国际原子能机构《核安保丛书》第24-G号

实施导则

关于脱离监控的核材料和其他放射性物质核安保措施的风险知情方案

由下列组织共同倡议编写：
国际原子能机构、国际刑事警察组织

IAEA INTERPOL

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。

关于脱离监控的核材料和其他放射性物质核安保措施的风险知情方案

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 24-G 号

关于脱离监控的核材料和其他放射性物质核安保措施的风险知情方案

实施导则

由下列组织共同倡议编写：
国际原子能机构和国际刑事警察组织

国 际 原 子 能 机 构
维也纳 • 2024 年

版 权 说 明

国际原子能机构印制
2024 年 2 月 • 奥地利

关于脱离监控的核材料和其他放射性物质核安保措施的风险知情方案

国际原子能机构，奥地利，2024 年 2 月
STI/PUB/1678
ISBN 978-92-0-542523-8（简装书：碱性纸）
978-92-0-542423-1（pdf 格式）
ISSN 2790-7023

前　言

根据《国际原子能机构规约》，国际原子能机构的主要目标是“加速和扩大原子能对全世界和平、健康及繁荣的贡献”。我们不仅要防止核武器扩散，还要确保核技术可以用于健康和农业等和平目的。所有核材料、其他放射性物质以及相关设施均须得到安全管理，并予以充分保护，防止发生违法犯罪行为或未经授权的蓄意行为。

核安保是每个国家的责任。国际合作对于支持各国建立和保持有效的核安保制度至关重要。众所周知，国际原子能机构在促成此类合作和为各国提供帮助方面发挥着核心作用。国际原子能机构的作用反映了其广泛的成员关系、职责和权力、独特的专长以及为各国提供技术支持、专家和实用指导方面的丰富经验。

自 2006 年起，国际原子能机构发布《核安保丛书》出版物，帮助各国建立有效的国家核安保制度。这些出版物是对《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 号和第 1540 号决议、《放射源安全和安保行为准则》等国际核安保法律文件的补充。

国际原子能机构成员国的专家们积极参与编制《导则》，确保其反映各国在核安保问题良好实践上达成一致。国际原子能机构核安保导则委员会成立于 2012 年 3 月，由成员国代表组成，负责在《核安保丛书》编制过程中对出版物草案进行审批。

国际原子能机构将继续与其成员国合作，确保世界各国人民都能享受和平核技术所带来的种种益处，帮助他们提高健康和福祉水平，促进繁荣。

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. 核安保侧重于预防、侦查和应对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的犯罪行为或未经授权故意行为。应该适当处理由国家确定的对核安保措施具有不利影响的其他行为。核恐怖主义威胁已被所有国家公认为必须关注的问题，因为核材料或其他放射性物质可能用于犯罪行为[1]，这一风险将对国家和国际安保构成严重威胁，并且可能给人员、财产和环境带来严重后果。

1.2. 本《实施导则》介绍了关于脱离监控[2]的核材料和其他放射性物质核安保措施的风险知情方案的概念和方法，包括进行威胁[3]和危害评估，然后，以此作为指引发展和实施核安保系统和措施的依据。在本出版物的编制过程中，运用了核安保、威胁评估和风险管理领域的国家经验、实践和导则出版物。本出版物补充“核安保基本法则”[3]和“核安保意见”出版物并与他们保持一致。

- 《核材料和核设施实物保护的核安保意见》（情况通报 INFCIRC 第 225 号第 5 次修订）[4]；
- 《关于放射性物质和相关设施的核安保意见》[5]；
- 《关于脱离监控的核材料和其他放射性物质的核安保意见》[6]。

1.3. 在本“实施导则”中，“风险”是指根据核安保事件的概率及发生后果（包括对人员、财产和环境造成的后果）确定的核安保事件造成不良后果的潜在可能性。风险通常包含三个组成部分：威胁、薄弱性和后果。风险知情方案是确定优先级和设计合适核安保系统和措施的先决条件[6]。通过威胁和风险评估，国家能

---

[1] 《核材料实物保护公约》及其修正案（第 7 条）[1]和《制止核恐怖主义行为国际公约》（第 2 条）[2]均要求缔约国惩罚对人员、财产和环境造成严重后果的所有违法行为。

[2] “脱离监控”一词用于描述存在未经适当授权而出现核材料或其他放射性物质的情形，其原因要么是因某种原因未能监控，要么是从未控制。

[3] 在本出版物中，“核安保威胁”一词的含义与“核安保基本法则”[3]中的定义相同。“威胁”一词单独出现时通常指的是威胁的源起方（也称为“敌对方”）或威胁物（也称为“装置”）。

够管理风险，并确定向组织与核安保系统和措施分配资源的优先级（例如人力和财力）。

1.4. 风险知情方案是一个迭代过程，在此过程中识别和评估威胁和风险，制订、评估和实施替代方案，并监督和管理相应行动的相关性和有效性。本出版物强调将威胁和风险评估作为风险知情方案的组成部分[4]，并与国际导则保持一致[7]。风险知情方案可以协助国家系统性地考虑威胁和风险，从而更有效、更高效地分配资源。

1.5. 本实施导则是对核材料、其他放射性物质、相关设施或相关活动的设计基准威胁的制订、使用和维护导则的补充[8]。关于威胁的更多信息与核安保措施技术信息，请查阅打击非法贩卖核材料和其他放射性物质相关的辅助导则[9]。

目的

1.6. 本出版物的目的是向各国提供关于制订风险知情方案的导则，促使将威胁和风险评估作为设计和实施可持续核安保系统和措施的依据，从而预防、侦查和应对涉及脱离监控的核材料或其他放射性物质的犯罪行为或未经授权故意行为。本出版物旨在为主管部门和其他有关组织的决策者、执法机构和专家提供指导。

范围

1.7. 本出版物侧重于风险知情方案及威胁和风险评估方法，从而制订关于报告已脱离监控的核材料或其他放射性物质以及已弃用、丢失、遗失或失窃但并未报告或以其他方式被发现的材料的核安保系统和措施。

1.8. 本出版物不包括受监控的核材料、其他放射性物质、相关设施或相关活动的威胁和风险评估。但是，本出版物考虑到了材料丢失、遗失或失窃的可能性。关于盗窃这类材料和蓄意破坏这类设施的威胁评估导则，请查阅国际原子能机构《核安保丛书》出版物（见参考文献[4, 5，8，10]）。本出版物的内容不包含核安保侦查应对系统和措施的设计和实施（见参考文献[11，12]）。

---

[4] “风险知情方案”一词的含义在很大程度上与“风险管理”术语中管理风险的循环过程相同。

结构

1.9. 在本引言之后，第 2 部分介绍了脱离监控的核材料和其他放射性物质的风险管理的依据，特别是进行威胁和风险评估的作用和职责及法律和监管框架，以及支持这些活动的国内和国际协调机制。第 3 部分介绍了关于识别核安保威胁的导则。本部分介绍了威胁的来源（“威胁来源”）以及威胁可能发生的方式。第 4 部分介绍了识别目标（“威胁对象”）及评估潜在后果的方法和程序。第 5 部分介绍了进行威胁和风险评估及评估威胁的可能性的方法。第 6 部分概述了在风险知情方案整合威胁和风险评估后如何支持识别替代措施以及实施、管理核安保系统和措施的过程。

1.10. 在正文之后，附录一至附录四以假设性和说明性的威胁和风险评估为例介绍了如何运用风险知情方案。这些附录相互关联，共同构成了风险知情方案的完整示例。附录一介绍了完整风险知情方案的流程图，包括威胁和风险评估活动。附录二介绍了使用以下两种方法进行威胁评估的示例：威胁叙述法和威胁评级法。附录三介绍了利用概率风险评估法进行风险评估的方法示例。附录四介绍了利用威胁和风险评估结果评估并确定设计和实施核安保系统和措施相关活动优先级的风险知情方案示例。在附录一至附录四中，我们都假设了一个“示例国家”概念。

2. 威胁评估和风险知情方案的依据

2.1. 大量放射源和大量核材料和其他放射性物质在世界各地广泛运用于科研、卫生、农业、教育和工业等领域。如果这类物质处于或脱离监控状态，就有可能用于犯罪行为或未经授权故意行为。脱离监控的核材料和其他放射性物质有关的犯罪行为或未经授权行为的潜在后果取决于这类物质的数量、形式、成分和放射性。如果用这类物质制成爆炸性“装置”[5]，可能会增加核材料或其他放射性物质有关的犯罪行为或未经授权行为的潜在影响，特别是在对战略场所使用时。这类行为可能会导致严重的健康、社会、心理和经济影响，带来财产损失以及政治和环境后果。可能的行为包括：

[5] 为了简化，本出版物中的“装置”一词是指放射性散布装置（RDD）、辐射辐照装置（RED）和简易核装置（IND）。该词的含义与《制止核恐怖主义行为国际公约》[2]中的定义一致。

(a) 有意在公共场所扩散放射性物质，例如使用放射性散布装置（RDD）；

(b) 以辐照周围人群为目的在公共场所放置放射性物质，例如使用辐射辐照装置（RED）；

(c) 使用简易核装置（IND）制造核爆炸。

2.2. 根据有关“核安保意见”的出版物[6]的意见，在设计脱离监控的核材料和其他放射性物质的核安保系统和措施时应该遵循以下四大步骤应对威胁：

- 威胁的识别；
- 目标和后果的识别与评估；
- 威胁和风险的评估；
- 采用风险知情方案，确定核安保系统和措施的优先顺序。

2.3. 在识别威胁时，应该包括考虑为达到目的而可能使用核材料或其他放射性物质实施犯罪行为或未经授权故意行为的潜在敌对方，以及可能获取核材料或其他放射性物质并实施这类行为的国内外人员或组织。

2.4. 在识别和评估涉及脱离监控的核材料或其他放射性物质的犯罪行为或未经授权故意行为的潜在目标时，应该包括考虑目标对敌对方的吸引力。这类吸引力可能与目标的易受攻击性或攻击该目标的潜在后果有关。

2.5. 在评估威胁时，应该考虑根据目前可获得数据和信息的分析而确定的可能实施犯罪行为或未经授权故意行为的个人或组织的动机、意图和能力。威胁评估的考虑因素还应当包括评估这类人员获取核材料或其他放射性物质的可能性以及通过已知脱离监控材料事件获得的经验。为了确保完整性，评估还可能包括反恐、执法机构提供的信息以及核材料、其他放射性物质、相关设施和相关活动的安全和安保工作相关的所有机构的情报。威胁评估还应该考虑将这类材料用于犯罪行为或未经授权故意行为的技术可行性和历史背景。

2.6. 风险评估包括考虑这类行为的可能性、成功的可能性以及后果的严重程度，风险评估能够用于支持确定拟实施的核安保系统和措施的优先级。将风险信息纳入核安保系统和措施的优先级以及全面管理核安保系统的过程即为风险知情方案。国际行业标准确定了开展风险评估的最佳方法[7]。本实施导则将这类实践进行了改造，并将其用于制订核安保系统和措施并确定他们的优先顺序。

国家的核安保政策和战略

2.7. 脱离监控的核材料和其他放射性物质的有效核安保系统和措施应该源自全面、综合的国家核安保政策和战略。国家核安保政策和战略应该以国家威胁和风险评估为指引，并确定负责开展国家核安保威胁和风险评估的主管部门，促进有关主管部门和组织之间的合作与协调。国家核安保政策和战略应该确定预防措施的范围和优先级，同时根据分级法制订核安保的侦查和应对措施。国家核安保政策和战略还应该要求根据新信息和条件变化定期更新威胁和风险评估，并应当根据威胁和风险评估的结果变化进行审查和更新。核安保系统和措施的设计还应该以威胁评估和风险知情方案的应用为依据[6]。

法律和监管框架

2.8. 为了制订和实施国家核安保政策和战略，应该建立适当的法律和监管框架[6，13]。这对于赋予主管部门职责以及建立威胁和风险评估合作协调机制尤为重要。法律和监管框架应该包括：

(a) 关于威胁风险评估的要求和风险知情方案的落实；
(b) 将脱离监控的核材料和其他放射性物质的威胁和风险评估任务和责任赋予主管部门；
(c) 将制订风险知情方案的具体责任以及实施该过程所需的所有必要法律和行政权力赋予有关主管部门；
(d) 要求所有相关主管部门与为实施脱离监控的核材料和其他放射性物质的核安保系统和措施而负责开展威胁和风险评估的主管部门充分合作；
(e) 要求负责制订威胁和风险评估的主管部门定期更新并根据需要更新这类评估；
(f) 要求负责实施核安保系统和措施的主管部门根据风险知情方案的结果设计这类系统和措施。

任务与职责

2.9. 负责开展脱离监控的核材料和其他放射性物质的威胁和风险评估的主管部门应该有开展威胁和风险评估的必要资源和能力，并与在各自负责领域做出风险知情决策的相关主管部门合作。

2.10. 指定主管部门应该确保收集和分析所有相关数据，并由有资格和有能力的工作人员开展威胁和风险评估。有关主管部门在设计核安保系统和措施以及确定优先级时，应该考虑评估的结果。所有主管部门应该在整个威胁和风险评估过程中相互合作，确保从各自的角度考虑评估结果，并提供有用信息以支持各自的风险知情方案。

2.11. 由于需要及时更新威胁和风险评估，所有相关主管部门均应该提供反馈意见，确保负责开展威胁和风险评估的主管部门能够及时评估具有核安保影响的所有事件。由于威胁和风险评估将用于确定核安保系统和措施的优先级，威胁和风险评估的周期可能需要与预算或计划周期保持一致，以确保决策者能够获取最新的信息和结果。

协调机制

2.12. 威胁和风险评估依赖多个主管部门提供的敏感信息。必须根据国家信息安保政策和规定以及国际义务，在国内和国际层面协调交流可靠而及时的核安保信息。信息交流的安排应该基于现有的核安保影响事件的报告规程和程序，例如核材料和其他放射性物质丢失、遗失或失窃等事件。负责威胁和风险评估的主管部门应该按照“按需知密”的原则，及时向所有其他相关主管部门通报最新的威胁和风险评估信息。如果由多个主管部门共同负责威胁和风险评估，密切合作和协调尤为重要。

国际合作

2.13. 有效参与国际活动将有助于获取信息和经验以改进威胁和风险评估的方法和程序。了解国家境外的核安保事件也会有助于了解国内的威胁。国际原子能机构“非法贩卖数据库”（ITDB）是一个提供最新案例报告信息的国际论坛，可以了解脱离监控的核材料或其他放射性物质的案例报告信息[14]。通过分析非法贩卖数据库中的数据，国家可以发现可能会对国家造成影响的威胁或跨境运输的信息以及有助于开展威胁和风险评估的信息。成员国可以将这些信息用作威胁和风险评估的考虑因素。

