations sur les cibles, comme les caractéristiques des cibles, l'agencement de l'installation, les plans et procédures du site, les plans et mesures de sécurité, les mesures de sûreté et de radioprotection, les opérations menées à l'installation, les opérations de transport, les points d'entrée possibles pour les cyberattaques, les procédures et plans d'appui des fournisseurs et les procédures liées à la chaîne d'approvisionnement et aux achats ;
r) les sources de financement, le montant du financement et les moyens d'y accéder ;
s) le risque d'exploitation d'initiés (y compris par collusion, coercition ou tromperie), le nombre possible d'initiés et le statut passif ou actif, violent ou non violent de ces initiés ;
t) les structures d'appui des agresseurs, notamment la présence ou l'absence de sympathisants sur place, d'organismes d'appui ou d'un soutien logistique.

PRODUIT : DOSSIER D'ÉVALUATION DE LA MENACE CONTRE LA SÉCURITÉ NUCLÉAIRE NATIONALE

5.20. Les résultats de l'évaluation de la menace contre la sécurité nucléaire nationale sont consignés dans le dossier d'évaluation de la menace contre la sécurité nucléaire nationale, qui présente la situation générale en ce qui concerne la menace contre la sécurité nucléaire ainsi que toutes les menaces crédibles connues qui devraient être prises en considération. Les explications complémentaires devraient fournir autant de détails que possible sur ces menaces et la crédibilité des informations.

5.21. Le dossier d'évaluation et les détails des sources de renseignements sont généralement protégés en tant qu'informations sensibles.

6. ÉLABORATION DE MENACES DE RÉFÉRENCE ET D'ÉNONCÉS DE LA MENACE REPRÉSENTATIVE

6.1. Comme indiqué à la section 5, l'évaluation de la menace contre la sécurité nucléaire nationale aboutit à l'élaboration d'un dossier d'évaluation de la menace contre la sécurité nucléaire nationale. Sur la base de cette évaluation, des énoncés de la menace peuvent être élaborés sous la forme de menaces de référence et/ou d'énoncés de la menace représentative. Ceux-ci décrivent les agresseurs crédibles contre lesquels les installations et les activités mettant en jeu l'utilisation ou l'entreposage de matières nucléaires ou d'autres matières radioactives doivent être protégés et présentent les attributs et caractéristiques de ces agresseurs.

APPROCHES RÉGLEMENTAIRES ET ÉNONCÉS DE LA MENACE

6.2. Il existe trois approches possibles de la réglementation de l'exploitation d'une installation ou d'une activité : l'approche basée sur les résultats, l'approche basée sur les prescriptions et l'approche combinée. Dans le cadre de l'approche basée sur les résultats, l'exploitant doit concevoir et mettre en œuvre un système de sécurité nucléaire permettant d'atteindre les objectifs de sécurité nucléaire définis par l'État, en tenant compte de la menace de référence communiquée par l'organisme de réglementation, du niveau de protection contre les actes malveillants requis et des interventions d'urgence. Dans le cadre de l'approche basée sur les prescriptions, l'organisme de réglementation établit les mesures de sécurité nucléaire qu'il juge nécessaires pour atteindre les objectifs de sécurité nucléaire définis pour chaque catégorie de matières nucléaires ou autres matières radioactives et chaque niveau de conséquences radiologiques potentielles, sans communiquer les informations sur la menace aux exploitants. Ces mesures forment un ensemble de base que l'exploitant doit mettre en œuvre. L'approche combinée intègre des éléments de ces deux approches. De plus amples informations sur chacune de ces approches figurent dans les références [13] et [14].

6.3. Comme indiqué au paragraphe 2.10, les énoncés de la menace représentative servent généralement à élaborer des prescriptions réglementaires pour un sous-ensemble particulier de matières, d'activités et/ou d'installations à protéger,

tandis que les menaces de référence sont souvent établies pour des installations ou des activités spécifiques. L'organisme de réglementation devrait adopter l'approche réglementaire qui convient le mieux pour répondre aux besoins de l'État, conformément au cadre juridique et réglementaire de ce dernier, avec les énoncés de la menace représentative et/ou les menaces de référence que cela suppose. Cette approche devrait être approuvée par l'État, étant donné qu'elle aura probablement des répercussions sur les ressources de l'organisme de réglementation lui-même et des exploitants.

6.4. L'utilisation d'une menace de référence et d'une approche basée sur les résultats comme fondements de la conception de systèmes et de mesures de sécurité nucléaire peut conduire à une allocation efficiente des ressources, car cela permet d'élaborer des prescriptions pour des systèmes et des mesures de protection et de sécurité nucléaire visant des menaces bien précises, et non des menaces d'ordre général. Cela permet également d'adapter le système de sécurité nucléaire aux particularités des matières, des activités ou des installations (y compris leurs systèmes de contrôle-commande), de dresser un état de référence par rapport auquel les systèmes et mesures de sécurité nucléaire peuvent être évalués (et modifiés si nécessaire) et de s'appuyer sur une base claire pour définir les responsabilités de l'exploitant en matière de sécurité nucléaire. En outre, l'utilisation d'une menace de référence permet d'avoir une base technique plus détaillée et plus précise pour les critères de conception et d'évaluation et peut donner une plus grande assurance que le niveau de protection est suffisant.

