IAEA BULLETIN
国际原子能机构通报
国际原子能机构旗舰出版物 | 2023年6月 | www.iaea.org/bulletin

核世界中的计算机安全

《国际原子能机构通报》

主办单位

国际原子能机构

新闻和宣传办公室

地　　址：维也纳国际中心
PO Box 100, 1400 Vienna, Austria

电　　话：(43-1) 2600-0

电子信箱：iaeabulletin@iaea.org

执行编辑：Emma Midgley

设计制作：Ritu Kenn

《国际原子能机构通报》可通过以下网址在线获得：

www.iaea.org/bulletin

封　　面：
（图/Adobestock.com）

请关注我们

IAEA

国际原子能机构（原子能机构）的使命是防止核武器扩散和帮助所有国家特别是发展中国家从核科学技术的和平、安全和可靠利用中受益。

1957年作为联合国下的一个自治机构成立的原子能机构是联合国系统内唯一拥有核技术专门知识的组织。原子能机构独特的专业实验室帮助向原子能机构成员国传播人体健康、粮食、水、工业和环境等领域的知识和专门技术。

原子能机构还作为加强核安保的全球平台。原子能机构编制了有关核安保的国际协商一致导则出版物《核安保丛书》。原子能机构的工作还侧重于协助最大限度地减少核材料和其他放射性物质落入恐怖分子和犯罪分子手中或核设施遭受恶意行为的风险。

原子能机构安全标准提供确保核安全的基本安全原则、要求和建议，并反映国际社会就构成保护人和环境免受电离辐射有害影响所需的高度安全达成的协商一致。这些原子能机构安全标准的制定针对服务于和平目的的各种核设施和核活动，以及减少现有辐射风险的防护行动。

原子能机构还通过其视察体系核查成员国根据《不扩散核武器条约》以及其他防扩散协定履行其将核材料和核设施仅用于和平目的的承诺情况。

原子能机构的工作具有多面性，涉及国家、地区和国际各个层面的广泛伙伴的参与。原子能机构的计划和预算通过其决策机关——由35名理事组成的理事会和由所有成员国组成的大会——的决定来制订。

原子能机构总部设在维也纳国际中心。外地办事处和联络处设在日内瓦、纽约、东京和多伦多。原子能机构在摩纳哥、塞伯斯多夫和维也纳运营着科学实验室。此外，原子能机构还向设在意大利的里雅斯特的阿布杜斯·萨拉姆国际理论物理中心提供支持和资金。

计算机安全在核安保和核安全中的重要作用

文/国际原子能机构总干事拉斐尔·马里亚诺·格罗西

数字化创新的发展速度令人震惊，甚至在过去几个月的时间里，人工智能等技术就取得了颠覆性进展。这些进展将有助于我们改进核设施的数控操作和自动化技术，其潜在好处包括提高运行效率、降低人工成本以及提高安全和安保。

先进核反应堆设计，如小型模块堆和微型反应堆，已包括使用人工智能和机器学习计划，以实现自动化、远程监控和维护以及共享控制室等创新功能。但人工智能和机器学习等数字化创新也构成了威胁，因此需要时刻保持警惕，以确保敏感资产的完整性，并保护核设施和辐射设施的信息。

虽然闸门和警卫一直被用来确保核设施免遭破坏或恶意行为，但今天我们越来越依赖数字系统。核设施仪器仪表和控制系统用于关键安全和安保应用，这提高了效率，但也意味着我们必须特别警惕地保护这些计算机系统。世界各国都认识到这是一个优先事项。

原子能机构在促进各国之间的合作以及在采用快速发展的技术促成技术专门知识和最佳实践的分享方面发挥着独特的作用。与此同时，我们就如何最大限度地减少和减轻伴随而来影响计算机安全的潜在漏洞向各国提供建议。仅在过去两年中，我们的全球计算机安全援助活动就增加了四分之一以上，特别侧重于在国家一级对计算机安全条例/检查和计算机安全演习的支持。

原子能机构一直在通过一系列活动应对成员国的核安保挑战，包括提供导则文件和培训，使成员国能够制定强有力的国家信息和计算机安全计划。这些导则还在开展国际实物保护咨询服务期间被用作评价一国信息和计算机安全计划的基准。

此外，我们正在启动一个短训班，旨在对专家进行起草计算机安全条例培训。不久，随着在线虚拟学习平台的推出，更多的国家将能够获得原子能机构计算机安全培训课程。

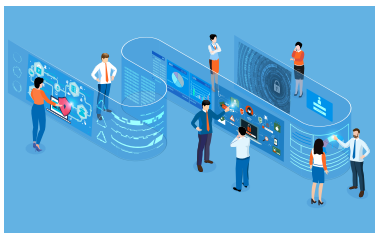
与此同时，原子能机构支持在国家和地区层面开展计算机安全演习，以提高人们对网络攻击威胁及其对核安保潜在影响的认识。我们促进国际专家和决策者之间的合作，并促进相关研究。

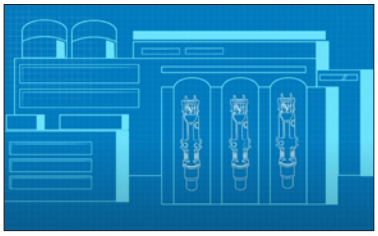
随着包括中低收入国家在内的各国越来越多地利用核技术来满足优先事项，包括清洁能源、癌症护理、营养和研究等方面的优先事项，原子能机构的计算机安全活动势必会增加。

在原子能机构“核世界中的计算机安全：安保促安全”国际会议上，我们将共同讨论关键问题和解决方案，并规划未来发展道路，使核行业能够充分利用数字化创新，同时领先一步防止一些人利用数字化创新制造危害。

“随着包括中低收入国家在内的各国越来越多地利用核技术来满足优先事项，包括清洁能源、癌症护理、营养和研究等方面的优先事项，原子能机构的计算机安全活动势必会增加。”

—国际原子能机构总干事拉斐尔·马里亚诺·格罗西





问答

世界观点

国际原子能机构最新动态

应对计算机安全威胁

国际原子能机构援助计划的演变

文/Vasiliki Tafili

数字网络化社会是指日常活动借助计算机化系统、人工智能和数字技术相互关联，而向数字网络化社会的转变正在对核安全和核安保产生巨大影响。数字技术在维护处理核材料或其他放射性物质设施的安全和安保功能方面的重要作用怎么强调都不过分。

“计算机化系统和数字技术对于使用核材料和其他放射性物质的设施和相关活动至关重要，”原子能机构核安保司司长Elena Buglova说，并强调，所有国家都需要实施计算机安全计划和加强核安保纵深防御。“随着技术的发展，保护敏感信息和资产的保密性、完整性和可用性需要时刻保持警惕，以防止和减少风险，并需要建立强大的信息和计算机安全计划。”

“和平利用核能，特别是发展核电计划，预计会大幅增加，因此必须将信息和计算机安全视为核安保的一个必要组成部分。”

—国际原子能机构核安保司司长Elena Buglova

2011年国际原子能机构大会第五十五届常会通过的一项核安保决议首次确定了处理计算机安全威胁、恶意网络攻击和数字技术可能带来的任何潜在漏洞的必要性，以及计算机安全对核安保的重要性。该决议注意到，国际原子能机构努力“提高对网络攻击日益严重的威胁及其对核安保的潜在影响的认识”，鼓励原子能机构制定适当的导则文件、提供培训课程，并主办更多专门针对核设施网络安全的专家会议，以协助各国保护自身免受网络攻击。

“作为2011年大会决议的后续行动，原子能机构活动侧重于提高国家和设施层面的计算机安全能力，”Buglova说，并表示，这些活动随后被纳入原子能机构后续的“核安保计划”，其中包括《2022–2025年核安保计划》概述的原子能机构计算机安全活动的当前实施细节。

国际原子能机构如何帮助各国建立或改善计算机安全?

建立健全和最新的计算机安全计划是保护各国各类关键基础设施免受网络攻击的关键要素。原子能机构一直灵活地向处于制定国家信息和计算机安全计划各个阶段的国家提供援助，包括提供导则文件和培训。

有四份原子能机构《核安保丛书》导则出版物和另外三份技术出版物提供了有关信息和计算机安全导则。该导则可用作制定国家计算机安全框架（包括国家战略）以及计算机安全条例和培训的基础。

这份原子能机构导则中的一项关键原则是通过保护信息和计算机化系统来维护核设施的关键功能，从而为设施和材料保持安全可靠的环境。具体实现方式包括：制定计算机安全计划（见第6页）、确定核安保功能、利用风险管理确定安保受损的潜在后果、确定敏感数字资产所需的计算机安全级别；以及在计算机安全方面实施分级方案和纵深防御概念。这些要素的设计和实施应能够防止破坏，有助于提高营运者检测和应对入侵的能力，并减轻网络攻击的潜在影响。

应各国的请求，原子能机构向广泛受众提供各种培训机会。这些受众包括主管部门、营运者、供应商和其他可能对实施计算机安全负

有责任的实体。他们还可以从开展计算机安全演习的专门知识中受益，开展计算机安全演习是原子能机构核安保计划的一部分。

此外，在原子能机构的“网络教育和培训网络学习平台”上，有四门关于计算机安全的电子学习课程可以免费获得，并有阿拉伯文、中文、英文、法文、俄文和西班牙文版本，可以通过注册或通过NUCLEUS帐户访问。一个创新的新虚拟化培训平台也将很快推出（见第12页）。

与此同时，原子能机构支持国家层面或地区层面的计算机安全演习，作为提高对网络攻击威胁及其对核安保潜在影响的认识工作的一部分。这些演习包括不同的情景，在这些情景中，敏感信息和计算机化系统被直接或间接作为攻击实物保护系统和电子系统的一部分（见第16页）。

研究是对原子能机构计算机安全活动的补充，主要是通过协调研究项目这一完善机制开展。近年来，为推进全球研究界在信息和计算机安全方面的努力，并提高应对新兴挑战和风险的准备工作，启动了多个协调研究项目（见第18页）。

未来会如何?

