Collection Sécurité nucléaire de l'AIEA – Nº 10

Guide d'application

Élaboration, utilisation et actualisation de la menace de référence

IAEA
Agence internationale de l'énergie atomique

LA COLLECTION SÉCURITÉ NUCLÉAIRE DE L'AIEA

Les publications de la **collection Sécurité nucléaire de l'AIEA** traitent des mesures à prendre (prévention, détection, intervention) contre le vol, le sabotage et la cession illégale de matières nucléaires et de sources radioactives et des installations connexes, l'accès non autorisé à ces matières, sources et installations et les autres actes malveillants dont elles peuvent faire l'objet. Ces publications sont conformes aux instruments internationaux relatifs à la sécurité nucléaire, notamment la Convention sur la protection physique des matières nucléaires telle qu'amendée, le Code de conduite sur la sûreté et la sécurité des sources radioactives, les résolutions 1373 et 1540 du Conseil de sécurité de l'ONU et la Convention internationale pour la répression des actes de terrorisme nucléaire, 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 énoncent les objectifs, les concepts et les principes de la sécurité nucléaire et servent de base pour l'élaboration de recommandations en matière de sécurité.
- Les **Recommandations**, qui présentent les pratiques exemplaires que les États Membres devraient adopter pour la mise en œuvre des Fondements de la sécurité nucléaire.
- Les **Guides d'application,** qui complètent les Recommandations dans certains grands domaines et proposent des mesures pour en assurer la mise en œuvre.
- Les **Orientations techniques**, comprenant les **Manuels de référence**, qui présentent des mesures détaillées et/ou donnent des conseils pour la mise en œuvre des Guides d'application dans des domaines ou des activités spécifiques, les **Guides de formation**, qui présentent les programmes et/ou les manuels des cours de formation de l'AIEA dans le domaine de la sécurité nucléaire, et les **Guides des services,** qui donnent des indications concernant la conduite et la portée des missions consultatives de l'AIEA sur la sécurité nucléaire.

RÉDACTION ET EXAMEN

Des experts internationaux aident le Secrétariat de l'AIEA à élaborer ces publications. Pour l'élaboration des Fondements de la sécurité nucléaire, des Recommandations et des Guides d'application, l'AIEA organise des réunions techniques à participation non limitée afin que les États Membres intéressés et les organisations internationales compétentes puissent examiner comme il se doit les projets de texte. En outre, pour faire en sorte que ces projets soient examinés de façon approfondie et largement acceptés au niveau international, le Secrétariat les soumet aux États Membres, qui disposent de 120 jours pour les examiner officiellement, ce qui leur donne la possibilité d'exprimer pleinement leurs vues avant que le texte soit publié.

Les publications de la catégorie Orientations techniques sont élaborées en consultation étroite avec des experts internationaux. Il n'est pas nécessaire d'organiser des réunions techniques, mais on peut le faire lorsque cela est jugé nécessaire pour recueillir un large éventail de points de vue.

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 spécifiques 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.

ÉLABORATION, UTILISATION ET ACTUALISATION DE LA MENACE DE RÉFÉRENCE

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

AFGHANISTAN, RÉP. ISLAMIQUE D'
AFRIQUE DU SUD
ALBANIE
ALGÉRIE
ALLEMAGNE
ANGOLA
ARABIE SAOUDITE
ARGENTINE
ARMÉNIE
AUSTRALIE
AUTRICHE
AZERBAÏDJAN
BAHREÏN
BANGLADESH
BÉLARUS
BELGIQUE
BELIZE
BÉNIN
BOLIVIE
BOSNIE-HERZÉGOVINE
BOTSWANA
BRÉSIL
BULGARIE
BURKINA FASO
BURUNDI
CAMBODGE
CAMEROUN
CANADA
CHILI
CHINE
CHYPRE
COLOMBIE
CONGO
CORÉE, RÉPUBLIQUE DE
COSTA RICA
CÔTE D'IVOIRE
CROATIE
CUBA
DANEMARK
DOMINIQUE
ÉGYPTE
EL SALVADOR
ÉMIRATS ARABES UNIS
ÉQUATEUR
ÉRYTHRÉE
ESPAGNE
ESTONIE
ÉTATS-UNIS D'AMÉRIQUE
ÉTHIOPIE
FÉDÉRATION DE RUSSIE
FINLANDE
FRANCE
GABON
GÉORGIE
GHANA
GRÈCE
GUATEMALA
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
L'EX-RÉPUBLIQUE YOUGOSLAVE DE MACÉDOINE
LIBAN
LIBÉRIA
LIBYE
LIECHTENSTEIN
LITUANIE
LUXEMBOURG
MADAGASCAR
MALAISIE
MALAWI
MALI
MALTE
MAROC
MAURICE
MAURITANIE, RÉP. ISLAMIQUE DE
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
SAINT-SIÈGE
SÉNÉGAL
SERBIE
SEYCHELLES
SIERRA LEONE
SINGAPOUR
SLOVAQUIE
SLOVÉNIE
SOUDAN
SRI LANKA
SUÈDE
SUISSE
TADJIKISTAN
TCHAD
THAÏLANDE
TUNISIE
TURQUIE
UKRAINE
URUGUAY
VENEZUELA, RÉP. BOLIVARIENNE DU
VIETNAM
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

ÉLABORATION, UTILISATION ET ACTUALISATION DE LA MENACE DE RÉFÉRENCE

GUIDE D'APPLICATION

AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE
VIENNE, 2012

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 2600 29302
téléphone : +43 1 2600 22417
courriel : sales.publications@iaea.org
http://www.iaea.org/books

Imprimé par l'AIEA en Autriche
Août 2012

ÉLABORATION, UTILISATION
ET ACTUALISATION DE LA MENACE
DE RÉFÉRENCE
AIEA, VIENNE, 2012
STI/PUB/1386
ISBN 978–92–0–232810–5
ISSN 1816–9317

AVANT-PROPOS

En application d'une résolution de la Conférence générale de l'AIEA de septembre 2002, l'AIEA a adopté une approche intégrée de la protection contre le terrorisme nucléaire. Cette approche coordonne ses activités concernant la protection physique des matières nucléaires et des installations nucléaires, la comptabilisation des matières nucléaires, la détection et l'intervention en cas de trafic des matières nucléaires et autres matières radioactives, la sécurité des sources radioactives, la sécurité du transport des matières nucléaires et autres matières radioactives, les interventions d'urgence et leur préparation dans les États Membres et à l'AIEA, et la promotion de l'adhésion des États aux instruments internationaux pertinents. L'AIEA aide en outre à déterminer les menaces et la vulnérabilité des matières nucléaires et autres matières radioactives du point de vue de la sécurité. Toutefois, les États ont la responsabilité d'assurer la protection physique des matières nucléaires et autres matières radioactives, ainsi que des installations connexes, de garantir la sécurité de ces matières lors de leur transport, et de lutter contre le trafic illicite et les mouvements fortuits de ces matières.

Le système de protection physique vise à prévenir des conséquences inacceptables résultant d'actions malveillantes. Plus les conséquences sont graves, plus il importe d'avoir un degré de confiance élevé dans l'efficacité de la protection physique, comme elle a été planifiée.

Cette nécessité d'un degré de confiance élevé dans l'efficacité de la protection physique des matières et installations nucléaires est reconnu depuis longtemps par tous ceux qui sont sensibilisés à cette question. Si des matières ou des installations nucléaires sont visées par un acte malveillant, le potentiel existe que les diverses conséquences radiologiques ou de prolifération soient inacceptables. Le niveau de confiance maximum dans la protection physique exige qu'il y ait une étroite corrélation entre les mesures de protection et la menace. Cette approche est fermement ancrée dans le principe fondamental selon lequel la protection physique des actifs nucléaires relevant de la compétence juridictionnelle d'un État devrait être basée sur l'évaluation par l'État de la menace pour ces actifs. Comme expliqué dans la présente publication, le fait de comprendre la menace peut conduire à une description détaillée des agresseurs potentiels (la menace de référence) laquelle, à son tour, est à la base d'un système de protection physique conçu de manière appropriée. Une telle corrélation directe donne l'assurance que la protection serait efficace contre une agression.

L'expérience internationale dans l'utilisation de la menace de référence pour protéger les actifs à haut risque est fondée dans une large mesure sur la protection des

matières et installations nucléaires. En outre, les documents sur la sécurité nucléaire qui définissent et recommandent une protection physique basée sur la menace — *Objectifs et principes fondamentaux de la protection physique* (GOV/2001/41/Appendice), *La protection physique des matières et installations nucléaires* (INFCIRC/225/Rev.4 (Corrigé)), et la Convention sur la protection physique des matières nucléaires (INFCIRC/274) *et son amendement* (adopté le 8 juillet 2005) — le font exclusivement pour la protection des matières nucléaires et des installations nucléaires. Compte tenu du contexte historique et de sa pertinence aujourd'hui encore, il a été nécessaire de s'appuyer sur cette expérience en matière de protection nucléaire pour élaborer la présente publication. Toutefois, l'approche générale peut aussi être appliquée pour la protection d'autres actifs qui nécessitent un degré élevé de confiance dans l'efficacité de leur protection, comme les matières fortement radioactives.

Des spécialistes d'Allemagne, d'Espagne, des États-Unis d'Amérique, de France, du Japon, de la Fédération de Russie et du Royaume-Uni ont apporté leur concours à l'AIEA pour l'élaboration de la présente publication. Un projet a été d'abord présenté en décembre 2006 à une réunion technique à participation non limitée, puis distribué pour observations à tous les États Membres. La présente publication est compatible avec les *Objectifs et principes fondamentaux de la protection physique,* la *Convention sur la protection physique des matières nucléaires et son amendement de 2005,* et *La protection physique des matières et installations nucléaires.*

NOTE DE L'ÉDITEUR

TABLE DES MATIÈRES

1. INTRODUCTION 1

1.1. Généralités 1
1.2. Objectif 1
1.3. Champ d'application 2
1.4. Structure 3

2. DESCRIPTION D'UNE MENACE DE RÉFÉRENCE 4

3. OBJET D'UNE MENACE DE RÉFÉRENCE 8

3.1. Nécessité d'une menace de référence 8
3.2. Intérêt d'une menace de référence 9

4. RÔLES ET RESPONSABILITÉS 10

4.1. L'État 11
4.2. Les autorités compétentes pour l'élaboration, l'utilisation et l'actualisation d'une menace de référence 11
4.3. Les organismes de renseignements 13
4.4. Les exploitants 13
4.5. Les autres organismes 14

5. ÉVALUATION DE LA MENACE 15

5.1. Conduite de l'évaluation de la menace 15
5.1.1. Apports 16
5.1.2. Processus d'analyse 17
5.1.3. Produit 18
5.2. Décision entre l'utilisation d'une menace de référence ou d'une autre approche basée sur la menace 18

6. ÉLABORATION D'UNE MENACE DE RÉFÉRENCE 20

6.1. Apport de la menace de référence 20
6.2. Processus 20
6.2.1. Phase I : Filtrer l'évacuation de la menace 21

6.2.2. Phase II : Traduire les informations sur des menaces spécifiques en termes d'attributs et caractéristiques représentatifs 22
6.2.3. Phase III : Modifier les attributs et caractéristiaues représentatifs compte tenu de facteurs politiques 23
6.3. Produit 25
6.4. Élaboration d'un énoncé de la menace 25

7. UTILISATION DE LA MENACE DE RÉFÉRENCE 27

8. ACTUALISATION DE LA MENACE DE RÉFÉRENCE 30

8.1. Apports 30
8.2. Processus 31
8.3. Produit 31

RÉFÉRENCES 32
GLOSSAIRE 33

1. INTRODUCTION

1.1. GÉNÉRALITÉS

Le document INFCIRC/225/Rev.4 (Corrigé) [1] intitulé “La protection physique des matières et des installations nucléaires” présente l’outil qu’est la menace de référence et recommande l’élaboration d’une menace de référence nationale. Conscients de l’importance accordée à la menace de référence dans le document INFCIRC/225, plusieurs États Membres de l’AIEA ont demandé que des ateliers soient organisés en vue de présenter une méthodologie sur l’élaboration, l’actualisation et l’utilisation d’une menace de référence. En complément des ateliers, un projet a été élaboré et distribué pour observations.