6.5. L'utilisation d'une menace de référence dans le cadre d'une approche basée sur les résultats exige davantage de ressources et de compétences de l'organisme de réglementation et de l'exploitant. La disponibilité des ressources et des compétences nécessaires au sein de l'organisme de réglementation et de l'exploitant, pour élaborer la menace de référence dans le premier cas et pour l'utiliser efficacement afin de concevoir des systèmes et des mesures de sécurité nucléaire dans le second cas, peut donc influencer la décision d'utiliser une menace de référence. Ces ressources et compétences devraient toutefois être mises à disposition par l'État si celui-ci estime nécessaire de disposer du niveau d'assurance fourni par une menace de référence.

6.6. Les États devraient envisager de baser leurs prescriptions pour la protection physique des matières et installations nucléaires sur une menace de référence en particulier concernant l'enlèvement non autorisé de matières nucléaires de catégorie 1 et le sabotage de matières nucléaires et d'installations nucléaires pouvant avoir de graves conséquences radiologiques, s'ils possèdent de telles matières ou installations [2]. Ils devraient également songer à élaborer une

menace de référence pour les autres cas dans lesquels un acte malveillant pourrait selon eux avoir des conséquences graves.

6.7. L'élaboration d'une menace de référence devrait être envisagée pour la protection des matières nucléaires, des autres matières radioactives et des activités et installations associées présentant un moindre risque dans les cas où :

a) L'évaluation de la menace contre la sécurité nucléaire nationale révèle l'existence d'une menace avec intention avérée de commettre un acte malveillant.
b) L'évaluation de la menace contre la sécurité nucléaire nationale met en évidence une menace de capacité élevée dont l'intention n'est pas avérée.
c) L'évaluation de la menace contre la sécurité nucléaire nationale est entachée d'une trop grande incertitude en raison d'une insuffisance des données ou d'un manque de confiance dans les sources de données.

6.8. Pour les nouvelles installations, les États peuvent prendre en considération les avantages à long terme qui pourraient découler de la conception de mesures de protection contre des menaces aux attributs et aux caractéristiques plus modérés que ceux indiqués dans l'évaluation de la menace existante contre la sécurité nucléaire nationale, ce afin de réduire les implications financières potentielles des mises à niveau à effectuer une fois l'installation en exploitation.

ÉLABORATION D'UNE MENACE DE RÉFÉRENCE

6.9. Une menace de référence devrait être élaborée à partir de l'évaluation de la menace contre la sécurité nucléaire nationale en suivant les cinq étapes suivantes :

1) examiner le dossier d'évaluation de la menace contre la sécurité nucléaire nationale pour repérer les menaces ayant la motivation, l'intention et/ou les capacités de commettre un acte malveillant ;
2) regrouper les attributs et les caractéristiques des agresseurs ;
3) adapter les attributs et caractéristiques des agresseurs en fonction des facteurs politiques ;
4) ajuster les attributs et caractéristiques des agresseurs en fonction d'installations et d'activités spécifiques ;
5) établir la menace de référence sous sa forme définitive.

Examen du dossier d'évaluation de la menace contre la sécurité nucléaire nationale

6.10. Les cibles contre lesquelles des actes malveillants pourraient avoir des conséquences radiologiques inacceptables, au sens défini par l'État, devraient être recensées. Elles devraient ensuite être examinées en parallèle avec les attributs et les caractéristiques des agresseurs potentiels décrits dans le dossier d'évaluation de la menace contre la sécurité nucléaire nationale, de manière à repérer les menaces pertinentes, susceptibles de provoquer des conséquences radiologiques inacceptables. Les motivations, les intentions et les capacités des agresseurs concernant ces cibles devraient également être examinées.

6.11. Les descriptions des agresseurs figurant dans le dossier d'évaluation de la menace contre la sécurité nucléaire nationale devraient être passées en revue afin de repérer les agresseurs qui ont les capacités de commettre un acte malveillant susceptible d'entraîner des conséquences radiologiques inacceptables. Les agresseurs n'ayant pas les capacités de commettre un tel acte peuvent être exclus de la suite de l'examen. Il convient toutefois de faire preuve de prudence à cet égard. En particulier, aucune menace ne devrait être écartée au motif que le système de sécurité nucléaire mis en place pour protéger une installation ou une activité suffit pour faire échec à l'agresseur concerné. Les mesures de sécurité nucléaire existantes ne devraient pas être prises en compte dans l'évaluation des capacités des agresseurs effectuée pour élaborer une menace de référence[6].