原子能机构核安保计算机安全计划在不断发展。小型模块堆和先进反应堆对先进技术和数字仪器仪表的依赖、人工智能的预期影响以及虚拟化学习环境的出现，给各国带来了挑战和需要扩大支持的领域（见第14页）。

“我们看到，各国、监管机构、营运者和其他利益相关方对核安全和核安保的潜在或实际影响的认识不断提高。”Buglova说，“和平利用核能，特别是发展核电计划，预计会大幅增加，因此必须将信息和计算机安全视为核安保的一个必要组成部分。”

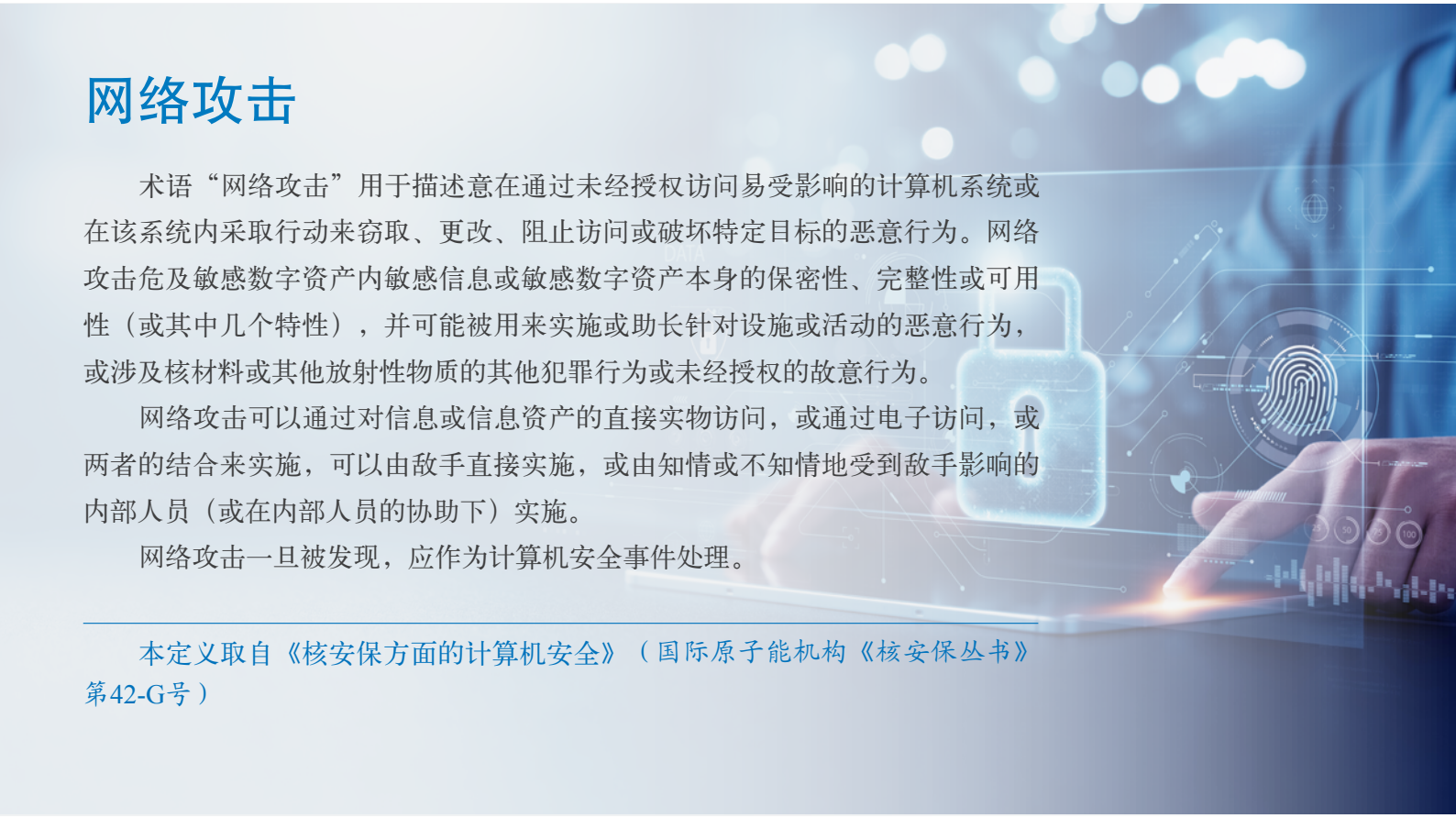
网络攻击

术语“网络攻击”用于描述意在通过未经授权访问易受影响的计算机系统或在该系统内采取行动来窃取、更改、阻止访问或破坏特定目标的恶意行为。网络攻击危及敏感数字资产内敏感信息或敏感数字资产本身的保密性、完整性或可用性（或其中几个特性），并可能被用来实施或助长针对设施或活动的恶意行为，或涉及核材料或其他放射性物质的其他犯罪行为或未经授权的故意行为。

网络攻击可以通过对信息或信息资产的直接实物访问，或通过电子访问，或两者的结合来实施，可以由敌手直接实施，或由知情或不知情地受到敌手影响的内部人员（或在内部人员的协助下）实施。

网络攻击一旦被发现，应作为计算机安全事件处理。

本定义取自《核安保方面的计算机安全》（国际原子能机构《核安保丛书》第42-G号）



如何制定计算机安全计划

文/Vasiliki Tafili 和Trent Nelson

处理核材料或其他放射性物质以及开展相关活动的设施是需要高度安全和安保的关键基础设施。通过对计算机安全采取全面和积极主动的方案，各组织可以保护这些设施中的敏感信息资产和计算机化系统不受损害。原子能机构建议的计算机安全方案的基础在于各国制定有关国家战略或政策的要求，并能够对实物保护、核安全以及核材料衡算和控制相关敏感信息和计算机系统进行保密和保护。这些要求也可以采取国家法规的形式，对制定和实施“计算机安全计划”*作出规定。

“计算机安全计划”是一个总体框架，包括实施计算机安全政策和程序有效计划的关键要素，计算机安全政策和程序将在核设施或放射源设施的整个寿期内采用。“计算机安全计划”的目的是保护敏感信息资产和对维护安全和安保功能至关重要的计算机化系统免受网络威胁，以减轻网络攻击的影响。

国家战略

全面而有效的计算机安全战略需要系统性方案，其中整合各种要素，包括维护国家核安保制度的法规、计划、安全保护措施和应急能力。

法规

有效的法规能为保护敏感计算机化系统提供法律框架，并确保各组织制定和适当实施“计算机安全计划”*。

“计算机安全计划”的关键要素：

作用和责任

具有问责制的组织作用和责任对于有效管理至关重要，特别是涉及关键基础设施的情况下。必须认识到组织层次结构以及权力划分和报告结构，以便在“计算机安全计划”内灌输高效和有效的协作和协同作用。

风险、脆弱性和合规管理

计算机安全风险管理涉及对敏感数字资产和计算机化系统的脆弱性和潜在后果的评价，利用分级方案实施计算机安全控制，抵御网络攻击。所采用的安保措施水平应与受保护的信息和（或）计算机化系统相关的风险水平相称。通过考虑脆弱性或威胁的后果，各组织可以确定减轻风险所需的安保措施水平。

安保设计和管理

计算机安全设计是防范网络威胁的一个关键方面。基本设计原则包括分级方案和纵深防御，即实施多层分区安保控制，以防止和减轻攻击。对安保的要求也必须纳入整个系统开发周期，包括通过明确的政策和协议约束第三方组织，以确保安保措施的一致性和有效性。

数字资产管理

计算机安全的有效性取决于通过系统的过程列出所有设施功能、资产和系统的全面清单，包括对保护核业务或保持核材料和其他放射性物质安全可靠使用至关重要的敏感数字资产。这类清单还要提供对组织支持访问控制、备份和其他安保措施至关重要的数据流和相互依赖关系，以保护这些资产免遭破坏或盗窃。

安保程序

执行的核安保政策和程序为防止盗窃、破坏或未经授权使用核材料和设施提供方向和责任。这些政策确保对敏感信息和资产的访问受到严格控制，并确保对有访问权限的个人进行适当的筛查和培训。