Ce projet avait pour but la mise en œuvre des recommandations figurant dans le document INFCIRC/225/Rev.4 (Corrigé) publié en 1999. Depuis, de nouveaux travaux ont permis de renforcer le régime international de protection physique des matières nucléaires et des matières radioactives et de leurs installations, notamment l’approbation par le Conseil des gouverneurs de l’AIEA en septembre 2001 des Objectifs et principes fondamentaux de la protection physique (GOV/2001/41/Appendice) [2] et l’approbation de la version révisée du Code de conduite sur la sûreté et la sécurité des sources radioactives par le Conseil des gouverneurs en 2004. Ces objectifs et principes ont ensuite été pris en compte dans l’amendement du 8 juillet 2005 à la Convention sur la protection physique des matières nucléaires [3]. Ce guide d’application est une mise à jour du projet de guide original dans laquelle ont été pris en compte les résultats de nouveaux travaux.

1.2. OBJECTIF

Une menace de référence définit de manière exhaustive les motivations, intentions et capacités d’agresseurs potentiels sur la base desquelles sont conçus et évalués les systèmes de protection. Ces définitions permettent de planifier la sécurité sur la base de la gestion des risques. Une menace de référence est établie à partir d’informations émanant de services de renseignements et d’autres données crédibles portant sur des menaces, mais elle ne se veut pas une affirmation de l’existence de menaces réelles. Par le passé, les États ont utilisé les menaces de référence dans leur système de réglementation pour pouvoir allouer des ressources appropriées à la protection des matières et installations nucléaires contre des actes malveillants d’agresseurs potentiels qui pourraient avoir de graves conséquences, notamment radiologiques ou de prolifération ; toutefois,

une menace de référence peut aussi être utilisée pour protéger tous actifs associés à des conséquences potentiellement graves (par ex. d'autres matières hautement radioactives).

La présente publication donne des orientations sur la manière d'élaborer, d'utiliser et d'actualiser une menace de référence. Elle s'adresse aux décideurs dans les organismes auxquels sont assignés des rôles et responsabilités en rapport avec l'élaboration, l'utilisation et l'actualisation de la menace de référence.

1.3. CHAMP D'APPLICATION

Le présent guide d'application :

— Décrit une menace de référence, ce qu'elle est et pour quelles raisons et dans quelles circonstances elle est utilisée ;
— Détermine et recommande les rôles et responsabilités des organismes qui devraient participer à l'élaboration, l'utilisation et l'actualisation d'une menace de référence ;
— Indique comment réaliser une évaluation nationale de la menace comme préalable à une menace de référence ;
— Explique comment une menace de référence peut être élaborée, y compris :
  • les informations requises pour son élaboration ;
  • les processus décisionnels pertinents ;
— Explique comment une menace de référence est incorporée dans le régime de sécurité nucléaire d'un État[1] ;
— Explique les conditions du réexamen de la menace de référence et comment celle-ci est réexaminée et actualisée.

[1] Le régime de sécurité nucléaire comprend toutes les activités de sécurité nucléaire dans un État pour la protection des matières nucléaires et radioactives et de leurs installations (y compris le transport) et pour la prévention du trafic illicite. Il englobe le cadre législatif et réglementaire, la désignation des autorités compétentes, la définition des responsabilités entre l'État et l'exploitant en ce qui concerne la sécurité nucléaire, les mesures administratives et les caractéristiques techniques dans l'installation, dans le transport ou aux points de contrôle pour empêcher l'enlèvement non autorisé et le trafic illicite de matières nucléaires ou radioactives et le sabotage radiologique d'installations nucléaires ou radiologiques. Il inclut également les mesures visant à faciliter l'atténuation des conséquences d'un tel acte malveillant s'il venait à se produire, y compris la récupération des matières volées.

La présente publication n'inclut ni les recommandations de mesures de protection physique ni les orientations sur la conception et l'évaluation des systèmes de protection physique.

1.4. STRUCTURE

Après la section 1 qui présente les généralités, la section 2 présente une menace de référence. La section 3 présente l'objectif et l'intérêt d'une menace de référence dans le régime de sécurité nucléaire d'un État. La section 4 indique les rôles et responsabilités pour l'élaboration, l'utilisation et l'actualisation d'une menace de référence. La section 5 indique l'approche pour effectuer une évaluation de la menace comme préalable à l'élaboration d'une menace de référence. La section 6 décrit le processus d'élaboration d'une menace de référence en partant du produit de l'évaluation de la menace. La section 7 montre comment une menace de référence est utilisée dans le régime de sécurité nucléaire d'un État. La section 8 examine comment une menace de référence est actualisée.

NOTE

La présente publication recommande que les informations émanant des services nationaux de renseignements et autres informations sensibles soient mises à profit et que les agences nationales de renseignements participent à l'élaboration des deux processus : l'évaluation de la menace et la menace de référence. Certaines de ces informations et nombre de leurs sources doivent être protégées. Cela suppose en principe le recours à un système national de classement des informations et à des mesures de protection correspondantes. La menace de référence elle-même, du fait qu'elle est utilisée dans la conception et l'évaluation des systèmes de protection physique, présenterait aussi de l'intérêt pour un agresseur qui voudrait perpétrer un acte malveillant. Il est donc essentiel qu'elle soit protégée de manière appropriée. Ceux qui ont accès à une menace de référence doivent habituellement avoir une autorisation en bonne et due forme, conformément à la législation et la réglementation nationales, ainsi que les moyens physiques de la stocker et de la protéger.

2. DESCRIPTION D'UNE MENACE DE RÉFÉRENCE

Un principe fondamental de la protection physique est qu'elle devrait être basée sur l'évaluation par l'État d'une menace existante [2]. Cette évaluation est formalisée dans un processus d'évaluation de la menace. Une menace de référence est établie à partir de cette évaluation de la menace par l'État en vue de faciliter l'élaboration de la protection physique. Pour définir la menace de référence, l'ensemble des menaces décrites dans l'évaluation de la menace par l'État est modifié pour prendre en compte d'autres facteurs, tels que des considérations techniques, économiques et politiques, ainsi que des exigences de planification particulières pour la conception d'un système de protection physique. Une analyse rigoureuse et une prise de décisions sont essentielles pour transformer l'évaluation de la menace en une menace de référence.

Une menace de référence décrit les attributs et caractéristiques d'agresseurs potentiels externes ou d'origine interne qui pourraient tenter de perpétrer un acte malveillant, comme un *enlèvement non autorisé* ou un *sabotage,* en fonction desquels un système de protection physique des matières nucléaires et autres matières radioactives ou de leurs installations est conçu et évalué [1]. La présente section développe cette description de la menace de référence et aborde le rapport entre les responsabilités de l'État et celles de l'exploitant[2] ainsi que le rapport entre la menace réelle et la menace de référence.

La définition d'une menace de référence se fonde sur quatre éléments importants, à savoir :

— *Les agresseurs externes et les agresseurs d'origine interne.* Par agresseur potentiel on entend tout individu ou groupe d'individus, y compris des agresseurs externes et des agresseurs d'origine interne, considéré comme ayant l'intention/les capacités de commettre un acte malveillant ;
— *Le rapport entre actes malveillants et conséquences inacceptables.* Certains actes malveillants[3], comme l'enlèvement non autorisé de matières ou le sabotage radiologique, peuvent avoir des conséquences inacceptables et doivent donc être empêchés à tout prix ;

[2] Un exploitant est une entité ou une personne autorisée à utiliser, entreposer ou transporter des matières nucléaires ou des matières radioactives. Il est habituellement soit détenteur d'une licence ou d'un autre type d'autorisation délivré par une autorité compétente, soit sous-traitant d'un tel détenteur de licence ou d'une autre entité dûment autorisée.

[3] Les actes malveillants pourraient aussi inclure la prise de contrôle de matériel ou d'installations à des fins de chantage.

— *Attributs et caractéristiques.* Les attributs et caractéristiques des agresseurs potentiels révèlent leurs motivations, intentions et capacités de commettre un acte malveillant. Les motivations peuvent être d'ordre économique, politique ou idéologique. Les intentions peuvent inclure la possession non autorisée de matières, le sabotage radiologique ou des perturbations de l'ordre public. Les capacités des agresseurs sont déterminées par : leur composition, y compris le nombre, le regroupement, l'inclusion éventuelle d'agresseurs d'origine interne et la collusion avec eux ; leur organisation ; ainsi que leurs aptitudes et leurs moyens, y compris les tactiques, les armes, les explosifs, les outils, les moyens de transport, le niveau d'accès et les compétences ;
— *Conception et évaluation.* Une menace de référence, définie au niveau de l'État, est un outil permettant d'établir des prescriptions axées sur les résultats pour la conception et l'évaluation des systèmes de protection physique. La connaissance des capacités des agresseurs dans ce domaine aide les exploitants et les autorités nationales à déterminer les critères de détection, de retardement et d'intervention pour la conception et l'évaluation d'un système de protection physique efficace.

Une menace de référence prend en compte cet ensemble de caractéristiques des agresseurs, la responsabilité de la protection à cet égard étant assumée par les exploitants et par des organismes nationaux, avec obligation de rendre des comptes. La répartition de ces responsabilités peut varier d'un État à l'autre. Les responsabilités pour la protection contre la menace de référence qui incombent à l'exploitant doivent être définies conformément à ses objectifs, ses capacités, ses ressources et ses pouvoirs.

Il est tout à fait possible que certaines menaces définies dans l'évaluation de la menace ne soient pas prises en compte dans la menace de référence et que la protection contre celles-ci demeure la responsabilité de l'État. Toutefois, même si l'État est tenu d'élaborer des mesures pour contrer ces menaces, l'exploitant peut toujours avoir à assumer un rôle d'assistance de l'État pour protéger les installations visées par ces menaces ou pour en atténuer les conséquences.

Un État peut décider d'avoir plus d'une menace de référence pour traduire des besoins de protection différents, par exemple :

— Différentes matières visées (par ex. matières nucléaires ou matières radioactives) ;
— Différents types d'installations (par ex. centrales nucléaires, réacteurs de recherche, moyens de transport) ;
— Différents objectifs d'agression (par ex. vol, sabotage radiologique, perturbation de l'économie).