6.12. Tous les agresseurs ayant vraisemblablement les capacités de commettre un acte malveillant susceptible d'entraîner des conséquences radiologiques inacceptables devraient faire l'objet d'un examen plus approfondi visant à établir s'ils ont aussi des motivations suffisantes ou l'intention de commettre un tel acte. Dans la négative, ils peuvent être exclus de la suite de l'examen. Cependant, il importe de faire preuve de prudence lorsqu'on envisage d'exclure un agresseur ayant d'importantes capacités uniquement au motif qu'il semble manquer de motivation ou d'intention. Avant de prendre une telle décision, il convient de déterminer si la motivation perçue de l'agresseur est cohérente avec les conséquences qui découleraient de l'acte malveillant envisagé et si les données utilisées pour évaluer la motivation et l'intention de cet agresseur sont suffisamment dignes de confiance.

---

[6] Il s'agit d'une hypothèse délibérément prudente. Il se pourrait, par exemple, que ces mesures de sécurité nucléaire soient plus tard supprimées par l'exploitant si la menace de référence ne tient pas compte des attributs et des caractéristiques des agresseurs contre lesquels elles seraient nécessaires et efficaces.

6.13. Les raisons pour lesquelles un agresseur décrit dans le dossier d'évaluation de la menace contre la sécurité nucléaire nationale n'a pas été pris en compte dans l'élaboration de la menace de référence devraient être parfaitement documentées. Tous les agresseurs écartés devraient être à nouveau pris en considération si de nouvelles informations touchant aux raisons de cette exclusion sont obtenues ultérieurement.

6.14. Ce processus d'élimination devrait se conclure par l'établissement d'une liste de tous les agresseurs crédibles ayant les capacités et, potentiellement, la motivation et l'intention de commettre un acte malveillant susceptible d'entraîner des conséquences radiologiques inacceptables.

Regroupement des attributs et caractéristiques des agresseurs

6.15. Les agresseurs pertinents identifiés à partir du dossier d'évaluation de la menace contre la sécurité nucléaire nationale devraient être classés par type. Les différents types, décrits de manière crédible, peuvent être désignés par des noms indicatifs pour plus de facilité (p. ex. terroristes, criminels, extrémistes) mais devraient être définis à partir d'attributs et de caractéristiques spécifiques. La menace posée par un type d'agresseur devrait traduire l'ensemble des attributs et caractéristiques des agresseurs de ce type.

6.16. Les attributs et caractéristiques associés à un type d'agresseur donné devraient être regroupés en un ensemble représentant non pas une combinaison des attributs et des caractéristiques les plus extrêmes de ce type d'agresseur mais un profil crédible pouvant correspondre à un agresseur réel.

Adaptation des attributs et caractéristiques des agresseurs en fonction des facteurs politiques

6.17. Les attributs et de caractéristiques des agresseurs devraient être examinés à la lumière des facteurs politiques pertinents recensés et modifiés, si nécessaire, pour garantir le maintien du niveau de sécurité. Le niveau de capacités présumé des agresseurs peut devoir être révisé à la suite de cet examen.

6.18. Par exemple, les attributs et caractéristiques des agresseurs peuvent être adaptés pour satisfaire au degré de prudence souhaité dans l'évaluation de la menace contre la sécurité nucléaire nationale. L'objectif peut être de corriger l'incertitude et les différences d'interprétation des données utilisées pour l'évaluation de la menace contre la sécurité nucléaire nationale, de garantir que les systèmes et mesures de sécurité nucléaire des exploitants restent efficaces malgré l'évolution

de la menace, ou d'inclure les attributs et les caractéristiques des menaces concernant lesquelles il n'existe alors que peu ou pas de renseignements, par mesure de précaution.

6.19. Les attributs et caractéristiques des agresseurs peuvent aussi être adaptés pour des raisons liées au rapport coûts-avantages. L'objectif pourrait être de concilier les avantages des cibles potentielles pour la société, les conséquences d'actes malveillants contre ces cibles pour la société et les coûts pour cette même société de la réduction des risques de tels actes par la mise en œuvre de mesures de sécurité nucléaire appropriées, en comparaison avec les mesures de protection d'autres biens susceptibles d'entraîner des conséquences de même gravité (p. ex. des explosifs, des produits chimiques ou agents biologiques) ou d'autres infrastructures critiques.

6.20. D'autres facteurs politiques peuvent devoir être pris en compte, notamment la répartition des responsabilités en matière de sécurité nucléaire entre l'État et les exploitants, les répercussions sur la confiance du public des décisions concernant l'acceptation des risques, la contribution des cibles potentielles au bien-être public (p. ex. les applications dans lesquelles des matières nucléaires ou radioactives sont utilisées), la confiance des États voisins dans la sécurité nucléaire d'un État et les menaces dans les États voisins.

6.21. La prudence et les autres facteurs politiques mentionnés ici pourraient inciter à revoir à la hausse les niveaux de capacité présumés des différents types d'agresseurs dans la menace de référence, tandis que les considérations touchant au rapport coûts-avantages pourraient pousser à revoir ces capacités à la baisse.

Ajustement des attributs et caractéristiques des agresseurs en fonction d'installations et d'activités spécifiques

6.22. Les attributs et caractéristiques globalement représentatifs des agresseurs, adaptés en fonction des facteurs politiques, devraient être ajustés pour tenir compte des particularités d'installations et d'activités spécifiques. En ce qui concerne les installations, il peut s'agir de l'emplacement et de l'accessibilité du site, des caractéristiques de conception propres à l'installation, des pratiques d'exploitation et des menaces locales spécifiques. Pour ce qui est des activités, il peut s'agir des procédures d'exploitation, des modes et voies de transport et des menaces propres à des lieux ou à des itinéraires particuliers.