人员管理

诚信、意识和培训对核工业的人员管理至关重要。应进行诚信评价，以确保人员可靠、能够胜任，并且没有任何可能损害安全或安保的利益冲突。保持合格和值得信赖的人员对于确保核安全和核安保至关重要。

---

* 更多细节载于原子能机构《核安保丛书》第17-T（Rev.1）号《核设施的计算机安全技术》。

超越实物保护

国际实物保护咨询服务如何促进加强计算机安全

文/ Vasiliki Tafili

近三十年来，各国一直利用国际原子能机构的国际实物保护咨询服务提供咨询，以确保核电厂、医院放射治疗装置等使用核材料和其他放射性物质的各类设施的实物保护。然而，由于技术的进步，数字系统现已成为这些设施运营的核心，以致带来许多新的核安保挑战。

为了应对包括核设施在内的设施遭受网络攻击的实际威胁，2012年，关于实物保护的信息和计算机安全被纳入国际实物保护咨询服务范围。自那时起，各国越来越多地要求将这一模块作为国际实物保护咨询服务评审的一部分，以支持其应对网络安全威胁的工作。

国际实物保护咨询服务作为原子能机构核安保计划的核心组成部分，根据相关国际文书和原子能机构核安保导则审查一国的现有实践，并应请求，通过在执行国际法律文书方面提供建议，协助各国加强国家核安保制度、系统和措施。

“自首次开展国际实物保护咨询服务工作组访问以来的27年里，这项服务已发展到能够应对现代挑战和需求，”原子能机构核安保司材料和设施核安保处处长Heather Looney说，“缺乏计算机安全措施，就无法确保防止核材料和其他放射性物质遭到盗窃、破坏或未经授权使用。通过邀请开展国际实物保护咨询服务工作组访问，各国可以受益于关于哪些方面可以改进以及如何改进的建议，”她补充说。

国际实物保护咨询服务采用模块化方案，提供五个模块，涵盖以下内容：对核材料和核设施核安保制度的国家审查；对核设施安保系统和措施的审查；对材料运输安保的审查；对放射性物质、相关设施和活动安保的审查；以及对信息和计算机安全的审查。自1996年首次开展国际实物保护咨询服务评审以来，迄今共进行了97次这类评审，有22个国家已要求将信息和计算机安全模块纳入国际实物保护咨询服务评审中。

“缺乏计算机安全措施，就无法确保防止核材料和其他放射性物质遭到盗窃、破坏或未经授权使用。通过邀请开展国际实物保护咨询服务工作组访问，各国可以受益于关于哪些方面可以改进以及如何改进的建议。”

—国际原子能机构核安保司材料和设施核安保处处长Heather Looney

国家在信息和计算机安全评定期间应抱有怎样的预期？

作为第一步，由国际核安保专家组成的国际实物保护咨询服务工作组将审查与信息和计算机安全计划有关的国家政策是如何制定和管理的。然后，工作组将考察立法和监管框架，将国家现行程序和实践与《核材料实物保护公约》及其2005年修订案规定的义务以及原子能机构《核安保丛书》相关出版物提供的导则进行比较。通过这种方式，他们可以确定各国是否制定了必要的政策和程序，以实现关键核设施和辐射设施的充分计算机安全。

在设施层面，计算机安全审查将着眼于计算机安全管理、计算机安全计划（见第6页）、访问控制、防御性计算机安全架构以及对计算机安全事件的检测和响应。工作组还可能评估交叉领域，如风险管理、分级方案、核安保文化和人力资源管理。

日本分别在2015年和2018年接受了国际实物保护咨询服务工作组访问及其后续工作组访问。“对日本来

自1996年以来，国际原子能机构的国际实物保护咨询服务一直在协助各国确定加强核材料和核设施保护的方式。（图/国际原子能机构）

说，审查计算机安全措施现状并根据审查人员的建议推动加强计算机安全措施，这是一次宝贵的经验，”日本原子能规制局核安保处国际核安保主任Hiroyuki Sugawara说，“针对国际实物保护咨询服务的审查结果，我们决定加强计算机安全措施，并增加具有该领域专门知识的检查人员数量。此外，原子能规制局在国家威胁评定中纳入了计算机安全威胁，并要求许可证持有者采取强有力的计算机安全措施，以及通过纳入网络攻击防范对策来加强计算机安全计划内容。”

法国在2018年接受国际实物保护咨询服务工作组访问之后，在国家核安保框架中明显加强了计算机安全。“国际实物保护咨询服务工作组要求各利益相关方作出强有力的承诺，为法国巩固核安保制度和促进核安保制度的实施提供了机会，”能源转型部防卫和安全局核安保办公室计算机安全项目负责人Frédéric Boën说，“专门负责计算机安全的工作人员有所增加，并根据国际标准和原子能机构核安保导则制定了监管准则。”

自2016年以来，原子能机构一直在维护国际实物保护咨询服务良好实践数据库，以便与国际核安保界分享此类工作组访问的成果，从而增强原子能机构向世界各国提供援助的影响。Looney说：“维护这个数据库并分享这些实例，将使国际实物保护咨询服务工作组访问的好处从东道国扩展到了国际核安保界，并使原子能机构向成员国提供援助的影响成倍增加。”

大多数国家层面的良好实践涉及核安保管理，这为计算机安全和协调奠定了基础。此外，还有40项与国家和设施层面的计算机安全相关的良好实践，原子能机构成员国通过指定的联络点可获得这些良好实践。

原子能机构继续支持各国加强国家核安保制度，而各国对在2023年和2024年接受国际实物保护咨询服务工作组访问的需求仍然很高。

国际原子能机构协助非洲国家制定计算机安全条例

文/ Andrea Rahandini

随着越来越多的国家扩大和平利用核技术，非洲对放射性同位素的需求预计将在未来几年内增长。癌症发病率上升，加大了对放射治疗、放射学和核医学的需求。工业、农业和科学领域对核应用的依赖有所增加，因而需要提高研究堆放射性同位素产量。这些重要的反应堆基于计算机化系统运行，而计算机化系统可能容易受到网络攻击。与核电厂一样，研究堆也需要防止、减轻和应对潜在恶意攻击的类似保护计划。保护所有类型的核设施免受这种潜在攻击是在非洲安全可靠地使用核技术的一个基本要素。

“这次培训班有助于我们制定和实施计算机安全计划，从而保护设施的敏感信息以及容易受到网络攻击的敏感数字资产。”

—埃及原子能管理局放射性同位素生产设施计算机工程师Nadia M. Nawwar

为应对这些威胁，非洲许多国家正在学习埃及、加纳和尼日利亚的经验，这三个国家都拥有并运营着一座核研究堆。在原子能机构的支持下，这三个国家正在制定和加强计算机安全条例，并实施计划，以妥善保护其设施免遭可能对设施核安全和核安保产生影响的恶意计算机行为。

“随着数字技术和计算机化系统被纳入核材料和其他放射性物质设施和业务的核安全、核安保以及运行方面，计算机安全变得越来越重要，”原子能机构核安保司高级信息和计算机安全官员Trent Nelson说，“原子能机构与非洲国家合作，制定、审查和加强计算机安全条例。”

在埃及，原子能机构与埃及核和辐射监管局合作，审查现有计算机安全条例，并解决监管方面的潜在差距。2022年，组织了一次国家培训班，旨在发展国家对核设施进行计算机安全检查的能力。这次培训班利用原子能机构核安保导则和检查人员可用的技术，为学员们更好地评估核设施和辐射设施计算机安全的有效性提供了知识和实践经验。

埃及原子能管理局放射性同位素生产设施计算机工程师Nadia M. Nawwar是参加这次培训班的22名学员之一。她说：“我了解到监管机构如何进行计算机安全检查以及营运者需要做出的必要计算机安全安排。自从参加了这次培训班，我们能够更有效地审查和验证计算机安全条例要素。这次培训班有助于我们制定和实施计算机安全计划，从而保护设施的敏感信息以及容易受到网络攻击的敏感数字资产。”

在加纳，原子能机构于2023年4月进行了一次专家工作组访问，以评定加纳核监管局目前的国家计算机安全条例和检查计划。

“加纳计算机安全的发展带来了一些挑战，包括当地缺乏这方面技术知识、如何整合法律问题与技术专门知识，以及如何管理所需的资源，”加纳核监管局核网络安全处处长Nelson Kodzotse Agbemava说，“在制定条例过程中，我们向原子能机构和其他国家寻求了专家评审支持，以确保对计

算机安全采取全面和系统的方案。”

同样，原子能机构在2022年10月对尼日利亚进行了一次专家工作组访问。“2019年，原子能机构牵头对我国进行了‘核安保综合支助计划’评审，确定了建立有效的计算机安全立法和监管框架的必要性，”尼日利亚核监管局首席监管官Ethel Ofoegbu说，“因此，原子能机构评价了国家计算机安全条例，找出了差距，以及提供了必要的建议。其中一项成果是制定了尼日利亚核设施和辐射设施及活动的计算机安全条例草案。”目前，尼日利亚正在审查该条例草案，并计划举办一次关于计算机检查的培训班。