2.14. 此外，参与国际组织以及其他双边和多边发起人举办的意识和培训研讨会，可以让工作人员熟悉最新的方法和程序，并帮助他们获得专门知识和能力。有关

国际组织可以就威胁评估相关的事项提供协助，或者直接通过双边或多边方式要求提供协助。

3. 核安保威胁的识别

3.1. 威胁可以通过“威胁来源”和“威胁对象”识别。识别“威胁来源”是基于考虑敌对方是谁，敌对方可能拥有或寻求拥有的核材料或其他放射性物质的类型，以及敌对方将如何利用这些材料造成伤害。对于脱离监控的核材料和其他放射性物质而言，如果敌对方可能拥有这些材料，“如何造成伤害”通常取决于敌对方可能使用的装置的类型。在识别“威胁对象”时应当考虑脱离监控的核材料或其他放射性物质可能用于哪些战略场所。图 1 总结了威胁评估过程需要考虑的具体组成要素。各国也可以考虑适用于其国家情形的其他要素。

3.2. “谁/为什么”要素是用于识别和描述哪些敌对方可能试图实施犯罪行为或未经授权故意行为。应该通过分析潜在的敌对方识别其动机[6]、意图和能力。这应该包括考虑敌对方试图在一个国家实施犯罪行为或未经授权故意行为对另一个国家的影响。在评估敌对方时，应该根据敌对方实施特定行为的可能性，获取材料和建造装置所需融资和技术的能力，以及对实施行为所需信息的了解程度。第 3.18 — 3.23 段更详细地介绍了分析敌对方的方法和流程。

[6] 在识别潜在的敌对方以及他们可能实施的犯罪行为或未经授权的故意行为时，动机可能是重要的考虑因素（例如敌对方的动机可能影响他们的目标选择）。但是，尽管核安保措施可以设法影响敌对方的意图和能力，但无法影响敌对方的动机。因此，考虑动机因素在威胁识别过程中发挥着重要作用，动机因素可能与威胁评估的其他方面或设计和实施的核安保制度和措施的关系不大。

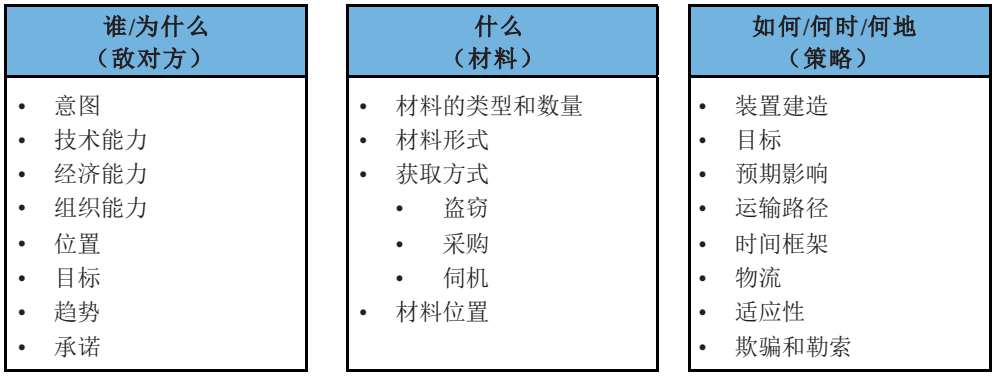


图 1. 威胁的组成要素。

3.3. “什么”要素识别敌对方可能使用的材料。如果国家储存或使用核材料和其他放射性物质的场所较少，则可以对相关设施和相关活动进行单独评估。如果国家的相关设施和相关活动较多，则可以对同类型的组别进行评估或单独评估，具体取决于评估的详细程度。除了相关设施和相关活动之外，还应该考虑到相关材料也可能从境外获取，或者通过非法贩运获取。在不同的可能性中，敌对方所获取材料的类型、存储或使用材料的场所的类型以及选择获取材料的方式或偷运入境或离境的方式会有所不同。在评估选择特定设施或材料的可能性时，应该根据敌对方的一般偏好、材料的可接近性或敌对方喜好的装置类型。获取材料的可能性取决于敌对方的能力和材料相关的薄弱性。通常来说，现有薄弱性评估信息可能会被敌对方用于评估获取材料的可能性。第 3.6—3.9 段介绍了如何评估从国家的相关设施和相关活动中获取材料的可能性。第 3.10—3.17 段介绍了脱离国家监控的材料和跨越国家边界的材料可能存在的薄弱点。

3.4. “如何/何时/何地”要素介绍了特定策略的特点。例如，假设敌对方已经获得了材料，敌对方在利用材料建造装置时可能需要采取两大关键步骤。第一步是使材料适合装置，或者处理材料，改变材料形式，使材料可用于装置。第二步是设计和建造装置。建造装置的设计和技能水平不同可能会导致装置的效果有所不同。复杂的设计可能需要更多的时间、人力和其他复杂的制造基础设施（例如专业工具或安全工作场所），而如果设计的复杂程度较低，建造可能更快和更可靠，无需专业设备。分析结果是根据敌对方所获取的材料和敌对方的能力，评估不同效能装置存在的可能性。其他情形（如贩卖）不一定涉及装置，可以视为敌对方与该装置相关的更大计划的一部分，也可以视为单独行为。已建成的装置通常需要运送到计划部署目标所在地。因此，最终目标（反过来会影响后果的严重程度）

和运输路线均需要考虑。评估敌对方在部署装置之前拦截的可能性时，必须考虑通过使用仪器警报、信息警报或其他常规执法活动及国家核安保侦查体系的警戒活动[11]进行检测的可能性。更多关于评估“如何/何时/何地”的详细导则，请参阅第 4.3—4.6 段。在评估装置的部署时，需要考虑装置的有效性和潜在后果。在评估影响时，应该考虑预期影响和可能的实际影响。关于评估具有核安保影响行动的后果的更详细导则，请参阅第 4.7—4.18 段。

3.5. 威胁评估是识别或评估敌对方或可能造成人员、财产、社会或环境伤害或破坏的行为，辨别和量化（如果可能）威胁。威胁评估通常是根据对敌对方的意图和能力评估，其中意图通常是根据频次（例如，每年尝试多少次）进行评估，能力是根据成功的可能性进行评估。常见方式包括以下三种（可组合使用）：

(a) 威胁的层级可以进行定性评估，简单地分为低级、中级或高级（或者如第 4 部分表 1 所述的级别），或者使用描述词或限定词描述更精确的威胁等级（有时也被称为“词语阶梯”）。这种最基本的定性威胁评估形式，必须以专家判断的启发为依据。

(b) 威胁层级也可以通过专家分析和经验数据进行定量评估。如果采用定量评估，很难评估概率值，因此，评估每种预估情形下的不确定性也非常重要。

(c) 在安保应用中，往往不会评估威胁相关的可能性。相反，通常是根据具有明确能力的特定真实或假设敌对方对安保措施进行评估。这种方法被称为设计基准威胁（DBT），因为识别的能力可用于有效确定设计安保系统和措施的性能规范。关于制订核设施设计基准威胁的程序，见《设计基准威胁的制订、利用和维护》[8]。其他的核安保应用（例如重大公共事件的核安保措施）也可以采用类似程序。

受监控的核材料和其他放射性物质的薄弱性

3.6. 为了实施涉及核材料或其他放射性物质的犯罪行为或未经授权故意行为，敌对方必须获取这类材料。[7] 敌对方可能试图从现有的设施和活动中获取材料，或者从持有已经脱离监控材料的其他人员或从境外获取材料。作为威胁评估的一部

[7] 正如上文第 1.9 段所述，本实施导则的适用对象范围是脱离监控的核材料和其他放射性物质，因此，针对核材料、其他放射性物质或其相关设施及相关活动（即破坏活动）的犯罪行为或未经授权故意行为不属于本出版物的适用范围。

分，评估被监控材料脱离监控的可能性非常重要。非法贩卖数据库中的信息表明，全球受监控材料可能因盗窃、意外丢失和未经授权处置而丢失或失踪[14]。

3.7. 评估被监控材料脱离监控的可能性的方法之一是，将已识别敌对方的能力与存储这类材料的相关设施和相关活动的薄弱性进行比较。

3.8. 相关设施的经营方或相关活动的组织者可能已经根据设计基准威胁或替代威胁评估对薄弱性进行了评估，因此他们可能了解核安保系统的工作情况，并制订了针对该特定威胁的措施。设计基准威胁应该定义为，设计良好的核安保系统不能防止具有等于或小于设计基准威胁能力的敌对方成功转移材料的可能性非常低。但是，应该对所有相关设施和活动的薄弱性进行评估，有些相关设施和活动并非由他们本身开展薄弱性评估。此外，如果识别出敌对方具有的能力超过设计基准威胁，或者定性为与设计基准威胁不同，则应当针对该设计基准威胁开展类似的额外评估，以评估该敌对方成功的可能性。应该考虑到通过设施或活动（包括在运输过程中）获取材料的多种替代方法，例如武装攻击、内部人员协助、伪造材料账目和盗窃。

3.9. 敌对方可能会设法通过更薄弱的设施或活动寻找材料。因此，敌对方获取材料的可能性可能大致等同于通过这些最薄弱环节获取材料的可能性。同样，敌对方选择从特定设施或运输路线获取材料的可能性与设施或运输路线的薄弱环节有关。敌对方更有可能选中那些薄弱点。在此情况下，任何薄弱性的变化也会导致威胁的变化。这就表明需要对替代方法进行分析。当一个地方的核安保系统和措施发生变化时，那里的核材料的薄弱性可能会发生变化，因此威胁也可能发生变化，包括威胁级别和最有可能发生的特定情形。

脱离监控的核材料和其他放射性物质的可获得性

3.10. 敌对方也可能试图获取已经脱离监控的核材料和其他放射性物质。几乎所有国家都有不同安保级别的放射性物质。有些核材料可能没有进行适当核算，有些放射源可能没有进行适当登记[5]。有些被遗弃、丢失、遗失或失窃的核材料和其他放射性物质可能没有报告为脱离监控。

3.11. 从 1993 年到 2012 年底，非法贩卖数据库已经收到了 2000 多份关于脱离监控的核材料和其他放射性物质的案例报告[14]。在开展威胁评估时，应该考虑关于脱离监控材料的报告。有些未经授权的人员出售核材料和其他放射性物质，有些

人员明显以犯罪为目的试图购买核材料和其他放射性物质。虽然许多声称出售这类材料的行为被证明是欺诈行为，而有些情况可能是敌对方实际采购脱离监控核材料和其他放射性物质，但未被发现。

3.12. 有些脱离监控的放射源可能只有敌对方才会发现，或者只会向敌对方出售。在评估敌对方获取脱离监控的材料的可能时，应该考虑到这些可能性。[8] 在极少数情况下，敌对方也可能购买或以其他方式获取内装脱离监控材料的完整装置，在开展威胁评估时也应该考虑到这种可能性。

3.13. 因此，在开展威胁评估时，应该考虑到敌对方从境内外获取已脱离监控的核材料或其他放射性物质的可能性，并且描述可能获取的材料的类型。评估这种可能性对于主管部门识别材料制造、使用、储存或运输的所有地点至关重要，主管部门还需要了解核材料和其他放射性物质在国内的常规用途、材料控制的历史、核材料账目和放射源登记情况以及其他放射性物质的其他机制。敌对方也有可能会获取丢失、遗失或失窃的核材料或其他放射性物质。从定义可以看出，这类案例的记录可能不完整或不准确，这种可能性将更难以确定，因此也可能需要评估适当的不确定性界限。

跨境转移

3.14. 非法贩卖数据库显示，脱离监控的核材料和其他放射性物质会发生过跨境转移。因此，敌对方获取脱离监控的核材料或其他放射性物质的可能性将取决于可提供这种材料的任何地点，而不仅限于国内。

3.15. 由于一个国家可能无法详细了解从其他国家获取材料的可能性，因此，很难评估已脱离监控材料造成的威胁。非法贩卖数据库中的数据可用于对可获取的材料数量进行保守评估。但是，未向非法贩卖数据库报告的已脱离监控的材料数量尚不清楚。在评估威胁时，主管部门需要决定这一因素的权重。

3.16. 作为国家层面威胁评估的一部分，除了脱离监控材料的类型和数量之外，主管部门还应该考虑这类材料转移入境和出境的过境路线。因此，主管部门应该考虑以下情形下的核材料或其他放射性物质：

---

[8] 在有些情况下，已脱离监控的核材料或其他放射性物质可能会在承运人或托运人不知情的情况下运输。

(a) 通过商业运输或私人车辆从指定的进出境口岸（陆运、空运或水运）入境或出境；

(b) 从指定的进出境口岸入境或出境；

(c) 过境（即入境后不在该国最终交付）。在许多情况下，既没有识别出这类材料，这类材料也不一定遵守国家内部控制程序。

3.17. 主管部门应该考虑敌对方利用全球供应链非法运输脱离监控的核材料和其他放射性物质的可能性。实施有效的边境监测系统和措施，并作为核安保侦查体系的一部分，可能有助于阻止、侦查或防止这类材料的跨境转移，并可以大幅降低风险[11]。国家的程序和能力的有效性以及敌对方对这些程序和能力的了解程度将会影响国外获取材料的评估威胁的等级。

敌对方的能力和意图分析

3.18. 第 3.10—3.17 段主要介绍了如何评估脱离监控的核材料和其他放射性物质用于犯罪行为或未经授权故意行为的可能性。这类材料用于上述行为的可能性在很大程度上取决于潜在的敌对方。本小节重点介绍了如何评估敌对方，包括评估敌对方的能力（例如技术或财务能力）和意图（特别是敌对方是否会使用核材料或其他放射性物质，如果会使用，则敌对方可能如何使用以及敌对方如何看待放射性和其他风险对自身的影响）。敌对方评估是一个动态过程。可能难以获取关于敌对方的能力和意图的可靠和最新信息，而可获取的信息可能相互矛盾或存在不确定性。之所以很难获取这类信息，部分是因为敌对方会采取措施隐瞒活动。此外，由于敌对方会根据情况变化而做出改变，以及国家防御措施的变化（例如提高某一特定场所的安保），这些通常都会导致特定敌对方实施特定行为的可能性发生变化。这些变化不一定会降低或提高总体可能性；这些变化只使敌对方将注意力转移到其他目标或其他行为上。不同类型行为的可能性评估也应该是动态变化的，随着国家核安保体系的完善，相对可能性会相应发生变化。

3.19. 评估敌对方的第一步是识别潜在的敌对方（如图 1“敌对方”栏所示）。负责评估威胁和风险的主管部门应该与执法部门和国家情报部门密切合作，深入了解国家掌握的特定敌对方的信息。国家也可以通过双边或多边协议或国际执法机构获取相关信息。犯罪行为或未经授权故意行为以及许多潜在敌对方的动机可能多种多样。如果能够识别敌对方是个人或特定团体，则可以更准确、更具体地掌

握敌对方的意图和能力特征。除此之外，查明个人或团体的具体类型有利于进行更有效的分析，并且可用于对目前尚不明确的敌对方进行分析。

3.20. 识别出的敌对方应该根据其意图确定其特征。敌对方的总体动机往往对其具体意图具有重大影响。动机可能包括财务、政治、意识形态或个人等方面。其特征的关键要素包括：

