国际原子能机构《核安保丛书》第10-G (Rev.1)号

实施导则

国家核安保威胁评定、设计基准威胁和代表性威胁声明

IAEA
国际原子能机构

国际原子能机构《核安保丛书》

国际原子能机构《核安保丛书》处理与防止和侦查涉及或针对核材料、其他放射性物质、相关设施或相关活动的犯罪行为或未经授权的故意行为并予以做出响应有关的核安保问题。这些出版物符合并补充国际核安保文书，例如《核材料实物保护公约》及其修订案、《制止核恐怖主义行为国际公约》、联合国安全理事会第 1373 号决议和第 1540 号决议以及《放射源安全和安保行为准则》。

国际原子能机构《核安保丛书》的类别

原子能机构《核安保丛书》出版物按以下类别发行：

- **核安保基本原则**详述国家核安保制度的目标和这种制度的基本要素。这些基本原则构成“核安保建议”的基础。
- **核安保建议**提出国家按照“核安保基本原则”为实现和保持有效的国家核安保制度应当采取的措施。
- **实施导则**就国家可以实施“核安保建议”中提出的措施的方法提供指导。因此，这些导则注重如何落实与广泛的核安保领域有关的建议。
- **技术导则**就具体技术主题提供指导，以补充“实施导则”中提供的指导。这些导则注重如何实施必要措施的细节。

起草和审查

《核安保丛书》出版物的编写和审查涉及原子能机构秘书处、成员国专家（协助秘书处起草这些出版物）以及审查和核准出版物草案的核安保导则委员会。适当时，在起草期间还举行不限人数的技术会议，为成员国和相关国际组织的专家提供机会审查和讨论文本草案。此外，为确保高水平的国际审查和达成高度国际共识，秘书处向所有成员国提交草案文本，以供进行 120 天的正式审查。

对于每份出版物，秘书处都要编写核安保导则委员会在编写和审查过程的相继阶段予以核准的以下内容：

- 说明预定新的或经修订的出版物的概要和工作计划、其预定用途、范围和目录；
- 提交成员国的出版物草案，以供在 120 天磋商期间发表意见；
- 考虑了成员国意见的最终出版物草案。

原子能机构《核安保丛书》出版物的起草和审查过程考虑到机密性，并且承认核安保与总体乃至具体的国家安保关切有着密不可分的联系。

一个基本的考虑因素是在这些出版物的技术内容上应当虑及相关的原子能机构安全标准和保障活动。特别是，在以上所述每个阶段由相关安全标准分委员会以及核安保导则委员会对涉及与安全有接口的领域的《核安保丛书》出版物（称作接口文件）进行审查。

国家核安保威胁评定、设计基准威胁和代表性威胁声明

国际原子能机构的成员国

阿富汗
阿尔巴尼亚
阿尔及利亚
安哥拉
安提瓜和巴布达
阿根廷
亚美尼亚
澳大利亚
奥地利
阿塞拜疆
巴哈马
巴林
孟加拉国
巴巴多斯
白俄罗斯
比利时
伯利兹
贝宁
多民族玻利维亚国
波斯尼亚和黑塞哥维那
博茨瓦纳
巴西
文莱达鲁萨兰国
保加利亚
布基纳法索
佛得角
布隆迪
柬埔寨
喀麦隆
加拿大
中非共和国
乍得
智利
中国
哥伦比亚
科摩罗
刚果
哥斯达黎加
科特迪瓦
克罗地亚
古巴
塞浦路斯
捷克共和国
刚果民主共和国
丹麦
吉布提
多米尼克
多米尼加共和国
厄瓜多尔
埃及
萨尔瓦多
厄立特里亚
爱沙尼亚
斯威士兰
埃塞俄比亚
斐济
芬兰
法国
加蓬
冈比亚
格鲁吉亚
德国
加纳
希腊
格林纳达
危地马拉
圭亚那
海地
教廷
洪都拉斯
匈牙利
冰岛
印度
印度尼西亚
伊朗伊斯兰共和国
伊拉克
爱尔兰
以色列
意大利
牙买加
日本
约旦
哈萨克斯坦
肯尼亚
大韩民国
科威特
吉尔吉斯斯坦
老挝人民民主共和国
拉脱维亚
黎巴嫩
莱索托
利比里亚
利比亚
列支敦士登
立陶宛
卢森堡
马达加斯加
马拉维
马来西亚
马里
马耳他
马绍尔群岛
毛里塔尼亚
毛里求斯
墨西哥
摩纳哥
蒙古
黑山
摩洛哥
莫桑比克
缅甸
纳米比亚
尼泊尔
荷兰
新西兰
尼加拉瓜
尼日尔
尼日利亚
北马其顿
挪威
阿曼
巴基斯坦
帕劳
巴拿马
巴布亚新几内亚
巴拉圭
秘鲁
菲律宾
波兰
葡萄牙
卡塔尔
摩尔多瓦共和国
罗马尼亚
俄罗斯联邦
卢旺达
圣基茨和尼维斯
圣卢西亚
圣文森特和格林纳丁斯
萨摩亚
圣马力诺
沙特阿拉伯
塞内加尔
塞尔维亚
塞舌尔
塞拉利昂
新加坡
斯洛伐克
斯洛文尼亚
南非
西班牙
斯里兰卡
苏丹
瑞典
瑞士
阿拉伯叙利亚共和国
塔吉克斯坦
泰国
多哥
汤加
特立尼达和多巴哥
突尼斯
土耳其
土库曼斯坦
乌干达
乌克兰
阿拉伯联合酋长国
大不列颠及北爱尔兰联合王国
坦桑尼亚联合共和国
美利坚合众国
乌拉圭
乌兹别克斯坦
瓦努阿图
委内瑞拉玻利瓦尔共和国
越南
也门
赞比亚
津巴布韦

国际原子能机构的《规约》于 1956 年 10 月 23 日经在纽约联合国总部举行的原子能机构《规约》会议核准，并于 1957 年 7 月 29 日生效。原子能机构总部设在维也纳，其主要目标是“加速和扩大原子能对全世界和平、健康及繁荣的贡献”。

国际原子能机构《核安保丛书》第 10-G（Rev.1）号

国家核安保威胁评定、设计基准威胁和代表性威胁声明

实施导则

国际原子能机构

2023 年 • 维也纳

版 权 声 明

国际原子能机构印制
2023 年 9 月 • 奥地利

国家核安保威胁评定、设计基准威胁和代表性威胁声明

国际原子能机构，奥地利，2023 年 9 月
STI/PUB/1926
ISBN 978-92-0-517422-8（简装书：碱性纸）
978-92-0-517622-2（pdf 格式）
ISSN 2790-7023

前　言

国际原子能机构《核安保丛书》就核安保各方面达成的国际共识提供指导，以支持各国积极履行其核安保责任。国际原子能机构开发并维护这些导则文件，作为其向成员国提供核安保相关国际支持与合作方面发挥核心作用的一部分。

国际原子能机构《核安保丛书》由机构与成员国专家合作，于2006年启动开发，之后不断更新。作为总干事，我承诺致力于确保国际原子能机构将持续维护和改进这套综合的、全面的、连贯更新的、用户友好的、适合用途的高质量核安保导则文件。在使用核科学和技术方面适当应用这些导则文件，确保提供高水平的核安保，使人们对核技术的持续应用保持必要的信心，从而造福所有人。

核安保是国家的责任。国际原子能机构《核安保丛书》是对核安保相关国际法律文书的补充，并成为帮助成员国履行其义务的重要参考。虽然核安保导则文件对成员国没有法律约束力，但它得到了广泛应用。它已成为绝大多数成员国不可或缺的参考文件，这些成员国已将这些核安保导则文件的相关建议纳入国家法规，以加强核电、研究堆和核燃料循环设施，以及核技术在医学、工业、农业和科学研究等领域应用中的核安保。

国际原子能机构《核安保丛书》提供的指导是以成员国的实践经验为基础，并通过达成国际共识产生的。核安保导则委员会的成员和其他专家的参与尤其重要，我对所有为这项工作贡献知识和专长的人们表示感谢。