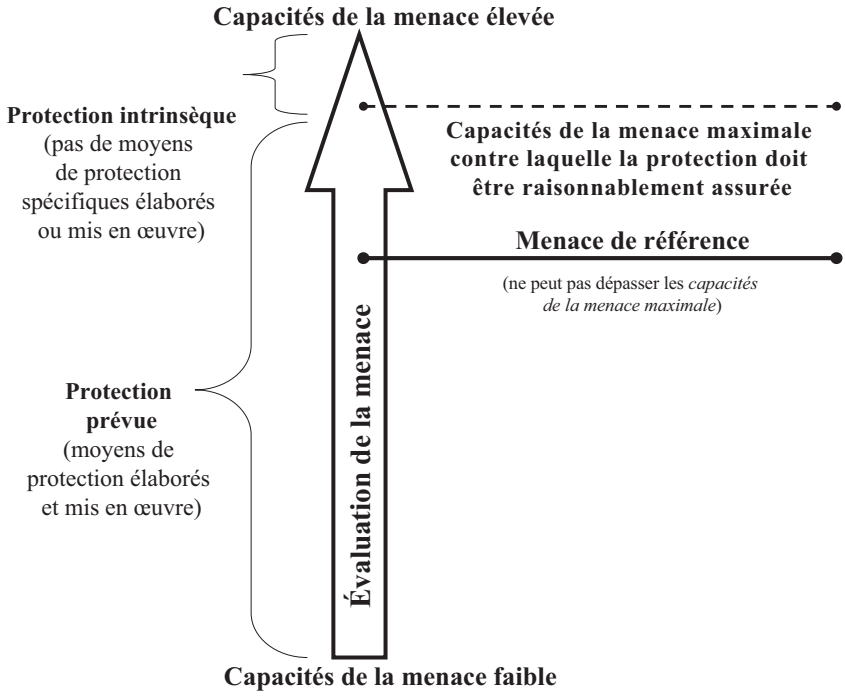

FIG. 1. Rapport entre les menaces qui sont intégrées dans la menace de référence et celles qui sont considérées dans une évaluation de la menace.

Ces distinctions soulignent l'intérêt de préciser l'utilisation pour laquelle une menace de référence est prévue, avant de l'élaborer.

La figure 1 indique le rapport entre les menaces potentielles dans l'évaluation de la menace et dans la menace de référence. Elle montre l'éventail de toutes les menaces, allant des capacités de la menace faible (au bas du diagramme) aux capacités de la menace élevée (au sommet du diagramme). Cet éventail représente les menaces avérées, réelles et dominantes qui entrent dans l'évaluation de la menace. Durant le processus d'élaboration de la menace de référence, ces menaces sont évaluées pour déterminer si elles pourraient servir de base à des prescriptions pour la conception de la protection physique. Certaines sont sélectionnées pour les raisons indiquées dans la section 6, d'autres sont affinées et développées plus avant. Le processus de sélection et d'affinement aboutit à la définition des capacités de la menace maximale contre laquelle une protection doit être raisonnablement assurée. Cette définition prend en compte les capacités de toutes les menaces potentielles contre lesquelles l'État a décidé

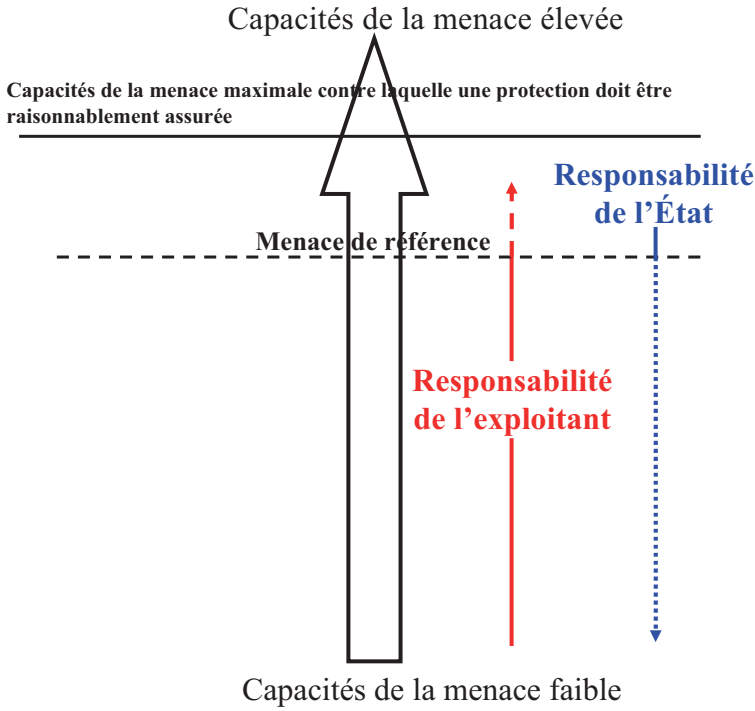

FIG. 2. Rôles et responsabilités pour assurer la protection contre des menaces.

d'élaborer des mesures de protection spécifiques (voir la ligne horizontale en pointillés). Le niveau de menace indiqué dans le diagramme comme menace de référence délimite le sous-ensemble des capacités des menaces qui sert de base pour réglementer la protection physique. La menace de référence peut englober toutes les menaces comprises dans les capacités de la menace maximale contre laquelle une protection doit être raisonnablement assurée, à condition que toutes ces menaces soient appropriées pour une menace de référence. Il convient de noter que ni les capacités de la menace maximale contre laquelle une protection doit être raisonnablement assurée ni la menace de référence ne représentent un agresseur isolé et identifiable ou désigné nommément. Ce sont des définitions représentatives dérivées de toutes les menaces crédibles préoccupantes.

La figure 2 indique le rapport entre les responsabilités de l'État et celles de l'exploitant pour la mise en œuvre d'une protection physique efficace contre des menaces. Comme il ressort de cette figure, l'État doit veiller à ce que tous les moyens de protection soient appliqués à toutes les menaces comprises dans les

capacités de la menace maximale contre laquelle une protection doit être raisonnablement assurée. La responsabilité de cette protection est partagée entre l'État et l'exploitant : l'exploitant est responsable au premier chef pour les capacités des menaces comprises dans la menace de référence, tandis que l'État est responsable au premier chef pour les menaces se situant entre la menace de référence et les capacités de la menace maximale contre laquelle une protection doit être raisonnablement assurée. Des moyens de protection ne doivent pas être élaborés ou assignés pour assurer la protection contre des capacités de menaces dépassant le seuil des capacités de la menace maximale contre laquelle une protection doit être raisonnablement assurée ; toutefois, les mesures de protection et d'atténuation existantes sont censées offrir un degré de protection intrinsèque contre ces capacités de menaces.

3. OBJET D'UNE MENACE DE RÉFÉRENCE

Une menace de référence est un outil qui offre une base commune à la planification de la protection physique par l'exploitant et à son approbation par l'autorité compétente en matière de sécurité nucléaire. La présente section examine les sujets de préoccupation qui font qu'une menace de référence est nécessaire ainsi que l'intérêt que celle-ci présente pour l'État et pour l'exploitant.

3.1. NÉCESSITÉ D'UNE MENACE DE RÉFÉRENCE

Un système de protection physique est conçu pour empêcher des agresseurs de parvenir à commettre un acte malveillant. Pour s'assurer que cet objectif est atteint, le concepteur chargé de la protection physique devrait comprendre les conditions dans lesquelles le système de protection doit opérer. Une description claire de ces menaces permet de définir ces conditions et est donc un préalable essentiel à une protection physique raisonnablement assurée et efficace. Dans l'idéal, les informations sur les menaces fournies par les services de renseignements et autres sources suffiraient pour la spécification de prescriptions en matière de conception et de performance d'un système de protection physique en vue de contribuer à la réalisation de cet objectif. Toutefois, les informations des services de renseignements sont souvent limitées, face à des menaces qui sont, par nature, dynamiques. Un système de protection physique conçu pour

empêcher uniquement la menace du moment peut ne pas être efficace face à la menace de demain.

Sans une description spécifique et suffisamment détaillée de la menace, il est difficile de déterminer avec précision le degré de protection qui serait approprié et efficace pour une installation ou une activité donnée. Compte tenu des conséquences potentiellement graves de certains actes malveillants et du coût élevé de la protection, il est peu probable que les incertitudes concernant le niveau de protection requis soient acceptables pour les autorités nationales compétentes. Une description très précise de la menace est nécessaire pour déterminer avec certitude que la protection est adéquate et suffisante.

Le concept de menace de référence[4] a été introduit pour répondre à la nécessité d'une description très précise de la menace. Une menace de référence est la description par l'État concerné de l'ensemble des attributs et caractéristiques représentatifs d'agresseurs, s'appuyant sur (mais ne se limitant pas nécessairement à) une évaluation de la menace, que l'État a décidé de prendre comme base pour la conception et l'évaluation de son système de protection physique.

3.2. INTÉRÊT D'UNE MENACE DE RÉFÉRENCE

La menace de référence fournit une base technique détaillée et précise pour les critères de conception et d'évaluation de la protection physique et, ce faisant, peut donner une plus grande assurance que le niveau de protection est suffisant. L'utilisation de la menace de référence pour élaborer un système de protection physique devrait mener à une allocation efficace de ressources pour la protection en réduisant le caractère arbitraire qui pourrait exister autrement dans l'établissement de prescriptions en matière de protection physique. En plus de favoriser une approche souple de la réglementation qui permet d'adapter la conception du système de protection physique de manière à prendre en compte des propriétés uniques des matières ou des installations, la menace de référence fixe une base de référence pour évaluer si des modifications dans la protection physique sont nécessaires et offre également une base claire pour la définition des responsabilités de l'exploitant en matière de protection physique.

Une menace de référence n'est pas une fin en soi mais plutôt un outil permettant d'atteindre une série d'objectifs. L'élaboration d'une menace de référence ne présente d'intérêt pour l'État que si celle-ci est utilisée pour la conception et l'évaluation de son système de protection physique. Il faut pour

[4] Comme indiqué plus haut, l'État peut décider d'en avoir plusieurs (voir section 2).

cela que la menace de référence soit prise en compte dans le cadre de réglementation et soit utilisée pour :

— Fixer des objectifs et des prescriptions axées sur les résultats pour les systèmes de protection physique ;
— Indiquer des critères de conception pour les systèmes de protection physique ;
— Définir des critères pour l'évaluation des systèmes de protection physique ;
— Établir la distinction entre les responsabilités de l'État et celles de l'exploitant.

Au niveau de l'exploitant, des méthodes de détection d'un acte de malveillance, des mesures de retardement et le type d'intervention devraient être élaborés et évalués pour répondre aux attributs et caractéristiques des agresseurs tels que décrits dans la menace de référence.

4. RÔLES ET RESPONSABILITÉS

La responsabilité générale de l'élaboration, l'utilisation et l'actualisation de la menace de référence incombe à l'État. La manière dont ces tâches sont accomplies sur le territoire d'un État dépend du dispositif propre à cet État pour l'élaboration de la politique générale, de la législation et de la réglementation. Un scenario dans lequel les différentes activités liées à la menace de référence sont entre les mains de plusieurs autorités compétentes – une pour l'élaboration et l'actualisation de la menace de référence, et une ou plusieurs autre(s) pour son utilisation – peut sembler plus souple. Il est recommandé que ces différentes activités soient toutes assignées à l'autorité compétente pour l'utilisation de la menace de référence (par ex. l'autorité compétente pour la supervision de la sécurité des matières nucléaires et radioactives et de leurs installations) du fait de l'éclairage qu'elle peut apporter sur l'impact d'une menace de référence pour la protection physique ; toutefois, le choix de l'autorité compétente pour l'élaboration et l'actualisation de la menace de référence reste une décision qui est du ressort de l'État. Si l'État décide que des autorités distinctes assumeront ces deux rôles, il importe, pour des besoins de coordination, que les menaces de référence élaborées s'intègrent dans le cadre réglementaire. En particulier, une coordination étroite est nécessaire entre ces deux autorités pour déterminer les types d'installations/titulaires de licence pour lesquels des menaces de référence sont requises (conformément au cadre réglementaire) et pour s'assurer que

l'élaboration de ces menaces de référence prend en compte les conséquences potentielles du vol ou du sabotage radiologique de matières nucléaires ou d'autres matières radioactives pour chaque type d'installation et de titulaire de licence.