(a) 敌对方是否有意将脱离监控的核材料或其他放射性物质用于犯罪行为或未经授权故意行为？

(b) 敌对方是否打算在国内实施这类行为？

(c) 敌对方是否打算将一个国家作为在另一个国家或针对另一个国家实施这类行为的中转地？

3.21. 对敌对方试图实施不同类型犯罪行为或未经授权故意行为的可能性可以进行定量分析（最好是分析概率分布）。如果必要，也可以进行定性评估（例如可能性的低、中或高）。在任何情况下，在总体威胁评估过程中，应该考虑并利用评估的不确定性。

3.22. 除了评估敌对方将脱离监控的核材料或其他放射性物质用于犯罪行为或未经授权故意行为的可能意图之外，还应该评估敌对方成功实施这类行为的能力。敌对方的能力通常分为两类：组织能力和物流能力。敌对方需要获取已脱离监控的材料，或者使用、储存或运输场所受到监控的材料。这两种选择可能都需要某些重要的资源。例如，如果有足够的财政资源，获取脱离监控的材料会相对容易，而获取受到监控的材料则需要更多的技术或人力资源。在获取材料后，建造装置也需要基础设施和专业知识。这类能力往往与材料安保一样受到严格控制和监管，敌对方可能很难获得。主管部门应该评估在国家境内获取这类能力的可能性，或者在国外获取并转移到国内的可能性。

3.23. 由于缺乏用于评估可能性的历史数据，主管部门对敌对方的意图和能力的评估过程通常会比较复杂。主管部门可以根据敌对方的声明、用于支持犯罪行为或未经授权故意行为活动的证据以及对敌对方的目标和偏好的了解评估其意图和能力。关于敌对方的信息可视为敏感信息，应该根据国家信息安保政策予以保护。虽然在根据这些数据评估可能性时存在较高的不确定性，但可以提供来自不同敌对方或敌对方不同类型威胁的相对指标。

4. 目标的识别与评估及其潜在后果

4.1. 第 3 部分主要介绍了威胁的识别，包括敌对方和实施犯罪行为或未经授权故意行为（装置中使用的脱离监控的核材料或其他放射性物质）。本部分介绍了识别和评估涉及脱离监控的核材料或其他放射性物质的核安保事件的目标和潜在后果的方法和方案导则。为了完成整体风险评估，有必要了解不同目标的吸引力以及根据不同目标部署不同装置的可能后果，因为敌对方试图对目标采取行动的可能性取决于特定方案对特定敌对方的价值。

4.2. 在《关于脱离监控的核材料和其他放射性物质的核安保意见》[6]中，“目标”的定义是核材料、其他放射性物质、相关设施、相关活动或其他可能被核安保威胁利用的场所或物体，包括重大公共事件、战略场所、敏感信息和敏感信息资产。本“实施导则”的重点研究对象是脱离监控的核材料和其他放射性物质，因此本出版物中“目标”一词的范围不包括受到监控的材料或相关设施和相关活动。

目标识别

4.3. 识别的目标可能非常具体的目标（例如特定建筑物、纪念物或事件）或者是某一类别目标（例如办公大楼、纪念物、体育赛事或具体城市的场所）。如果总体威胁评估缺乏具体情报，识别具体目标得到的目标清单（随后必须确定目标的优先顺序）将比于识别目标类别得到的清单更长。在有些情况下，如果某些类别目标中的某些特定地点比同类别中的其他地方更明显或可能性更高，则应当对特定目标和目标类别进行综合分析。考虑到获取核材料或其他放射性物质的难度以及含有这类物质的装置相对稀少，目标清单应当限制为高值最高的目标（例如成功的可能性大或影响大），而不是所有潜在目标。

4.4. 在识别目标时，可能对人员、财产和环境造成的后果可以分为以下类别：

(a) 建筑物、纪念物或重要的象征性场所：这些场所可能包括政府建筑物、重要私人机构、纪念物、宫殿、博物馆、宗教场所或具有重大文化遗产价值或具有政治意义的场所。有些场所也可能因与其他国家存在联系而具有价值（例如大使馆或领事馆）。

(b) 关键基础设施：这些场所可能包括电力、水、自然资源、运输或通讯等设施的关键节点。水坝、发电厂、炼油厂、水处理厂、桥梁或其他为大量人群提供

必要服务的其他设施和信息系统或构筑物，也可能是具有吸引力的潜在目标。

(c) 人口中心：人口密集地区可能对以造成伤害、死亡或重大破坏为目标的敌对方具有吸引力。特定人群（例如少数民族团队或宗教团体）的集中区域也可能成为目标。

(d) 特殊事件可能会同时具备特定象征性和范围小人数多的特点，并且可能对敌对方具有吸引力。这类目标可能包括重大体育比赛、政治集会、国家庆典或宗教节日等活动。

(e) 环境资源或生态系统。

4.5. 识别出的目标可以根据被选中的可能性、对敌对方的吸引力或攻击的潜在后果确定优先级。主管部门应该认识到，不同的敌对方可能更偏好不同类型的目标，这取决于他们的目标和能力。此外，有些目标可能比其他类型的核安保事件更具吸引力。不同目标的相对吸引力将取决于敌对方的目标，并且通常与敌对方期望的影响力有关，包括：

(a) 受影响的人口 — 谁、多少；

(b) 破坏和损害的经济影响；

(c) 目标的经济或物流重要性；

(d) 目标的象征价值。

4.6. 吸引力还可能取决于目标的薄弱性（即易受攻击、易于逃脱以及成功的可能性）。因此，对目标吸引力的评估与评估目标的薄弱性以及核安保事件的潜在后果密切相关。目标的相对吸引力可能会随着目标防御措施或敌对方目标的变化而变化。

核安保事件的后果

4.7. 核安保事件的后果将取决于事件的性质、地点和其他情况。后果可能会从最初的直接影响升级到后续的二级和三级影响。[9] 对于涉及核材料和其他放射性物

[9] 二级和三级影响是指核安保事件造成的除了攻击的直接影响之外的其他后果。例如，在港口引爆放射性扩散装置可能会产生直接影响（例如人员伤亡和财产损失），但也可能导致在调查和采取补救措施期间关闭港口，从而造成贸易量减少以及可能关闭依赖于该港口的企业。这类额外后果分别为二级和三级影响。

质的犯罪行为或未经授权故意行为，应该评估人员（通常是健康或社会影响）、财产（通常是经济影响）和环境的潜在后果。在开展威胁评估的过程中，必须了解潜在后果，并且在进行风险评估时应该开展一定速度的详细评估。第4.7—4.18段重点介绍了这类后果的评估。

4.8. 在核安保事件中，应该将人类健康的潜在后果作为风险评估的一部分。这些可能包括装置造成的（例如爆炸造成的）人员伤亡（死亡和伤害），以及接触核材料或其他放射性物质产生的放射线或吸入放射性核素，这可能会导致死亡、严重伤害、或者组织或器官功能的重大伤害。如果是简易核装置，其影响包括核爆炸产生的辐射诱发效应、核爆炸和热辐射的非放射效应以及与辐射有关的长期放射效应。

4.9. 核安保事件的经济成本可能会来源于许多方面，特别是在解决对人员、财产和环境的影响方面。这些费用可能包括治疗病人（或担心生病人员）的成本、清理受影响区（或者清理处理土壤、建筑物和不易清除的物质）的成本、以及疏散、搬迁、业务中断和业务恢复的成本。除了事件的直接成本之外，也可能对国家的经济产生间接影响。

4.10. 核安保事件也可能造成环境后果。放射性物质可能被故意用于污染诸如土壤、地下水或生态脆弱的区域，这些区域可能不容易净化，或者装置的分散放射性核素可能进入这类环境。一个地区受到污染后，可能会导致居民永久性遗弃该地区，或者避免使用该地区的农产品和其他工业产品。放射性核素的半衰期较长，这意味着，污染影响的持续时间可能也会比较长。

4.11. 最后，犯罪行为或未经授权故意行为可能会对国家、地区或全世界产生社会后果。受影响的个人或社区可能会出现愤怒或焦虑情绪。在地方层面，人们可能会撤离该地区，以后也避免进入该地区。在国家层面，政治进程（如选举）可能会中断或受影响。社会后果也可能会超出事件发生的国家，例如供应链中断、人员大规模流动或外交格局的复杂化。这些后果非常难以预测或量化，在很多情况下，后果的严重程度取决于主管机构对行为本身的应对情况。因此，在评估这类后果时需要非常小心。[10]

[10] 还值得注意的是，这里介绍的四种类型的后果，即健康、经济、环境和社会后果，并非相互独立存在。一种类型的后果可能会直接影响其他类型的后果。例如，由于爆炸造成的放射性污染（环境后果），造成爆炸现场附近的居民担忧（社会后果），并且可能导致居民放弃该地区以及商业活动大幅减少（经济影响）。

4.12. 后果可以通过多种方式进行评估，包括定性评级或详细的后果建模。

4.13. 后果的定性评级包括主题专家根据定性说明对各类别中的潜在后果的评级，例如“严重”、“中度”和“微小”。表 1 介绍了一种后果矩阵的示例，包括四种不同类型的影响以及五种类型的评级。

4.14. 定性评定法通常用大类别描述核安保事件对人员、财产和环境造成的后果。这些类别所代表的后果级别可能因级别顺序的变化而有所不同（例如表 1 中的“健康影响”行）。其目的应该是创建足够广泛的类别范围，以帮助主题专家选择正确的类别描述事件的后果，同时保持不同类别之间的意义区别。因此，适当的类别范畴允许后果评估存在一定的不确定性，同时确保相应的情形能够可靠归入相应类别。类别的定义可能包括对某些类型的后果的定量测量（例如健康、经济和环境影响），而其他类别（如社会后果）可能只能从定性的角度确定。该方案可以在共同框架内对不同的影响因素进行评估。但是，在确定类别时应该特别注意确保使用同样定性术语描述的影响在每一种类型的影响中具有可比性。这就是所谓的跨越类型的尺度校准。确保评级尺度的类别能够反映所有级别的影响也很重要：一个常见的错误是，将最高级别设置得太低，以至于无法区分极端影响与重大影响。

4.15. 详细的后果建模可用于模拟敌对方选择的行为（例如装置部署）对目标场所的影响。要素评估（例如爆炸影响、放射性物质的扩散、个人和集体的剂量分配以及污染的级别和程度等）通过事件的数学模型进行评估，而不是根据主观评估确定。这类模型可能非常简单（例如基于风向的受影响象限上的爆炸半径和均匀扩散），也可能非常详细（例如气流的计算流体动力学模型），并且应该以经验数据（如果可能）为依据。实际上，即使使用了详细的模型，由于各种不可预知的因素（例如风速和风向），后果级别的评估通常也会存在很大的不确定性，所以评估值通常会有相对较大的误差区间。

表 1. 定性后果矩阵示例

影响要素	1	2	3	4	5
健康影响	可能不会造成人员伤亡	可能造成十人以下的人员伤亡	可能造成十人以上的人员伤亡	可能造成 100 人以上的人员伤亡	可能造成 1000 人以上的人员伤亡
经济影响	相当于重建建筑物的成本	城市地区的成本很高	城市的成本很高	成本为 GDP 的 1%至 10%之间 [a]	成本超过 GDP 的 10% [a]
环境影响	无显著污染	小范围或临时污染	小范围重大污染	大范围出现可测量的污染，或小范围出现关键资源无法可用	污染导致大范围关键资源不可用
社会影响	人口行为没有出现重大变化，地方或国家的社会功能没有受到影响	限定地理区域的非必要社会功能出现短暂或微小损失	限定地理区域的非必要社会功能出现重大损失	在持续时期内出现功能失调行为和破坏重要社会功能	对政府和机构失去信心 普遍忽视官方指示 大规模抢劫和内乱

注： 数字和说明仅供参考，需要根据国情和优先事项加以调整。

[a] GDP：国内生产总值。

4.16. 后果评估的共同终点包括核安保事件的伤亡人数和经济成本。在有些情况下，核安保事件的伤亡人数和经济成本可以通过每个伤亡人员的名义货币价值（例如统计寿命价值[11]）加上经济成本进行计算。

4.17. 评估社会后果是一项艰难挑战。虽然将社会影响纳入后果评估显然非常重要（而且实际上，社会影响可能是敌对方意图造成的主要后果，对国家来说也最重要），但社会后果极难评估，哪怕定性。此外，国家应对核安保事件的措施可能会严重影响社会后果，因此并不完全由事件本身决定。社会后果评估目前还没有人们普遍接受的方法。因此，各国需要确定自身的方案，以便将社会影响纳入后果评估。

4.18. 由于后果取决于一系列要素，包括所使用的放射性物质、装置的特点、目标的特点、应对措施的有效性以及靠近目标的人员、财产和环境，后果评估所涉及的范围非常广泛。因此，后果评估的级别应足以区分不同情形。对于简单的分析，后果评估可以分为多种级别（例如表 1 中的 1 至 5 级或定性类别描述），并在数值计算过程中使用数字表示经济影响的中心评估。或者，将所有单位从后果评估中删除，使用“标准化影响评级”表示相对后果。标准化影响评级可用于显示相对影响级别，而不涉及具体的货币金额。

5. 威胁和风险评估方法

5.1. 第 3 部分和第 4 部分介绍了威胁和风险评估的要素。本节将介绍如何将这些要素组合成有效评估的常用方法。图 2 显示了威胁和风险的要素以及彼此之间的相互关系。在使用这种方法时，威胁通常包括意图和能力，并且可以通过特定类型的核安保事件的潜在后果和成功的可能性（从敌对方的角度来看）进行了解。风险包括一系列的威胁、薄弱性和后果，可以进行定量计算（例如，作为预期损失 — 每年的后果），或者通过相对级别进行定性分析（例如，低、中、高）。由于风险评估取决于威胁、薄弱性和后果的评估，威胁评估通常在风险评估之前完成，并用作风险评估信息。