国际原子能机构在帮助成员国开展评估活动和咨询服务时，也会使用《核安保丛书》中的相关导则文件。这有助于成员国应用这些导则文件，从而使有益经验和见解得以分享。上述评估活动和咨询服务过程中形成的反馈意见，以及在使用和应用核安保导则文件中对相关事件和经验的总结，在定期修订这些核安保导则文件时都会考虑借鉴。

我认为，国际原子能机构《核安保丛书》相关导则文件及其应用为确保核技术应用领域的高水平核安保作出了宝贵贡献。我鼓励所有成员国推广和应用这些导则文件，并与国际原子能机构合作，在现在和将来维护这些文件的质量。

编者按

国际原子能机构《核安保丛书》发布的导则对各国不具有约束力，但各国可利用这种导则协助其履行国际法律文书规定的义务以及在本国范围内履行其核安保责任。用“应当”表述的导则旨在提出国际良好实践和表示对各国有必要采取建议的措施或等效替代措施的国际共识。

安保相关术语按其所在出版物中或该出版物所支持的更高一级导则中的定义加以理解。在其他情况下，词语均按其通常理解的意义使用。

附录被视为出版物的一个不可分割的组成部分。附录中的资料具有与正文文本相同的地位。附件用于提供实例或补充资料或解释。附件不是主文本不可分割的组成部分。

虽已尽力保持本出版物中所载信息的准确性，但是国际原子能机构及其成员国对使用本出版物可能产生的后果均不承担任何责任。

使用某些国家或领土的特定名称并不意味着国际原子能机构作为出版者对这类国家或领土、其当局和机构或其边界划定的法律地位作出任何判断。

提及具体公司或产品的名称（不论表明注册与否）并不意味着国际原子能机构有意侵犯所有权，也不应被解释为国际原子能机构的认可或推介。

目 录

1. 引 言

背景

1.1. 《核安保基本法则》确立了核安保制度的目标和基本要素[1]。《核安保建议》提出了核安保制度应针对下列材料和相关设施解决哪些问题：

(a) 核材料和核设施[2]；

(b) 放射性物质和相关设施[3]；

(c) 脱离监管控制的核材料和其他放射性物质[4]。

1.2. 威胁的识别和评定为选择、设计和实施核安保措施提供了重要依据。对于受监管控制的核材料和其他放射性物质，以及相关设施和相关活动，会以设计基准威胁或代表性威胁声明的形式来表示潜在敌手的意图和能力，以保护其免受这些威胁的影响。

1.3. 本出版物是国际原子能机构《核安保丛书》第 10 号《设计基准威胁的制订、利用和维护》[1] 的修订版，旨在反映该领域的发展情况，并确保术语与 2009 年之后出版的参考文献[1－4]相一致。

1.4. 此外，本出版物的范围有所扩大，阐明了如何利用设计基准威胁的替代方案，解释了如何针对具体应用制订设计基准威胁，并更好地解决了涉及网络攻击的威胁[5]。

目的

1.5. 本出版物旨在为评定包括实体、计算机安保领域的国家核安保威胁，为制订、利用和维护设计基准威胁和代表性威胁声明提供具体方法步骤。包括下列步骤：

[1] 国际原子能机构，《设计基准威胁的制订、利用和维护》，国际原子能机构《核安保丛书》第 10 号，国际原子能机构，维也纳（2009 年）。

(a) 明确国家、主管部门（包括监管机构[2]）和营运单位的责任和义务；

(b) 识别和评定核安保相关威胁；

(c) 利用国家核安保威胁评定的结果，来制订威胁声明，如设计基准威胁和代表性威胁声明；

(d) 利用设计基准威胁和/或代表性威胁声明，来制订核安保系统和措施以及核安保要求；

(e) 维护国家核安保威胁评定及其文件的有效性；

(f) 维护设计基准威胁和代表性威胁声明的有效性。

1.6. 本出版物意在供国家、主管部门（包括监管机构）、相关技术和科学支持组织，以及包括发货人和承运人在内，与核材料和其他放射性物质有关的设施和活动营运单位使用。

范围

1.7. 本出版物中描述的概念和方法适用于评定国家核安保威胁，包括实体和计算机安保方面，适用于制订、利用和维护设计基准威胁和代表性威胁声明，以保护受到监管控制的核材料和其他放射性物质以及相关设施和相关活动。

1.8. 本出版物不包括关于制订风险知情方法和进行威胁和风险评定的导则，这些导则是脱离监管控制的核材料和其他放射性物质核安保的基础；关于这方面的导则，可见国际原子能机构《核安保丛书》第24-G号《关于脱离监管控制的核材料和其他放射性物质的核安保措施的风险知情方法》[6]。

结构

1.9. 在引言之后，第 2 节提出了国家核安保威胁评定是风险知情方法的一部分。第 3 节概述了进行国家核安保威胁评定的过程，以及威胁评定及

[2] 有些国家设有多个监管机构，负责核材料安全、其他放射性物质安全，以及相关设施安全和相关活动安全。在本出版物中，术语“监管机构”是指与已知环境相关的机构（或多个机构）。

制订、利用和有效性维护文件、设计基准威胁和代表性威胁声明。第 4 节概述了参与国家核安保威胁评定过程的各组织的责任和义务。第 5 节针对如何进行国家核安保威胁评定提供了更详细的指南。第 6 节描述了制订设计基准威胁和代表性威胁声明，第 7 节针对设计基准威胁和代表性威胁声明的利用提供了指南。第 8 节针对国家核安保威胁评定及其文件和威胁声明的有效性维护提供了指南。本出版物的附录提供了一个设计基准威胁模板。

2. 国家核安保威胁评定和风险知情方法的利用

2.1. 国际公约和国际原子能机构《核安保丛书》相关导则强调了威胁评定、在核安保方面采用风险知情方法的重要性。值得注意的是，经修订的《核材料实物保护公约》[7，8]的基本原则 G（威胁）和参考文献[2]规定：**“国家的实物保护应基于国家对当前威胁的评估。”**

2.2. 参考文献[1]的基本要素 9 如下：

> “核安保制度采用基于分级保护和纵深防御原则的风险知情方法，包括在分配用于核安保系统和核安保措施的资源以及在开展核安保相关活动方面采用分级保护和纵深防御原则，应考虑下列方面：
>
> (a) 国家对当前的内部和外部核安保威胁的评定；
> (b) 所确定的核安保威胁目标的相对吸引力和易受攻击性；
> (c) 核材料、其他放射性物质、相关设施和相关活动的特性；
> (d) 涉及或直接针对核材料、其他放射性物质、相关设施、相关活动、敏感信息或敏感信息资产的犯罪行为或未经授权的故意行为，以及国家确定的对核安保具有不利影响的其他行为的潜在有害后果。”

2.3. 此外，参考文献[2]的第 3.10 段规定：

> “国家应根据威胁评定或设计基准威胁，确定对使用、贮存和运输中的核材料以及核设施的实物保护要求，这取决于擅自转移或破坏核材料和核设施的相关后果。”

参考文献[3]的第 3.17 和 3.18 段规定：

“国家应评估放射性物质、相关设施和相关活动对其国家的威胁。国家应定期审查其国家威胁，并评估威胁所发生的任何变化对其核安保制度设计或更新造成的影响……监管机构应将威胁评定的结果作为确定放射性物质安保要求和对其妥当性进行定期评估的共同基础。”

2.4. 下列各小节更详细地讨论了利用风险知情方法进行国家核安保威胁评定的几个问题；敌手及其属性和特征；以及信息安保。

风险知情方法和威胁声明

2.5. 核安保制度的基本要素 9[1]是采用基于分级保护和纵深防御原则的风险知情方法，包括在分配用于核安保系统和核安保措施的资源时，以及在开展核安保相关活动时采用这种方法。对核安保采用风险知情方法应考虑潜在目标的威胁、吸引力和易受攻击性，以及恶意行为造成的潜在后果。

2.6. 参考文献[2]的第 3.41 段建议“国家应确保其实物保护制度通过风险管理的方式将擅自转移和破坏核材料的风险确定和维持在可接受的水平。”风险管理应包括定期重新评估恶意行为的威胁和潜在后果，并应确保制订适当的核安保系统和措施，以防止或降低成功实施恶意行为的可能性。