Des recommandations concernant les rôles et responsabilités sont exposées ci-dessous. Certaines responsabilités sont définies pour des autorités gouvernementales de haut niveau et figurent donc dans la partie intitulée « L'État ». D'autres responsabilités concernent des organismes spécifiques au sein de l'État et figurent sous les intitulés correspondants.

4.1. L'ÉTAT

L'État devrait s'assurer que :

— Le cadre juridique permet la prise en compte d'une menace de référence, soit par un instrument juridiquement contraignant, soit par un acte administratif ;
— L'autorité compétente pour l'élaboration de la menace de référence a les compétences et les pouvoirs nécessaires pour entreprendre cette tâche, pour se procurer les informations appropriées et pour obtenir l'assistance d'autres organismes nationaux pour élaborer et actualiser la menace de référence ;
— Des organismes nationaux appropriés participent au processus d'évaluation de la menace ;
— Les organismes participant au processus de la menace de référence sont recensés et leur rôle est spécifié ;
— Une coordination efficace existe entre l'exploitant et les nombreux organismes qui, au sein d'un État, contribuent à la protection contre la menace référence.

4.2. LES AUTORITÉ(S) COMPÉTENTE(S) POUR L'ÉLABORATION, L'UTILISATION ET L'ACTUALISATION D'UNE MENACE DE RÉFÉRENCE

La responsabilité de l'élaboration, de l'utilisation et de l'actualisation de la menace de référence peut incomber à une seule autorité ou être répartie entre plusieurs autorités. Dans un cas comme dans l'autre, il importe que les tâches suivantes soient clairement assignées.

Pour l'élaboration et l'actualisation de la menace de référence, l'autorité compétente a pour tâche de :

— Coordonner le processus visant à déterminer si la menace de référence est le mécanisme approprié pour mettre en œuvre une approche de la protection basée sur la menace dans le but de fournir une assurance raisonnable d'un niveau de protection adéquat[5] ;
— Lancer la procédure d'élaboration d'un document d'évaluation de la menace pour la menace de référence ;
— Coordonner le processus d'élaboration de la menace de référence et documenter les hypothèses et les décisions ;
— Veiller à ce que les conclusions relatives à la menace de référence soient compatibles avec d'autres prescriptions juridiques, législatives ou réglementaires ;
— Vérifier l'adéquation du cadre réglementaire en vigueur pour que les services appropriés de l'État soient habilités, dans la mesure nécessaire, à apporter leur contribution complémentaire à la protection et à l'atténuation des conséquences. Dans le cas contraire, prendre les mesures nécessaires pour améliorer le cadre réglementaire ;
— Obtenir l'agrément, pour la menace référence, de tous les organismes nationaux compétents ;
— Diffuser la menace de référence, ou certains de ses éléments, auprès des intéressés qui sont chargés d'assurer la protection physique et des intéressés qui participent à l'élaboration et au réexamen de la menace de référence ;
— Déterminer comment la menace de référence doit être réexaminée et actualisée de manière satisfaisante ;
— Décider du moment opportun d'entreprendre une actualisation formelle de la menace de référence ;
— Adopter, appliquer et vérifier les mesures de sécurité et les règles de confidentialité appropriées pour protéger les informations qui concernent, et figurent dans, la menace de référence.

Pour que la menace de référence soit incorporée dans le système de sécurité réglementaire et utilisée pour l'élaboration des mesures de protection appropriées, l'autorité compétente a pour tâche de :

— Expliciter l'utilisation prévue de la menace de référence pour aider à définir le type de menace de référence requis ;
— Vérifier que le cadre réglementaire existant est adéquat pour que les exploitants puissent utiliser la menace de référence ;

[5] Si la rigueur associée à la menace référence n'est pas jugée appropriée, il faut que l'autorité compétente détermine une autre approche basée sur la menace dans le but de fournir une assurance adéquate de protection appropriée.

— Consigner la menace de référence dans le cadre réglementaire ;
— Décider comment utiliser la menace de référence et quelles exigences réglementaires devraient s'appliquer ;
— Veiller à ce que les prescriptions pour la protection physique découlant de la menace de référence soient compatibles avec les exigences légales ou réglementaires.

4.3. LES ORGANISMES DE RENSEIGNEMENTS

La participation des organismes de renseignements chargés de la collecte et de l'analyse d'informations est essentielle pour élaborer une menace crédible comme base pour évaluer les mesures de protection physique. L'expertise en matière de renseignements existe dans plusieurs organismes, comme le ministère des affaires étrangères, les autorités chargées de faire appliquer la loi et les services de renseignement militaire. Ces organismes sont familiarisés avec les processus de collecte et d'évaluation des renseignements et sont très compétents pour émettre les appréciations qui s'imposent. Ils peuvent avoir accès à des sources d'informations, y compris des contacts internationaux, dont l'autorité compétente pour l'élaboration de la menace de référence ne disposerait peut-être pas autrement. Les responsabilités spécifiques des organismes de renseignements sont notamment les suivantes :

— Collecte et communication d'informations sur des menaces potentielles visant des cibles à haut risque ou stratégiques ;
— Coordonner l'analyse des données disponibles pour s'assurer que le document consécutif d'évaluation de la menace et la menace de référence s'appuient sur des données crédibles.

4.4. LES EXPLOITANTS

Un système de protection physique, et les mesures spécifiques qui le fondent, sont soit élaborés par l'exploitant (puis validés par l'organisme de réglementation), soit directement définis par l'organisme de réglementation. Dans un cas comme dans l'autre, l'exploitant assume au premier chef la responsabilité de la mise en œuvre des mesures de protection. Le fait que l'exploitant connaisse l'impact que des mesures spécifiques ont sur le plan financier, opérationnel et de la sûreté peut influer sur la répartition de la responsabilité des mesures de sécurité entre l'exploitant et d'autres entités. En conséquence, la contribution de l'exploitant, qu'elle soit officielle ou non, devrait

être prise en considération dans l'élaboration de la menace de référence. L'exploitant devrait :

— Fournir à l'autorité compétente pour l'élaboration de la menace de référence, sur demande, un retour d'information sur l'impact, au plan financier, opérationnel et de la sûreté, de décisions potentielles en rapport avec la menace de référence ;
— Communiquer des renseignements complémentaires sur tout sujet de préoccupation concernant des menaces d'origine interne et sur tout incident qui pourrait être d'origine malveillante ;
— Élaborer et appliquer les mesures de protection nécessaires contre la menace de référence, y compris les mesures concernant les systèmes de sécurité, le contrôle des matières nucléaires, la préparation des interventions d'urgence, l'application de la loi et le transport.

4.5. LES AUTRES ORGANISMES

Diverses agences et autorités (par ex. les autorités de police nationales et locales, les forces armées, les autorités de contrôle aux frontières et les autorités douanières) jouent un rôle dans la protection, soit indépendamment soit en coordination avec d'autres et elles devraient aussi être impliquées, ou consultées, dans le processus d'élaboration d'une menace de référence. Elles peuvent avoir des responsabilités similaires à celles de l'exploitant pour :

— Élaborer les mesures de protection requises contre la menace de référence qui relèvent de leur domaine de compétence tel que défini ;
— Assurer un retour d'information à l'autorité compétente pour l'élaboration de la menace de référence en ce qui concerne l'impact financier et opérationnel de décisions potentielles sur la menace de référence[6].

[6] Ce retour d'information garantirait que l'autorité compétente pour l'élaboration de la menace de référence a tenu compte de l'impact de décisions concernant cette menace. Par exemple, l'impact de la décision d'inclure dans la menace de référence des capacités pour une chute d'aéronef.

5. ÉVALUATION DE LA MENACE

L'établissement d'une base de la menace pour la conception de la protection physique comprend deux stades principaux : le premier est l'évaluation de la menace ; le second est le processus d'évaluation et de prise de décisions aboutissant à une menace de référence[7]. La présente section décrit en détail le premier de ces stades : les mesures et processus qui constituent à proprement parler l'évaluation de la menace. Le second stade est traité dans la Section 6.

L'évaluation de la menace et l'élaboration de la menace de référence demandant toutes deux un véritable travail collectif, l'autorité compétente a besoin de réunir des experts de disciplines pertinentes, comme indiqué dans la section 4, avant d'entreprendre l'évaluation de la menace.

5.1. CONDUITE DE L'ÉVALUATION DE LA MENACE

Une évaluation de la menace est un processus formel qui consiste à collecter, organiser et évaluer des informations sur des menaces existantes ou potentielles qui pourraient produire ou entraîner un acte malveillant. Pour qu'une évaluation de la menace puisse servir réellement de base à la protection basée sur la menace, il importe que plusieurs organismes dotés de domaines de compétence différents travaillent en collaboration étroite. Il s'agit notamment d'organismes dotés de responsabilités et d'une expérience dans la collecte et l'analyse de renseignements, mais qui ont peut-être une expérience limitée des types d'installations et de matières à protéger, ainsi que d'organismes — comme l'organisme de réglementation — qui sont familiarisés avec les conditions opérationnelles et les stratégies de protection, mais qui n'ont peut-être pas d'expérience dans le processus d'évaluation de la menace. Une relation de travail étroite entre tous les organismes concernés est essentielle pour produire un document d'évaluation de la menace qui soit efficace.

Lorsque c'est possible, les personnes compétentes de l'organisme de réglementation devraient s'occuper d'obtenir les agréments et l'autorisation requise pour participer directement à l'évaluation de la menace. Leur point de vue peut ainsi être intégré dans l'évaluation de sorte que celle-ci soit mieux adaptée pour répondre aux problèmes identifiés.

[7] Dans certaines situations, la menace de référence peut ne pas être l'outil approprié pour mettre en œuvre une protection basée sur la menace. Dans ces cas-là, un autre énoncé de la menace devrait être élaboré comme base pour la sécurité. Ce point est étudié à la fin de la section 5.

Le processus d'évaluation de la menace peut être décrit en termes d'apports d'informations, d'analyse et de produit (voir fig. 3).

5.1.1. Apports

Les apports à l'évaluation de la menace devraient consister en une compilation exhaustive d'informations sur tous les agresseurs potentiels et sur leurs motivations, intentions et capacités. Toutes les sources d'information nationales et internationales fiables devraient être considérées. Les sources d'informations devraient inclure les services de renseignements et les services chargés de faire appliquer la loi, les rapports officiels du gouvernement, d'autres sources de documents classifiés ou non classifiés, les rapports des exploitants sur les incidents et les informations accréditées dans les médias. En plus des informations sur la menace portant sur les matières ou installations spécifiques concernées, les informations pertinentes sur les caractéristiques d'agressions visant des industries stratégiques ou à haut risque similaires devraient être prises en considération.

Ce processus de collecte d'informations inclurait, par exemple, les détails d'événements passés et d'événements planifiés, ainsi que les informations s'appuyant sur des indices, les preuves d'un entraînement suivi par exemple, d'une éventuelle intention de s'en prendre à des actifs et installations stratégiques ou protégés. Parmi les facteurs que l'évaluation de la menace devrait considérer, figurent entre autres :

— La menace mondiale et la menace nationale ;
— Les capacités plausibles, même si elles ne sont pas encore démontrées ;
— Les problèmes de menace d'origine interne.