[11] 统计寿命价值的概念旨在表示人们愿意为减少风险而付出的量，因此，平均而言，预计死于风险的人数将减少一人。

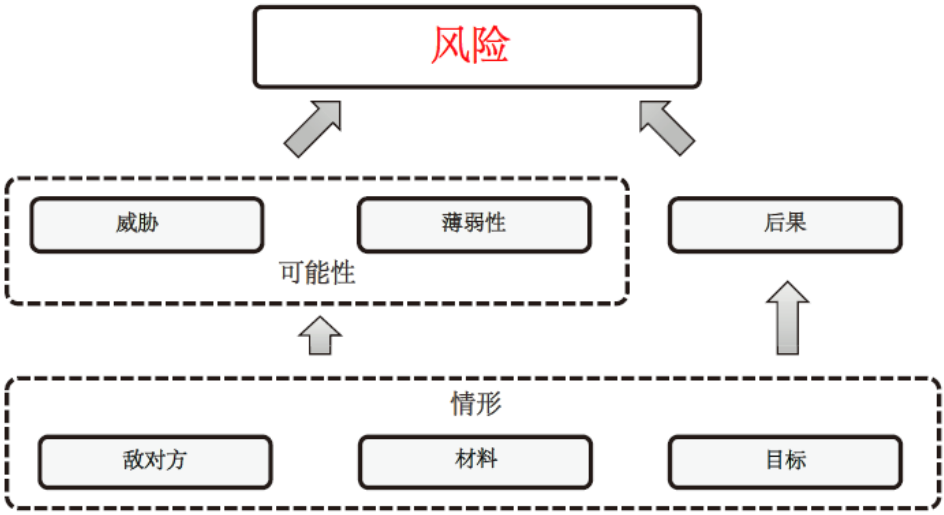


图 2. 威胁、风险及辅助要素之间的关系。

5.2. 威胁和风险评估分为许多类型，各种情形也适用于许多不同的方法。所选择的特定方法应该适用于正在评估的具体情形以及可用的资源和技术能力。评估应该采用定性还是定量方法是需要做出的重要决定。一般来说，如果定性（例如低、中、高）评估足以为确定优先级的决策提供信息，应该使用定性方法。但是，如果需要更精确地确定威胁或风险的特征，或者对不同的威胁或风险进行更明确区分，则应该选择更偏向定量的方法。

5.3. 威胁和风险评估的重点也有所不同，最常见的两种是战略和战术评估。战略评估考虑的时间跨度更大，重点是管理资源和制订提高能力的计划。战术评估通常在明显的时间限制下开展，并用于通报在特定情况下的业务决策。由于本出版物的重点是威胁和风险评估，用于支持核安保措施的设计和实施，因此这里介绍的评估为战略性评估。

5.4. 由于多种原因，核安保的威胁评估与其他威胁评估有所不同。例如，相对于较常规的武器（例如枪支和爆炸物），核材料和其他放射性物质的技术和科学特性是威胁性质和程度的重要因素。此外，核材料和其他放射性物质的可获得性和潜在使用是威胁评估的决定性方面，这就意味着，相对于依靠获取枪支和爆炸物的犯罪行为或未经授权故意行为，核材料和其他放射性物质的威胁评估的范围更小、更具体。此外，核安保事件的数量有限，这就意味着准确评估威胁和风险的经验基础有限。

威胁评估方法

5.5. 威胁评估可以使用多种技术。两种常用方法是：

(a) 威胁描述法：用于描述威胁的级别和特征的定性方法；

(b) 威胁评级法：用于评估威胁组成要素的半定量方法，并将要素纳入总体威胁评估。

这些方法可以单独使用，也可以组合使用。威胁描述法所产生的威胁描述可以有效用于评估威胁级别并支持定性风险评估方法。由于威胁描述法不提供定量评估，不适合与定量风险评估方法一起使用，除非辅之以提供量化的方法。威胁评级法可以与定性或定量风险评估方法结合使用，因为评级可以很容易地转换成相对可能性评估。

5.6. 在这两种情况下，评估方法都遵循一个常用的三级分析循环，类似于图 3 所示。循环的第一步是主管部门规划威胁评估，收集新的或已有的威胁信息来源，评估信息的质量和可信度，并将其与相同的威胁、事件或活动相关的信息联系起来。第二步是分析，即对信息进行整合和分析，从而形成统一的信息。在威胁评估的最后一步，负责威胁评估的主管部门将评估在评估过程中考虑的威胁相对级别或可能性，并制订威胁描述法或威胁评级法。

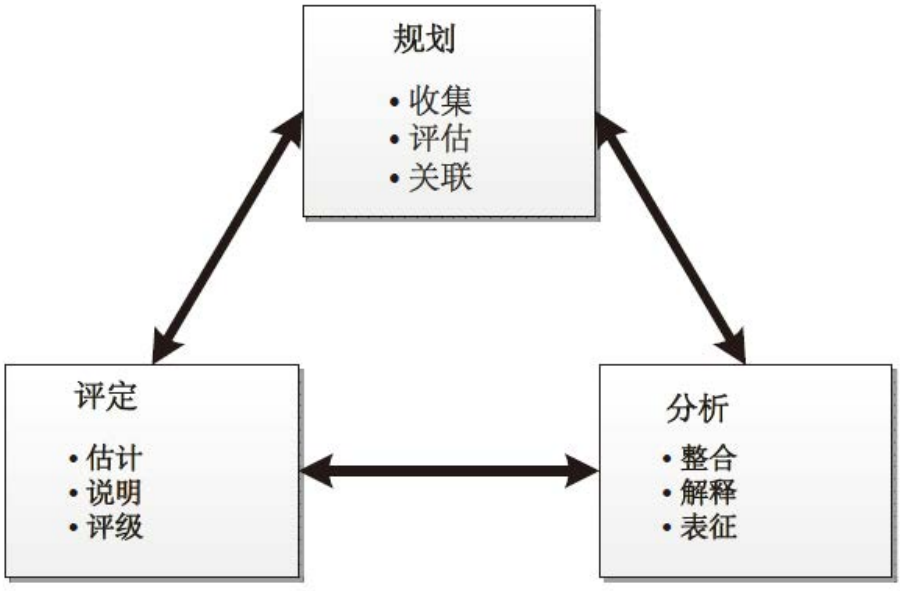


图 3. 显示关键活动的威胁评估过程。

威胁描述法

5.7. 威胁描述法提供了一种评估威胁的定性措施。主题专家编制关于敌对方的意图、能力和动机的详细信息。威胁评估可用于了解敌对方的组织、能力、运营和支持机制。这些信息对于评估不同敌对方可能采取的行动类型、目标和实施行动的方式非常有用。

5.8. 威胁描述法是使用一系列主要基于假设的标准技术重建单个核安保事件的过程，识别一系列相互关联的核安保事件，了解敌对方的网络，并分析相关活动的范围和模式。通过威胁描述法，分析师可以采用精准评估和陈述反映不确定性和不可预测性，并补充不完整的信息[15]。

5.9. 威胁描述法包括两项主要技术：分析核安保事件以及敌对方的具体特征。分析核安保事件，从已知的核安保事件寻找偏好的趋势和指标。事件分析可能涉及到放射性物质的类型、事件的发生地点、敌对方的能力水平以及敌方行动的性质。具体敌对方的特征分析包括考虑敌对方的意图、能力、组织和财政资源以及过去的活动、偏好和倾向。

5.10. 这些分析的支持技术包括使用地理信息系统展示敌对方、核安保事件和相关活动的位置之间的关系、了解这种关系的数据库结构以及个人和群体之间的关联图（例如社交网络分析工具）。有关这类技术的示例，请参见附录二。

5.11. 威胁描述法的结果是描述敌对方的具体特征和趋势。表 2 列出了一组概念性敌对方示例。

威胁评级法

5.12. 威胁评级法提供了一种评估威胁的定量方法。威胁评级法通过一系列评级尺度和定性描述词（也称为“词语阶梯”）将威胁的相对可能性评估与威胁类型的描述性说明相结合。威胁评级法中用于全面了解威胁的方法与威胁描述法类似，但威胁评级法的评估阶段集中在评估威胁不同方面的相对可能性。这些方面通常包括能力和意图，并可能包括核安保事件的其他方面，例如材料类型、装置类型或目标类型。然后使用预先确定的技术将这些方面的威胁评估结果与总体“威胁评分”相结合。用于组合不同方面威胁评级的技术必须在数学方面具有合理性。值得注意的是，相对于核安保的具体定量威胁评估而言，用于评估不同威胁（或威胁方面）的尺度可以相互校准，但不得涉及其他类型的威胁。因此，与其他类

型的袭击相比（例如涉及爆炸物和枪支的威胁），核安保相关的“高”威胁可能属于相对较低的威胁。另一方面，在所有危害评估中，核安保相关的威胁将与其他威胁一起进行评估。

表 2. 描述性威胁评估结果示例

威胁	意图	能力
团体 A	如果团体 A 持有材料，他们将有可能将其用于放射性散布装置，以污染市区，造成较高的经济成本损失。但是，他们不太可能参与任何会导致大量伤亡的活动。	团体 A 与吸毒集团和有组织犯罪集团有联系，通过这些联系或单独联系就可能获得放射性物质。
团体 B	团体 B 不希望造成大规模的人员伤亡，但他们倾向于实施有针对性的袭击。有针对性的污染食物或水源可能是适合他们的策略。	团体 B 与走私集团和有组织犯罪集团有联系，通过这些联系或单独联系就可能获得放射性物质。
团体 C	团体 C 几乎有意参与任何会造成重大破坏、损害或大规模伤亡的袭击。他们过去曾发动过这类袭击，并对多项有计划的未遂攻击事件负责。他们有意获取可用于放射性散布装置的放射性物质。 如果他们能够获得这类材料，并用于建造简易核装置，或者获得已经建成的核装置，他们就会在城市人口中心引爆。	由于团体 C 与有组织犯罪集团和走私集团的联系有限，通过非法贩卖者获得材料或装置的能力会相应降低。该团体拥有大量的资源，可以从受管制的设施或活动中直接盗窃材料。

注：所有描述均为假设。IND — 简易核装置；RDD — 放射性散布装置。

5.13. 评级过程是威胁评级法中最为关键的要素。该过程应该遵循良好做法，由主题专家推导数据，并应该包括对不同评级的明确定义。被评估的属性（标准、因素或类别）应该是正交型，也就是说，这些属性应该不能因为重叠而导致某方面威胁的重复计数。每项需要评级的属性通常会使用单独的评估尺度。例如“财务资源”和“技术能力”可以使用单独的尺度，然后应该进行单独评估。良好做法之一是使用描述性文本解释尺度上的各种级别。常见的尺度通常包含五个、七个或十个级别，既提供差异化，又不会使评估过程过于复杂，但是级别数量本身并不是准确性或精确度指标，因为判断的不确定性仍然存在。记录每个评级中的不确定因素或确定因素仍然是评估的重要方面。

5.14. 对于每种属性的评级应当纳入对每个敌对方的整体评级，以显示整体威胁。评级组合的方式有很多种，取决于具体的评级方法。其中最常见的有：

(a) 最高评级：将任何属性的最高评级用于敌对方的总体威胁评级。这种方法是一种保守的威胁评估，是基于敌对方会寻求减少弱点的观点，因此得分较低领域的属性评级可能会有所增加。

(b) 平均评级：计算不同属性的平均得分，通常先计算单项评估的数值（例如以1－5 级），然后取平均值。这种方法中每项属性的权重相同。最接近平均值的数值将用于总体威胁评分。这种方法倾向于降低评级非常高或非常低的特定属性的影响，但实际上这些属性需要仔细研究。

(c) 最低评级：将任何属性的最低评级用于敌对方的总体威胁评级。这种方法是假定最低的评级代表了敌对方必须克服的最苛刻的障碍，并且认为如果不克服这项障碍，敌对方就不会成功。

(d) 转换为可能性：每项属性（例如动机、能力和意图）的可能性值转换为得分，通常具有不确定性界限，然后将这些界限相乘就得到了敌对方的整体可能性。使用这种方法时需要特别注意，应当确保可能性值足够明确地反映威胁之间有意义的区别。例如，有些评估可能需要区分罕见事件（例如核安保事件）和更常见的事件（例如洪水或地震）。在此情况下，可能性可能会因为数量级而有所变化。

(e) 自定义权重：这种方法将威胁评级与平均评级法相结合，但不同属性的评级根据其在总体威胁中的重要性而有不同的加权比重。（在上文的平均法中，所有属性的权重相同。）例如，敌对方拥有完成攻击的足够技术能力比敌对方具有强大的组织能力更重要。在此情况下，技术能力评估应该对总体威胁评级的影响更大，因此在计算平均值时，技术能力评级的权重应该更高。

5.15. 开展威胁评级的重要好处之一就是可以将其转化或解释为可能性评估，而可能性评估可用于支持定量风险评估法。表 3 介绍了一种特定威胁尺度的示例。这些描述也可能适用于威胁描述法。附录二则介绍了威胁评分过程和词语阶梯的示例。

表 3. 描述总体威胁级别的词语阶梯示例

威胁评估级别	说 明
非常高	敌对方目前已经具备攻击目标的相应能力和意图 根据评估，攻击的可能性非常高
高	敌对方具有攻击目标的能力，且该攻击在该团体的意图范围之内 根据评估，攻击的可能性较高
中	敌对方具有攻击目标的部分能力，该攻击符合该团体的意图，或者敌对方具有攻击目标的能力，但其意图可能取决于当时的情况 根据评估，有可能会发动攻击
低	敌对方目前几乎没有具备攻击目标的相应能力和意图 根据评估，攻击的可能性较低
非常低	敌对方目前不具备攻击目标的相应能力和意图 根据评估，攻击的可能性很低

风险评估的方法

5.16. 在核安保方面，风险通常被认为由以下三个部分组成：威胁、薄弱性和后果。风险评估将特定核安保事件的估计可能性（即：威胁和薄弱性）与其后果结合起来，以提供对设计或改进核安保系统和措施有用的整体措施。如果认为特定的核安保事件可能发生，或者会导致重大后果，或者两者兼具，则可能被认为是“高风险”。通过评估可能的核安保事件造成的经济损失的预期值，风险评估能够提供可用于与防止核安保事件的系统和措施的成本相比较（在某些情况下）的估计值，从而以评估这些系统和措施的成本效益。实际上，由于风险评估的不确定性，进行这类比较时，应当非常谨慎，从而避免出现评估比实际更可靠或更准确的印象，以免误导负责主管部门采取相关措施。

5.17. 与威胁评估一样，风险评估中的详细程度、复杂程度以及量化分析的程度应该根据计划支持的优先级决策具体制订。不同的风险评估方法适用于不同研究领域。本小节概述了两种常用的方法（一种是定性法，另一种是定量法），这些方法适用于确定实施核安保系统和措施的优先级。这些方法包括：

(a) 风险登记表：将识别出的情形反映在可能性和后果尺度矩阵上，以便以可视化的方式进行风险比较。这种方法可以是定性或半定量方法。

(b) 概率风险评估：这是一种基于情景的方法，通过将导致事件的主要元素或“步骤”与结果结合起来（通常以图形方式将其显示为事件树、决策树或故障树），估计每种特定情景的最终结果。该方法结合了每项主要元素（在事件树中称为“节点”）的可能性（或概率）量化评估，以获取情景的总体可能性。这种方法与概率安全评估相似[16]。

5.18. 这两种方法（尤其是后者）均依赖于使用数学模型表示可能的事件，并由主题专家根据判断确定可能性（这些无法从经验观测的频率中获取）和其他参数[17]。下文将讨论使用主题专家或模型估算风险的关键原则，并将不确定性纳入估算和结果。

5.19. 关于风险管理的国际行业标准确定了风险评估的三大关键步骤：风险识别、风险分析和风险评估[7]。尽管本出版物中所述的风险评估方法并没有在每一个步骤的描述中明确地使用这些名称，但他们确实包括了所有三个步骤。风险识别是通过方法讨论中的情景选择或情景发展识别风险。风险分析是通过评估可能性和完成风险计算广泛分析风险。风险评估是通过不确定性分析和敏感性分析的描述评估风险。