2.7. 国家核安保威胁评定是对包括实体威胁和计算机安保威胁在内的现有核安保相关威胁进行评估，以确定潜在敌手的属性和特征。国家核安保威胁评定过程会利用全球、区域和国家信息。

2.8. 国家核安保威胁评定过程的结果记录在国家核安保威胁评定文件中，并可用于制订威胁声明。威胁声明列出在保护与核材料和其他放射性物质有关的活动和设施时所依据的可信的潜在敌手的属性和特征。

2.9. 设计基准威胁和代表性威胁声明等威胁声明中提供的核安保相关的当前威胁评定，可用于促进对个别设施和活动的核安保和风险管理采取风险知情方法。威胁声明有助于对核安保系统和措施进行设计和评估，这些系统和措施考虑了成功实施恶意行为的潜在后果。

2.10. 国家可以选择以设计基准威胁或代表性威胁声明的形式编制威胁声明，也可以同时采用这两种形式，并对不同类型的设施和活动采取适当的监管方法[3]。代表性威胁声明可用于制订监管要求，侧重于对受保护的产生较低后果的具体材料或设施子集制订合规性要求，而设计基准威胁可用于实施监管要求，侧重于采用基于性能的方法来保护产生较高后果的具体设施或活动。例如，主管部门可以利用代表性威胁声明来保护使用和贮存中的 I 类放射源，对其制订合规性监管要求，而营运单位可以利用设计基准威胁来设计和评定核安保系统，以满足基于性能的要求，为具体的 I 类放射源提供针对攻击场景的有效防护。

2.11. 根据国家核安保威胁评定的结果，各国可针对不同类别的核材料和其他放射性物质以及不同类型的设施和活动（如 I 类放射源、辐照装置、放射性物质运输）、敌手的不同目的（如盗窃、破坏），以及可能成为网络攻击特别目标的资产（例如敏感信息或核安全、核安保、核材料衡算与控制或应急响应的计算机系统），选择制订不同的代表性威胁声明。

2.12. 同样，各国可根据国家核安保威胁评定，针对具体设施或活动中具有较高风险的材料（如研究堆、乏燃料运输），选择制订不同的设计基准威胁。这些设计基准威胁将考虑设施或活动的细节（例如设计、位置）、政策因素（例如保持公众信心所需的保守程度），以及国家和营运单位的能力和资源。

2.13. 由于国家核安保威胁评定过程中确定的一些威胁被认为超出了设计基准，设计基准威胁或代表性威胁声明可能不包括这些威胁。即使营运单位的核安保系统提供了某些固有的保护，国家核安保突发事件响应计划中也需要考虑对这些威胁的防护，协调国家应对措施和营运单位的突然事件响应计划。尽管国家应制订措施应对这些威胁，但营运单位仍可在协助国家防范这些核安保威胁或减轻其后果方面发挥作用。

2.14. 关于核安保风险的决定是基于一个国家所关注的当前的威胁、出现新威胁和突发威胁的可能性，以及如何在保守性与成本和运行影响之间取

[3] 关于规范性监管方案和绩效型监管方案的更详细信息，可见参考文献[2，3，8，9]。

得平衡的决定。此类决定还可能需要考虑国际和区域威胁、政治和金融因素、公众对风险的看法以及从以往核安保威胁评定中总结的教训。

潜在敌手及其属性和特征

2.15. 潜在敌手可能包括谋求获取和利用核材料或其他放射性物质来制造核爆炸装置、放射性散布装置或辐照装置的恐怖分子、其他犯罪分子和极端分子。这些敌手还可能谋求破坏使用、贮存核材料或其他放射性物质的设施或核材料或其他放射性物质的运输活动。

2.16. 潜在敌手的特征是动机、意图和能力。例如，动机可能是经济、政治或意识形态上的，也可能是源于不满或受到胁迫。意图可能包括未经授权持有核材料或其他放射性物质，获取敏感信息或敏感信息资产，蓄意破坏，或使设施或活动的营运单位或国家在公众面前陷入困境。敌手的能力取决于涉及的个人数量、组织和协调水平，以及是否有内部敌手参与等特征。能力还包括个人和组织的能力、资产和相关技能，如战术、武器、炸药、运输、实体和计算机相关工具、软件漏洞的知识，以及对设施或其计算机系统的访问级别。

2.17. 敌手可能包括内部敌手[9]：授权访问相关设施或相关活动或敏感信息或敏感信息资产的个人，他们可能进行或协助进行涉及或直接针对核材料、其他放射性物质、相关设施或相关活动或国家确定的对核安保具有不利影响的犯罪行为或未经授权的故意行为。敌手可能会通过获得对设施的授权访问权限（例如被雇佣为承包商）来谋求成为内部敌手，从而利用这种访问权限，或者现有人员通过培养或获得实施或促进恶意行为的意图而成为内部敌手威胁。

2.18. 内部敌手和外部敌手之间串通的可能性也应予以考虑。例如，内部敌手可能以实体或与计算机相关的方式实施未经授权的行为，为外部敌手实行恶意行为提供便利。

2.19. 国家不仅应考虑涉及实体访问设施或活动的潜在恶意行为，还应考虑利用网络攻击的行为。此类攻击可能针对用于核安全（包括仪器仪表和控制系统）、核材料衡算与控制、核安保或应急响应（包括通信和报警系统）的计算机系统。敌手也可能采取混合型攻击，即对计算机系统的攻击

与实体攻击结合起来，例如利用电子伪造的访问凭证进行武装入侵，旨在破坏或盗窃材料。

2.20. 应考虑内部敌手和外部敌手都有可能采取行动，从而损害计算机系统信息的机密性、完整性和可用性。这种行为可能由内部敌手来促成，也可能由外部敌手通过远程网络攻击来促成。还应考虑通过供应链将恶意软件植入计算机系统的情况。

2.21. 还应考虑场外攻击的可能性。场外攻击可能涉及远程操作设备，如无人机、导弹或定向能武器。

信息安保考虑因素

2.22. 在制订和维护威胁声明时，应考虑与威胁有关的所有可信信息，包括国家情报和其他敏感信息。需要保护其中某些信息和许多来源。用于核安保系统设计和评估的设计基准威胁或代表性威胁声明应作为敏感信息加以保护，即包括软件在内的任何形式的信息，如果在未经授权的情况下披露、修改、变更、销毁或拒绝利用这些信息，可能会危及核安保。

2.23. 关于保护核安保敏感信息的详细导则，可见国际原子能机构《核安保丛书》第 23-G 号《核信息安保》[10]。

3. 概述国家核安保威胁评定及其文件、设计基准威胁和代表性威胁声明的制订、利用和有效性维护的过程

3.1. 国家核安保威胁评定及其文件、设计基准威胁和代表性威胁声明的制订、利用和有效性维护过程如图 1 所示，该过程包括五个步骤：

(1) 明确责任和义务；
(2) 进行国家核安保威胁评定，并编制文件；
(3) 制订设计基准威胁和/或代表性威胁声明；
(4) 在监管框架内利用设计基准威胁和/或代表性威胁声明；
(5) 维护国家核安保威胁评定、设计基准威胁和/或代表性威胁声明的有效性；

3.2. 在步骤 1 中，国家应根据其法律和监管框架，确定监管机构和其他主管部门以及营运单位在这一过程中的责任和义务。

3.3. 在步骤 2（进行国家核安保威胁评定）中，负责实施该评定的主管部门应与其他有关主管部门共同收集情报和其他威胁信息，包括来自开放资源、过去核安保事件和非核相关活动安保事件的信息。主管部门应对收集到的信息进行分析，并评估其与核安保的潜在相关性。主管部门还应对威胁信息的可信度进行评估，并剔除不可信的信息。