Il est très important d'évaluer le degré de crédibilité des informations qui sont utilisées pour l'évaluation de la menace. Les informations émanant des services de renseignements et des services chargés de faire appliquer la loi devraient être assorties d'une appréciation sur le degré de confiance qui peut leur être accordé. Pour être tout à fait crédibles, les informations devraient provenir de sources ayant la réputation de remonter jusqu'aux auteurs de ces informations, de transmettre celles-ci fidèlement et d'être fiables. Les informations provenant de sources librement accessibles (c.-à-d. les médias) ne devraient être utilisées que si elles sont jugées exactes et factuelles. Le degré de confiance à accorder à toute information, à savoir si la source l'a acquise de première main et si elle est réputée fiable, doit entrer en ligne de compte pour décider de la manière dont cette information est à utiliser par la suite.

5.1.2. Processus d'analyse

Une fois les informations collectées, les données sont analysées pour identifier et documenter les motivations, intentions et capacités crédibles des menaces potentielles. Comme le travail d'analyse fait souvent apparaître le besoin d'informations supplémentaires, la collecte et l'analyse sont des activités continues. L'analyse devrait se concentrer particulièrement sur les menaces potentielles qui peuvent être pertinentes pour des matières nucléaires et autres matières radioactives ainsi que sur leurs installations et leur transport. Le processus consiste à évaluer ce que l'on connaît et à en déduire comment le groupe d'agresseurs ou l'agresseur pourrait se comporter à l'avenir. Les capacités des services de renseignements de collecter des données de manière exhaustive et de les évaluer avec précision influeront sur le degré de confiance accordé à la menace de référence et devraient donc être prises en compte.

L'objectif est de fournir une évaluation crédible des menaces potentielles ainsi que de leur composition et de leurs motivations, intentions et capacités. Il ne s'agit pas de définir des scénarios spécifiques ou les tactiques que l'agresseur est susceptible d'employer.

L'autorité compétente et les autres participants au processus d'évaluation de la menace devraient prendre en considération au moins les attributs et caractéristiques suivants pour chaque menace interne ou externe qui a été mise en évidence ; il se peut toutefois qu'il n'y ait pas de données disponibles sur tous les attributs et caractéristiques énumérés pour chaque menace :

— *Motivations* : politique, financière, idéologique, personnelle ;
— Consentement à mettre sa propre vie en péril ;
— *Intentions* : commettre un sabotage radiologique contre des matières ou une installation, commettre un vol, semer la panique dans la population et provoquer des perturbations sociales, déclencher une instabilité politique, causer un lourd bilan de morts et de blessés ;
— *Taille du groupe* : force d'attaque, coordonnateurs, personnes d'appui ;
— *Armes* : type, nombre, disponibilité ;
— *Explosifs* : type, quantité, disponibilité, sophistication du système de déclenchement, produit industriel ou improvisé ;
— *Outils* : mécaniques, thermiques, manuels, électriques, électroniques, électromagnétiques, matériel de communication ;
— *Modes de transport* : public, privé, terrestre, maritime, aérien, type, nombre, disponibilité ;
— *Compétences techniques* : ingénierie, utilisation d'explosifs ou de produits chimiques, expérience paramilitaire, talents de communication ;

— *Cybercompétences* : aptitude à utiliser des systèmes de commande informatiques et automatisés pour appuyer directement des attaques physiques, pour recueillir des renseignements, pour lancer des attaques informatiques, pour recueillir des fonds, etc.
— *Éléments de connaissance* : cibles, plans de situation et procédures, mesures de sécurité, mesures de sûreté et procédures de radioprotection, opérations, utilisation potentielle de matières nucléaires ou d'autres matières radioactives ;
— *Financement* : source, montant et disponibilité ;
— Questions concernant la menace interne : collusion, participation passive ou active, engagement violent ou non-violent, nombre d'agresseurs d'origine interne ;
— *Structure d'appui* : présence ou absence de sympathisants sur place, organisation d'appui, appui logistique ;
— *Tactiques* : tendre un piège, recourir à la ruse, ou à la force.

L'évaluation de la menace devrait s'intéresser à traiter ces différents attributs non seulement séparément mais, en plus, en les associant entre eux.

Toutes les menaces sont analysées à ce stade-là, sauf si la crédibilité des informations correspondantes est manifestement douteuse.

5.1.3. Produit

Le produit de cette première étape est un document d'évaluation de la menace qui présente le contexte général et toutes les menaces crédibles connues que l'État doit prendre en considération. Le texte explicatif devrait fournir le plus de détails possibles sur ces menaces et sur la crédibilité des informations. Ce document d'évaluation de la menace est utilisé pour établir les attributs et caractéristiques de l'agresseur qui constituent la menace de référence. Les évaluations de la menace et les détails sur les sources de renseignements sont en règle générale des informations sensibles et protégées.

5.2. DÉCISION ENTRE L'UTILISATION D'UNE MENACE DE RÉFÉRENCE OU D'UNE AUTRE APPROCHE BASÉE SUR LA MENACE

Une approche de la protection physique basée sur la menace devrait être prise dans le but de fournir une assurance raisonnable d'un niveau de protection

adéquat. Conformément à l'approche graduée[8], une menace de référence formelle n'est peut-être pas nécessaire dans toutes les situations pour offrir une assurance raisonnable. C'est pourquoi l'autorité compétente pour l'élaboration de la menace de référence devrait s'employer à décider – essentiellement sur la base des conséquences d'actes malveillants – s'il convient d'utiliser une menace de référence ou plutôt d'adopter une autre approche basée sur la menace.

Pour pouvoir décider si une menace de référence est l'outil approprié ou pas pour mettre en œuvre une protection basée sur la menace, il est nécessaire de comparer les avantages de l'approche de la menace de référence et le coût de son utilisation avec ceux d'une autre approche. La menace de référence fournit une base technique plus détaillée et précise pour les critères de conception et d'évaluation et, ce faisant, peut donner une plus grande assurance que le niveau de protection est suffisant ; toutefois, elle exige des ressources et des compétences plus importantes de la part de l'organisme de réglementation et de l'exploitant. C'est à l'État qu'il appartient de décider si une assurance accrue est requise et appropriée et si les avantages compensent le coût. Néanmoins, les critères de décision suivants sont recommandés :

— L'élaboration d'une menace de référence est recommandée si l'État établit que les conséquences potentielles d'un acte malveillant seraient graves[9];
— L'élaboration d'une menace de référence devrait tout de même être envisagée pour la protection d'actifs auxquels sont associées des conséquences moindres si :
- l'évaluation de la menace révèle l'existence d'une menace avec intention avérée de commettre un acte malveillant affectant l'actif en question ;
- l'évaluation de la menace met en évidence une menace de capacité élevée dont l'intention n'est pas avérée ;
- l'évaluation de la menace est entachée d'une trop grande incertitude due à l'insuffisance des informations ou au faible niveau de confiance accordé aux sources dont émanent les informations.

[8] Une approche graduée consiste à établir et à imposer des prescriptions en matière de protection physique en tenant compte de l'attractivité relative et de la nature des matières nucléaire/radioactives, des conséquences potentielles de l'enlèvement non autorisé de matières nucléaires/radioactives ou des conséquences potentielles d'un acte de sabotage radiologique contre des matières nucléaires/radioactives ou leurs installations.

[9] La notion de conséquences graves varie d'un État à l'autre. Elle est utilisée ici pour désigner des conséquences que l'État juge suffisamment graves pour qu'elles nécessitent un degré élevé d'assurance de succès de la prévention d'actes malveillants qui auraient de telles conséquences.

Le manque de disponibilité des capacités et des ressources nécessaires pour l'élaboration de mesures de sécurité, tant au niveau de l'autorité compétente chargée de définir la menace de référence qu'au niveau de l'exploitant chargé de l'utiliser, peut aussi influer sur la décision de poursuivre avec la menace de référence. Toutefois, l'insuffisance des capacités et des ressources ne devrait pas être une raison pour renoncer à utiliser une menace de référence. S'il ressort des considérations susmentionnées qu'il est nécessaire d'avoir le niveau d'assurance associée à une approche de la menace de référence, il faudra peut-être que l'État mette à disposition les ressources et les capacités nécessaires.

Quelle que soit l'approche utilisée, l'autorité compétente devrait veiller à ce que la protection qui en résulte soit basée sur la menace. L'autorité compétente devrait documenter les arguments appuyant sa décision d'utiliser la menace de référence ou une autre approche.

6. ÉLABORATION D'UNE MENACE DE RÉFÉRENCE

La méthodologie à suivre pour élaborer une menace de référence suppose l'utilisation du document d'évaluation de la menace et, à l'issue d'un processus de sélection et de prise de décision, la définition de la menace de référence. La présente section décrit en détail le processus d'élaboration d'une menace de référence.

6.1. APPORT À LA MENACE DE RÉFÉRENCE

Le principal apport est le document d'évaluation de la menace. le présent document contribue à l'assurance que la menace de référence identifiée est réaliste et crédible. Les conséquences jugées inacceptables par l'État doivent être comprises par l'autorité compétente pour l'élaboration de la menace de référence.

6.2. PROCESSUS

Le processus d'élaboration de la menace de référence comprend une analyse plus approfondie et, surtout, une prise de décision. Le processus d'analyse et de prise de décision comporte trois grandes phases :

1) Filtrer les résultats de l'évaluation de la menace pour retenir les menaces ayant des motivations, intentions et/ou capacités de commettre un acte malveillant ;
2) À l'issue de ce travail de sélection, établir la liste des attributs et caractéristiques représentatifs de l'agresseur postulé ;
3) Modifier cette liste sur la base de considérations politiques pertinentes.

6.2.1. Phase 1 : Filtrer l'évaluation de la menace

Dans cette phase, l'autorité compétente étudie les cibles possibles d'actes malveillants potentiels qui pourraient produire des conséquences inacceptables, puis les compare aux attributs et caractéristiques des agresseurs postulés tels que décrits dans le document d'évaluation de la menace.

La phase 1 comprend deux étapes :

- *A : Examen des capacités.* Les menaces décrites dans le document d'évaluation de la menace sont examinées pour déterminer si elles possèdent ou non les capacités nécessaires pour commettre un acte malveillant qui pourrait avoir des conséquences inacceptables. Si les capacités de la menace ne suffisent pas pour qu'il en résulte des conséquences inacceptables, cette menace n'est pas retenue dans le processus de la menace de référence. Toutefois, il importe de procéder avec une extrême prudence. Une menace ne devrait pas être exclue au motif que la protection physique existante est suffisante. L'impact de toutes mesures de protection physique existantes sur la menace ne devrait pas être pris en considération[10]. Seules les menaces dont les capacités sont les plus faibles sont susceptibles d'être exclues à ce stade de la prise de décision. Les menaces restantes doivent encore être filtrées au stade B.
- *B : Examen des motivations et des intentions.* Après le stade A, les menaces sont examinées du point de vue de leurs motivations et intentions. Si, en plus d'avoir des capacités suffisantes, la menace est considérée comme ayant aussi des motivations suffisantes (ou une intention réelle) de commettre un acte malveillant, cette menace est alors retenue pour être examinée plus avant dans la phase 2 du processus. En l'absence de motivation ou d'intention, la menace risque d'être exclue ; toutefois, la prudence s'impose avant d'exclure une menace de capacité élevée, au motif d'une absence perçue de motivation ou d'intention réelle. Avant de prendre

[10] En effet, il se peut que, plus tard, ces mesures soient supprimées par un exploitant si la menace de référence n'inclut pas les caractéristiques de la menace contre lesquelles ces mesures auraient été efficaces et utiles.

cette décision, l'autorité compétente devrait considérer d'une part si l'absence perçue de motivation dans la menace écarte complètement la possibilité d'un acte aux conséquences inacceptables et, d'autre part, si le degré de confiance dans les données utilisées pour évaluer la motivation et l'intention de la menace est suffisant pour justifier l'exclusion de la menace.