风险登记表法

5.20. 风险登记表是已识别出的风险的清单或目录，类似于项目管理中的风险登记表。风险登记表用于记录风险、后果的严重程度、风险发生的可能性以及为降低风险而采取的措施。每一种一般风险通常会进行最差情况分析，从而得到少数似乎合理的代表性情景。但是，有些技术将使用一系列的标准的可能性较高的常见（或标称）情景。这类情景可以作为各种风险情景中和相互之间相对评估的基准。风险反映后果的严重程度往往分为以下几个方面（可能包括以下任何一项或全部）：人员伤亡、经济损失、社会混乱和环境破坏。

5.21. 风险登记表通常用于比较各种的风险（例如自然灾害、核安保事件和工业事故），并协助在所有危害事件中分配预算。风险登记表通常在较高层面（即战略层面）登记，由主题专家利用对数尺度评估相对可能性和严重程度。

5.22. 风险登记表应该包括以下要素：

(a) 时间框架：由于登记表是一项需要定期更新的文件，记录风险评估的时间以及评估的有效期非常重要。如果威胁发生变化，或者为减轻风险而实施的措施发生变化，则风险可能也会发生变化。这些变化应该在适当的时候纳入未来进行的评估。

(b) 风险描述：由于风险登记表只使用了少量的代表性情景，风险描述应该包括确定每项已识别情景的所有参数，并将参数用于评估风险。其中包括：

- 关于目标的设想；
- 装置的类型；
- 所用材料的数量；
- 敌对方的能力；
- 反映装置可能质量（例如可靠性、效率或产量）的任何假设；
- 导致核安保事件的顺序假设；
- 事件发生时的相关条件（例如天气或受影响人口）；
- 缓解措施的可能有效性。

(c) 发生的可能性或频率：这是用于评估事件发生的可能性（用概率或几率表示，例如低概率（<30％）、中概率（31％－70％）或高概率（>70％））或者预计发生的频率（用频率表示，例如每年 10 次，每年 1 次，10 年一次，100 年一次）。事件的可能性可以根据需要在绝对范围内进行评估，但以相对频率或可能性评估事件通常会更重要（通常也更可靠）（例如，核恐怖行为的可能性远低于洪水，而远高于小行星撞毁地球）。相对尺度可以足以根据目标进行风险评估。

(d) 后果的严重程度：这是用于评估核安保事件可能造成的后果。这可能包括对不同后果的多项单独评估，这些评估可以与单独的总体评估相结合。就可能性而言，严重程度的相对措施可能比后果的绝对评估更重要（也更有用）。

(e) 其他对策：这些是为了防止或降低事件的后果而采取的行动。他们可能包括计划中的响应措施，在可能性和严重性计算中可能已经纳入了响应措施。他们还可能包括可能采取的具体行动，从而降低特定事件的可能性或严重程度。在后一种情况中，对策措施通常在风险登记表上以箭头形式显示，显示对策措施可能降低风险的规模和方向。

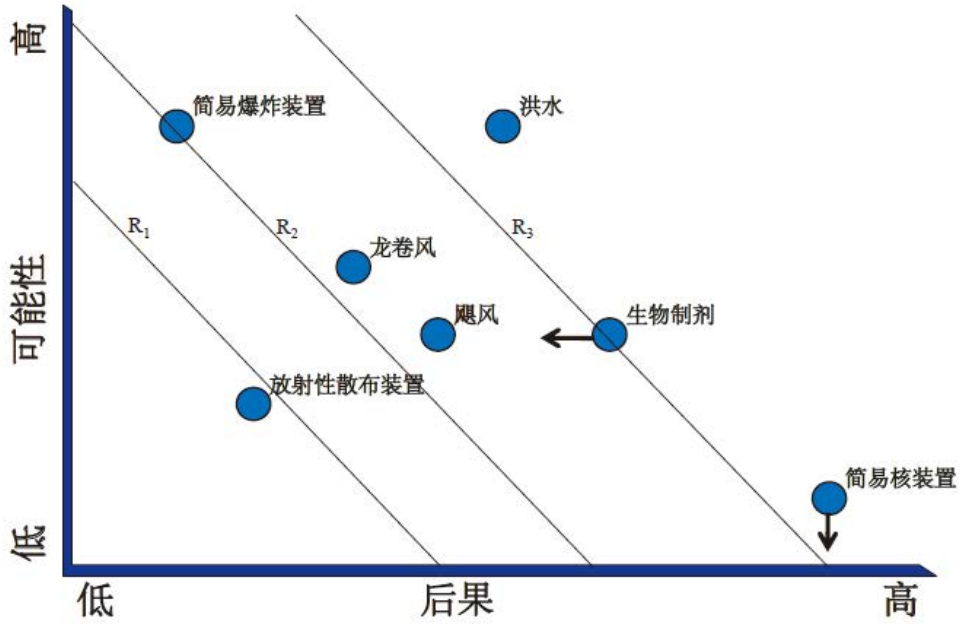
5.23. 图 4 显示了附带名义数据的风险登记图示例。该示例的图表显示，简易核装置情景的后果最严重，但可能性最低。洪水的可能性可能与使用简易爆炸装置

（IED）大致相同，但后果更为严重。生物制剂攻击（“生物制剂”）符号中的箭头表示通过使用特定的医疗对策可能减轻的后果（并非可能性）。简易核装置符号中的箭头表示通过实施改进核安保措施可以降低的简易核装置攻击的可能性（并非后果）。其他措施或措施组合可能会同时降低可能性和后果。在此情况下，箭头将朝对角方向指向与风险降低相关的新可能性和后果。最后，对角线是等风险线条：线上的所有的点具有相同的风险等级。这类线条可以帮助决策者用相同风险等级比较不同的情景。

概率风险评估法

5.24. 概率风险评估可用于用定量或半定量的方式评估各种特定情景中的风险。在评估核安保事件的风险时，情景通常由关键要素构成，并且通常以故障树、事件树或决策树的形式表示。

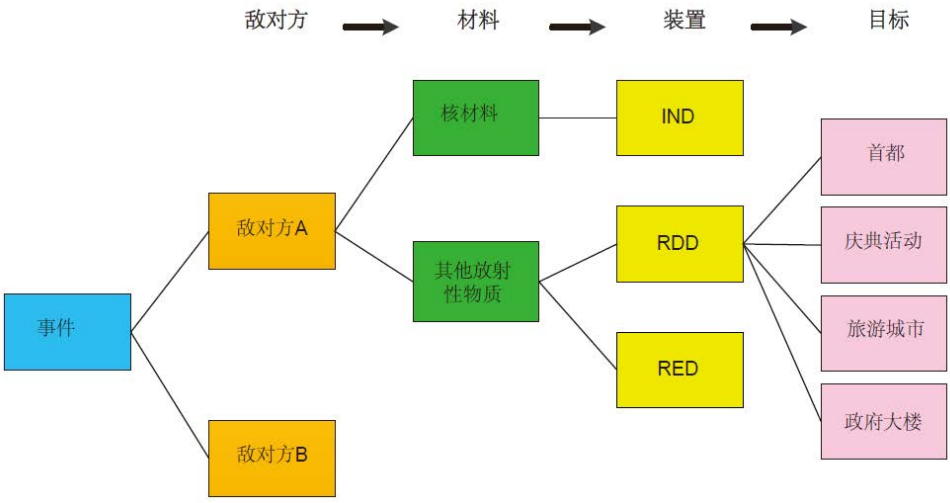
5.25. 概率风险评估法是通过定义核安保事件的重要元素并构建包含每一个元素中所有可能实例的“情景空间”来构建风险情景的系统性方法。重要因素可能包括敌对方从各种选项中选择特定行动的决策、敌对方的行动过程中的中间步骤的成败或用于阻止敌对方行为的核安保措施的有效性（或其他方面）。这些要素可以在事件树中描述和展示为分支点，事件树中的不同路径代表不同的单独情景。事件树中的每个分支点称为一个节点或一个层面。事件树的末端节点（不再有任何额外分支）有时称为“树叶”，代表不同的最终结果。计算风险时，分别从事件树的每个末端节点评估后果。主管部门应该决定认为重要的后果（例如，人员伤亡、环境污染、经济影响和社会影响），并应该据此进行评估。各项情景可能性的计算方式是事件树中每一个分支情景的可能性的乘积。



注：所有可能性和后果评估都只是概念性的评估，并不反映实际数值。R_1 <R_2 <R_3（线条代表相同的风险）。IED — 简易爆炸装置；IND — 简易核装置；RDD — 放射性散布装置。

图 4. 用于确定所有危害资源优先级的所有危害风险登记表示例。

5.26. 事件树是通过识别事件树中每个节点的不同可能性构建而成。图 5 显示了简易事件树的部分内容。在本示例中考虑了两个敌对团体以及他们可能获取的两种类型的材料，并且他们可以据此建造多种类型的装置。在本示例中考虑了四个可能目标。在实际情况中，潜在目标的数量可能更多，或者目标的类别或类型更广，而不是特定的建筑物或事件。



注：本示例只显示了事件树的部分内容。IND — 简易核装置；RDD —放射性散布装置；RED — 辐射辐照装置。

图 5. 用于开发风险情景的事件树示例。

5.27. 下一步是评估通过事件树的每条路径的可能性。在本示例中，所有路径节点的所有可能性将生成 48 个单独情景，主管部门需要评估每个节点的每种选项的可能性，以便计算每种情景的可能性。

5.28. 为了方便说明，专门对示例中的事件图进行了简化处理，并非用于解决开展概率风险评估所涉及的所有问题。实际上，可能性评估可能取决于其他节点，在可能性复杂的节点处，可能需要额外建模或计算才能获取可能性的值。该事件树显示了如何使用事件树构建一组完整的情景。精心构建的事件树应该能够用于识别一系列完整的合理情景，并确定能够反映出潜在核安保事件的所有重大风险。

评估风险情景的可能性

5.29. 了解风险的一项关键因素是评估不同类型潜在核安保事件的可能性，而这在本质上就是一个不确定的过程。本小节介绍了评估可能性的一般方法、其各自的优缺点以及开展分析所需的资源。本小节还将绝对评估和相对评估进行了对比。主要考虑如下：

(a) 可能性通常会进行量化，以便用于风险评估，而风险取决于实施涉及核材料或其他放射性物质的犯罪行为或未经授权故意行为的可能性以及成功的可能性（以及后果）。

(b) 可能性评估在本质上是不确定的，因此不仅需要评估可能性，还需要评估可能性的不确定性。这可以描述为评估中的误差（即±绝对值或比例值），通过概率分布或适当文字说明近似数字。

(c) 可能性评估分为绝对概率或频率。然而，这种方法通常非常困难，并且在对替代方案进行风险评估时也可能不一定必要。相对可能性（即一组情景中的哪一项的可能性更高以及高多少）可能更容易评估，并且可能已经足够，除非必须将这些攻击的可能性与其他危害进行比较。

5.30. 评估可能性的方法之一是由主题专家推导概率值。这种方法使得风险评估能够利用国家的专业知识和信息，并且适用于具体的国情和具体情况。然而，专家推导是一个非常漫长的过程。如果推导不谨慎，可能会对产生许多结构性偏差。关于避免或降低这类偏差影响的方法，请参阅国际原子能机构《安全标准丛书》第 RS-G-1.9 号“放射源分类”[18]。

5.31. 或者，可以开发模型生成概率估计值。模型可能涉及多种可能的情景，更为灵活，并且适用于大量替代方案的分析。用于这类目的的常见建模类型包括事件树、故障树和博弈论模型。关于建模方法的综合评述，请参阅参考文献。[19]

不确定性分析

5.32. 所有风险评估都涉及不确定的数据和判断，涉及预测或模拟真实事件的能力限制，涉及不确定或模糊结果。不确定性的每个方面都应该通过以下方式确定：

(a) 专家推导的风险评估成果的不确定性应该识别为推导或建模过程的不确定性的组成部分。不确定性通常通过可能的值的分布描述。主题专家可能需要提供多个分布点的估计值（例如平均值及每一侧的极限值，通常是 5%和 95%），这些可以通过分布为何出现偏差或偏离进行解释。在建模的情况下，可以使用统计方法推导风险评估成果估计值的分布。

(b) 在整个风险计算过程中，应该考虑成果的不确定性以及与这些计算相关的其他不确定性。由于在多个参数中直接计算多项不确定性的分布情况很快就会

变得在数学上难以处理，其他方法（例如，蒙特卡罗（Monte Carlo）抽样法）常常用于评估结果中的不确定性分布[20]。

(c) 向决策者传达风险评估成果和计算中的不确定性以及相应的结果的不确定性至关重要。用数字表示结果时（例如，风险），估计值应该包含范围指数而不是单个数字，报告结果应该避免出现误导性精确指数（例如，在谈到多个重要数据时引用在不确定的结果）。

5.33. 不确定性分析之所以重要，是因为他提供了风险评估结果的可靠指数作为决策依据。特别是在问题复杂或有争议的情况下，在经验证的模型中包含不确定因素有助于确保决策的依据是最佳可用信息。

6. 风险知情方案的使用

6.1. 核安保事件的潜在后果可能是灾难性的。因此，各国应该采取一切适当措施防止核安保事件的发生。但是，各国的资源始终有限，因此国家应该采取正确方法识别哪些核安保措施可能是降低风险的最有效方法。风险知情方案可以协助各国评估选项和确定核安保措施的优先级。

6.2. 风险知情方案是一个迭代过程：识别并评估风险；开发、评估、选择和实施降低风险的措施；监测由此产生的措施的有效性；并根据需要做出调整[7]。风险知情方案可用于有效指导预防、侦查、响应、缓解和恢复工作，以最大限度地降低风险。风险知情方案支持多种决策，包括：战略规划；决策；制订预算；确定研究和开发的优先级；以及设计核安保作业。