考虑到各国提出的援助请求越来越多，原子能机构正在编制一份协助各国制定计算机安全条例关键要素的技术文件。原子能机构还将在2023年8月启动原子能机构计算机安全条例要素起草短训班时，随时准备协助更多国家起草计算机安全领域条例。这种短训班的目的是同时协助多个国家制定其国家特定的计算机安全条例，而不是由原子能机构逐一协助每个国家。在8月举办首次讲习班之后，这种短训班将在所有地区每半年举办一次。参加者将有机会共同起草其国家计算机安全战略，这是强有力的计算机安全计划的监管基础。

国际原子能机构计算机安全条例要素起草短训班将于2023年8月推出，旨在协助各国制定国家计算机安全条例。

核设施和辐射设施的虚拟计算机安全培训创新

文/ Anjarika Strohal

当今无处不在、不断增加的数字技术趋势正在迅速而显著地改变我们的生活。今天的关键基础设施，包括核电和其他和平利用核技术的基础设施，严重依赖数字技术才能顺利可靠地运行。人工智能等快速发展的新技术有望解决问题和改善数控操作，将可能有助于改善核应用。因此，目前先进反应堆设计正在采用和考虑这些技术。

不幸的是，虽然这些数字技术确实带来了许多好处，但它们也可能引入许多潜在的未知漏洞。这是因为网络入侵或对核设施的恶意网络攻击的威胁始终存在，可能会利用这些相同的技术。

由于日益复杂的网络攻击数量之大和范围广泛，核工业迫切需要进行核设施和辐射设施的计算机安全培训。为了帮助满足这一需求，原子能机构开发了一系列培训课程，所涉专题从计算机安全基础知识到更先进的仪控系统计算机安全不一而足。

在提供这些以实际操作体验式学习为特点的定制、高端和复杂的培训课程过程中，原子能机构发现需要一个简单的在线平台，以使课程标准化，并允许培训实体更广泛和更普遍地使用这些课程，而无需原子能机构现场协助。新冠肺炎疫情的旅行限制和虚拟技术的广泛使用，进一步凸显了这一需求，并加速了该平台的发展。

这个虚拟培训工具被称为“学习者”，旨在通过提供培训材料和在虚拟环境中体验实际操作练习，为核能界提供灵活、有吸引力的计算机安全培训课程。参与者只需要一台电脑和可靠的互联网连接，就可以获得所有必要的课程材料。“新平台有望在提高计算机安全意识和核安保培训、建立更强大的专家群体以及帮助加强核设施和放射性物质相关设施的安全和安保方面发挥关键作用。”原子能机构核安保司司长Elena Buglova表示。

自2023年6月起，原子能机构将在全球范围内提供“学习者”平台，以加强核设施以及放射源设施和活动的计算机安全。

计算机安全培训
和其他活动

奥地利技术研究所作为原子能机构核安保信息和计算机安全协作中心，与原子能机构合作创建了“学习者”平台。

“虚拟学习环境通过支持各种培训目的，为提高操作能力和战略能力提供了极大价值。”奥地利技术研究所数字安全和安保中心负责人Helmut Leopold说，“通过模拟真实环境，该平台使学习者能够获得对有效核安保管理至关重要的实际技能和经验。”

通过学习来加强计算机安全

原子能机构“学习者”平台可应请求提供，以加强核安保培训。平台设计用户友好，方便国际受众，提供多语种支持。平台有各种功能，如指导性练习、即时反馈、专题介绍精选和多屏幕支持。这些特性使平台适应性强，可供培训机构和直接用户使用。

“学习者”被设计成一个用来开发、提供和使用交互式模拟环境的平台，使用开源技术构建。其他模块包括计算平台、基础设施供应和软件供应的标准化方案，从而便于与原子能机构现有的培训提供者和打算使用该平台的其他组织之间的分享和知识交流。

已根据原子能机构关于计算机安全的核安保导则，按六个主题领域创建和组织了12项实际操作练习。Buglova补充说：“通过使用代表真实设施的虚拟化环境，‘学习者’平台加强了实用技能的发展，支持更公平地获取知识和技能。”

“学习者”平台是原子能机构提高认识、加强合作以及向各国提供支持以应对核行业日益严重的网络安全威胁工作的一个方面。在过去五年中，已向120多个国家提供了能力建设活动。此外，通过专家工作组访问；国家、地区和国际培训班；技术会议和网络研讨会提供的有针对性支持，促进了积极协作、知识共享和技能发展。此外，原子能机构支持各国组织大规模的网络安全演习。

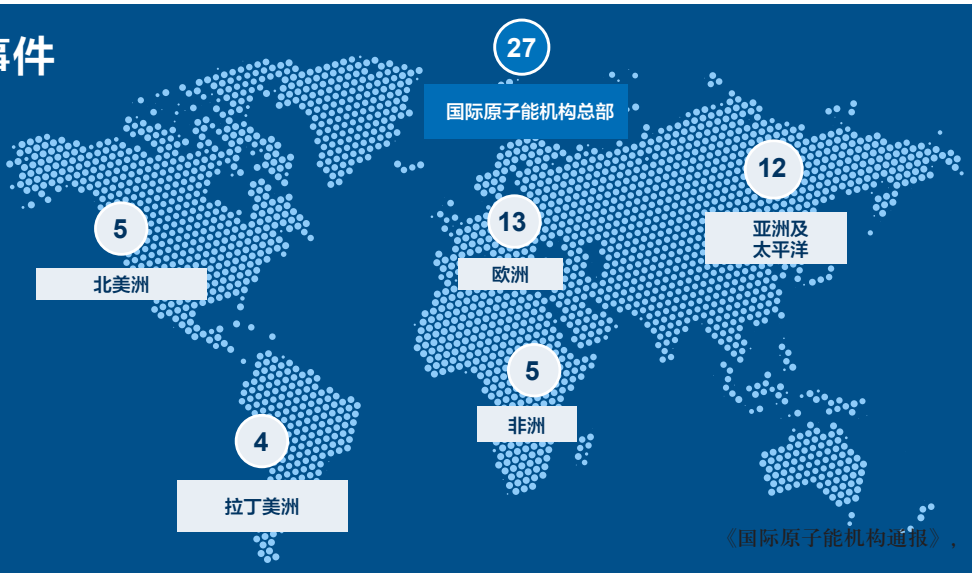
实际操作培训和示范中心

展望未来，继续投资于此类能力建设举措以确保全球核安保达到最高标准，这一点至关重要。原子能机构最先进的核安保培训和示范中心将于2023年下半年启用，通过实际操作培训经验以帮助加强各国应对核恐怖主义的能力。核安保培训和示范中心提供的创新培训课程将包括与计算机安全有关的主题，并将包括可能针对核设施或放射源设施和活动的网络攻击情景。

“通过模拟真实环境，该平台使学习者能够获得对有效核安保管理至关重要的实际技能和经验。”

—奥地利技术研究所数字安全和安保中心负责人Helmut Leopold

按地区分列的事件



人工智能将如何改变核世界中的信息和计算机安全

文/ Mitchell Hewes

人工智能和机器学习技术有可能会彻底改变世界，通过改变我们创造、消费和使用信息的方式，迎来前所未有的进步和创新。随着人工智能技术变得越来越复杂，它们将改变行业、简化流程，甚至可能影响我们的生活方式。核行业也不例外，在核设施和辐射设施的许多流程和操作中，可以预期人工智能会带来好处。

与此同时，人工智能的快速发展也带来了大量风险。恶意行为者可能利用人工智能发起更先进、更有针对性的攻击，或利用人工智能破坏核设施和辐射设施中的网络、系统和敏感信息的完整性。

“它不会取代工作人员，而是建立资源和增加洞察能力，使早期检测和应对计算机安全问题切实可行。”

—美国佐治亚理工学院助理教授Fan Zhang

对信息和计算机安全的好处

原子能机构正在为人工智能带来的变革做准备，促进该领域的国际合作，以确保所有国家能够受益于各种机会，同时也在为减轻风险作准备。原子能机构正在通过技术会议和协调研究项目等机制，支持对人工智能技术的开发、认识和应用，以及对抗恶意行为者的对策和防御。

也许人工智能在信息和计算机安全方面最显著的优势是减少对人为分析和干预的依赖。人工智能赋能系统可以全天候运行，以监测网络和系统的威胁。通过使这些任务自动化，核安保专业人员便有时间专注于更具战略性的任务，并在事件发生时更有效地应对。

“人工智能可以快速识别威胁，并自动向人类专家提供协调响应活动所需的信息，这种自适应学习能力可以用来增强信息和计算机安全，”参加原子能机构旨在支持加强计算机安全研究协调研究项目的美国佐治亚理工学院助理教授Fan Zhang说，“它不会取代工作人员，而是建立资源和增加洞察能力，使早期检测和应对计算机安全问题切实可行。”