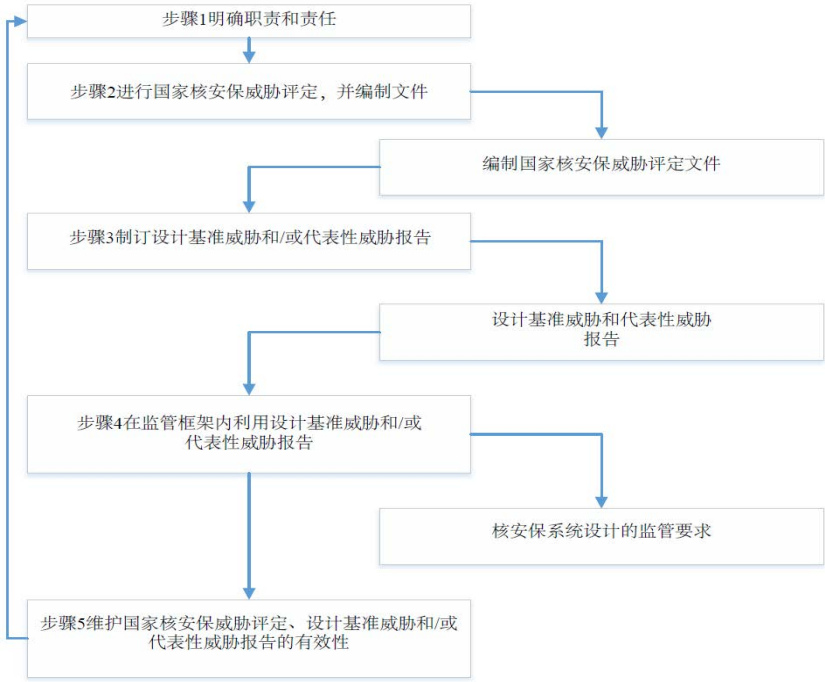

图 1. 国家核安保威胁评定及其文件、设计基准威胁和代表性威胁声明的制订、利用和有效性维护过程。

根据余下的信息，主管部门应识别潜在敌手，并确定潜在敌手行动的可能性以及潜在敌手的属性和特征。最后，主管部门应评估具体敌手的能力是否与潜在目标相关。这一过程的结果应记录在国家核安保威胁评定文件中。

3.4. 在步骤 3 中，根据国家核安保威胁评定的结果，负责制订威胁声明的主管部门应酌情与其他主管部门达成协议，制订针对材料、设施或活动的设计基准威胁和/或制订适用于不同类型和类别的核材料、其他放射性物质、相关设施和相关活动的代表性威胁声明。

3.5. 在步骤 4 中，监管机构的行动将取决于所采取的监管方法：

(a) 对于基于性能的方法，监管机构应向相关营运单位分发设计基准威胁，营运单位应制订针对设施的攻击场景，并利用这些场景设计核安保系统，以应对设计基准威胁，并实现国家法律框架中确立的核安保目标。

(b) 对于合规性方法，监管机构应根据代表性威胁声明和国家法律框架中确立的核安保目标制订监管要求，并应确保营运单位按照这些要求实施核安保系统和措施。

(c) 对于综合性方法，监管机构的行动应涵盖基于性能的方法和合规性方法两方面的内容。

3.6. 在步骤 5 中，主管部门应审查并酌情修订国家核安保威胁评定及其文件、设计基准威胁和/或代表性威胁声明。如果威胁环境发生变化和/或要纳入核安保事件的教训，可根据规定的审查周期决定是否修订这些文件。如果需要立即考虑新威胁或突发威胁，主管部门应与营运单位共同采取必要的行动来管理这些威胁，如有必要，应将这些威胁与现有的设计基准威胁或代表性威胁声明分开处理，直至对设计基准威胁和代表性威胁声明进行修订。这一过程应纳入国家的核安保制度。

3.7. 第 4－8 节对每个步骤进行了更详细的讨论，包括对国家、主管部门和营运单位实施这些步骤提供更具体的指导。

4. 责任和义务

4.1. 国家、相关主管部门（包括监管机构）和营运单位在进行国家核安保威胁评定、制订设计基准威胁和/或代表性威胁声明方面具有责任和义务。在开展国家核安保威胁评定工作之前，应明确这些责任和义务。

国家

4.2. 国家负责指定、协调和监督领导和参与下列工作的主管部门：

(a) 进行国家核安保威胁评定，并维护该评定及其文件的有效性；

(b) 制订和维护设计基准威胁和/或代表性威胁声明的有效性；

(c) 利用设计基准威胁和/或代表性威胁声明。[4]

4.3. 核安保事件可能引发核或辐射紧急情况。国际原子能机构《安全标准丛书》第 GSR 号第 7 部分《核或放射紧急情况的应急准备与响应》[11]的第 4.22 段规定：“政府应确保危害评定涵盖为核安保目的而进行的威胁评定的结果。”

主管部门

4.4. 所有相关主管部门都应参与国家核安保威胁评定过程，以便在评定中尽可能全面地识别和考虑各种可信的威胁。

4.5. 识别和评定可信威胁的相关专门知识可能存在于国家的多个组织中，例如情报组织（含安保机构）、内政部和外交部、计算机安保中心、执法机构、军事部门、核安保监管机构等相关组织。此类组织拥有熟悉信息收集、分析过程并擅长做出必要判断的工作人员。此外，此类组织还可以访问特定的信息来源，包括从与其他国家或区域或国际组织接触获得的信息。

4.6. 主管部门的责任包括下列方面：

(a) 收集和整理关于潜在威胁的信息；

(b) 分析可用的威胁信息，以确保其可信度；

(c) 与其他主管部门共享相关威胁信息；

(d) 与其他主管部门协调，以确定与核安保有关的可信威胁子集；

[4] 国家可以指定不同的主管部门负责不同的过程；但是，必须明确主管部门的职责和责任，建立和执行主管部门之间的协调机制。

(e) 在威胁评定过程中开展合作，识别潜在敌手，并形成国家核安保威胁评定文件；

(f) 根据国家核安保威胁评定的结果，制订设计基准威胁和/或代表性威胁声明；

(g) 维护国家核安保威胁评定及其文件、设计基准威胁和代表性威胁声明的有效性；

(h) 酌情与相关应急响应组织共享国家核安保威胁评定文件；[5]

(i) 在实施危害评定[12]时，考虑国家核安保威胁评定；

(j) 落实信息安保因素。

4.7. 有些主管部门（如国家和地方警察机关、武装部队、边境控制主管部门和海关）在国家中承担比较广泛的职责范围，包括独自或是与其他部门一起在防范核安保相关威胁方面发挥重要作用。有些主管部门还可能负责在发生核安保事件时向营运单位提供支持。在制订设计基准威胁和/或代表性威胁声明以及监管要求的过程中，应有此类主管部门的参与或向其征求意见。

4.8. 核安保监管机构酌情与其他主管部门协调，负责下列工作：

(a) 根据代表性威胁声明为营运单位制订合规性要求，和/或向营运单位提供设计基准威胁和基于性能的要求，以用于制订攻击场景和设计核安保系统和措施；

(b) 确保营运单位适当审查（必要时修订）安保和应急安排，同时考虑到已制订的攻击场景和威胁评定的结果。

营运单位

4.9. 营运单位应实施满足下列一项或两项要求的核安保系统和措施：

(a) 满足监管要求，包括根据代表性威胁声明制订的相关合规性要求；

(b) 应防范对于根据设计基准威胁制订的一系列针对设施或活动的攻击场景。

---

[5] 鉴于核安保领域的响应是指对核安保事件的响应，本出版物使用“应急响应组织”一词以避免误解。使用“应急响应组织”一词符合第GSR号第7部分[11]对“响应组织”的定义。

4.10. 在某些情况下，营运单位对具体核安保措施的经济、运行和安全影响的知识可能会影响营运单位与主管部门之间在核安保措施方面的责任分工。在制订设计基准威胁、代表性威胁声明和监管要求时，应考虑营运单位的输入，不管是正式的还是非正式的。具体而言，营运单位应提供下列信息：