6.3. 迭代风险知情方案的目标应该是不断改进和加强国家的核安保系统和措施。图 6 显示了一种风险知情方案示例。以下段落中介绍了该示例的五大主要步骤。

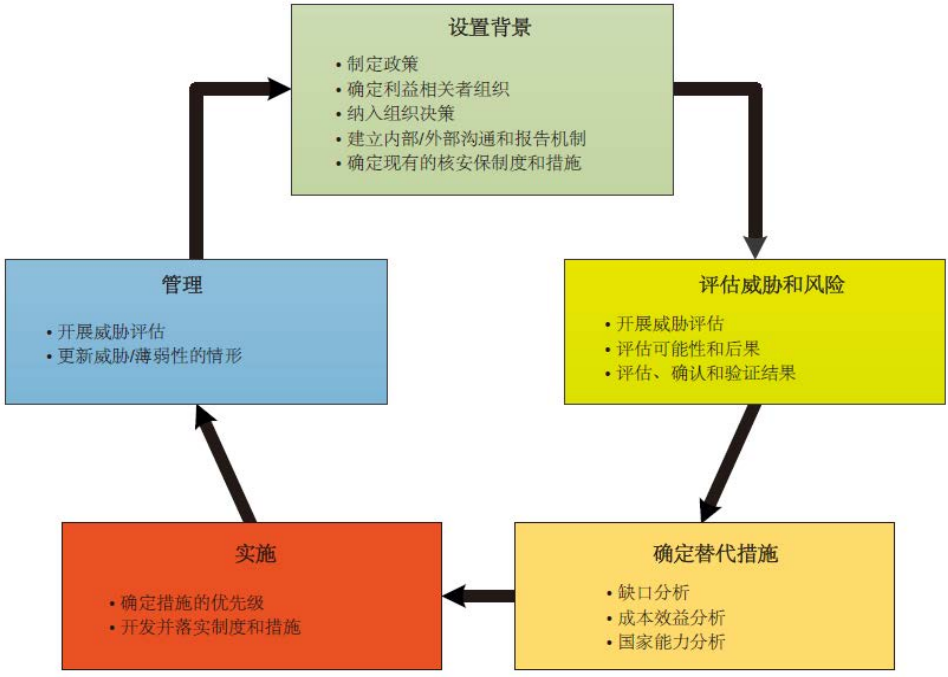


图 6. 通过风险知情方案实施核安保系统和措施的示例。

6.4. 应当定期重复这一循环（定期支持决策需求或情况的重大变化），以改进分析和结果以及核安保系统和措施的有效性。内部和外部利益相关者之间的沟通和讨论在整个过程中都非常重要，可用于确保国家目标的实现。

6.5. 威胁评估以及纳入风险知情方案的风险评估也在识别风险方面发挥了不可或缺的作用。威胁评估对于评估核安保的替代战略或系统和措施（因为预计敌对方会根据这类措施的变化进行调整）以及监测威胁行为的趋势和核安保系统和措施的有效性也非常重要。

设置背景

6.6. 在这一步骤中，由指定的主管部门确定需要管理哪些类型的风险、谁负责管理、哪些决策取决于风险信息（以及哪种类型的信息）以及谁是使用风险知情方案的利益相关者。此外，还要确定实施风险知情方案的资源，包括必要的预算、

人员和组织结构。制订利益相关者之间的沟通程序，并对核安保职能和活动进行初步调查。

威胁和风险的评估

6.7. 在这一步骤中，指定的主管部门应当根据当前的核安保政策、系统和措施评估风险。作为这一步骤的一部分，指定的主管部门应当对威胁、薄弱点及敌对方采取的与核安保相关的行动可能产生的后果进行评估。评估方法应该根据决策的类型、可用数据的数质量以及可用资源的级别和类型制订。方法可能包括从与主题专家简单的桌上演练到详细的风险计算。无论选择何种方法，保持所用方法的透明度非常重要，以便决策者可以信任程序和数据的有效性。

替代核安保系统和措施的识别

6.8. 负责落实核安保系统和措施的主管部门应该能够利用风险评估的结果识别潜在改进措施，以更好地处理高风险的脱离监控的核材料和其他放射性物质有关的犯罪行为或未经授权行为。替代性的核安保措施的示例可以包括对受监管设施和活动的额外安保措施或经过强化的保护能力，或经过强化的边界监测能力或执法意识，或制订的保护特定目标的新程序和流程。在识别、优化和设计核安保系统和措施时，应该考虑纵深防御的概念。

6.9. 指定的主管部门可以采用以下三种常用方法确定和评估备选方案：缺口分析、成本效益分析和国家能力分析。

缺口分析

6.10. 如果没有足够的能力解决实际威胁，就会出现缺口。缺口分析涉及根据威胁评估找到必要考虑的核安保系统和措施的以下要素或功能：要么不存在，要么没有落实，要么无法应对相关威胁的要素或功能。通常可以通过检测导致最高风险的威胁识别缺口，并通过增加能力、改变运营或降低薄弱性确定应对这类威胁的机会。

成本效益分析

6.11. 成本效益分析用于比较核安保措施的成本与措施产生的效益（降低风险）。成本效益分析应该考虑措施的整个生命周期的成本，其中可能包括设备、安装、运行、维护、人力资源和培训成本以及升级或停运成本。降低的风险通常转化为货币形式，以便与措施成本进行比较。成本效益分析支持分级法，以改进核安保系统和措施。措施的部分“成本”也可能是非货币性质的，例如计划和程序的更改以及资产的重新配置。

国家能力分析

6.12. 国家能力分析涉及对整套核安保系统和措施的评估，并作为综合系统应对威胁。如果需要模拟敌对方的多变意图，通常会使用这种方法，敌对方的意图可能会因为实施的特定核安保措施而发生变化。例如，提高一个战略场所的安保可能会使敌对方更有可能攻击其他场所。同时提高这两个场所的安保可能会使敌对方决定尝试不同类型的攻击。因此，提高一个场所的安保的实际价值只能在其他场所的安保发生变化（或不变化）的情况下进行评估。对国家能力分析最简单的方法是评估多个完整的替代系统和措施的风险，并从特定类型的措施纳入最佳表现措施集合的次数推断其价值。

6.13. 在评估系统和措施对风险的影响时，需要特别注意的是，敌对方可能会根据新的或额外的核安保措施调整攻击方案。因此，在通常情况下，相对于静态威胁（即敌对方只考虑对一个目标发动一种类型的攻击），如果敌对方只须简单改变战术，整体风险的降低程度较小。在有些情况下，提高一个场所的安保可能会导致敌对方选择另外的方案，该方案甚至在先前的系统和措施下会更加成功。在这种情况下，提高某些场所的安保实际上可能会增加整体风险。了解敌对方的倾向和可能的应对行动可用于确保额外的安保能够按照预期降低风险。

6.14. 由于国家的所有核安保系统和措施的责任往往分散在多个不同的主管部门之中，所以必须协调资源利用情况和降低风险的方法。适当的协调有助于确保有利于提高一个主管部门效率的系统和措施能够及时被另一主管部门采用。

核安保系统和措施的实施

6.15. 国家决定行动方针后，就可以实施（设计、部署和维护）核安保系统和措施。在实施过程中，应该遵循适当的管理方法，确保项目符合预算情况并及时按照规范要求完成。

6.16. 在设计核安保系统和措施并确定优先级别后，实施通常包括开发、采购、部署、运行、维护和能力的可持续性[11]。在实施过程中，应该考虑到与核安保系统和措施有关的敏感信息和敏感信息资产的保护。

6.17. 确定优先级别和实施过程的风险知情方案不同于基于风险的方案，在基于风险的方案中，风险是决定优先级别的主要因素。在确定核安保系统和措施的优先级别时，应该考虑许多因素，例如预算因素、政治因素、措施的可行性和适用性、措施的表现或产生的其他费用。风险是确定总体优先级别决策的因素之一，决策者应该结合其他因素考虑风险情况。

风险管理

6.18. 部署和实施核安保系统和措施不应该是一次性行动。还应该对这些系统和措施进行管理、维护和维持，并应该根据形势的变化进行升级或调整。为了确保系统和措施能够按照设计实施，还应该对他们进行测试。在测试过程中，应当重新评估核安保系统和实际措施的有效性（即他们实际上是否按照预期正常发挥作用）。此外，还应该不断监测威胁和薄弱点，识别可能影响威胁的变化，例如新敌对方的信息、敌对方的目标或能力变化，并制订新的核安保系统和措施，还要考虑其他因素。监测过程的结果应该用于更新背景信息和风险分析信息，以便再次重复风险知情方案循环。

效果评估

6.19. 设计有效性度量标准评估核安保系统和措施如何防止、侦查和应对涉及脱离监控的核材料和其他放射性物质。在实践中，计算有用的度量标准特别困难，因为试图盗窃核材料或者实施具有核安保影响的行为非常罕见。在没有通过真实事件获得实际经验的情况下，应该制订模型或代理量度标准。

6.20. 在培训训练中，应当考虑核安保系统和措施发挥作用所需的所有资源，从而说明措施的执行情况，并提供关于所实施系统的总体有效性的信息。在通常情况

下，在将训练结果、其他性能指标（例如平均故障间隔时间）和模型相结合后，可以用来评估核安保系统和措施的性能。

趋势分析

6.21. 除了根据已经识别出的威胁评估核安保系统和措施的有效性之外，更新威胁评估以反映能力变化也同样重要。趋势分析需要考虑的因素可能包括：

- 已知的敌对方是否改变了行为？敌对方是否显示出额外的能力或专业知识？敌对方是否与其他国家的行动者建立了新的联系？
- 是否有新的敌对方可能会考虑实施影响核安保的行为？
- 敌对方是否有意将某个国家作为目标，作为核材料或其他放射性物质的安全港或来源？
- 通过某个国家的商业交通或走私交通线路是否发生了明显变化？材料的数量增加后是否需要进行额外审查？
- 核安保系统和措施是否进行过重大修改？是否有新的场所用于储存或使用核材料或其他放射性物质，或者这些物质的数量或类型是否发生过显著变化？

6.22. 识别国家核安保系统和措施的威胁和变化趋势是确定何时更新或启动风险知情方案循环的重要步骤。该循环应该定期重复，并与决策过程保持一致。此外，如果国家的核安保侦查应对系统和措施[10、11]或威胁发生重大变化，则应该进行风险评估，并重复风险知情方案循环。

附 录 一

威胁评估和风险知情方案模板

I.1. 本附录中的流程图（见图 7）显示了完整的风险知情方案循环。本出版物中介绍的所有重要步骤都整合为一个简单的总体流程。

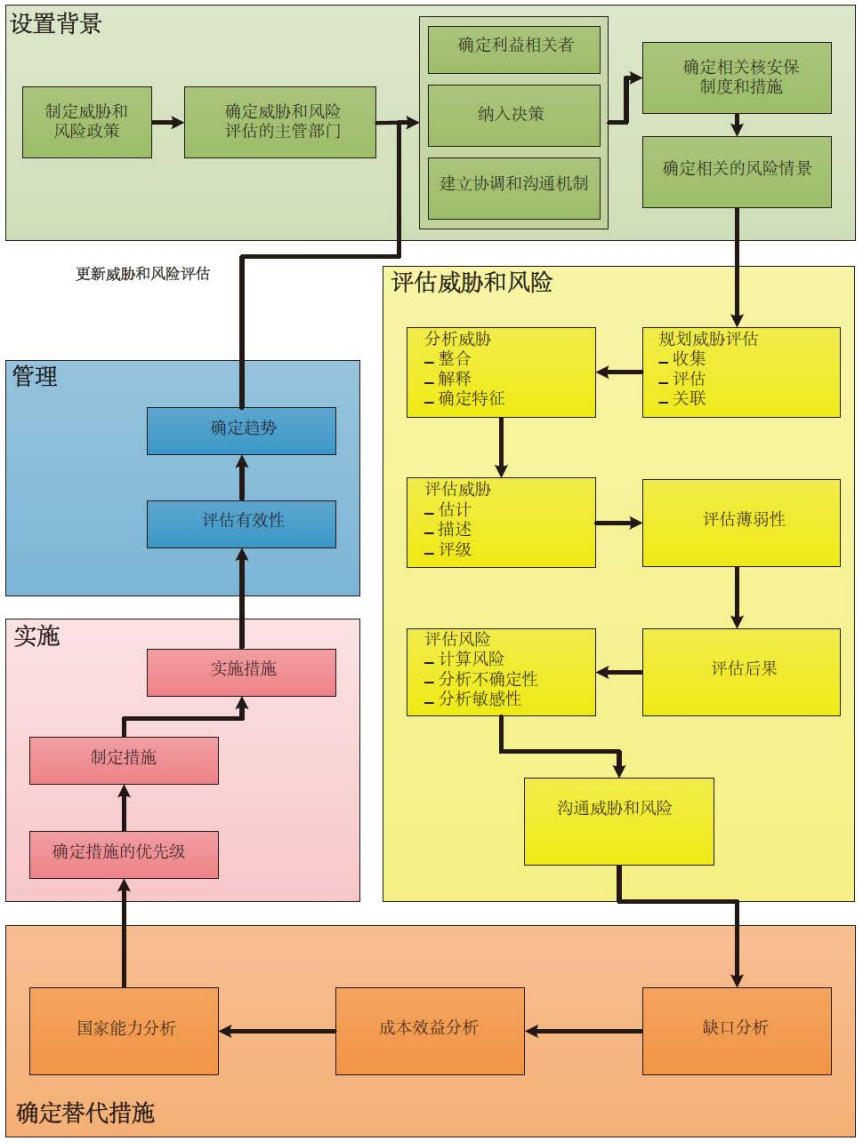


图 7. 威胁评估和风险知情方案模板。

附 录 二

威胁评估示例

评估背景

II.1. 为简洁起见，本示例中省略了评估过程中的所有论证、过程和分析。本示例所显示为流程输出示例以及如何向利益相关者展示结果。

II.2. 在附录二至附录四中，我们都假设了一个“示例国家”概念。示例国家有一座核电厂和一座研究反应堆，但没有完整的核燃料循环。示例国家还有储存和使用放射性物质和放射源的医院以及根据示例国家监管机构的许可储存大量放射源的其他行业（如建筑）。

II.3. 示例国家由多个主管部门负责监管相关设施和相关活动中的核材料和其他放射性物质，并负责检测和应对核安保事件。所有这些主管部门与负责威胁和风险评估的主管部门合作和协作，共同实施脱离监控的核材料和其他放射性物质的核安保措施的风险知情方案。此外，示例国家的主管部门概括描述了用于支持威胁评估的信息和情报的已知缺口、相关性和及时性。

II.4. 风险知情方案可以促进多项决策流程，其有助于确定稀缺资源的优先级别。示例国家乐观地认为风险管理过程将有助于保护资源。

材料和敌对方的识别

II.5. 示例国家的主管部门实施了威胁识别程序，该程序考虑了敌对方及脱离监控的核材料和其他放射性物质。非法贩卖数据库的事件分析数据显示：

(a) 示例国家含有放射性物质的建筑仪表失窃，并且未能找回。

(b) 示例国家西部邻国的事故数量比其北部、东部和南部邻国多三倍以上。

(c) 示例国家或其邻国从未丢失、遗失或失窃过适用于简易核装置的核材料；然而，不能完全忽视从这些国家或其他国家获取核材料的可能性。

II.6. 主管部门评估并决定，在确定威胁和风险时需要考虑三类潜在敌对方：

(a) 国际敌对团体，他们可能在示例国家境内采取行动，或者利用示例国家作为对另一国实施行为的中转站。

(b) 主张推翻现任政府并实施其他暴力行为的国内敌对团体。

(c) 具有特定议程和暴力倾向的个人或小团体。

II.7. 主管部门向威胁分析人员提供了关于团体倾向及已知计划和目标的信息。主管部门收集了最近发生的相关事件（表明团体倾向的行为或者涉及核安保的行为），并确定了这些事件的关联关系。