Établissement de la menace de référence sous sa forme définitive

6.23. Les observations des autres autorités compétentes et des parties concernées devraient être prises en considération avant que la menace de référence soit utilisée dans le cadre réglementaire. La décision finale concernant le contenu d'une menace de référence et la responsabilité générale à cet égard devraient revenir à l'autorité compétente chargée par l'État de diriger l'élaboration de cette menace.

6.24. Un modèle de menace de référence figure dans l'appendice.

ÉLABORATION D'UN ÉNONCÉ DE LA MENACE REPRÉSENTATIVE

6.25. À l'instar de la menace de référence, l'énoncé de la menace représentative devrait être élaboré sur la base de l'évaluation de la menace contre la sécurité nucléaire nationale. La procédure est la même que pour la menace de référence, décrite aux paragraphes 6.9 à 6.24, mais elle est généralement moins rigoureuse à chaque étape et peut faire intervenir moins d'organismes. De plus, les attributs et caractéristiques des agresseurs ne doivent pas être ajustés en fonction d'une installation ou d'une activité spécifique.

6.26. Les énoncés de la menace représentative devraient être établis en suivant les quatre étapes suivantes :

1) examiner le dossier d'évaluation de la menace contre la sécurité nucléaire nationale pour repérer les menaces ayant la motivation, l'intention et/ou les capacités de commettre un acte malveillant ;
2) regrouper les attributs et caractéristiques des agresseurs en ensembles représentatifs ;
3) adapter les attributs et caractéristiques représentatifs des agresseurs en fonction des considérations politiques pertinentes ;
4) établir l'énoncé de la menace représentative sous sa forme définitive.

MENACES COMPRISES OU NON DANS LA MENACE DE RÉFÉRENCE

6.27. L'évaluation de la menace contre la sécurité nucléaire nationale permet souvent de détecter un large éventail de capacités d'agresseurs. En tenant compte des menaces connues, réelles et actuelles, l'État devrait définir un niveau de menace ou de capacité au-delà duquel la responsabilité de l'intervention lui

incomberait à lui plutôt qu'à l'exploitant, qui pourrait ne pas avoir les moyens et/ou les ressources nécessaires en matière de protection et d'intervention pour faire face à de telles capacités et aux conséquences qui en découleraient. Toutefois, l'exploitant pourrait avoir un rôle à jouer en aidant l'État à assurer la protection face à ces menaces contre la sécurité nucléaire ou à en atténuer les conséquences.

6.28. Les menaces de référence devraient être fondées sur les agresseurs dont les capacités sont inférieures à ce niveau ; l'exploitant n'aurait donc pas la responsabilité première de la protection et de l'intervention face à des agresseurs aux capacités supérieures, cette responsabilité incombant avant tout à l'État. Ce dernier devra tenir compte du coût, des conséquences opérationnelles et d'autres considérations pour déterminer ce niveau.

7. UTILISATION DES MENACES DE RÉFÉRENCE ET DES ÉNONCÉS DE LA MENACE REPRÉSENTATIVE

7.1. Comme indiqué aux paragraphes 6.2 à 6.8, les États peuvent choisir d'appliquer une approche réglementaire basée sur les résultats, une approche réglementaire basée sur les prescriptions ou une approche combinée. La présente section traite de l'utilisation des menaces de référence et des énoncés de la menace représentative dans le cadre de ces différentes approches.

APPROCHE RÉGLEMENTAIRE BASÉE SUR LES RÉSULTATS

7.2. Dans le cadre d'une approche réglementaire basée sur les résultats, les menaces de référence et les objectifs de sécurité nucléaire de l'État forment la base de la conception, de la mise en œuvre et de l'évaluation des systèmes et mesures de sécurité nucléaire.

7.3. L'utilisation de menaces de référence dans le cadre d'une approche basée sur les résultats suppose ce qui suit :

a) L'organisme de réglementation devrait transmettre les menaces de référence aux exploitants.
b) Chaque exploitant devrait, en coopération avec l'organisme de réglementation, définir des scénarios d'attaque crédibles sur la base des menaces de référence fournies.

c) Les exploitants devraient concevoir des systèmes et des mesures de sécurité nucléaire efficaces contre les scénarios d'attaque définis pour leur installation ou activité respective.
d) Chaque exploitant devrait décrire son système de sécurité nucléaire dans son plan de sécurité et soumettre ce plan à l'organisme de réglementation pour approbation, si nécessaire.
e) L'organisme de réglementation devrait évaluer l'efficacité du système de sécurité nucléaire de chaque exploitant sur la base du plan de sécurité soumis.
f) Une fois le plan de sécurité approuvé, l'exploitant peut exploiter son installation ou mener son activité.