(a) 应考虑针对设施和活动的核安保相关威胁的输入，以纳入设计基准威胁和/或代表性威胁声明；

(b) 如果认为有必要，按照法律和监管框架要求，就有关设计基准威胁、代表性威胁声明和/或监管要求的潜在决定对经济、运行、安保和安全的影响向监管机构提供反馈意见；

(c) 如认为有必要，按照法律和监管框架要求，就有关可能发生的实体攻击、网络攻击和混合型攻击的攻击场景以及敌手属性和特征提供支持信息。

5. 进行国家核安保威胁评定

5.1. 国家核安保威胁评定的目的是对可信的威胁进行评估，对潜在敌手的动机、意图和能力进行描述。不包含对具体攻击场景的描述。

5.2. 对潜在威胁进行足够详细和具体的描述，可用于确定为核材料和其他放射性物质、相关设施和相关活动提供适当和充分的保护水平，并为有效设计核安保系统提供依据。

5.3. 在国家核安保威胁评定过程中，需要对当前的威胁和可信的潜在威胁信息进行收集和分析，并对潜在敌手的属性和特征信息进行汇集和整合。国家核安保威胁评定的输出是对核安保相关威胁的详细描述，称为国家核安保威胁评定文件。具有不同专业知识领域和责任领域的所有相关组织应进行紧密合作，收集和分析这些信息。要使国家核安保威胁评定发挥效力，所有相关组织之间必须建立紧密合作关系。应对国家核安保威胁评定的实施进行记录，为定期审查和修订程序提供支持，以保持评定的有效性。

5.4. 第 4 节已经对实施下列各小节所述行动并确保完成行动的责任和义务进行了描述。

输入：相关威胁信息的收集

5.5. 国家核安保威胁评定过程的首要任务是收集和整理有关所有潜在敌手及其动机、意图和能力的全面信息。这些信息可能包括敏感信息和非敏感信息，应涉及实体和计算机相关的能力，以及潜在内部敌手和外部敌手。

5.6. 应识别潜在的信息来源，并收集相关信息。应考虑信息的敏感性，以确保对信息及其来源采取适当的安保措施。如果在威胁评定过程中尚未建立所有相关组织共享威胁信息的机制，则应建立这一机制，并应确保敏感信息的安全。要建立共享威胁信息的机制安排，可能需要达成书面协议。

5.7. 与威胁有关的情报和其他信息来源可能会为设计核安保系统提供足够的信息。然而，由于情报的局限性和威胁的动态性，仅针对当前已知威胁而设计的核安保系统可能无法有效抵御未来的威胁。

5.8. 国家核安保威胁评定不应依赖单一来源。利用多种来源的情报和威胁信息，进行一次连贯的评定，以实现最全面、可靠和有力的国家核安保威胁评定。在收集数据时，应考虑所有可信的和相关的国家和国际情报和威胁信息来源。

5.9. 信息和情报来源范围应酌情涵盖情报组织（含安保机构）、计算机和信息安全组织、执法机构、国际刑警组织、核安保监管机构等主管部门、海关和边境机构、军事部门、发货人和承运人、政府官方报告、营运单位的事件报告、由国际组织维护的数据库等开放资源。

5.10. 技术和科学支持组织、商业实体和开放数据库可作为潜在威胁的额外信息来源，特别是对计算机安保的威胁。营运单位还可能掌握与此类威胁及其属性和特征相关的信息。

5.11. 对其他类型关键基础设施构成的潜在威胁的属性和特征相关信息应被视为类似的核安保威胁。

5.12. 应收集近期和历史核安保事件的信息，包括涉及计算机安保的事件信息（如适用）。

5.13. 信息收集任务应旨在识别所有相关类型的威胁，包括下列威胁：

(a) 全球、国家和地方威胁；

(b) 实体攻击、网络攻击和混合攻击；

(c) 内部敌手威胁、外部敌手以及内部敌手与外部敌手串通造成的威胁。

5.14. 还应考虑可信的敌手的能力，即使尚未证实。还应考虑计划在较长时间内发动多阶段攻击的持久潜在敌手、可能的技术发展、攻击的潜在频率和供应链被攻击的可能性（例如，硬件和/或修改后的软件在交付前被破坏）。

相关威胁信息的分析

5.15. 相关威胁信息收集完成后，在开始分析之前，应利用信息管理工具对这些信息进行整理以便索引和分类。有效地组织所有情报和其他可用信息，以确保分析所有必要信息。之后，应对组织有序的信息进行分析，以确定核安保相关的潜在敌手的可信动机、意图和能力，并形成文件。

5.16. 信息收集的全面性和分析的准确性将影响由该过程产生的设计基准威胁和/或代表性威胁声明的可信度。

5.17. 信息收集和分析可能是迭代的过程。事实证明，通常需要分析更多信息，或者说需要信息确定此前未知的威胁或新威胁。对威胁信息的分析涉及对基于这些信息的已知信息进行评估，并对敌手的属性和特征未来可能发生的变化做出判断。

5.18. 在分析过程中，应对国家核安保威胁评定所利用信息的可信度进行评估。一般来说，在评估威胁信息的可信度时，同时考虑信息来源的可信度和技术专业知识非常重要。执法机构和情报机构，包括安保机构，应根据其判断，给出其所提供的信息的可信度。易获取的开源信息（例如来自公共媒体或社交网络）可能是有用信息，但应仔细斟酌其准确性。在决定以后如何利用某条信息时，应考虑该信息的可信度。在评估信息的可信度时，有些信息也可能因为与分析无关而被排除，并且可能会出现额外的信息缺口（例如，当可能填补缺口的信息被判断为不够可信时）。

5.19. 国家核安保威胁评定过程应至少涵盖每个已确定威胁的敌手的下列属性和特征（尽管可能无法获得所有威胁的所有列出属性和特征的数据）：

(a) 敌手的动机，例如政治、经济、意识形态和/或个人动机（如由于不满或胁迫）；

(b) 敌手的持久性；

(c) 敌手的献身程度，包括风险规避程度和冒生命危险的意愿；

(d) 已证实的敌手能力，包括对过去发生的核安保事件的特征描述；

(e) 敌手的意图，例如破坏材料或设施，擅自转移核材料或其他放射性物质，盗窃敏感信息；

(f) 敌手的团伙数量，包括攻击力量、协调人员和支持人员；

(g) 敌手可用武器的种类和数量；

(h) 敌手可用炸药的种类和数量，无论是以装置形式还是简易的形式，以及引爆机制的复杂程度；

(i) 敌手可用的工具，如机械、热或电磁设备、手动或电子设备或通信设备；

(j) 敌手可用的运输方式，包括类型（公共、私人）、方式（陆地、海上、空中）以及车辆类型和数量；

(k) 接触目标可能的方式，包括实体和计算机方式；

(l) 对运行和（或）人员的影响；

(m) 潜在敌手的战术，例如隐蔽、欺骗、武力、侦察活动或社会工程；

(n) 敌手制定计划的技能，例如机会转移核安保人员注意力或协调多个较小群体同时攻击的能力；

(o) 敌手可用的实际技能、知识和经验，包括工程技术技能、炸药、化学品和通讯的使用以及军事或准军事经验；

(p) 计算机和计算机安保技能的掌握，如控制系统、计算机安保措施、逆向工程和薄弱环节测试、通信协议工程、社会工程、源代码混淆、属性重定向、网络监视和流量操纵的知识；

(q) 对目标信息的了解或接触，如目标特征、设施布局、场址平面图和程序、安保计划、安保措施、安全和辐射防护措施、设施和运输运行、

网络攻击的可能切入点、供应商支持程序和计划以及供应链和采购程序；

(r) 资金来源和数量，以及如何获得资金；

(s) 利用内部敌手的可能性（包括串通、胁迫或欺骗）、内部敌手的可能人数以及被动或主动参与、暴力或非暴力参与；

(t) 敌手的支持结构，例如是否存在当地同情者、支持组织或后勤支持。

输出：国家核安保威胁评定文件

5.20. 国家核安保威胁评定过程的成果记录在国家核安保威胁评定文件中，该文件要对国家需要考虑的整体威胁环境和所有已知可信的威胁进行描述。辅助性分析说明应尽可能提供这些威胁和信息可信度的详细情况。

5.21. 国家核安保威胁评定文件和情报来源细节通常都作为敏感信息加以保护。

6. 设计基准威胁和代表性威胁声明的制订

6.1. 如第 5 节所述，国家核安保威胁评定过程的成果是提供国家核安保威胁评定文件。以国家核安保威胁评定为依据，可以制订设计基准威胁和/或代表性威胁声明的形式的威胁声明。这些声明要对保护使用或贮存核材料或其他放射性物质的设施和活动时所依据的可信敌手，以及这些敌手的属性和特征进行描述。