通过利用先进的机器学习算法，人工智能还可以通过识别计算机系统中的异常数据，帮助核设施和辐射设施加强对网络攻击的防御。人工智能辅助安保系统可以持续监测和分析大量数据，以确定是否存在与设施正常运行不符的活动。网络攻击可能会提供虚假数据，恶意误导核设施操作人员。在这种情况下，人工智能辅助系统可以用来提醒核电厂操作人员，即使是与正常运行有最微小变化也会发出警报。通过提高态势感知能力，人工智能还可以及早发现犯罪行为，并提示作出必要的事件响应。

面对的挑战

人工智能在核设施和辐射设施中提供的好处在很大程度上取决于人工智能的训练方式。人工智能的智能程度取决于它所使用的训练数据，如果没有正确的输入，人工智能可能会被操纵，从而给出错误的读数和结果。这仍是将人工智能用于核安保的一个重大障碍。即使人工智能技术最近取得了进步，用它来替代人力也是不可行的。实物保护、材料衡算和控制以及直接测量这些确保核安保的基本活动，需要人力投入。

理解人工智能模型如何以及为何作出某一决定或预测，是人工智能在核安保方面的另一个挑战。“透明度和可解释性是人类可理解人工智能所作决定或预测背后的推理，两者均属于人工智能模型的最重要问题。理解这些模型如何得出结论往往具有挑战性，这使得人们很难信任和确保其输出的完整性，”原子能机构核安保司信息管理处处长Scott Purvis说，“当这些模型取代提供直接测量的传感器并取代根据每个设施的独特特征获得的人类经验时，尤其会出现问题。除非事先对人工智能算法有全面深入的了解，认识到所作决定的方式和原因，否则不可能对系统的完整性进行任何保证。”

原子能机构关于核安保方面的计算机安全导则包括人类制衡的最佳实践，以指导设施意识到哪些过程可以通过人工智能实现自动化，哪些过程至少在这种快速发展的新技术的风险为人们所认知之前，应继续采取人为监督。它们还提供一种重要资源，使各国能够落实重要的计算机安全措施，以检测、预防和应对网络攻击。

此外，原子能机构还制定了一个协调研究项目，以支持加强计算机安全研究。题为“加强核设施计算机安全事件分析”的这项协调研究项目汇集了13个国家的代表，致力于提高核设施的计算机安全能力，包括人工智能技术，以检测表明有针对性网络攻击的异常情况。

人工智能技术使用中的对抗

人工智能已展露出造福人类和平利用核技术的潜力。随着人工智能不断用于增强核设施和辐射设施的流程和操作，人们也必须认识到与更广泛采用人工智能相关的风险。各组织必须保持强有力的计算机安全计划，在受益于人工智能的同时，确保核安保。

人工智能还可以通过识别计算机系统中的异常数据，帮助核设施和辐射设施加强对网络攻击的防御。（图/ Adobestock）

这样做，需要从根本上转变对信任和敏感性的看法。必须考虑系统中的每一个潜在故障点，甚至是与系统设计无关的故障点。恶意行为者会利用人工智能创造更复杂的恶意软件，自动进行网络攻击，利用模型中的偏差和漏洞，或通过模仿合法用户行为绕过安全措施。防御者和攻击者之间的这场装备竞赛将需要不断的创新和适应。

更多地使用人工智能技术来加强核设施的计算机安全措施，会带来极大的好处，包括加强威胁检测、安全措施积极主动、减少对人为干预的依赖以及加强事件响应。通过在应对风险的同时拥抱人工智能的好处，各组织可以在面对不断变化的网络威胁时显著加强计算机安全。

计算机安全演习如何助力提高应对核安保网络攻击的准备

文/Emma Midgley

历史上，核设施一直侧重于通过设置枪支、警卫和闸门等实物保护措施来确保核材料免受恶意攻击。这些措施仍被用来在核设施周围成功构筑堡垒，防止核材料或其他放射性物质遭到盗窃、破坏或对控制系统的未经授权访问。然而，近几十年来，在我们日益数字化的世界中，网络攻击的威胁已经升级。任何国家，甚至那些拥有最先进核电和研究计划的国家，都可能受到攻击。制定计算机安全和应对核设施网络威胁的国家框架已是必不可少。通过大规模演习，原子能机构协助各国改进对网络攻击的防范，并协助各国改进对核设施网络攻击的检测和应对策略。

“在事件发生之前，为应对计算机安全事件制定政策、明确的作用和责任以及详细的程序至关重要。”
—国际原子能机构核安保司高级信息和计算机安全官员Trent Nelson

原子能机构为核电厂和辐射设施制定了计算机安全演习，并已在世界各地国家层面开展进行。这些演习使各国能够演练和准备应对核设施网络安全遭到破坏的最坏情景。通过这些理论情景，可以找出政策、程序和流程中的薄弱环节，并确定需要通过缓解技术、能力建设和（或）组织变动来填补的差距。除了协助各国开展大规模演习以测试核设施的计算机安全外，原子能机构关于计算机安全的核安保导则还提供了重要资源，可以使各国采取重要的计算机安全措施，以检测、预防和应对网络攻击。

“在事件发生之前，为应对计算机安全事件制定政策、明确的作用和责任以及详细的程序至关重要。”原子能机构核安保司高级信息和计算机安全官员Trent Nelson说，“这就是原子能机构能够在许多方面提供帮助之处：从演习和导则，到分享最佳实践和程序，以确保有效的沟通和强有力的安全保护。”

使核设施容易受到网络攻击的因素包括人员、供应链的复杂性，以及使用计算机化系统支持核功能的多个利益相关方之间共享敏感信息。

“设想一种攻击，它让一个供应商妥协并伪造一项工作指令，导致一个有授权访问权限的受信任技术人员做出一个微妙的错误行动，”Trent Nelson说，“这只是恶意行为者可以找到绕过安全系统的一种方式。”

减少网络攻击潜在影响的一个重要方面是提高利益相关方的认识和增加利益相关方之间的有效沟通，因为这些群体中的任何一个，或这些群体中的任何个人，都可能成为恶意行为者的目标。谈到核设施的防御，有四个关键参与者：监管机构、设施营运者、技术支持组织（计算机安全事件响应小组和（或）计算机安全操作中心）以及第三方组织，如供应商和支持组织。开展演习是测试利益相关方之间沟通、报告和通知的一种良好方式，也是验证和确认组织结构安全和安保的一种良好方式。

虽然理想的情景是，网络攻击者会发现不可能渗透到核设施的计算机安全系统，但由于恶意行为者在不断

减少任何网络攻击潜在影响的一个重要因素是利益相关方之间提高认识和有效沟通。
（图/Adobestock）

演变，加上人性不可靠，这就意味着几乎不可能预测下一次大规模袭击会如何展开。因此，及时发现攻击是关键。在最近于斯洛文尼亚举行的演习中，通过一次理论上的网络攻击帮助验证和确认了防御网络攻击的检测和响应能力。

“计算机安全不是一个项目或一个过程，而是一个需要持续努力、关注和实践的终身旅程，”斯洛文尼亚核安全管理局网络安全处处长Samo Tomaži说，“像在斯洛文尼亚进行的演习使核部门的所有相关实体能够评估他们在网络攻击成功的情况下其事件响应预案的稳健性。”

如果发生严重的计算机安全事件，并有可能导致核安全事件或核安保事件，除了核设施的通常利益相关方之外，计算机安全事件响应小组也应参与其中。例如，这种事件可能涉及违反安保政策或安保程序，影响敏感的数字资产或系统，或失去敏感信息和对核安全关键功能的控制。

在这种情况下，一旦发现计算机安全事件或损害，计算机安全事件响应小组应与设施利益相关方合作，调查事件、收集取证数据、分析发生的一切和发生地点以及协助遏制和消除入侵，以帮助营运者恢复核设施的正常运行。在应急结束时，收集计算机取证证据，以帮助对攻击事件进行刑事调查，并确保有效的信息共享，以便在未来进一步加强核设施的计算机安全措施。

在斯洛文尼亚的演习中，检测网络攻击对于能够应对这一理论上的安保事件以及测试和验证事件响应程序至关重要。这些演习为测试安全、安保和应急准备之间的关系提供了支持，并通过识别潜在的薄弱环节和提出必要的修改来加强核安保制度，以提高其对潜在网络安全威胁的总体准备。此外，这些演习还提供了测试国家和国际层面进行通知和报告的通讯渠道的机会。总之，定期进行计算机安全演习是维护核设施安保的一个重要方面。

通过协调研究项目改进计算机安全异常检测技术

文/Rodney Busquim e Silva 和 Andrea Rahandini

识别控制关键安全和安保功能的计算机系统运行中的异常情况，需要大量的专门知识，而且需要对所需的行动进行测试、分析和修正，从而加以完善。

“异常检测在早期评估针对核设施和辐射设施计算机系统的可能威胁方面发挥着重要作用。”原子能机构核安保司信息管理处处长Scott Purvis说，“通常情况下，异常检测技术基于人工智能应用，如机器学习、统计型或知识型方法或其他技术。这类技术用于识别与预期网络通信或过程测量存在的偏差，这可能是显示入侵者绕过计算机防御系统的第一个指标，并能够提供对网络攻击的实时检测。