7.4. Les organismes d'intervention d'urgence compétents, notamment l'organisme de réglementation et l'exploitant, devraient utiliser les résultats de l'évaluation de la menace contre la sécurité nucléaire nationale pour évaluer les dangers en vue d'établir des mesures d'urgence adéquates s'agissant de la préparation et de la conduite des interventions en cas de situation d'urgence nucléaire ou radiologique déclenchée par un événement de sécurité nucléaire et de la coordination et l'intégration des interventions d'urgence.

APPROCHE RÉGLEMENTAIRE BASÉE SUR LES PRESCRIPTIONS

7.5. Dans le cadre d'une approche réglementaire basée sur les prescriptions, l'organisme de réglementation devrait utiliser les énoncés de la menace représentative correspondant aux différentes catégories de matières et aux différents types d'installation ou d'activité pour élaborer des prescriptions réglementaires, en tenant compte des objectifs de sécurité nucléaire définis par l'État. Ces prescriptions devraient indiquer les systèmes et les mesures de sécurité nucléaire qu'il convient d'appliquer pour assurer une protection suffisante en vue d'atteindre les objectifs du régime de sécurité nucléaire de l'État. Des orientations susceptibles d'aider les États à élaborer de telles prescriptions figurent dans les références [13] à [16].

7.6. L'utilisation d'énoncés de la menace représentative dans le cadre d'une approche basée sur les prescriptions suppose ce qui suit :

a) L'organisme de réglementation devrait définir des scénarios d'attaque crédibles sur la base des différents énoncés de la menace représentative et concevoir des mesures de sécurité nucléaire pour différentes catégories de matières et différents types d'installations et d'activités.

b) L'organisme de réglementation devrait examiner les mesures recommandées ou suggérées dans les publications pertinentes de l'AIEA, notamment les références [2, 3, 9] et [13] à [16], selon qu'il convient, et déterminer si ces mesures suffisent pour atteindre les objectifs de sécurité nucléaire ou si des mesures supplémentaires doivent être prises pour assurer le niveau de protection demandé dans l'énoncé de la menace représentative.
c) L'organisme de réglementation devrait élaborer des prescriptions réglementaires concernant l'application des mesures de sécurité nucléaire.
d) Les exploitants devraient mettre en œuvre les mesures de sécurité nucléaire spécifiées dans les prescriptions réglementaires.

APPROCHE COMBINÉE

7.7. Comme indiqué au paragraphe 6.2 et dans les références [13] et [14], des éléments de l'approche basée sur les prescriptions et de l'approche basée sur les résultats sont utilisés dans le cadre d'une approche combinée.

7.8. L'État peut appliquer une approche basée sur les résultats pour les installations et activités lorsque les avantages sont supérieurs aux coûts, par exemple qu'une plus grande assurance est souhaitable compte tenu des conséquences que pourrait avoir un événement de sécurité nucléaire. Une approche basée sur les prescriptions pourrait être appliquée aux matières et aux installations et activités associées dans les cas où les conséquences potentielles d'un événement de sécurité nucléaire sont moins graves. L'État peut aussi décider qu'une approche basée sur les résultats devrait être utilisée pour certaines menaces et une approche basée sur les prescriptions pour d'autres.

ÉLABORATION DE SCÉNARIOS D'ATTAQUE

7.9. Pour élaborer des scénarios d'attaque, il est nécessaire de comprendre comment les attributs et caractéristiques des agresseurs pourraient être utilisés pour commettre un acte malveillant et de savoir si et comment différents agresseurs pourraient coopérer pour commettre un tel acte.

7.10. Un scénario d'attaque est un ensemble postulé ou présumé de conditions et d'événements couramment utilisé dans des analyses ou des évaluations pour représenter des conditions et des événements futurs possibles pouvant être modélisés, comme des événements de sécurité nucléaire. Il peut représenter les conditions à un moment donné ou lors d'un événement précis ou une

succession de conditions ou d'événements (y compris de processus) menant ou faisant suite à un événement de sécurité nucléaire, comme des conséquences potentielles différées.

7.11. Les scénarios d'attaque devraient tenir compte de toutes les combinaisons crédibles d'attributs et de caractéristiques définis dans un énoncé de la menace représentative ou une menace de référence, y compris de la possibilité de collusion entre initiés et agresseurs externes et de combinaison d'attaque physique et de cyberattaque. Ils devraient définir : a) les voies d'accès possibles ; b) les délais d'intrusion selon les tactiques d'attaque présumées et le temps nécessaire aux mesures de sécurité physique et informatique ; et c) les probabilités de détection en fonction des capteurs et des mesures de surveillance et des tactiques présumées utilisées pour les contourner ou les déjouer.

7.12. Il convient en particulier d'étudier les scénarios d'attaque impliquant une cyberattaque. En effet, s'il est peu probable qu'une cyberattaque permette à elle seule un enlèvement non autorisé de matières, elle pourrait compromettre les mesures de sécurité nucléaire mises en place pour dissuader, détecter, retarder ou contrer une tentative d'enlèvement non autorisé ou de sabotage. Elle pourrait également endommager les fonctions de sûreté, de sécurité, de comptabilité et de contrôle des matières nucléaires et de préparation et de conduite des interventions d'urgence pour faciliter une attaque physique.