监管方法和威胁声明

6.2. 在管理设施或活动的运行时，存在三种监管方法：基于性能的方法、合规性方法和综合性方法。在基于性能的方法中，营运单位需要设计和实施核安保系统，以满足国家规定的核安保目标，同时要考虑监管机构分发的设计基准威胁、针对防范恶意行为的有效性水平，提供突发事件响应措施。在合规性方法中，监管机构在未与营运单位共享威胁信息的情况下，制订必要的具体核安保措施，以满足每类核材料或其他放射性物质、每级潜在放射后果所规定的核安保目标。这为营运单位提供了一套“基

准”实施措施。综合性方法涵盖合规性方法和基于性能的方法两方面的内容。关于这些监管方法的更详细信息，可见参考文献[13，14]。

6.3. 如第 2.10 段所述，代表性威胁声明经常用于为受保护的特定材料、活动及/或设施子集制订合规性监管要求，而设计基准威胁则通常针对特定的设施或活动。监管机构应根据国家的法律和监管框架，采取最适合国家需要的监管方案和相应的代表性威胁声明和/或设计基准威胁。监管机构选择的监管方法应得到国家的批准，因为其选择可能会对监管机构和营运单位产生资源影响。

6.4. 在基于性能的监管方法中，利用设计基准威胁作为设计核安保系统和措施的依据，可以制订针对具体相关威胁，而非一般威胁的保护与核安保系统和措施要求，从而实现资源的有效分配。利用基于性能的方法和设计基准威胁不仅可以定制核安保系统的设计，以适应材料、活动或设施（包括其仪器仪表和控制系统）的独特特征，而且可以为核安保系统和措施的评估（以及必要时修改）设定基准，并为界定营运单位的核安保责任提供明确依据。利用设计基准威胁还为设计和评定标准提供了更详细和精确的技术基础，保证为其提供更好的、充分的保护。

6.5. 在基于性能的方法中，利用设计基准威胁意味着监管机构和营运单位将需要更多的资源和能力。因此，监管机构界定设计基准威胁所需的资源和能力，以及营运单位有效利用设计基准威胁设计核安保系统和措施的能力，可能会影响其是否决定制订设计基准威胁。但是，如果国家确定有必要具备与设计基准威胁相关的保证水平，则国家应提供必要的资源和能力。

6.6. 国家应考虑将其对核材料和核设施的实物保护要求建立在设计基准威胁的基础上，特别是对擅自转移 I 类核材料和破坏核材料和核设施的威胁，如果国家拥有此类材料或设施[2]，有可能造成较高的放射后果。如果国家已确定恶意行为的潜在后果会很严重，也应考虑制订设计基准威胁。

6.7. 在下列任何情况下，要保护潜在后果轻微的核材料或其他放射性物质、相关活动或相关设施，应考虑制订设计基准威胁：

(a) 国家核安保威胁评定表明存在已知企图实施恶意行为的威胁。

(b) 国家核安保威胁评定表明存在意图未知的能力极强的威胁。

(c) 由于数据数量有限或对数据来源信心不足，在国家核安保威胁评定中存在太多的不确定性。

6.8. 对于新设施，为了减少在设施运行后追加升级的费用问题，对于比当前国家核安保威胁评定更为保守的威胁属性和特征设计防护措施，国家可能考虑设计保护措施的可能长远利益。

制订设计基准威胁

6.9. 应根据国家核安保威胁评定，通过下列五个任务来制订设计基准威胁：

(1) 筛选国家核安保威胁评定文件，以识别具有实施恶意行为的动机、意图和/或能力的相关威胁；
(2) 整理敌手属性和特征；
(3) 根据政策因素，调整已整理的敌手属性和特征；
(4) 针对设施和活动调整敌手属性和特征；
(5) 确定和制订设计基准威胁。

筛选国家核安保威胁评定文件

6.10. 恶意行为可能导致不可接受的放射后果，应确定国家所界定的不可接受的放射后果。之后，应将这些目标与国家核安保威胁评定文件中描述的潜在敌手属性和特征结合起来，以确定与这些目标有关并可能导致不可接受放射后果的威胁。这种考虑应包括审查敌手针对这些目标的动机、意图和能力。

6.11. 应对国家核安保威胁评定文件中所描述的敌手进行审查，以确定哪些敌手具备实施可能导致不可接受放射后果的恶意行为的必要能力。如果已知敌手的能力不足以实施这种行为，那么不再把该敌手考虑进去。然而，对此决定需要相当谨慎行事。特别是，不应以保护某种设施或活动的现有核安保系统足以击败敌手为基础，将威胁排除在进一步考虑之外。在

设计基准威胁的制订过程中判断敌手的能力时，不应考虑现有的核安保措施。[6]

6.12. 之后，应对被视为有足够能力实施可能导致不可接受放射性后果的恶意行为的每个敌手进行审查，以确定该敌手是否确信有足够的动机或意图实施此类行为。如果确定没有足够的动机或意图，可将该敌手排除在进一步考虑之外。然而，仅仅以缺乏动机或意图为基础将能力极强的敌手排除在外，应相当谨慎行事。关于是否排除敌手的决定应考虑察觉到的敌手动机是否符合此类恶意行为的潜在后果相，以及用于评定其动机和意图的数据是否具有足够的可信度。

6.13. 在国家核安保威胁评定文件中，其所描述的将任何敌手排除在设计基准威胁的进一步考虑之外的理由都应该完整归档。如果以后又获得了可能影响排除理由的新信息，对于任何被排除在进一步考虑之外的敌手，应该重新加以考虑。

6.14. 在筛选过程结束时，应列出所有具备能力、可能具有动机和意图实施可能导致不可接受放射后果的恶意行为的可信敌手名单。

整理敌手属性和特征

6.15. 应将国家核安保威胁评定文件中确定的每个相关敌手归类到适当的敌手类型，并应对每种敌手类型做出可信描述。为便于参考，可以给敌手类型贴上说明性标签（例如“恐怖分子”、“罪犯”、“极端分子”），但应根据其具体属性和特征对其进行定义。某种敌手类型构成的威胁应反映归类到这种敌手类型的各种敌手的属性和特征范围。

6.16. 应对与已知敌手类型相关的属性和特征进行整理。已整理的属性和特征不应仅代表不同敌手的最极端属性和特征的组合，而应是实际发生在一个敌手身上的可信组合。

[6] 这是一个审慎保守的假设。例如，如果设计基准威胁不包括需要采取有效措施应对的敌手属性和特征，那么营运商后期可能会取消这些核安保措施。

根据政策因素，调整已整理的敌手属性和特征

6.17. 任何所确定的相关政策因素都可作为依据来评定已整理的敌手属性和特征。这可能导致对已整理的敌手属性和特征进行调整，以实现可持续的安保水平，并可能导致假想敌手的能力水平发生变化。

6.18. 例如，调整已整理的敌手属性和特征，以适应国家核安保威胁评定所需的保守程度。这种调整可能旨在抵消国家核安保威胁评定中数据的不确定性和不同解读；确保营运单位的核安保系统和措施随着威胁的演变而持续有效；或者作为一种谨慎方案，涵盖目前几乎或根本没有其情报的威胁的属性和特征。

6.19. 成本-利益因素也可能导致对已整理的敌手属性和特征进行调整。这可能包括对潜在目标相关的社会利益、针对这些目标的成功恶意行为的社会后果和社会用于减少这些行为风险的费用三者之间进行权衡，实施与造成类似严重后果的其他资产或基础设施的保护（如炸药、化学品、生物制剂）相当的适当核安保措施；

6.20. 还可能需要考虑其他政策因素，例如国家和营运单位之间的核安保责任分工、接受风险的决定对公众信心的影响、潜在目标对公共福利的贡献（如正在使用核材料或放射性物质的应用领域）、邻国对国家核安保的信心和邻国的威胁。

6.21. 这里提到的保守程度和其他政策因素可能会导致设计基准威胁中已整理的敌手属性和特征的假设能力水平提升，而成本-利益因素可能会导致该能力水平下降。

针对设施和活动调整敌手属性和特征

6.22. 应根据政策因素，针对设施和活动的特征对具有广泛代表性的敌手属性和特征进行调整。对于设施，这些因素可能包括场址位置和可达性、设施的具体设计特征、设施的运行惯例和任何具体的当地威胁。对于活动，这些因素可能包括运行程序、运输方式和路线，以及任何针对特定地点或路线的威胁。