这些技术很重要，因为能力极强的恶意行为者可能会引入恶意软件，损害数字系统的安全或安保功能，同时伪造从传感器和指示器发送到操作员的数据。这意味着操作员可能没有意识到恶意活动的发生，最初会根据控制室显示的内容做出反应，有可能被误导而采取错误行动。只有通过自动检测这种网络攻击中最小的异常情况，才能正确地通知操作员。

为了应对这一重要工作领域和其他计算机安全挑战，原子能机构在2016年启动了一项专门协调研究项目。

通过协调研究项目进行研究和发展是原子能机构为促进核安保加强计算机安全活动不可或缺的一部分。这些项目产生了一系列研究和可操作结论，补充了原子能机构正在进行的努力，从而加强各国预防、检测和应对有可能直接或间接影响核设施和辐射设施安全和安保的计算机安全事件以及在发生这类事件后进行恢复的能力。

“敌手变得越来越复杂，他们的网络能力对开发异常检测工具提出了越来越多的挑战，”Purvis说，“开发异常检测技术需要获得现实且实物一致的网络和电厂流程数据，以训练和测试检测模型。”

“我们开发并使用ANS模拟器来生成一个数据库，用于训练我们的机器学习模型，并评价其效率。原子能机构这项协调研究项目联合国际合作伙伴一起开展研究，创造了这一领域的新知识。”

—巴西圣保罗大学理工学院教授Ricardo Marques

用于建立能力的网络攻击情景

题为“加强核设施计算机安全事件分析”的2016年协调研究项目产生了重要成果，例如，成功地进一步研究出有针对性的工具和技术，而以前，如果不暴露核设施和辐射设施的敏感信息，就不可能对这些工具和技术进行研究。

由来自13个国家和17个组织的研究人员组成的协调研究项目团队开发了一个称为“亚舍拉”（Asherah）核电厂的虚构设施，圣保罗大学以该设施为基础开发了一个模拟器（ANS）。他们共同开发了核设施内的真实网络攻击情景。有了这些网络攻击情景，就可以探索和评估计算机安全措施的有效性，以及数字资产遭到破坏的潜在操作后果。此外，该团队还致力于数据收集和分析，以及网络攻击检测技术的开发和测试。

“我们开发并使用ANS模拟器来生成一个数据库，用于训练我们的机器学

圣保罗大学根据“亚舍拉”虚构核电厂设施开发了一个模拟器。（图/国际原子能机构）

习模型，并评价其效率。原子能机构这项协调研究项目联合国际合作伙伴一起开展研究，创造了这一领域的新知识。”巴西圣保罗大学理工学院教授Ricardo Marques说，“协调研究项目参与者之间的合作对于验证所做的工作至关重要。”

此外，这项协调研究项目的成果还被用于大量不同学科的研究生和研究人员的持续教育和培训。这进一步加强了研究和努力，以不断提高核设施和辐射设施的计算机安全。

“我作为博士生的部分研究就是利用ANS模拟器及其人机界面进行的，该界面使用户能够观察模拟器并与模拟器交流，是在原子能机构协调研究项目中开发的。”来自中国清华大学的博士生Si Wen说，“我进行了异常检测技术的研究，ANS模拟器对于产生必要的数据来训练和评估针对核电厂开发的检测算法至关重要。如果没有所有参与研究机构之间的合作以及协调研究项目团队开发的工具，我就不可能进行关于核电厂数字系统网络安全的博士研究，”她补充说。

协调研究项目的成果包括ANS模拟器、工具和导则，可供世界各地感兴趣的研究机构使用，可以通过有关国家主管机构向原子能机构提交申请表获得，申请表可在原子能机构“核安保信息门户”下载。

最近在2023年，原子能机构启动了一个题为“加强辐射探测系统计算机安全”的新协调研究项目，旨在研究改进辐射探测设备计算机安全的方法和技术。来自11个国家的12个组织（包括国家实验室、大学和国家研究机构）参与了这个新协调研究项目，计划开展的研究项目将涉及诸如云计算等新兴数字技术的应用，并继续探索和开发创新型异常检测技术。

确保下一代核反应堆的数字技术安全

文/Joanne Liou

所有创新都会带来可能改变行业的潜在利益，但也会带来潜在风险。在核领域，包括小型模块堆在内的先进核反应堆正在纳入创新技术，特别是产生新颖解决方案的数字技术。

人们对小型模块堆的兴趣日益浓厚。这些先进核反应堆具有有限的电功率，通常每台机组最高300兆瓦，约为传统核反应堆发电能力的三分之一。然而，在这些新反应堆中使用尖端的数字技术在核安全和核安保方面带来了新的挑战。全球有80多种处于不同发展阶段的小型模块堆设计和概念。

“部署小型模块堆的一个挑战是如何在保持遵守核安全和核安保标准的同时，加快其技术发展，并展示其准备水平。”原子能机构信息技术安全官员Rodney Busquim e Silva说，“这加强了在小型模块堆寿期中考虑和维护数字仪器仪表和控制以及计算机安全解决方案的必要性。”

“交换信息的必要性可能会引入网络犯罪分子可以利用的途径，因此需要对通信基础设施进行强有力的网络安全考虑。”

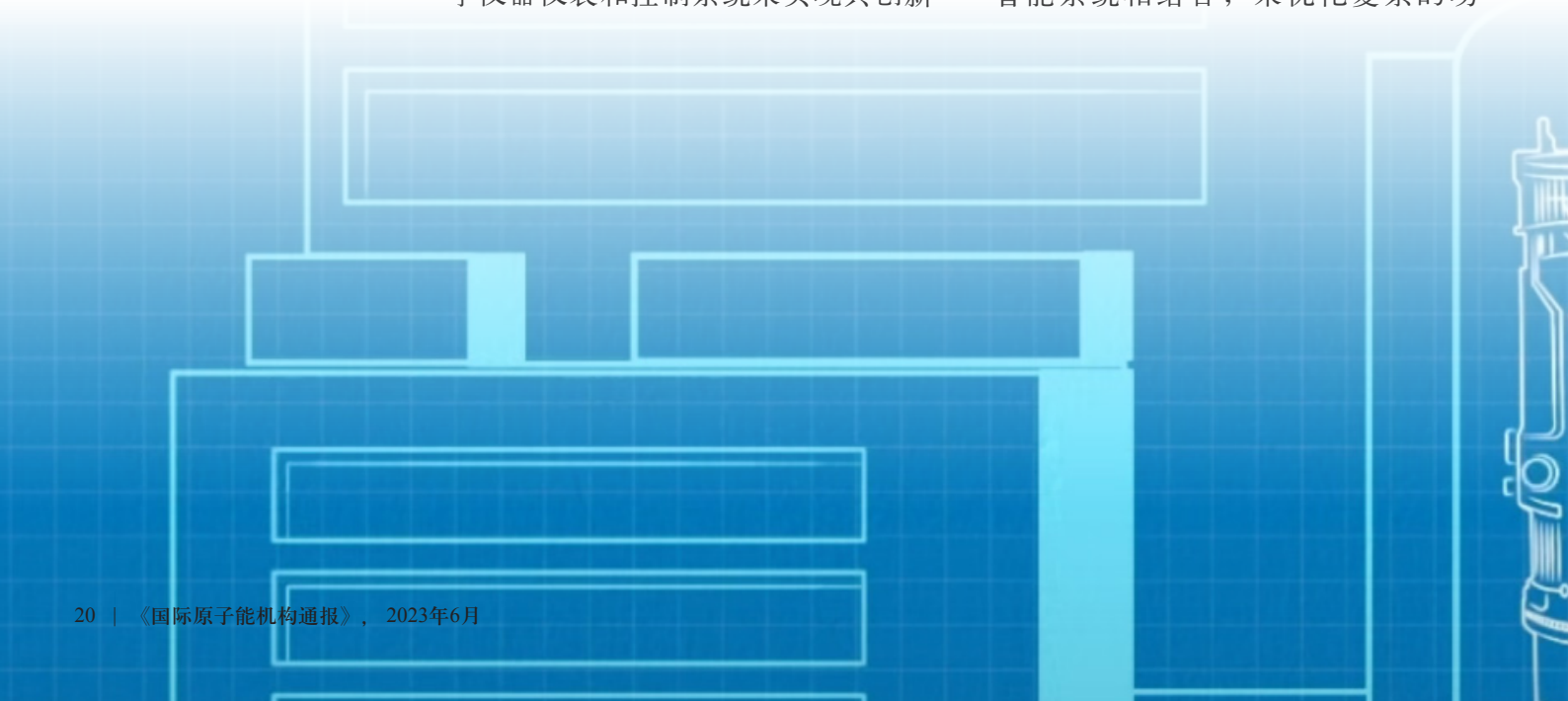
—英国计算机安全专家Mike St.John Green

计算机化解决方案和挑战

小型模块堆的创新设计依赖于数字仪器仪表和控制系统来实现其创新功能。自动化、远程监控和维护以及其他新功能所需的数字技术的增加，突出了对计算机化解决方案的需要。

一些小型模块堆的设计是为了在偏远地区部署核电和减少现场工作人员数量，这可能导致需要持续可靠的远程监控。鉴于数字仪器仪表和控制系统的设计，应用计算机安全措施应是小型模块堆现场与支持中心之间安全通信的先决条件。“交换信息的必要性可能会引入网络犯罪分子可以利用的途径，因此需要对通信基础设施进行强有力的网络安全考虑。”英国计算机安全专家Mike St.John Green表示，“远程操作必须保护信息的保密性、可用性和完整性，以确保小型模块堆和相关基础设施的安全可靠运行。”