Compte tenu de l'importance de la décision à prendre, il importe que les raisons de toute exclusion soient parfaitement documentées[11]. Le produit de cette phase est un nouveau document d'évaluation de la menace qui inclut l'éventail des menaces crédibles ayant les capacités et éventuellement la motivation ou l'intention de commettre un acte malveillant aux conséquences inacceptables. Les menaces qui sont mises à l'écart à la suite du filtrage devraient toujours être considérées pour un nouvel examen si de nouveaux éléments d'information sont obtenus ultérieurement.

6.2.2. Phase 2 : Traduire les informations sur des menaces spécifiques en termes d'attributs et caractéristiques représentatifs

Les menaces figurant dans le nouveau document d'évaluation de la menace établi dans la phase 1 devraient être réexaminées du point de vue de leurs motivations, intentions et capacités. Les descriptions de la menace dans la phase 1 devraient être traduites en un ensemble de caractéristiques d'agresseurs qui sont représentatives pour des menaces spécifiques. Toutes les caractéristiques de la menace (à savoir les motivations, les intentions et toutes les capacités détaillées y compris le nombre d'agresseurs) identifiées dans le processus d'évaluation de la menace devraient être examinées.

Les caractéristiques représentatives ne devraient pas représenter simplement une combinaison des pires caractéristiques de chaque menace dans l'évaluation des menaces, au risque d'aboutir à une définition non réaliste des agresseurs. De fait, certaines de ces caractéristiques de la menace peuvent même être incompatibles entre elles. À la place, une approche mesurée devrait être suivie ; il s'agit d'établir une ou plusieurs descriptions d'agresseurs vraisemblables qui représentent l'éventail des caractéristiques figurant dans l'évaluation de la menace.

[11] Les informations relatives aux menaces qui sont exclues peuvent avoir un caractère sensible et devraient donc être correctement protégées.

Le produit de cet effort est une définition concise mais complète des moyens et caractéristiques représentatifs des agresseurs à partir desquels peut être conçu et évalué un système de protection.

6.2.3. Phase 3 : Modifier les attributs et caractéristiques représentatifs compte tenu de facteurs politiques

Les caractéristiques représentatives d'agresseurs déterminées dans la phase 2 devraient être évaluées en tenant compte de facteurs politiques pertinents identifiés par l'autorité compétente en coordination avec d'autres autorités nationales. Il peut en résulter une modification des caractéristiques représentatives d'agresseurs développées dans la phase 2 pour pouvoir accroître la durabilité des niveaux de sécurité. En outre, il conviendrait de mettre en balance d'un côté les avantages que l'exploitation continue des installations représente pour la société et, de l'autre, le coût de la protection et les risques associés aux conséquences d'un acte malveillant potentiel. L'autorité compétente devrait considérer les facteurs décisionnels tout en cherchant à maintenir une base technique pour la menace de référence comme prévu dans l'évaluation de la menace.

En évaluant les résultats de la phase 2, les facteurs suivants devraient être pris en compte dans le processus décisionnel. Ils peuvent conduire à modifier encore les caractéristiques représentatives d'agresseurs, comme suit :

- Degré de prudence de la menace de référence :
  - — Corriger les incertitudes et les différences d'interprétation des données utilisées dans l'évaluation initiale de la menace ;
  - — Créer une menace de référence solide pour permettre à la protection physique de rester crédible à mesure que la menace évolue ;
  - — Inclure les caractéristiques des menaces potentielles sur lesquelles il n'est obtenu aucun renseignement par mesure de prudence ;
- Bilan coûts-avantages-conséquences
  - — Mettre en balance les avantages pour la société que l'actif en question représente, les conséquences pour la société d'actes malveillants commis contre cet actif et le coût pour la société de la réduction des risques de tels actes ;
  - — Mettre en œuvre une protection physique appropriée comparable à celle d'autres actifs et infrastructures présentant un degré de risque similaire, par exemple la protection contre des explosifs, des produits chimiques ou des agents biologiques ;
- Facteurs politiques :
  - — Impact des décisions sur la confiance du public ;

— Contribution relative des actifs au bien-être public ;
— Confiance des États voisins dans la protection ;
— Situations de menace dans des États voisins.

Ces facteurs pourraient modifier le niveau des capacités de l'agresseur s'ils étaient appliqués à ses attributs et caractéristiques représentatifs. L'impact du degré de prudence et des facteurs politiques risquerait d'entraîner une augmentation des capacités de l'agresseur, alors que le bilan coûts–avantages se traduirait vraisemblablement par une diminution de ces capacités.

Les implications financières des décisions concernant la menace de référence devraient être prises en compte par l'autorité compétente. Bien qu'il ne faille pas laisser des préoccupations de coûts conduire à une minimisation de la menace, de telles considérations peuvent avoir un impact pour savoir qui, de l'État ou des exploitants, interviendra contre une menace particulière, et de quelle manière. Une menace de référence dont les capacités seraient d'un niveau exagérément élevé pourrait nécessiter la mobilisation de ressources d'un montant démesuré. Pour de nouvelles installations, un État peut souhaiter considérer les avantages à long terme que présente la conception d'une protection contre une menace plus modérée que la menace de référence, compte tenu des implications financières des mises à niveau à effectuer une fois que l'installation est en exploitation.

L'autorité compétente, en concertation avec d'autres autorités nationales, a besoin de décider quel niveau de risque est acceptable et contre quel niveau de menace il prévoit une protection, compte tenu de la disponibilité des ressources en matière de protection, des avantages que l'actif représente pour la société et d'autres priorités. Le risque, dans ce sens, est la combinaison de la gravité des conséquences d'un acte malveillant potentiel et la probabilité d'aboutissement de cet acte.

Avant de finaliser et d'utiliser la menace de référence, l'autorité compétente devrait coordonner son contenu avec les autres autorités nationales appropriées. L'autorité compétente devrait solliciter les observations d'autres parties concernées mais l'ultime décision sur le contenu de la menace de référence, et la responsabilité de ce contenu, devraient lui appartenir.

6.3. PRODUIT

Le processus de définition de la menace de référence débouche sur deux résultats. Le premier résultat est le document sur la menace de référence[12]. La menace de référence est cet ensemble d'attributs et caractéristiques de menaces contre lesquelles les organismes de l'État et les exploitants assument la responsabilité de la protection, avec obligation de rendre des comptes à cet égard. Toutefois, le second résultat est l'identification de toutes les menaces qui ne sont pas appropriées pour être incluses dans une menace de référence mais contre esquelles l'État exige qu'une protection soit raisonnablement assurée. Ces menaces seraient neutralisées essentiellement par l'État.

Le diagramme de la figure 3 représente le processus d'évaluation de la menace et d'élaboration de la menace de référence comme indiqué dans les sections 5 et 6.

6.4. ÉLABORATION DUN ÉNONCÉ DE LA MENACE

L'autre approche basée sur la menace considère un grand nombre des facteurs indiqués dans les sections 6.1 à 6.3 du présent guide d'application, mais de manière moins rigoureuse et en faisant intervenir éventuellement moins d'organismes. Pour autant, un processus formel d'élaboration d'un autre système de protection basé sur la menace devrait être entrepris. Il consisterait à :

— Identifier, à partir de l'évaluation, les menaces dont les motivations, intentions ou capacités correspondent aux actifs à protéger ;
— Déterminer l'influence des facteurs d'ordre politique (Section 6) sur les capacités de la menace identifiée ;
— Documenter ces capacités dans l'énoncé de la menace qui servira à l'organisme de réglementation pour définir des prescriptions en matière de conception et d'évaluation du système de protection physique. Pour l'exploitant ces prescriptions sont généralement de nature normative.

Leur élaboration devrait tenir compte des capacités des menaces figurant dans l'énoncé de la menace et appliquer un degré de prudence suffisant pour obtenir le niveau d'assurance souhaité. Cet énoncé de la menace et les prescriptions en matière de protection qui en résultent devraient être réexaminés

[12] Un État peut avoir plus d'une menace de référence, pour traduire une approche graduée ou des menaces qui varient (voir section 2).

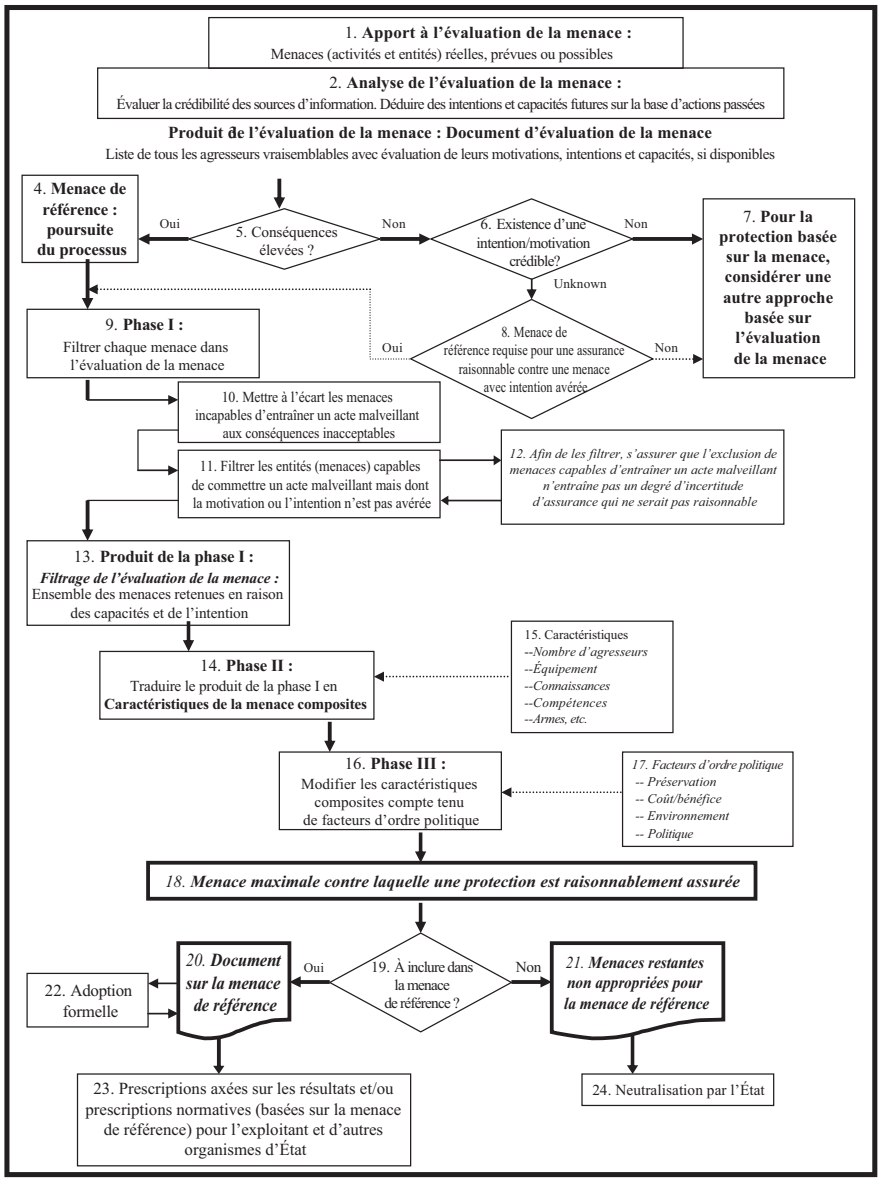

FIG. 3. Élaboration d'une menace de référence

périodiquement pour s'assurer qu'ils offrent toujours une assurance raisonnable de protection adéquate. S'il apparaît clairement qu'une assurance raisonnable ne peut pas être obtenue par le biais de cette approche, la menace de référence devrait alors être reconsidérée.