确定和制订设计基准威胁

6.23. 在监管框架中利用设计基准威胁之前，应考虑其他主管部门和受影响方的意见。关于设计基准威胁内容以及对该内容的总体责任，还是应由国家指定领导制订过程的主管部门最终决定。

6.24. 附录中提供了设计基准威胁模板。

制订代表性威胁声明

6.25. 与设计基准威胁一样，应在国家核安保威胁评定的基础上制订代表性威胁声明。代表性威胁声明的制订过程遵循第 6.9－6.24 段中所述的针对设计基准威胁的方案，但每个步骤都以较宽松的方式进行，涉及的组织可能会较少。此外，敌手的属性和特征并不针对特定的设施或活动而量身定制。

6.26. 制订代表性威胁声明的过程应包括下列四项任务：

(1) 筛选国家核安保威胁评定文件，以识别具有实施恶意行为的动机、意图和/或能力的相关威胁；
(2) 将敌手属性和特征整理成代表属性和特征范围的集合；
(3) 根据相关政策因素，调整代表性敌手属性和特征；
(4) 确定和制订代表性威胁声明。

设计基准威胁范围内和范围外的威胁

6.27. 在国家核安保威胁评定过程中，可能会确定广泛的敌手能力。考虑到已知的、实际的和普遍存在的威胁，国家将需要确定威胁或敌手能力的水平，如果威胁或敌手能力超过该水平，由于营运单位的保护和响应能力和/或资源不足以应对如此高的能力和潜在后果，国家将代替营运单位来承担应对责任。然而，营运单位仍可在协助国家防范这些核安保威胁或减轻其后果方面发挥作用。

6.28. 因此，设计基准威胁应基于能力低于该阈值的敌手，这意味着营运单位对防范和应对具有更高能力的敌手不承担主要责任。对于能力超过这

一阈值的敌手，国家将承担主要应对责任。国家确定这一阈值时，需要对费用、运行影响和其他因素进行权衡。

7. 设计基准威胁和代表性威胁声明的利用

7.1. 如第 6.2－6.8 段所述，国家可选择采用基于性能的监管方法、合规性监管方法或综合性监管方法。本节将讨论各种监管方法对设计基准威胁和代表性威胁声明的利用。

基于性能的监管方法

7.2. 在基于性能的监管方法中，设计基准威胁和国家核安保目标为设计、实施和评定核安保系统和措施提供了依据。

7.3. 基于性能的监管方法利用设计基准威胁的过程包括下列任务：

(a) 监管机构应向营运单位分发设计基准威胁。

(b) 各营运单位应与监管机构合作，以提供的设计基准威胁为基础界定可信的攻击场景。

(c) 各营运单位应设计核安保系统和措施，以有效抵御其设施或活动所确定的攻击。

(d) 各营运单位应在其安全计划中对其核安保系统设计进行描述，必要时应将该计划提交监管机构批准。

(e) 监管机构应以提交的安全计划为基础，对各营运单位的核安保系统设计的有效性进行评估。

(f) 安保计划获得批准后，营运单位可运行其设施或活动。

7.4. 相关应急响应组织，包括监管机构和营运单位，应在危害评定中利用国家核安保威胁评定结果，以便为核安保事件引发的核或放射紧急情况的应急准备与响应以及协调综合应急响应，建立适当的应急安排。

合规性监管方法

7.5. 在合规性监管方法中，考虑到国家确定的核安保目标，监管机构应利用适用于每种类别材料和每种类型设施或活动的代表性威胁声明，来制订合规性监管要求。合规性监管要求应规定为确保实现充分保护而实施的和安保制度和措施，以实现国家核安保制度目标。关于帮助国家制订此类合规性监管要求的导则，可见参考文献[13－16]。

7.6. 合规性监管方法利用代表性威胁声明的过程包括下列任务：

(a) 监管机构应根据各个代表性威胁声明，确定可信的攻击场景，并为不同类别的材料、不同类型的设施和活动设计核安保措施。

(b) 监管机构应酌情考虑参考文献[2，3，9，13－16]等国际原子能机构的相关出版物中建议的措施，并确定这些措施是否足以满足核安保目标，或是否需要增加额外措施以提供相关代表性威胁声明所需的保护水平。

(c) 监管机构应制订适用于所设计的核安保措施的合规性监管要求。

(d) 营运单位应落实相关监管要求规定的核安保措施。

综合性方案

7.7. 如第 6.2 段和参考文献[13，14]所述，综合性监管方法采用了合规性方法和基于性能的方法两方面的内容。

7.8. 如果利益大于成本，例如由于核安保事件可能造成的潜在后果，需要提供适当的更大保证时，国家可对设施和活动采用基于性能的方法。如果核安保事件可能导致的潜在后果不太严重，可对材料、相关设施和相关活动采用合规性方法。国家还可以决定，采用基于性能的方法应对一些威胁，采用合规性方法应对其他一些威胁。

开发攻击场景

7.9. 攻击场景的制订取决于如何理解利用敌手属性和特征实施恶意行为，以及不同的敌手是否以及如何合作实施这种行为。

7.10. 攻击场景是一组通常用于分析或评定的假定或假设条件和事件，以代表将要建立模型的未来可能的条件和事件，如可能的核安保事件。攻击场景可能代表单个时间点或单个事件的条件，或导致核安保事件或源自核安保事件的一段时间内的条件或事件（包括过程）历史，包括潜在的延迟影响。

7.11. 攻击场景应定义为包括代表性威胁声明或设计基准威胁中所界定的敌手属性和特征的所有可信组合，包括内部敌手和外部敌手之间的串通，以及实体攻击和网络攻击的组合。场景应定义 (a) 可能的敌手路径，(b) 基于假定攻击战术的渗透时间以及实体和计算机安保措施的延迟时间，以及 (c) 基于传感器和监控措施的探测概率以及逃避或击败它们的假定战术。

7.12. 尤其要考虑网络攻击的攻击场景。虽然单独的网络攻击可能不足以擅自转移材料，但网络攻击可能会破坏威慑、探测、延迟或应对擅自转移或破坏行为的核安保措施。网络攻击还可能导致安全、安保、核材料衡算与控制或支持此类攻击的应急准备和响应功能退化。

7.13. 影响攻击可行性的因素可能包括攻击的复杂性；所需工具和其他资源的数量和复杂程度；敌手的技能和能力；敌手对设施和访问点的知识（包括敌手藏身之处或工具，以及系统中可利用的弱点）；外部敌手的数量；响应部队的能力；涉及内部敌手的数量、性质及串通程度；以及实体屏障、计算机安保措施、探测和监控技术的有效性。

8. 国家核安保威胁评定及其文件和威胁声明的有效性维护与审查

8.1. 应定期审查国家核安保威胁评定文件，以评估其是否仍然代表对国家核安保的可信威胁的全面和平衡看法，并在必要时其进行修订。

8.2. 如果国家核安保威胁评定文件需要修订、反映政策因素的变化，或要考虑从核安保系统和措施的设计和评估或从核安保事件中获得的经验，那么可能需要对设计基准威胁和代表性威胁声明进行审查（必要时进行修订）。

8.3. 例如，可以每 12-18 个月对国家核安保威胁评定、设计基准威胁和代表性威胁声明进行定期审查。定期审查应遵循与实施国家核安保威胁评定相同的程序。

8.4. 对于不确定不断变化的新威胁和能力是否与核安保直接相关，此类考量可纳入国家核安保威胁评定的审查，以确定这些威胁与核材料、其他放射性物质、相关设施和相关活动之间的任何可能关联。

8.5. 许多其他情况可能需要在定期审查程序之外对国家核安保威胁评定、设计基准威胁和代表性威胁声明进行审查。可能触发此类审查的条件或事件包括：

(a) 在国内或其他地方发生的，显著改变人们对核安保威胁的看法或核安保威胁的实际程度的任何事件或行为，无论是否与核材料、其他放射性物质、相关设施或相关活动具有直接关联。