人工智能和机器学习也支持小型模块堆的运行。人工智能技术可创造能够处理复杂问题的系统，而机器学习技术则学习如何基于数据完成特定任务。核工业试图通过将核设施和监控系统的数字模拟与人工智能系统相结合，来优化复杂的功



能，从而提高运行效率。然而，这些好处确实伴随着网络攻击的可能性。例如，人工智能和机器学习所需的基于软件算法依赖于数据库，而这些数据库可能会被操纵，从而导致人工智能的错误决策。

来自中国清华大学的博士生Si Wen说：“这些系统在开发过程、交付或软件安装过程中，可能会受到代码注入的影响，例如，故意向它们输入损坏的数据。总的挑战是如何使人工智能和机器学习算法具有足够的透明度。必须以可接受的风险水平对人工智能和机器学习的可接受使用进行明确定义。”

安保始于设计

专家们一致认为，核设施的计算机安全必须从一开始就加以考虑。这种积极主动的作法被称为“安保始于设计”，它借鉴了最佳实践和经验教训，并执行一种“始于设计”的概念，这种概念同样适用于核安全、核保障和核退役。

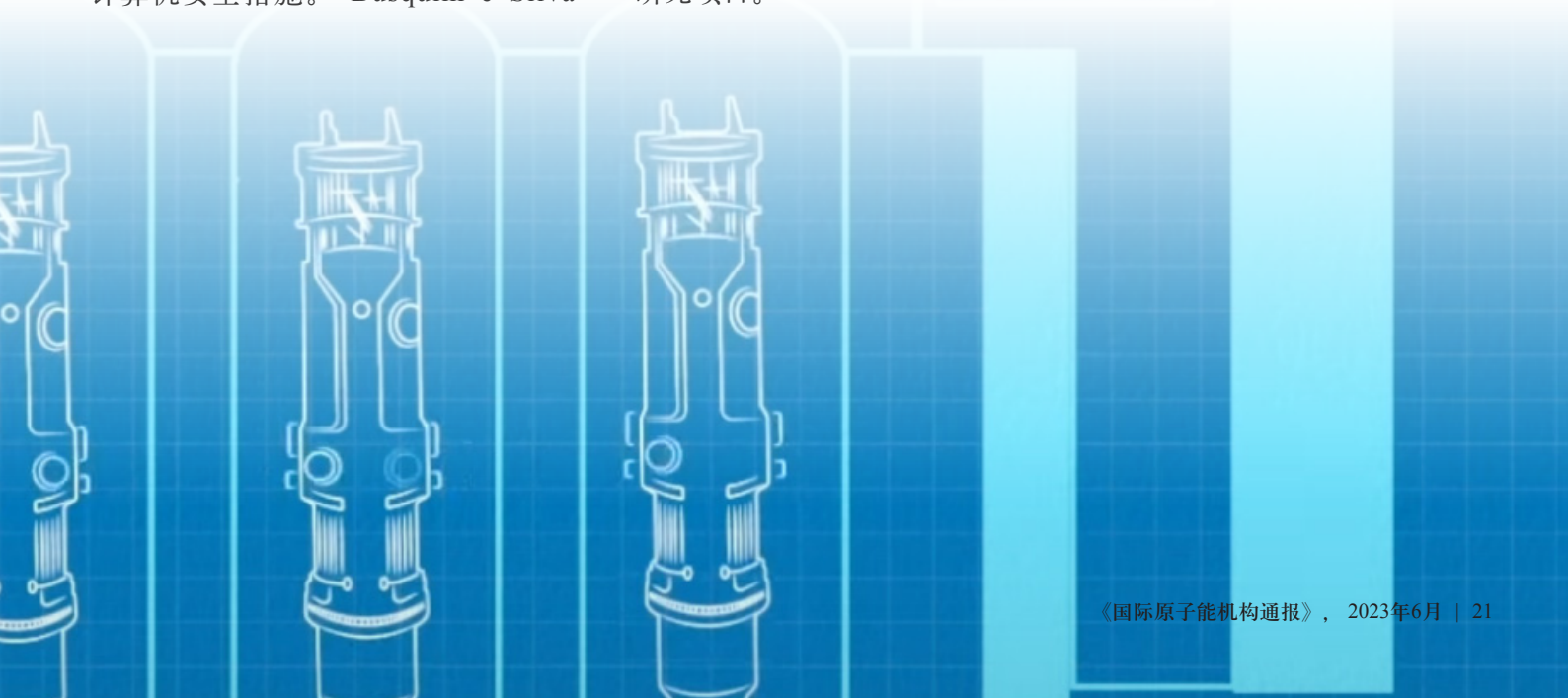
“计算机安全始于设计”旨在通过一种方案从源头上降低安保风险，这种方案考虑在设施寿期或流程的所有阶段采取系统和一致的安保。“在小型模块堆的整个寿期中，从设计到运行再到退役，都需要考虑和维护计算机安全措施。”Busquim e Silva说，“当从一开始就考虑安保（包括网络安全）时，设施开发者可以作出将使设施更安全可靠、更高效和更具成本效益的设计选择。”

国际原子能机构的作用

原子能机构将来自核组织和其他组织的专家联系起来，讨论和确定与小型模块堆的技术和运行特性有关的计算机安全相关问题和挑战。例如，2022年2月，原子能机构主办了一次小型模块堆仪器仪表和控制系统与计算机安全技术会议，以促进国际专家之间的合作和信息交流。与会者一致认为，有必要协调各国的方案和法规，以使小型模块堆国际市场变得可行。“标准化小型模块堆的仪器仪表和控制方案开启了一个全新的技术领域。新操作模式所需的自动化程度不断提高，以及数字系统的广泛使用，要求从设计层面采取计算机安全措施和工程解决方案，以确保电厂的安全可靠运行，”出席会议的阿根廷核监管局代表Jorge Casanova说。

2023年3月，原子能机构还举办了一次讲习班，进一步探讨小型模块堆计算机安全及仪器仪表和控制相关技术能力的发展。此外，原子能机构计划于2024年就该主题启动一个协调研究项目。

全球有80多种处于不同发展阶段的小型模块堆设计和概念。



加强计算机安全以促进核安全和核安保

文/国际原子能机构副总干事兼核安全和安保部部长莉迪·埃夫拉尔

核安全和核安保有着相同的目标和愿景：保护人、社会和环境免受电离辐射的潜在有害影响。虽然处理核安全和核安保的活动有所不同，但建立一个良好协调的方案来管理它们的接口至关重要，要确保相关措施的实施能够利用可用的相互促进机会，同时既不损害安全，也不损害安保。

众所周知，在核设施和辐射设施中，实物安保系统和措施必不可少，保护通常用于维护核安全的设备、系统和装置免受蓄意破坏行为的影响，这种破坏行为可能导致具有放射性后果的释放。通常，在旧的设计和应用中，安全系统只需要用实物安保措施来保护。然而，当今无处不在且不断发展的技术趋势，显著增加了数字系统在核设施和辐射设施运行效率中的作用，特别是与负责设施重要功能有关的系统，如仪器仪表和控制系统，包括既用于安全又用于安保的系统。

这些系统的安保需要保持严格警惕，以识别漏洞和阻止对数字控制系统的未经授权访问，这种访问可能导致安全或安保功能受到损害。在这方面，计算机安全对于安全和安保之间的相互作用越来越重要，正在作为其他关键领域的一部分加以处理，这

些领域包括：监管基础结构、核设施设计和建造的工程规定、核设施访问控制、放射源分类；放射源和放射性物质（包括乏燃料和放射性废物）管理、失控源的探测和回收，以及应急计划和应变计划。

在国家层面上，政策制定者在制定计算机安全条例时，需要将核安全和核安保一并考虑。明确的责任分配、领导力和风险管理是安全和安保接口的基础，对于实施有效的计算机安保措施同样重要。与此同时，计算机安全在本质上是一个全球性挑战。

在这方面，国际合作的重要性和原子能机构的核心作用得到了广泛认可。原子能机构的安全标准和核安保导则突出强调了核安全与核安保之间的接口。约十年来，原子能机构一直在信息和计算机安全技术领域为各国制定和提供一整套援助，支持它们采取有效措施应对可能影响核安保的网络攻击。此外，原子能机构支持建立核安全与核安保系统和措施之间的协同作用，以确保在这两个领域采取的行动相辅相成，而不是相互损害。