7.13. Plusieurs facteurs influencent la faisabilité d'une attaque, notamment la complexité de cette attaque, la quantité et le niveau de sophistication des outils et autres ressources nécessaires, les compétences et les capacités des agresseurs, leur connaissance de l'installation et des points d'accès (notamment des endroits où ils peuvent se cacher ou dissimuler des outils, et des points faibles des systèmes qu'ils peuvent exploiter), le nombre total d'agresseurs externes, les capacités des forces d'intervention, le nombre et la nature des initiés impliqués et leur degré de collusion, et l'efficacité des barrières physiques, des mesures de sécurité informatique et des technologies de détection et de surveillance.

8. MAINTIEN DE LA VALIDITÉ ET RÉEXAMEN DE L'ÉVALUATION DE LA MENACE CONTRE LA SÉCURITÉ NUCLÉAIRE NATIONALE ET DU DOSSIER ASSOCIÉ AINSI QUE DES ÉNONCÉS DE LA MENACE

8.1. Le dossier d'évaluation de la menace contre la sécurité nucléaire nationale devrait être réexaminé périodiquement pour déterminer si l'évaluation donne toujours une image exhaustive et équilibrée des menaces crédibles contre la sécurité nucléaire dans l'État, et l'évaluation devrait être révisée si nécessaire.

8.2. Les menaces de référence et les énoncés de la menace représentative devraient aussi être réexaminés (et révisés, le cas échéant) pour tenir compte de la révision éventuelle du dossier d'évaluation de la menace contre la sécurité nucléaire nationale, de l'évolution des facteurs politiques ou de l'expérience acquise lors de la conception et de l'évaluation des systèmes et mesures de sécurité nucléaire ou d'un événement de sécurité nucléaire.

8.3. L'évaluation de la menace contre la sécurité nucléaire nationale, les menaces de référence et les énoncés de la menace représentative pourraient être réexaminés tous les 12 à 18 mois, par exemple, en suivant la procédure d'élaboration de l'évaluation de la menace contre la sécurité nucléaire nationale.

8.4. Les menaces nouvelles et émergentes et les capacités qui a priori ne touchent pas directement à la sécurité nucléaire pourraient être prises en compte dans le réexamen de l'évaluation de la menace contre la sécurité nucléaire nationale afin de déterminer si elles sont pertinentes pour les matières nucléaires, les autres matières radioactives et les installations et activités associées.

8.5. Il se peut que l'évaluation de la menace contre la sécurité nucléaire nationale, les menaces de référence et les énoncés de la menace représentative doivent être réexaminés en dehors du processus d'examen périodique. Les conditions et événements susceptibles d'exiger un réexamen comprennent :

a) Tout acte ou événement, dans l'État ou en dehors, directement lié ou non aux matières nucléaires, aux autres matières radioactives ou aux installations ou activités associées, qui modifie sensiblement la perception ou le niveau réel de la menace contre la sécurité nucléaire.

b) Des changements importants au niveau de la gouvernance, de la législation ou des arrangements internationaux qui ont des répercussions sur la responsabilité des autorités compétentes ou de l'exploitant, par exemple une modification du dispositif d'intervention ou des responsabilités organisationnelles.
c) Des modifications des installations ou activités associées aux matières nucléaires ou à d'autres matières radioactives qui pourraient entraîner une modification des conséquences potentielles ou en faire apparaître de nouvelles. Il pourrait s'agir, par exemple, de la construction d'une installation de type différent, de l'utilisation de matières ayant un plus haut niveau d'enrichissement, de nouvelles pratiques mettant en jeu des matières, de la réexpédition d'uranium hautement enrichi, de la modification des opérations en vue de l'utilisation de matières de plus basse catégorie ou d'améliorations de la sûreté nucléaire.
d) Une proposition de réexamen émanant d'une autorité compétente, d'un organisme d'appui technique ou scientifique ou d'un exploitant.

8.6. L'évaluation de la menace contre la sécurité nucléaire nationale, les menaces de référence et les énoncés de la menace représentative ne sont pas systématiquement révisés à la suite de leur réexamen. Toutefois, s'il apparaît que l'évaluation de la menace contre la sécurité nucléaire nationale ne tient pas compte comme il se doit de toutes les menaces crédibles, y compris les menaces nouvelles et émergentes, cette évaluation et le dossier associé devraient être révisés en collaboration avec tous les organismes concernés. Si des modifications substantielles ou fondamentales sont effectuées, les menaces de référence et les énoncés de la menace représentative devraient également être révisés.

CONTRER LES MENACES NOUVELLES ET ÉMERGENTES

8.7. Il est possible que, en dehors du processus de réexamen périodique, des éléments viennent suggérer ou démontrer que des agresseurs possèdent des capacités physiques ou informatiques nouvelles ou inattendues qui, en raison de leur niveau de menace, exigent une intervention immédiate de l'État. Des renseignements et des informations à ce sujet peuvent être obtenus par des voies officielles ou informelles.