(b) 影响主管部门或营运单位责任的政府政策、法律或国际安排的显著变化，例如应对安排或组织责任的变化。

(c) 可能改变或引起新的潜在后果、与核材料和其他放射性物质有关的设施或活动的变化。例如，这种变化可能包括建造不同类型的设施、使用高浓缩材料、以新的方式使用材料、收回高浓铀、改变运行以使用较低类别的材料或核安全改进措施。

(d) 主管部门、技术或科学支持组织或营运单位提出进行审查。

8.6. 审查结果不一定会对国家核安保威胁评定、设计基准威胁或代表性威胁声明进行修订。但是，如果审查表明国家核安保威胁评定不能充分应对所有可信威胁，包括新威胁和突发威胁，则应在所有相关组织的参与下对国家核安保威胁评定及其文件进行修订。如果国家核安保威胁评定发生重大根本性变化，则应对设计基准威胁和代表性威胁声明进行修订。

应对新威胁和突发威胁

8.7. 在常规审查过程之外，可能会出现这样的情况：事实证明或有人怀疑，敌手拥有新的或意想不到的实体或计算机相关能力，其威胁足以使国家立即采取行动。可以通过官方和非正式渠道获得这些事项的情报和威胁信息。

8.8. 除了设计基准威胁和代表性威胁声明的制订和有效性维护的过程之外，监管机构和其他主管部门还应制订一个主管部门之间以及主管部门与相关营运单位之间共享威胁信息的流程。当威胁级别迅速发生变化，没有足够时间对国家核安保威胁评定进行全面重新评估时，这一点尤其必要。

8.9. 如果营运单位通过非正式渠道收到有关威胁变化的信息，则营运单位应酌情通知监管机构和其他主管部门，让其评定威胁变化的潜在影响的可信度、相关性和严重性，并确定国家和/或营运单位的应对方式和应对紧急程度。

8.10. 在这种情况下，建立一个预先确定的高威胁级别系统，并由营运单位在每个高威胁级别上实施预先确定的附加核安保措施，可以提供附加防护。

附 录

设计基准威胁模板

A.1. 表 1 是如何在设计基准威胁中体现敌手属性和特征的示例。

A.2. 代表性威胁声明可以使用类似格式，通常细节较少，也可以使用不太正式的格式。

表 1. 设计基准威胁的敌手属性和特征示例列表

	武装	非武装
行动		
盗窃 [a]	填写是或否	填写是或否
破坏 [b]	填写是或否	填写是或否
共同属性和特征		
数量	填写数量	填写数量
资金水平	填写低或高	填写低或高
内部支持	填写主动或被动，和暴力或非暴力	填写主动或被动，和暴力或非暴力
战术	填写隐蔽和/或武力	填写隐蔽和/或武力
规划技能	填写规划转移注意力的能力，和/或敌手协调较小群体同时攻击，和/或设施布局的知识和/或规划混合攻击的能力	填写规划转移注意力的能力，和/或敌手协调较小群体同时攻击，和/或设施布局的知识和/或规划混合攻击的能力

表 1. 设计基准威胁的敌手属性和特征示例清单（续）

	武装	非武装
实体属性和特征		
杀人的意愿	填写是或否	填写是或否
死亡的意愿	填写是或否	填写是或否
路径	填写空中、公路、铁路、水路和/或地下	填写空中、公路、铁路、水路和/或地下
武器类型	填写自动武器、半自动武器、随身佩带武器和/或刀具	不适用
炸药	填写炸药的类型和数量	不适用
工具	填写电动工具、手动工具和/或现场可用工具	填写电动工具、手动工具和/或现场可用工具
技术技能	填写复杂的爆破破坏、破坏通信线路和/或运行设施设备	填写复杂的爆破破坏，破坏通信线路和/或运行设施设备
参与的内部敌手	填写访问授权、保安、设备技术维护和/或材料处理	填写访问授权、保安、设备技术维护和/或材料处理
网络属性和特征		
软件工具	填写标准软件工具、恶意软件工具和/或自行开发的工具	填写标准软件工具、恶意软件工具和/或自行开发的工具

表 1. 设计基准威胁的敌手属性和特征示例清单（续）

	武装	非武装
专业知识	填写社会工程、使用商业工具、开发新软件工具、办公域、过程控制域和/或应用 IT 系统的知识	填写社会工程、使用商业工具、开发新软件工具、办公域、过程控制域和/或应用 IT 系统的知识
硬件工具	填写计算机、手机、连接电缆和/或路由器	填写计算机、手机、连接电缆和/或路由器
影响供应链的能力	填写是或否	填写是或否
敌手的持久性	填写长期和/或重复攻击能力	填写长期和/或重复攻击能力
参与的内部敌手	填写访问授权，普通用户、管理员和/或第三方供应商控制 I&C 系统的进程	填写访问授权，普通用户、管理员和/或第三方供应商控制 I&C 系统的进程

注意： I&C — 仪器仪表和控制；IT — 信息技术。

[a] 可以填写转移和/或一次性或长期盗窃的材料数量标准。

[b] 可以填写放射后果标准。

参考文献

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).

[4] EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, UNITED NATIONS OFFICE ON DRUGS AND CRIME, WORLD CUSTOMS ORGANIZATION, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).

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

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 24-G, IAEA, Vienna (2015).

[7] The Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1, IAEA, Vienna (1980).

[8] Amendment to the Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1/Mod.1, IAEA, Vienna (2016).

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

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).

[11] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, INTERPOL, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, PREPARATORY COMMISSION FOR THE COMPREHENSIVE NUCLEAR-TEST-BAN TREATY ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, WORLD METEOROLOGICAL ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSR Part 7, IAEA, Vienna (2015).

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

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 27-G, IAEA, Vienna (2018).

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

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

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Material in Transport, IAEA Nuclear Security Series No. 26-G, IAEA, Vienna (2015).

术 语 表

设计基准威胁。在实物保护系统设计和评定时所依据的试图实施擅自转移或蓄意破坏的潜在内部敌手和/或外部敌手的属性和特征。

代表性威胁声明。试图实施擅自转移或破坏的潜在内部敌手和/或外部敌手的属性和特征，旨在用于制订规定材料和/或设施保护的合规性要求。

威胁评定。基于现有的情报、执法和开源信息对威胁的评估，该评估对这些威胁所具有的动机、意图和能力进行描述。

威胁声明。在国家核安保威胁评定的基础上，以设计基准威胁或代表性威胁声明的形式对可信敌手（包括属性和特征）的描述。

IAEA
国 际 原 子 能 机 构

No. 27

当 地 订 购

国际原子能机构的定价出版物可从下列来源或当地主要书商处购买。
未定价出版物应直接向国际原子能机构发订单。联系方式见本列表末尾。

北美

Bernan / Rowman & Littlefield
15250 NBN Way, Blue Ridge Summit, PA 17214, USA
电话：+1 800 462 6420 • 传真：+1 800 338 4550
电子信箱：orders@rowman.com • 网址：www.rowman.com/bernan

世界其他地区

请联系您当地的首选供应商或我们的主要经销商：

Eurospan Group
Gray's Inn House
127 Clerkenwell Road
London EC1R 5DB
United Kingdom

交易订单和查询：
电话：+44 (0) 176 760 4972 • 传真：+44 (0) 176 760 1640
电子信箱：eurospan@turpin-distribution.com

单个订单：
www.eurospanbookstore.com/iaea

欲了解更多信息：
电话：+44 (0) 207 240 0856 • 传真：+44 (0) 207 379 0609
电子信箱：info@eurospangroup.com • 网址：www.eurospangroup.com

定价和未定价出版物的订单均可直接发送至：

Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
电话：+43 1 2600 22529 或 22530 • 传真：+43 1 26007 22529
电子信箱：sales.publications@iaea.org • 网址：https://www.iaea.org/zh/chu-ban-wu

本出版物提供了进行国家核安保威胁评定（包括实体和计算机安全方面），以及制订、利用和维护设计基准威胁和代表性威胁声明的步骤。本出版物意在供国家、主管部门（包括监管机构）、相关技术和科学支持组织，以及包括发货人和承运人在内的、与核材料和其他放射性物质有关的设施和活动的营运者使用。

国际原子能机构
维也纳