7. UTILISATION DE LA MENACE DE RÉFÉRENCE

L'utilisation de la menace de référence par l'organisme de réglementation devrait tenir compte des pouvoirs et des responsabilités de tous les organismes concernés, comme prévu par le régime de sécurité nucléaire de l'État. La répartition des responsabilités de la protection physique entre l'organisme de réglementation, les exploitants et les autres organismes de l'État varie d'un État à l'autre, comme il ressort de l'utilisation de la menace de référence. Lors de l'utilisation de la menace de référence, l'organisme de réglementation, en coordination avec d'autres autorités nationales, devrait prendre en compte les facteurs pertinents, tels que :

— Les contraintes juridiques et réglementaires prévues par la constitution nationale et/ou la législation sur les armes, le code pénal ou l'ordre public et la sécurité publique ;
— Les responsabilités et compétences d'autres entités du service public, par exemple les forces armées, les forces de l'ordre et autres responsables de la réglementation ;
— Les compétences et les ressources de l'exploitant, mais aussi les contraintes techniques, culturelles et financières qui pèsent sur ses activités.

En connaissance de cause, l'organisme de réglementation, en concertation avec d'autres autorités nationales, devrait identifier les responsabilités des exploitants et s'assurer que les différentes autorités nationales concernées comprennent bien le rôle, les fonctions et les responsabilités qui leur incombent en ce qui concerne la protection physique contre la menace de référence.

L'État s'assure que le partage des responsabilités de la protection entre différentes entités ne nuit pas à l'exhaustivité de cette protection et que les contributions respectives de ces entités à la protection sont coordonnées efficacement. L'organisme de réglementation pourrait prêter assistance à l'État à cet égard.

La menace de référence, ou certains de ses éléments, devrait être communiquée à ceux qui en ont besoin et qui sont autorisés à la recevoir. Il faut

qu'un compromis soit trouvé entre le besoin des informations contenues dans la menace de référence et le besoin de protection des informations sensibles émanant des services de renseignement, ainsi que des conclusions qui en sont tirées. À cette fin, l'autorité compétente pour la diffusion de la menace de référence devrait envisager de communiquer celle-ci aux des groupes suivants :

— Ceux qui ont besoin de connaître la menace de référence (soit dans son intégralité, soit en partie) pour pouvoir assumer leurs responsabilités en matière de protection physique. Il s'agit notamment des exploitants, des intervenants nationaux et des autorités de sécurité publique ;
— Ceux qui ont participé au processus d'élaboration de la menace de référence pour des conseils sur les mises à jour nécessaires, mais qui ne sont pas eux-mêmes chargés d'assurer la protection.

Il peut être judicieux d'élaborer une version de la menace de référence qui soit moins sensible en termes d'informations classifiées de sorte qu'elle puisse être plus facilement communiquée pour être utilisée par des entités qui n'auraient normalement pas besoin de protéger des informations classifiées. Toute diffusion de la menace de référence devrait être effectuée en conformité avec le cadre constitutionnel, législatif, réglementaire et organisationnel de l'État.

Le cadre réglementaire d'un État détermine en principe si une menace de référence est : 1) consignée dans un instrument juridiquement contraignant ; ou 2) mise en application en vertu d'un acte administratif, comme une directive ou une instruction. Si une menace de référence fait explicitement partie du cadre réglementaire et acquiert de ce fait un statut juridique, l'organisme de réglementation devrait s'assurer que le document sur la menace de référence et les prescriptions en matière de protection physique qui en découlent sont compatibles avec d'autres prescriptions juridiques.

Un État pourrait suivre plusieurs approches différentes pour formaliser l'utilisation d'une menace de référence par l'exploitant/les exploitants, notamment :

a) L'organisme de réglementation fournit la menace de référence à l'exploitant en exigeant de manière générale une protection contre les caractéristiques de l'agresseur qui sont spécifiées ; l'exploitant est tenu d'interpréter la menace de référence et de concevoir et mettre en œuvre un système de protection physique efficace ;
b) L'organisme de réglementation fixe des prescriptions axées sur les résultats des systèmes de protection physique qui sont efficaces contre la menace de référence ; l'exploitant est tenu de concevoir et de mettre en œuvre un

système de protection physique qui satisfait à ces prescriptions axées sur les résultats ;

c) L'organisme de réglementation spécifie des mesures de protection normatives basées sur la menace de référence ; l'exploitant est tenu de satisfaire à ces prescriptions normatives.

Les critères de sélection d'une approche basée sur les résultats a) et b) ou d'une approche normative c) dépendent du cadre législatif et de la structure organisationnelle de l'État ainsi que d'un certain nombre d'autres facteurs tels que :

— La compétence de l'exploitant pour interpréter les prescriptions axées sur les résultats et pour concevoir, mettre en œuvre et évaluer un système de protection physique efficace ;
— Le nombre d'installations et d'exploitants régis par la réglementation, et la mesure dans laquelle les prescriptions normatives réduisent la marge de manœuvre de l'exploitant pour l'élaboration de mesures de protection appropriées ;
— La gravité des conséquences potentielles des actes malveillants qui doivent être empêchés.

La consignation d'une menace de référence dans le cadre réglementaire permet la gestion des risques d'un acte malveillant grâce à l'élaboration de mesures et systèmes de sécurité appropriés. L'organisme de réglementation devrait ensuite évaluer les systèmes de protection physique existants pour s'assurer qu'ils sont efficaces contre la menace de référence. Aux fins d'une telle évaluation, une menace de référence est utilisée comme base pour :

— Élaborer des scénarios d'agresseurs potentiels susceptibles de commettre des actes malveillants ;
— Analyser la performance du système de protection physique pour déterminer son efficacité et pour évaluer toute perte d'efficacité possible contre l'agresseur potentiel ;
— Identifier toutes vulnérabilités du système de protection physique ;
— Améliorer le système (si nécessaire), analyser et hiérarchiser les possibilités de renforcement de son efficacité et faire un bilan coût-avantages.

La conception et l'évaluation de la protection physique sortent du cadre du présent guide d'application. Toutefois, l'utilisation de critères de conception basés sur la menace, comme la menace de référence, favorise une approche stratégique de la protection physique. Il importe que l'organisme de

réglementation adopte des méthodes systématiques et bien documentées pour évaluer les propositions de l'exploitant concernant la protection physique et les plans de préparation et conduite des interventions d'urgence ainsi que toutes propositions de modifications. De telles méthodes prévoient en principe l'évaluation des efforts faits par l'exploitant pour élaborer des scénarios d'agressions détaillés sur la base de la menace de référence, pour recenser les zones vitales, pour élaborer des stratégies de protection physique et pour instaurer une culture de sécurité.

8. ACTUALISATION DE LA MENACE DE RÉFÉRENCE

8.1. APPORTS

Un processus de réexamen systématique devrait être mis en place pour assurer la validité de la menace de référence. Il devrait comprendre une évaluation continue du contexte courant de la menace. Il devrait inclure aussi une évaluation des menaces évoluant très vite qui sont à gérer de toute urgence. Dans de telles circonstances, il se peut qu'il faille prendre des mesures de sécurité supplémentaires avant le réexamen systématique de la menace de référence. La manière de gérer les menaces nouvelles varie d'un État à l'autre.

Si l'organisation du réexamen de la menace de référence est essentiellement la responsabilité de l'autorité compétente, le processus devrait être entrepris avec le concours d'autres autorités nationales. L'autorité compétente devrait décider de la périodicité qui convient pour des réexamens systématiques de la menace de référence. Cette périodicité dépend de facteurs tels que la législation et la réglementation nationales relatives à la protection physique, la stabilité du contexte de la menace, le degré de prudence intégré dans la menace de référence et la disponibilité des ressources. Le réexamen de la menace de référence ne débouche pas nécessairement sur sa révision.

Un certain nombre d'événements peuvent pousser à envisager un réexamen de la menace de référence en dehors du processus de réexamen périodique. L'autorité compétente devrait décider quel(le)s conditions/événements déclencheurs sont appropriés. Ces événements déclencheurs peuvent être notamment :

— Un événement ou une action, d'origine intérieure ou extérieure à l'État, qui change considérablement la perception ou le niveau réel de la menace ;

— Des changements importants au niveau de la gouvernance, du dispositif juridique ou des arrangements internationaux qui affectent la responsabilité des autorités nationales ou de l'exploitant, par exemple l'introduction du recours à la force létale, la modification du dispositif d'intervention ou des responsabilités organisationnelles ;
— Des changements dans les activités liées aux matières nucléaires impliquant des conséquences potentielles nouvelles, par exemple la construction d'un type différent d'installation, l'utilisation de matières d'enrichissement supérieur ou un nouveau mode opératoire ;
— Un réexamen proposé par une partie prenante.

8.2. PROCESSUS

Une fois que l'autorité compétente a déterminé qu'un réexamen (et éventuellement une révision) de la menace de référence est nécessaire, elle devrait entreprendre le même processus que celui suivi pour définir la menace de référence originale, en commençant par l'évaluation de la menace. L'autorité compétente serait responsable de la conduite et de la coordination du processus de réexamen et de révision.

Il importe que l'autorité compétente fasse participer au processus de réexamen les organismes qui ont participé à l'élaboration de la menace de référence, ainsi que tous autres organismes identifiés comme détenteurs d'informations pertinentes ou étant susceptibles d'être affectés.

8.3. PRODUIT

Le réexamen permet de décider s'il est nécessaire ou pas de réviser la menace de référence existante et de la republier. Si une actualisation de la menace de référence est nécessaire, le processus d'analyse et de prise de décisions est le même que celui qui a été suivi pour son élaboration. Toutefois, l'autorité compétente prend aussi en considération les enseignements tirés de l'utilisation de la menace de référence, en particulier en ce qui concerne la coordination des différents organismes.

L'actualisation de la menace de référence devrait être suivie d'une évaluation de l'adéquation du système de protection physique existant par rapport à la nouvelle menace de référence et les mesures qui s'imposent devraient être prises.

RÉFÉRENCES

[1] La protection physique des matières et installations nucléaires, document INFCIRC/225/Rev.4 (Corrigé), AIEA, Vienne (2000).

[2] Objectifs et principes fondamentaux de la protection physique (GOV/2001/41/Appendice), AIEA, Vienne (2001).

[3] Convention sur la protection physique des matières nucléaires (INFCIRC/274) et amendement de 2005, AIEA, Vienne (2005).

GLOSSAIRE

conséquence inacceptable. Seuil fixé par l'État au-delà duquel la gravité de la conséquence justifie l'utilisation de ressources pour empêcher qu'elle ne se produise. Les ressources sont utilisées par les organismes chargés d'assurer la protection (définition résultant de longues consultations dans les États Membres[13]).