8.8. En plus d'élaborer les menaces de référence et les énoncés de la menace représentative et de maintenir leur validité, l'organisme de réglementation et les autres autorités compétentes devraient mettre en place un mécanisme d'échange d'informations sur les menaces entre les autorités compétentes et entre

ces autorités et les exploitants concernés. C'est d'autant plus important dans les cas où le niveau de la menace change rapidement et que le temps manque pour procéder à un réexamen complet de l'évaluation de la menace contre la sécurité nucléaire nationale.

8.9. Si un exploitant reçoit des informations sur un tel changement de la menace par des voies informelles, il devrait en informer l'organisme de réglementation et les autres autorités compétentes, le cas échéant, pour leur permettre d'évaluer la crédibilité, la pertinence et la gravité des conséquences potentielles de ce changement et de déterminer comment, et avec quel degré d'urgence, l'État et/ou l'exploitant doivent réagir.

8.10. La mise en place d'un système définissant des niveaux de menace élevés et les mesures de sécurité nucléaire supplémentaires à appliquer par l'exploitant à chaque niveau peut offrir une protection supplémentaire dans de telles situations.

Appendice

MODÈLE DE MENACE DE RÉFÉRENCE

A.1. Le tableau 1 montre à titre d'exemple comment les attributs et caractéristiques d'un agresseur peuvent être indiqués dans une menace de référence.

A.2. Un format similaire, généralement moins détaillé, ou un format plus informel peuvent être utilisés pour les énoncés de la menace représentative.

TABLEAU 1. EXEMPLE DE MENACE DE RÉFÉRENCE LISTANT LES ATTRIBUTS ET CARACTÉRISTIQUES D'UN AGRESSEUR

	Armé	Non armé
Acte		
Vol[a]	*Oui* ou *non*	*Oui* ou *non*
Sabotage[b]	*Oui* ou *non*	*Oui* ou *non*
Attributs et caractéristiques ordinaires		
Nombre	Indiquer un nombre	Indiquer un nombre
Ressources financières	*Faibles* ou *élevées*	*Faibles* ou *élevées*
Soutien d'initiés	*Actifs* ou *passifs*, *violents* ou *non violents*	*Actifs* ou *passifs*, *violents* ou *non violents*
Tactique	*Furtivité* et/ou *force*	*Furtivité* et/ou *force*
Compétences de planification	*Capacité de planifier une diversion*, et/ou *attaques simultanées par de plus petits groupes*, et/ou *connaissance de l'agencement de l'installation* et/ou *capacité de planifier une attaque combinée*	*Capacité de planifier une diversion*, et/ou *attaques simultanées par de plus petits groupes*, et/ou *connaissance de l'agencement de l'installation* et/ou *capacité de planifier une attaque combinée*

TABLEAU 1. EXEMPLE DE MENACE DE RÉFÉRENCE LISTANT LES ATTRIBUTS ET CARACTÉRISTIQUES D'UN AGRESSEUR (suite)

	Armé	Non armé
Attributs et caractéristiques physiques		
Disposition à tuer	*Oui* ou *non*	*Oui* ou *non*
Disposition à mourir	*Oui* ou *non*	*Oui* ou *non*
Voie d'accès	*Aérienne*, *routière*, *ferroviaire*, *maritime* et/ou *souterraine*	*Aérienne*, *routière*, *ferroviaire*, *maritime* et/ou *souterraine*
Type d'armes	*Armes automatiques*, *armes semi-automatiques*, *armes de poing* et/ou *couteaux*	Sans objet
Explosifs	Indiquer le type et la quantité d'explosifs	Sans objet
Outils	*Outils électriques*, *outils manuels* et/ou *outils disponibles sur place*	*Outils électriques*, *outils manuels* et/ou *outils disponibles sur place*
Compétences techniques	*Ouverture de brèche à l'explosif*, *mise hors service des lignes de communication* et/ou *exploitation du matériel de l'installation*	*Ouverture de brèche à l'explosif*, *mise hors service des lignes de communication* et/ou *exploitation du matériel de l'installation*
Rôle des initiés	*Autorisation d'accès*, *agent de sécurité*, *maintenance technique du matériel* et/ou *manipulation du matériel*	*Autorisation d'accès*, *agent de sécurité*, *maintenance technique du matériel* et/ou *manipulation du matériel*
Attributs et caractéristiques informatiques		
Logiciels	*Logiciels standard*, *logiciels malveillants* et/ou *outils développés par l'agresseur*	*Logiciels standard*, *logiciels malveillants* et/ou *outils développés par l'agresseur*

TABLEAU 1. EXEMPLE DE MENACE DE RÉFÉRENCE LISTANT LES ATTRIBUTS ET CARACTÉRISTIQUES D'UN AGRESSEUR (suite)