目标识别

II.8. 示例国家威胁和风险评估主管部门识别了涉及脱离监控的核材料或其他放射性物质的行为的几个关键潜在目标。威胁分析的主要目标如下：

- 示例国家首都的市区；
- 示例国家的主要旅游城市的主要购物区；
- 示例国家重要机构所在的几栋关键政府大楼；
- 每年的国庆节庆祝活动。

II.9. 由于示例国家识别的目标数量相对较少，因此对这些目标进行了单独评估。如果主管部门决定评估更多的潜在目标，则可将目标分组为不同的目标类型。

后果识别

II.10. 示例国家主管部门召集一批爆炸物、辐射和犯罪行为或未经授权故意行为领域的专家，根据已识别目标，评估一系列潜在行为的可能后果。专家们考虑了许多会影响实际后果值的变量，包括放射性物质的数量和类型、行为实施时的气象条件、目标的性质以及行为本身的特点。专家组随后提供了一系列情景后果的估计数量级。估计可以提供每种情景的伤亡和经济成本（为了简单起见，经济成本包括环境和社会后果）。综合后果值（价值）和标准化后果评级可以按照如下方式计算：

$$\text{价值} = \text{伤亡人数} \times \text{名义伤亡值} + \text{经济成本} + \text{环境成本} + \text{社会成本} \quad (1)$$

$$\text{标准化后果评级} = 100 \times \frac{\text{价值}}{\text{最大（价值）}} \quad (2)$$

II.11. 由于主管部门的目标是赋予各类情景的相对严重程度，所以综合后果值的计算方式为：伤亡人数乘以 100 万货币单位（仅用于说明目的）的平均成本价值，加上经济成本。结果值可以通过最高值进行标准化，从而创建了从 0 到 100 的标准化后果评级。由此分析得出的结果表如表 4 所示。

表 4. 示例国家概念情景中的相对严重程度

情景	人体健康（伤亡人数）	经济成本（百万货币单位）	标准化后果评级
首都的简易核装置	20 000	250 000	100
旅游城市的简易核装置	10 000	100 000	40.74
首都的放射性散布装置	500	500	0.37
政府大楼的放射性散布装置	20	100	0.04
庆典上的放射性散布装置	2 000	250	0.83
旅游城市的辐射辐照装置	150	10	0.06
庆典上的辐射辐照装置	350	50	0.15
政府大楼的辐射辐照装置	15	5	0.01
污染事件	800	250	0.39

注：数字为假设数据，不适用于示例之外的情形。IND — 简易核装置；RDD — 放射性散布装置；RED — 辐射辐照装置。

威胁评估

II.12. 示例国家的威胁和风险评估主管部门协调各主管部门对识别的三类敌对方进行威胁描述。向专家提供了显示已知或可疑非法贩运核材料或其他放射性物质事件的数据和图表。然后按照材料类型、位置和事件以及材料的来源或合法使用情况对事件进行了详细分析。还向主题专家提供了描述所述目标、最近的活动和各个已知团体言论的信息，以便能够对该团体使用常见评估和方法。表 5 列出了专家们所达成共识的一种示例。

表 5. 三个敌对方的威胁描述分析示例

敌对方	意 图	能 力
国际团体	该团体寻求造成高昂的经济成本或大量人员伤亡。	该团体试图购买或盗窃放射性物质，但他们的阴谋已被执法机构阻止。该团体通过犯罪活动获取了大量资金，但内部安保措施使其难以招聘技术专家或与能够获取放射性物质的人员接触。
国内团体	该团体的目标是给示例国家政府造成经济成本损失，以实现领土自治，不会造成大规模的人员伤亡，因为其可能会招致国际社会的愤慨。	该团体基于家庭关系建立了明显的层级结构，参与贩毒等高利润的犯罪活动。 已知的成员中均无物理学或工程学方面的高级大学学位，尽管他们已经证明能够制造简易常规武器。他们未试图购买过核材料或其他放射性物质。
单个敌对方	单个敌对方的主要目的是对雇主造成成本损失，让他们蒙羞。虽然他个人可能愿意造成重伤或死亡，但大规模伤亡并不是他的目的。	他可以获取核材料或其他放射性物质以及处理这类材料的专门知识，但从未建造过完整的装置。因此，可能只会采取涉及辐射辐照装置或造成有限污染的行动。

II.13. 负责威胁评估和风险评估的主管部门采用了威胁评级法，并组织主题专家根据敌对方的类型推导评估每种具体情景的级别。具体的做法是将评估分为多个子类别。能力可以分为组织、技术和财务等三方面的能力。意图可以分为意识形态和目标等两方面的图章。建造装置的可能性可以分为材料、获取材料的难度和建造装置的难度。最后，目标的薄弱性涉及目标类型和攻击时机等两个方面。每种标准或因素都根据确定的评级尺度（也称为“词语阶梯”）进行评估，评级尺度确立了每项评级的标准。表 6－8 显示了国内某叛乱团体在年度庆典上部署放射性散布装置的评估示例，详细介绍见第 II.14－II.16 段。

表 6. 能力和意图威胁评级示例

威胁评估组成要素的评级	能力			意图	
	组织	技术知识	财务/物流	意识形态/倾向	目标/动机
非常高					
高					
中					
低					
非常低					

表 7. 材料和薄弱性威胁评级示例

威胁评估组成要素的评级	材料			目标的薄弱性	
	材料的种类	获取	装置	目标类型	机会/时间框架
非常高					
高					
中					
低					
非常低					

表 8. 威胁评级摘要示例

威胁评估总体评级
非常高
高
中
低
非常低

II.14. 国内团体的组织强大，资金充足，但对核材料或其他放射性物质没有兴趣或不了解。虽然他们通常不会造成平民伤亡，但他们有强烈的动机实施提升形象和名声的行为。

II.15. 示例国家有该团体需要的放射性物质，但使用权限受到严格控制。然而，一旦获取材料，很容易建造装置。目标为非常脆弱的民用设施，但确保造成最大影响力的时间非常有限。

II.16. 总体而言，综合各种因素，国内组织在示例国家举办的年度庆典活动中部署放射性散布装置的威胁评级为高：能力和意图的评级均为高；材料和目标的吸引力评级为很高。如何进行这类评估（以及总体威胁评级）将取决于使用的方法。

II.17. 对每一对敌对方情景进行的类似评估，以评估潜在的行为。这些评级将用于支持对脱离监控的核材料和其他放射性物质用于核安保事件的评估选项的相对可能性评估。根据每一项标准评估的支持证据进行总体评估，并通过主题专家审查验证。

附 录 三

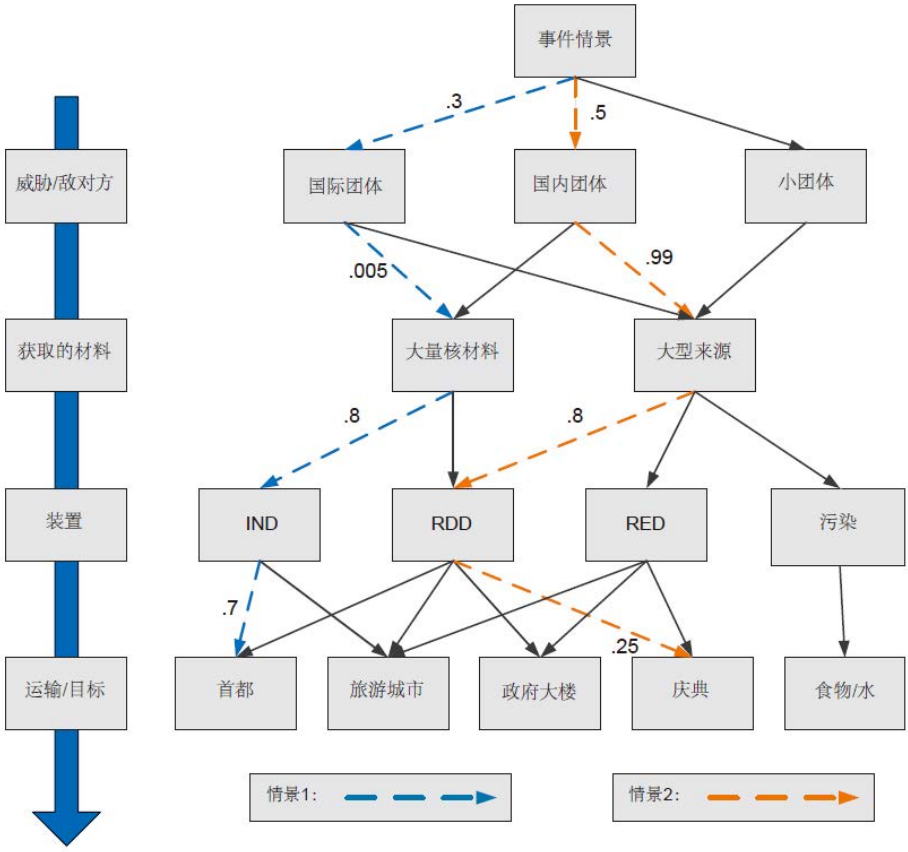
风险评估示例

III.1. 以下示例通过为示例国家创建事件树，演示如何使用概率风险评估法。估计事件树情景的可能性计算值，并提供样本分析结果。本示例的依据是附录二中的威胁评估示例，并使用了示例结果。

情景结构

III.2. 图 8 介绍了事件树节点和每一个节点的所有可选方案。事件树代表了描述涉及脱离监控的材料的核安保事件所需要的节点类型的最小集合。为了简单起见，每一个节点处选择的数量保持为最小。每一个节点的可能性被视为概率分布。在这类事件树中，某些节点的可能性通常取决于其他节点的值。例如，装置节点取决于所获取的材料。国家的风险评估工作中需要或最好引入额外的相关性。

III.3. 创建事件树的特定情景通过事件树中的路径表示。例如，一种情景是国内团体获取了大量资源，并决定将资源用作放射性散布装置以攻击年度庆典（图中情景 2，用橙色表示）。在完全展开后，事件树可以包含多达 120 种情景（三个可能的敌对方×两种材料×四种类型的装置×五种潜在目标）。然而，在排除不切实际的组合后（例如，大型伽马源不适合用于建造简易核装置，人们认为简易核装置不会造成食物和水污染），风险模型中前后一致的情景减少到 36。风险评估是通过评估每种情景的可能性，并在情景发生后通过评估后果完成。附录二评估了后果，相关后果评估见附录二表 4。就风险评估而言，标准化的后果评级可以用于估计后果。



注：在示例事件树中，可能获取两类材料，一个是大型来源（第 1 类来源[18]）和大量核材料（SQ of NM）。IND — 简易核装置；RDD — 放射性散布装置；RED — 辐射辐照装置。

图 8. 突出显示两种情景的事件树示例。

可能性评估

III.4. 评估情景的可能性通过评估每一种情景要素的可能性完成（考虑有关的相关性）。图 8 列出了示例国家的一些可能性评估示例。图中所述的可能性评估是指事件树中每个级别的相对可能性。换句话说，对于事件树中一个级别中的既定替代方案而言，可能性值评估用于评估下一个级别的替代方案的相对可能性。这类评估值可以从主题专家那里获取，完整的风险评估应该包含不确定性分布。需要特别注意的是，只有事件树的可能分支才具有可能性。在图 8 中，23 项评估足以确定所有情景的可能性。

风险评估

III.5. 情景风险的评估方式为：计算情景可能性，再乘以后果评级值（标准化后果评级，见附录二表 4）。在本示例中，可以使用电子表格自动完成所有情景扩展和计算。但是，表 9 中的示例显示了图 8 中两项突出情景的计算方式。

表 9. 两种情景的风险计算方式示例

情景 1：国际团体获取了大量核材料，并在首都部署了一个简易核装置		
可能性 =	0.3 × 0.005 × 0.8 × 0.7	= 0.000 84
情景风险 [a] =	0.000 84 × 100	= 0.084
情景 2：国内团体获取大型放射源，并在庆典上部署了一个放射性散布装置		
可能性 =	0.5 × 0.99 × 0.8 × 0.25	= 0.099
情景风险 =	0.099 × 0.83	= 0.082

注：IND — 简易核装置；RDD — 放射性散布装置；SQ of NM — 大量核材料。

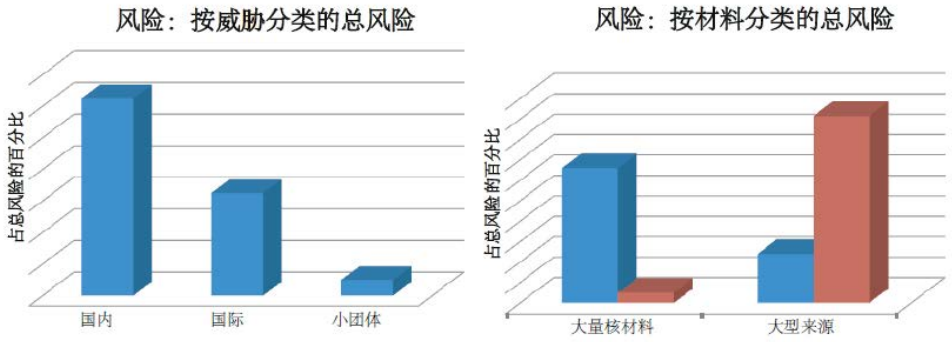
[a] 情景风险 = 可能性 × 标准化的后果评级。见附录二表 4。

III.6. 情景 1 是在首都部署的简易核装置。情景 2 是在年度庆典上部署的放射性散布装置。情景 2 的评估可能性约为情景 1 的 100 倍（0.099 比 0.00084），情景 1 导致后果约为情景 2 的 100 倍（100 比 0.83）。相对可能性的差额与后果的差额相互抵消，这两种情景的风险大致相同。因此，风险值可用于情景之间的比较，而不是风险的大约绝对值。

III.7. 情景 1 和情景 2 介绍了关于两种特定情景计算方式的详细信息。总体风险评估中的情形非常多，通常不可能单独检查每种情景。相反，情景可以按照特征（例如，相同的敌对方或相同的材料）进行分组。选取风险的特定方面（例如，敌对方或目标），检查与特定威胁团体或目标相关联的所有情景的风险总和，从而有效描述风险。在本示例中，图 9 显示了两种这类描述。应该注意的是，在本示例中，简易核装置和放射性散布装置的各种情景具有大致相同的风险，但在考虑所有情景后，简易核装置的风险将远大于放射性散布装置风险。

III.8. 左图显示了国内、国际和小型敌对团体的风险。在此情况下，国内团体的风险最大，小型团体的风险最小。右图显示了风险评估中两种材料类型的风险和可

能性之间的差异。每对蓝色条代表风险。在图中，大量核材料的风险更大。每对棕色条代表使用该材料的情景的可能性。大型来源的可能性更高。风险与可能性之间的差额即为后果。其他装置可以使用大型来源，但是简易核装置中必须包含核材料。然而，简易核装置有可能导致更严重的后果（根据本概念性示例评估），因此后果的差额大于可能性的差额。对可能性、后果和风险之间相互作用的了解是风险评估的重要部分。