énoncé de la menace. Document qui fait la synthèse de l'évaluation de la menace et qui est modifié pour tenir compte de considérations politiques. La menace de référence est un exemple d'énoncé de la menace (définition élaborée après de longues consultations dans les États Membres[14]).

évaluation de la menace. Évaluation des menaces existantes, comprenant habituellement des informations émanant de services de renseignements, qui décrivent les motivations, intentions et capacités dont ces menaces sont pourvues pour commettre des actes malveillants (définition élaborée après de longues consultations dans les États Membres[15]).

exploitant. Tout organisme ou toute personne qui a demandé ou obtenu une autorisation et/ou qui est responsable de la sécurité nucléaire, de la sécurité radiologique, de la sécurité des déchets radioactifs ou de la sécurité du transport lors de l'exécution d'activités ou en ce qui concerne toute installation nucléaire ou source de rayonnements ionisants. Il peut s'agir notamment de particuliers, d'organismes publics, d'expéditeurs ou de transporteurs, de titulaires d'autorisation, d'hôpitaux, de travailleurs indépendants, etc. (cf. Glossaire de sûreté de l'AIEA : Terminologie employée en sûreté nucléaire et radioprotection — Édition 2007).

menace. Entité ayant la motivation, l'intention et les capacités de commettre un acte malveillant (définition élaborée après de longues consultations dans les États Membres[16]).

sabotage. Tout acte délibéré dirigé contre une installation nucléaire ou des matières nucléaires en cours d'utilisation, en entreposage ou en cours de transport, qui est susceptible, directement ou indirectement, de porter atteinte à la santé et à la

[13] Clarification nécessaire pour faire la différence avec les critères quantifiés.
[14] Terme défini ici conformément à son acception dans le domaine de la sécurité.
[15] Terme défini ici conformément à son acception dans le domaine de la sécurité.
[16] Terme défini ici conformément à son acception dans le domaine de la sécurité.

sécurité du personnel ou du public ou à l'environnement en provoquant une exposition à des rayonnements ou un relâchement de substances radioactives. (Convention sur la protection physique des matières nucléaires et des installations nucléaires).

Nº 22

IAEA
Agence internationale de l'énergie atomique

Lieux de vente des publications de l'AIEA

Dans les pays suivants, vous pouvez vous procurer les publications de l'AIEA chez nos dépositaires ci-dessous ou auprès de grandes librairies. Le paiement peut être effectué en monnaie locale ou avec des coupons Unesco.

ALLEMAGNE
UNO-Verlag, Vertriebs- und Verlags GmbH, Am Hofgarten 10, 53113 Bonn
Téléphone : + 49 228 94 90 20 • Télécopie : +49 228 94 90 20 ou +49 228 94 90 222
Courriel : bestellung@uno-verlag.de • Site web : http://www.uno-verlag.de

AUSTRALIE
DA Information Services, 648 Whitehorse Road, MITCHAM 3132
Téléphone : +61 3 9210 7777 • Télécopie : +61 3 9210 7788
Courriel : service@dadirect.com.au • Site web : http://www.dadirect.com.au

BELGIQUE
Jean de Lannoy, 202 avenue du Roi, 1190 Bruxelles
Téléphone : +32 2 538 43 08 • Télécopie : +32 2 538 08 41
Courriel : jean.de.lannoy@infoboard.be • Site web : http://www.jean-de-lannoy.be

CANADA
Bernan Associates, 4501 Forbes Blvd, Suite 200, Lanham, MD 20706-4346, États-Unis d'Amérique
Téléphone : 1-800-865-3457 • Télécopie : 1-800-865-3450
Courriel : customercare@bernan.com • Site web : http://www.bernan.com

Renouf Publishing Company Ltd., 1-5369 Canotek Rd., Ottawa, Ontario, K1J 9J3
Téléphone : +613 745 2665 • Télécopie : +613 745 7660
Courriel : order.dept@renoufbooks.com • Site web : http://www.renoufbooks.com

CHINE
Publications de l'AIEA en chinois : China Nuclear Energy Industry Corporation, Translation Section, P.O. Box 2103, Beijing

CORÉE, RÉPUBLIQUE DE
KINS Inc., Information Business Dept. Samho Bldg. 2nd Floor, 275-1 Yang Jae-dong SeoCho-G, Seoul 137-130
Téléphone : +02 589 1740 • Télécopie : +02 589 1746 • Site web : http://www.kins.re.kr

ESPAGNE
Díaz de Santos, S.A., c/Juan Bravo, 3A, 28006 Madrid
Téléphone : +34 91 781 94 80 • Télécopie : +34 91 575 55 63
Courriel : compras@diazdesantos.es, carmela@diazdesantos.es, barcelona@diazdesantos.es, julio@diazdesantos.es • Site web : http://www.diazdesantos.es

ÉTATS-UNIS D'AMÉRIQUE
Bernan Associates, 4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4346
Téléphone : 1-800-865-3457 • Télécopie : 1-800-865-3450
Courriel : customercare@bernan.com • Site web : http://www.bernan.com

Renouf Publishing Company Ltd., 812 Proctor Ave., Ogdensburg, NY, 13669
Téléphone : +888 551 7470 (nº vert) • Télécopie : +888 568 8546 (nº vert)
Courriel : order.dept@renoufbooks.com • Site web : http://www.renoufbooks.com

FINLANDE
Akateeminen Kirjakauppa, PO BOX 128 (Keskuskatu 1), 00101 Helsinki
Téléphone : +358 9 121 41 • Télécopie : +358 9 121 4450
Courriel : akatilaus@akateeminen.com • Site web : http://www.akateeminen.com

FRANCE
Form-Edit, 5 rue Janssen, B.P. 25, 75921 Paris Cedex 19
Téléphone : +33 1 42 01 49 49 • Télécopie : +33 1 42 01 90 90
Courriel : formedit@formedit.fr • Site web : http://www. formedit.fr

Lavoisier SAS, 145 rue de Provigny, 94236 Cachan Cedex
Téléphone : + 33 1 47 40 67 02 • Télécopie : +33 1 47 40 67 02
Courriel : romuald.verrier@lavoisier.fr • Site web : http://www.lavoisier.fr

HONGRIE
Librotrade Ltd., Book Import, P.O. Box 126, 1656 Budapest
Téléphone : +36 1 257 7777 • Télécopie : +36 1 257 7472 • Courriel : books@librotrade.hu

INDE
Allied Publishers Group, 1st Floor, Dubash House, 15, J. N. Heredia Marg, Ballard Estate, Mumbai 400 001
Téléphone : +91 22 22617926/27 • Télécopie : +91 22 22617928
Courriel : alliedpl@vsnl.com • Site web : http://www.alliedpublishers.com

Bookwell, 2/72, Nirankari Colony, Delhi 110009
Téléphone : +91 11 23268786, +91 11 23257264 • Télécopie : +91 11 23281315
Courriel : bookwell@vsnl.net

ITALIE
Libreria Scientifica Dott. Lucio di Biasio « AEIOU », Via Coronelli 6, 20146 Milan
Téléphone : +39 02 48 95 45 52 ou 48 95 45 62 • Télécopie : +39 02 48 95 45 48
Courriel : info@libreriaaeiou.eu • Site web : www.libreriaaeiou.eu

JAPON
Maruzen Company, Ltd., 13-6 Nihonbashi, 3 chome, Chuo-ku, Tokyo 103-0027
Téléphone : +81 3 3275 8582 • Télécopie : +81 3 3275 9072
Courriel : journal@maruzen.co.jp • Site web : http://www.maruzen.co.jp

NOUVELLE-ZÉLANDE
DA Information Services, 648 Whitehorse Road, Mitcham Victoria 3132, Australie
Téléphone : +61 3 9210 7777 • Télécopie : +61 3 9210 7788
Courriel : service@dadirect.com.au • Site web : http://www.dadirect.com.au

ORGANISATION DES NATIONS UNIES
Dépt. I004, Bureau DC2-0853, First Avenue at 46th Street, New York, N.Y. 10017, États-Unis d'Amérique
(ONU) Téléphone : +800 253-9646 ou +212 963-8302 • Télécopie : +212 963-3489
Courriel : publications@un.org • Site web : http://www.un.org

PAYS-BAS
De Lindeboom Internationale Publicaties B.V., M.A. de Ruyterstraat 20A, 7482 BZ Haaksbergen
Téléphone : +31 (0) 53 5740004 • Télécopie : +31 (0) 53 5729296
Courriel : books@delindeboom.com • Site web : http://www.delindeboom.com

Martinus Nijhoff International, Koraalrood 50, P.O. Box 1853, 2700 CZ Zoetermeer
Téléphone : +31 793 684 400 • Télécopie : +31 793 615 698
Courriel : info@nijhoff.nl • Site web : http://www.nijhoff.nl

Swets and Zeitlinger b.v., P.O. Box 830, 2160 SZ Lisse
Téléphone : +31 252 435 111 • Télécopie : +31 252 415 888
Courriel : infoho@swets.nl • Site web : http://www.swets.nl

RÉPUBLIQUE TCHÈQUE
Suweco CZ, S.R.O., Klecakova 347, 180 21 Prague 9
Téléphone : +420 26603 5364 • Télécopie : +420 28482 1646
Courriel : nakup@suweco.cz • Site web : http://www.suweco.cz

ROYAUME-UNI
The Stationery Office Ltd, International Sales Agency, P.O. Box 29, Norwich, NR3 1 GN
Téléphone (commandes) : +44 870 600 5552 • (demandes de renseignements) : +44 207 873 8372 •
Télécopie : +44 207 873 8203
Courriel (commandes) : book.orders@tso.co.uk • (demandes de renseignements) : book.enquiries@tso.co.uk •
Site web : http://www.tso.co.uk

Commandes en ligne
DELTA Int. Book Wholesalers Ltd., 39 Alexandra Road, Addlestone, Surrey, KT15 2PQ
Courriel : info@profbooks.com • Site web : http://www.profbooks.com

Ouvrages sur l'environnement
Earthprint Ltd., P.O. Box 119, Stevenage SG1 4TP
Téléphone : +44 1438748111 • Télécopie : +44 1438748844
Courriel : orders@earthprint.com • Site web : http://www.earthprint.com

SLOVÉNIE
Cankarjeva Zalozba d.d., Kopitarjeva 2, 1512 Ljubljana
Téléphone : +386 1 432 31 44 • Télécopie : +386 1 230 14 35
Courriel : import.books@cankarjeva-z.si • Site web : http://www.cankarjeva-z.si/uvoz

Les commandes et demandes d'information peuvent aussi 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 2600 29302
Courriel : sales.publications@iaea.org • Site web : http://www.iaea.org/books

12-14882

La présente publication donne des orientations sur la manière d'élaborer, d'utiliser et d'actualiser une menace de référence. Elle s'adresse à des décideurs assumant un rôle et des responsabilités dans l'élaboration, l'utilisation et l'actualisation de la menace de référence. Le présent guide décrit une menace de référence ; il détermine et recommande les rôles et responsabilités des organismes qui devraient participer à l'élaboration, l'utilisation et l'actualisation d'une menace de référence ; il indique comment conduire une évaluation nationale de la menace comme préalable à une menace de référence ; il explique comment une menace de référence est incorporée dans le régime de sécurité nucléaire d'un État ; enfin il précise les conditions et les modalités d'exécution du réexamen et de l'actualisation de la menace de référence.

AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE
VIENNE
ISBN 978–92–0–232810–5
ISSN 1816–9317