	Armé	Non armé
Compétences	*Ingénierie sociale*, *utilisation d'outils commerciaux*, *développement de logiciels, bureautique*, *contrôle de processus* et/ou *connaissance du système informatique appliqué*	*Ingénierie sociale*, *utilisation d'outils commerciaux*, *développement de logiciels, bureautique*, *contrôle de processus* et/ou *connaissance du système informatique appliqué*
Matériel	*Ordinateur*, *téléphone portable*, *connexion aux câbles* et/ou *routeurs*	*Ordinateur*, *téléphone portable*, *connexion aux câbles* et/ou *routeurs*
Capacité d'influencer la chaîne d'approvisionnement	*Oui* ou *non*	*Oui* ou *non*
Ténacité de l'agresseur	*Capacité d'attaque à long terme* et/ou *capacité d'attaque répétée*	*Capacité d'attaque à long terme* et/ou *capacité d'attaque répétée*
Rôle des initiés	*Autorisation d'accès*, *contrôle des processus des systèmes de contrôle-commande par les utilisateurs normaux*, *administrateur* et/ou *fournisseur tiers*	*Autorisation d'accès*, *contrôle des processus des systèmes de contrôle-commande par les utilisateurs normaux*, *administrateur* et/ou *fournisseur tiers*

[a] Des critères concernant la quantité de matières enlevée et/ou la récurrence du vol peuvent être ajoutés.

[b] Des critères concernant les conséquences radiologiques peuvent être ajoutés.

RÉFÉRENCES

[1] 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).

[2] 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).

[3] 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).

[4] 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).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G, IAEA, Vienna (in preparation).

[6] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, ORGANISATION INTERNATIONALE DE POLICE CRIMINELLE-INTERPOL, Approche tenant compte des risques pour les mesures de sécurité nucléaire visant les matières nucléaires et autres matières radioactives non soumises à un contrôle réglementaire, nº 24-G de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2022).

[7] Convention sur la protection physique des matières nucléaires, INFCIRC/274/Rev.1, AIEA, Vienne (1980).

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

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8-G (Rev. 1), IAEA, Vienna (2020).

[10] 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).

[11] AGENCE DE L'OCDE POUR L'ÉNERGIE NUCLÉAIRE, AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, BUREAU DE LA COORDINATION DES AFFAIRES HUMANITAIRES DE L'ONU, COMMISSION PRÉPARATOIRE DE L'ORGANISATION DU TRAITÉ D'INTERDICTION COMPLÈTE DES ESSAIS NUCLÉAIRES, INTERPOL, ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE, ORGANISATION DES NATIONS UNIES POUR L'ALIMENTATION ET L'AGRICULTURE, ORGANISATION INTERNATIONALE DU TRAVAIL, ORGANISATION MARITIME INTERNATIONALE, ORGANISATION MÉTÉOROLOGIQUE MONDIALE, ORGANISATION MONDIALE DE LA SANTÉ, ORGANISATION PANAMÉRICAINE DE LA SANTÉ, PROGRAMME DES NATIONS UNIES POUR L'ENVIRONNEMENT, Préparation et conduite des interventions en cas de situation d'urgence nucléaire ou radiologique, nº GSR Part 7 de la collection Normes de sûreté de l'AIEA, AIEA, Vienne (2017).

[12] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR OFFICE, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, Arrangements for Preparedness for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GS-G-2.1, IAEA, Vienna (2007).

[13] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Protection physique des matières nucléaires et des installations nucléaires (Guide d'application de la publication INFCIRC/225/Révision 5), nº 27-G de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2019).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Material in Use and Storage and of Associated Facilities, IAEA Nuclear Security Series No. 11-G (Rev. 1), IAEA, Vienna (2019).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Material in Transport, IAEA Nuclear Security Series No. 9-G (Rev. 1), IAEA, Vienna (2020).

[16] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Sécurité des matières nucléaires en cours de transport, nº 26-G de la collection Sécurité nucléaire de l'AIEA, AIEA, Vienne (2019).

GLOSSAIRE

énoncé de la menace. Description des agresseurs crédibles (y compris de leurs attributs et caractéristiques) sous la forme d'une menace de référence ou d'un énoncé de la menace représentative, élaborée sur la base de l'évaluation de la menace contre la sécurité nucléaire nationale.

énoncé de la menace représentative. Attributs et caractéristiques d'initiés et/ou d'agresseurs externes potentiels susceptibles de tenter un enlèvement non autorisé ou un acte de sabotage, servant à l'élaboration de prescriptions réglementaires pour la protection de matières et/ou d'installations données.

évaluation de la menace. Évaluation des menaces — effectuée à partir des informations fournies par les services de renseignement et les forces de l'ordre et des informations en libre accès — qui décrit les motivations, les intentions et les capacités de ces menaces.

menace de référence. Attributs et caractéristiques d'initiés et/ou d'agresseurs externes potentiels susceptibles de tenter un enlèvement non autorisé ou un acte de sabotage contre lesquels un système de protection physique est conçu et évalué.

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

La présente publication décrit les étapes à suivre pour réaliser une évaluation de la menace contre la sécurité nucléaire nationale, en tenant compte des aspects physiques et informatiques, et pour élaborer, utiliser et actualiser les menaces de référence et les énoncés de la menace représentative. Elle est destinée aux États, aux autorités compétentes (y compris l'organisme de réglementation), aux organismes d'appui technique et scientifique compétents, aux exploitants d'installations mettant en jeu des matières nucléaires et autres matières radioactives et aux personnes menant des activités connexes, y compris les expéditeurs et les transporteurs.

AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE
VIENNE