注：蓝色条代表风险。棕色条代表使用该材料的情景的可能性。SQ of NM — 大量核材料。

图 9. 风险描述的两个示例。

III.9. 了解风险的另一个关键因素是显示评估的不确定性。图 10 显示了潜在目标位置的不确定性风险图表示例。除了平均风险（用每个目标的颜色条表示）之外，图表还用一条线表示每个目标的风险评估的不确定性。每个目标的线条顶端和底端分别代表不确定性分布的 95%和 5%，通常用蒙特卡罗法计算不确定性概率的分布。在本图表中，分析员可以识别风险的重大区别。例如，首都的风险显然比任何其他目标大；然而，旅游城市和年度庆典的不确定性分布有重叠。

III.10.因此，在风险评估中，了解不确定性对结果的影响至关重要。在一些具有较大不确定性的评估中，可能难以可靠区分高平均值和低平均值的风险。在很多情况下，只有异常值（最高和最低风险）可以清楚区分出来，而且很多风险的级别类似。仅使用风险的平均值往往会使风险评估看起来更为准确，因此可能会产生误导。这些图表可以帮助风险分析员完成风险评估，并将风险传达给决策者。

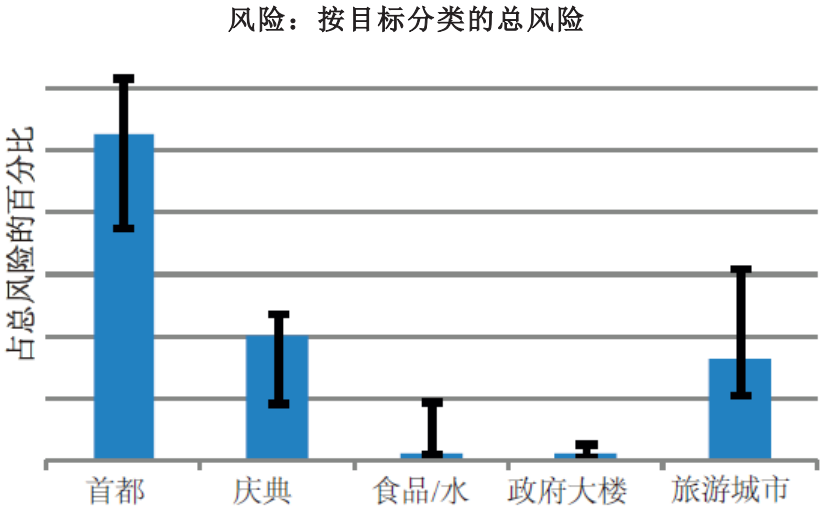


图 10. 包含不确定性区间的风险图示例。

附 录 四

风险知情方案示例

IV.1. 下列示例展示了通过威胁和风险评估的输入和输出（分别见附录二和附录三）将威胁和风险评估的结果作为风险知情方案的组成部分。本附录重点介绍了风险知情方案循环的后半部分：替代方案的分析和选择，所选择系统和措施的实施以及计划的持续管理（包括更新威胁评估，评估已实施的核安保系统和措施的有效性）。

识别、确定优先级别和实施

IV.2. 在完成附录三描述的风险评估之后，有关主管部门（负责威胁和风险评估的主管部门以及负责不同目标安保的主管部门）可以识别可能采取的系统和措施，从而降低与核安保相关的行为风险。在某些情况下，只能对一项措施进行评估；在其他情况下，可以对多种替代措施进行评估。表 10 列出了拟评估的可能系统和措施。对于每个系统或每项措施而言，主管部门应当评估降低系统或措施预期实现的核安保事件可能性的减少量以及落实系统或措施的成本。

IV.3. 这些系统和措施应当同时进行单独评估和组合评估，以识别每一种支出级别的风险减少量。图 11 显示了成本效益分析的图表（效益被定义为风险减少量）。表 10 中每一个点均表示各个目标地点的一个安保选项（即一组可能的系统和测量）。这些框代表可能一次性实施的一组选定选项，以通过最佳方式改善安保。蓝线代表提供每单位成本最低风险的安保选项（标记为“最佳安保选项”）。

表 10. 示例国家的潜在核安保系统和措施

目标位置	系统或测量选项	说 明
首都	基准线	首都当当前的能力
	增加警力	增加首都的巡逻警察人数
	增加传感器	购买并在首都周围部署辐射探测器
旅游城市	基准线	旅游城市的现有能力
	加强程序	开展培训，提供支持能力供旅游城市的警务人员分辨和识别核安保威胁
政府大楼	基准线	政府大楼当前的能力
	增加物理保护	改进保护建筑物的物理屏障（锁具、入口系统、门窗和混凝土屏障）
	安保系统	安装带门窗报警、辐射检测和视频监视器的安保系统
国庆节庆典	基准线	当前保护庆典的能力
	周边安保	通过设置障碍改善周边安保，确保人们通过需要进行检测的狭口进入区域
	加强程序	开展认识情况通报，并为警务人员提供能够识别核安保威胁的追溯能力
	加强巡逻	在庆典活动期间，增加安保人员的数量，降低巡逻的可预测性
食物和水	基准线	食品加工厂和水系统当前的能力
	加强监测	监测特定的食物和水样

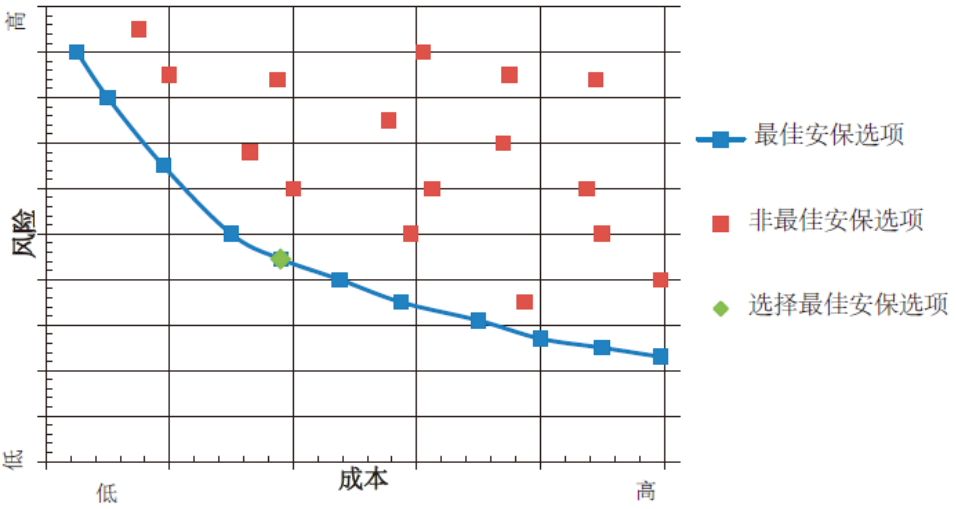


图 11. 显示安保选项和所选选项的成本效益分析图。

IV.4. 由于示例国家在实施前四个方案后可以大幅降低风险，主管部门同意在图表所示的那个点落实最佳选项（标记为选择的选项）。该选项包含以下改进措施：增加首都的警力，强化旅游城市的防护措施，在周年庆典现场周边建立安保边界。应该注意的是，除了降低风险之外，其他因素也可能会影响决策。但是，在这一简单示例中，选项中只包括了降低风险的因素。

风险管理

IV.5. 示例国家在所选择的选项中实施了四组系统和措施，并采用最佳方法进行计划管理和系统部署。作为管理方案的一部分，年度庆祝活动的周边能力应当在类似的小型公共活动中进行演练，并修改流程以应对演练中出现的事件和问题。在年度庆典上部署修改后的周边能力和流程。在首都招聘和训练额外警力。虽然无法直接衡量新资产在应对有核安保影响的潜在行为时的潜在表现（由于其稀缺性），但可以衡量犯罪的减少情况，并将其作为防止具有核安保影响的行为能力的一项替代指标。此外，还应当创建装置模型，以此作为未公布的练习以测试执法机构的意识，并评估执法机构检测和阻止潜在行为的能力。最后，在实施之后为旅游城市开发新流程，并评估对游客和当地居民的影响。

IV.6. 威胁和风险评估的主管部门通过监测示例国家内的活动保持对脱离监控的潜在材料的意识，并向非法贩卖数据库和国际刑警组织警报系统报告。威胁评估应当定期更新关于不同敌对方意图和能力的新信息。在更新威胁评估时，风险评估也会更新。更新后的风险评估由主管部门按照“按需知密”的原则在示例国家政府内部进行通报。示例国家应当根据预算和采购周期演练整个风险管理过程，从而不断提高示例国家应对脱离监控材料相关的具有核安保影响的行为的能力。

参考文献

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

[2] International Convention for the Suppression of Acts of Nuclear Terrorism, Resolution A/RES/59/290, United Nations, New York (2005).

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

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

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

[6] 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 CRIMES, 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).

[7] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Risk Management: Principles and Guidelines, ISO 31000:2009, ISO, Geneva (2009).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).

[9] EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CRIMINAL POLICE ORGANIZATION, WORLD CUSTOMS ORGANIZATION, Combating Illicit Trafficking in Nuclear and other Radioactive Material, IAEA Nuclear Security Series No. 6, IAEA, Vienna (2007).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Systems and Measures for the Detection of Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 21, IAEA, Vienna (2013).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, Radiological Crime Scene Management, IAEA Nuclear Security Series No. 22-G, IAEA, Vienna (2014).

[13] STOIBER, C., CHERF, A., TONHAUSER, W., DE LOURDES VEZ CARMONA, M., Handbook on Nuclear Law: Implementing Legislation, IAEA, Vienna (2010).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Incident and Trafficking Database (ITDB): Incidents of nuclear and other radioactive material out of regulatory control, 2014 Fact Sheet (2014), http://www-ns.iaea.org/downloads/security/itdb-fact-sheet.pdf

[15] INTERNATIONAL CRIMINAL POLICE ORGANIZATION—INTERPOL, Guidelines on Criminal Intelligence Analysis, Version 4 (LEJEUNE, P., MASON-PONTING, J., Eds), Criminal Analysis Sub-Directorate, INTERPOL General Secretariat, Lyon (2002).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-3, IAEA, Vienna (2010).

[17] KEENEY, R.L., VON WINTERFELDT, D., Eliciting probabilities from experts in complex technical problems, IEEE Trans. Eng. Manage. **38** 3 (1991) 191–201.

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Categorization of Radioactive Sources, IAEA Safety Standards Series No. RS-G-1.9, IAEA, Vienna (2005).

[19] LAW, A., Simulation Modeling and Analysis, 4th edn, McGraw-Hill, New York (2006).

[20] METROPOLIS, N., ULAM, S., The Monte Carlo Method, J. Am. Stat. Assoc. **44** 247 (1949) 335–341.

术语表

相关活动：持有、生产、加工、使用、贮存、处理、处置或运输核材料或其他放射性物质。

相关设施：生产、加工、使用、处理、贮存或处置核材料或其他放射性物质且需要批准的设施，包括相关建筑物和装置。

授权：主管部门授予运行相关设施或开展相关活动的书面许可，或授予这类许可的文件。

主管部门：由成员国指定的、履行一项或多项核安保职能的政府组织或机构。主管部门包括监管机构、执法机构、海关和边防机构、情报和安保机构以及卫生机构。

分级法：采取与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的犯罪行为或未经授权故意行为或国家确定的对核安保具有不利影响的其他行为的潜在后果相称的核安保措施。

简易核装置（IND）：包含有放射性物质的装置，旨在形成核当量反应。此类装置可能是通过非常简易的方式制造的，也可能是对核武器的简易改装。

核材料：《国际原子能机构规约》第二十条所定义的任何特殊可裂变材料或原材料。

核安保事件：对核安保具有潜在或实际影响而必须加以处理的事件。

核安保措施：旨在防止核安保威胁演变为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的犯罪行为或故意的未经授权的行为或探测或应对核安保事件的措施。

核安保系统：一套综合性的核安保措施。

核安保威胁：具有实施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的犯罪行为或未经授权故意行为或国家确定的对核安保具有不利影响的其他行为的动机、意图和能力的个人或团伙。

其他放射性物质：不属于核材料的任何放射性物质。

脱离监控：见“监控”。

辐射辐照装置（RED）：含有放射性物质的装置，旨在特意将公众遭受辐射。

放射性物质：根据国家法律、法规或监管机构规定，由于其放射性而需接受监管控制的物质。在国家没有作此指定的情况下，放射性物质系最新版“国际基本安全标准”[1]要求保护的任何物质。

放射性散布装置（RDD）：采用常规爆炸物或其他手段扩散放射性物质的装置。

监控：任何主管部门按照有关安全、安保或保障的法律和监管规定的要求对核材料或其他放射性物质、相关设施或相关活动实施的任何形式的制度性控制。“脱离监控”一词用于描述这样一种情况，即达到足够数量就应该置于监控之下，但是却没有实施监控的核材料或其他放射性物质，其原因要么是因为某种缘故没有监控败，要么是从未监控。

风险：根据核安保事件的概率及相关后果确定的核安保事件造成不良后果的潜在可能性。

风险评估：系统性识别、评估、分析和评价危险，并据此确定优先级别、制订或比较行动过程并做出决策的整个过程。

战略位置：对一国具有高度安保利益而被作为利用核材料或其他放射性物质进行恐怖袭击的潜在目标的场所，或已发现的脱离监控的核材料或其他放射性物质的场所。

威胁评估：根据可利用情报、执法信息和公开来源信息对威胁所作的评价，内容是描述这种威胁的动机、意图和能力。

薄弱性：导致实体、资产、系统、网络、设施、活动或地理区域可能被利用或容易受到威胁的物理特征或操作属性。

薄弱性评估：评价某个特定目标的整个安保系统的特性和有效性，并将评价形成文件的过程。

---

[1] 欧洲联盟委员会、联合国粮食及农业组织、国际原子能机构、国际劳工组织、经济合作与发展组织核能机构、泛美卫生组织、联合国环境规划署、世界卫生组织，《国际辐射防护和辐射源安全的基本安全标准》，国际原子能机构《安全标准丛书》编号：GSR第3部分，国际原子能机构，维也纳（2014年）。

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我们的主要经销商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。

定价出版物订单

请联系您当地的首选供应商或我们的主要经销商：

Eurospan
1 Bedford Row
London WC1R 4BU
United Kingdom

交易订单和查询：
电话：+44 (0) 1235 465576
电子信箱：trade.orders@marston.co.uk

个人订单：
电话：+44 (0) 1235 465577
电子信箱：direct.orders@marston.co.uk
网址：www.eurospanbookstore.com/iaea

欲了解更多信息：
电话：+44 (0) 207 240 0856
电子信箱：info@eurospan.co.uk
网址：www.eurospan.co.uk

定价和未定价出版物的订单均可直接发送至：

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

所有国家都已经公认，需要严正关注核恐怖主义威胁问题。核材料或其他放射性物质可能用于犯罪行为，这一风险将对国家和国际安全造成严重威胁，并且可能为人员、财产和环境带来严重后果。本实施导则介绍了规划、设计和实施脱离监控的核材料和其他放射性物质核安保措施的风险知情方案的概念和方法。

国际原子能机构
维也纳