展望未来，技术进步将进一步提高强大的计算机安全对国家和设施核安全和核安保的重要性。人工智能等快速发展的技术在解决一些问题和改善数控操作方面大有可为。与此同时，它们也带来了新的挑战，需要加以解决。同样，无线和自动化技术今天也被考虑并用于先进核反应堆设计，如小型模块堆和微型反应堆。随着网络威胁在不断迅速演变，原子能机构为促进核安全和核安保而对成员国加强计算机安全需求的支持，需要灵活应对这些新技术带来的所有新机遇和挑战，以便提供最有效的标准、最佳实践、培训和导则。这正是原子能机构核安全和安保部不断努力实现的目标。

在国家层面上，政策制定者在制定计算机安全条例时，需要将核安全和核安保一并考虑。

—国际原子能机构副总干事兼核安全和安保部部长莉迪·埃夫拉尔

应对日益数字化世界中的各种威胁

文/ Wolfgang Picot

2022年5月，奥地利技术研究所成为国际原子能机构核安保方面第一个信息和计算机安全协作中心。奥地利技术研究所为核设施和活动计算机安全方面的国际和地区培训班和演习提供支持，开发技术示范模块以提高对网络威胁的认识，并帮助为塞伯斯多夫新核安保培训和示范中心编写培训材料。为更好地了解这一合作，我们采访了奥地利技术研究所数字安全和安保中心负责人Helmut Leopold。

问：一般来说，计算机安全方面的新兴风险和新兴威胁是什么？

答：当今的许多现代数字设备在建造时都考虑了较广泛的网络，其中许多设备需要接入互联网来运作。每个软件的开发都包括可能导致漏洞的潜在错误。接口保护不力和用户不负责任的行为，增加了对信息技术系统运行的安全威胁。攻击者利用数字系统的漏洞获得访问权限。

攻击方法和工具随着数字化创新进程的发展而发展。现在，黑客软件在互联网上很容易获得，使攻击变得更容易，甚至资质很差的攻击者也能做到。我们面对的是一个由有组织犯罪、经济和工业间谍活动以及网络恐怖主义驱动的多样化网络攻击生态系统。

因此，当前广泛的网络攻击威胁着用户、公司和当局，并且可能与有针对性的虚假信息活动一起攻击整个国家的数字基础设施，动摇我们社会的基础。

问：核工业是否面临同样的挑战？

答：企业和个人消费者主要使用数据驱动和通信导向的信息技术。相比之下，生产设施和关键基础设施使用所谓的操作技术，监测和控制所确定的生产过程的行为和结果。传统上，操作技术的互连程度远低于信息技术。然而，随着技术的进步，这两个领域已经融合，操作技术的软件和设备越来越多地嵌入更广泛的网络中。

“我们一直在与原子能机构同事密切合作，为核安保培训和示范中心开发培训模块、演示和练习。”

—奥地利技术研究所数字安全和安保中心负责人Helmut Leopold

这种发展存在问题，因为网络安全意识在操作技术领域的普及程度不如信息技术领域。

因此，这些对信息技术安全的新兴威胁变得与工业生产和关键基础设施的操作技术相关。由于核工业传统上采取保守的方案，将控制系统隔离起来，因此这对核工业也变得越来越重要。

问：奥地利技术研究所开展了哪些活动来加强核安保方面的网络安全？

答：奥地利技术研究所的研究计划仔细研究不断变化的威胁情景如何

影响操作技术系统，旨在开发专门知识和新的解决方案，以提高关键基础设施抵御网络攻击的韧性。这项工作是制定新的全球安保标准、关键系统要素认证程序和新系统架构的基础，以便从设计之初就将坚实的网络安全措施嵌入操作技术系统。

奥地利技术研究所还提供全面的培训和教育，为应对网络安全攻击作准备。在“虚拟化”信息技术系统（即所谓的“网络靶场”）的复杂模拟中，用户、系统开发人员、操作人员和政府代表对现实的网络攻击情景作出反应。这种模拟对于确保信息技术和操作技术系统有韧性并且能够有效抵御网络威胁至关重要。

问：奥地利技术研究所和国际原子能机构开发的虚拟学习环境有什么优势?

答：实际经验是最有效的学习过程。奥地利技术研究所和国际原子能机构开发了一个“网络靶场”，对现有关键数字基础设施进行“数字孪生”创建，并提供高度现实的应用情景培训。

政府和行业用户可以在这里评价和测试保护机制和业务流程的有效性。

“网络靶场”经验支持建立公共和私营组织的可持续防御能力。

问：除了虚拟培训，奥地利技术研究所在计算机安全方面的工作和专门知识如何促进核安保?

答：例如，我们可以通过开发监控“边缘”设备的软件来帮助抵御攻击者，边缘设备通常将组织单位的内部网络连接到互联网。攻击者在制造破坏之前，往往利用这些设备作为系统的入口点。我们利用异常检测经验来训练分析软件，监测通常用于特定类型核设施的边缘设备。

如果边缘设备以奇怪的方式运行，此类软件可发出警报或采取对策。这样，营运者可在网络攻击造成重大损害之前，迅速发现并阻止网络攻击。

问：一年前，奥地利技术研究所被指定为国际原子能机构核安保方面第一个计算机安全协作中心，至今仍是唯一的此类中心。这对奥地利技术研究所的工作意味着什么?

答：我们对被指定为协作中心感到无比自豪，并继续支持提供关于核行业仪器仪表和控制系统的计算机安全地区培训班。我们在2022年举办了两次此类培训班，利用我们合营项目的一些成果开发了一个虚拟学习平台。

我们还参加了开发小型模块堆的计算机安全活动。

目前，我们正在协助国际原子能机构筹备2023年“核世界中的计算机安全：安保促安全”国际会议，我们将在会上演示我们的虚拟培训平台、主持小组会议、介绍与我们在该领域研究有关的论文等。

问：奥地利技术研究所在核安保培训和示范中心的参与情况如何?

答：我们一直在与原子能机构同事密切合作，为核安保培训和示范中心开发培训模块、演示和练习。我们将计算机安全模块纳入与核材料和其他放射性物质实物保护有关的培训课程，以及与探测和应对脱离监管控制的核材料和其他放射性物质有关的培训课程。这一安排旨在加强计算机安全概念，将其作为核安保的一个不可或缺的组成部分。

国际合作如何保护世界免遭网络威胁

Tighe Smith是国际电工委员会核设施仪表控制与电气系统分委会（SC45A）A9工作组召集人。他被任命为A9工作组的领导，该工作组在电工委员会中负责网络安全领域。电工委员会是一个全球性非营利组织，负责制定电气设备（包括核电厂电气设备）的设计、建造和运行的国际标准。电工委员会成立于1906年，成员覆盖170多个国家，发布了1万项国际标准。

由于数字设备的广泛使用，核工业在维护计算机安全方面面临着重大挑战。这一趋势在日常生活中显而易见，通过云计算远程控制的智能冰箱、照明和其他设备已司空见惯。核设施中的许多系统以前没有任何数字组件，现在有了数字元素。这些数字元素的计算能力、可重复编程性和互连能力在支持运行、核安全和核安保方面提供了无与伦比的效率。

小型模块堆和其他新型反应堆设计正在一个数字优先的世界中发展，计算机系统的使用比之前的传统反应堆更加广泛。它们可以设计成远程操作，甚至自主操作，利用计算机网络基础设施与中央操作员联络。这种作法可以使操作员和自动化系统能够分析大量数据，以提高核设施的运行效率。

然而，核工业的这种数字现代化带来了更多挑战，因为如果缺乏足够的计算机安全，弱项或漏洞可能会被恶意行为者利用，成为对其中某个设施攻击的一部分。

为了应对核设施中快速发展的数字技术格局所带来的挑战，以及支持国家和设施之间采取统一方案的必要性，国际电工委员会采取了一种基于后果和风险知情的方案，该方案与原子能机构《核安保丛书》中的信息和计算机安全导则一致。我们建议采用分级方案，而不是规定性方案，使组织能够根据网络攻击的潜在后果确定产品或流程所需的控制级别。例如，计算机安全计划的第一步是审查核设施的功能，评定其对安全和安保的影响，以及确定适当的安保要求水平。

预防、检测和缓解

预测网络攻击未来将如何发展，这比较具有挑战性，因此，电工委员会与原子能机构密切合作，制定了标准，建议核设施的计算机安全计划除

了预防之外，还应注重检测、响应和恢复。即使遭到了网络攻击，也应该有适当的机制来恢复和确保必要功能正常运转，从而确保安全或安保不会受到损害。

我们的世界在日益数字化，加上人工智能和机器学习快速发展，可能会使核设施的计算机安全变得令人生畏。尽管存在这些挑战，但为了继续安全可靠地运营这些设施，国际合作至关重要。半个多世纪以来，原子能机构、国际社会和核工业在标准化方面携手合作，支持和平利用核技术的安全和安保。随着气候变化和能源安全等全球问题变得更加紧迫，许多国家在寻求利用新型和创新型核技术作为生产低碳能源的一种方式，这使得标准化对于维护核设施的安全和安保更加重要。

核世界的通力合作

原子能机构和电工委员会为努力制定核设施的信息和计算机安全标准作出了重要贡献。原子能机构通过国际协商一致编制《核安保丛书》导则出版物，概述确保信息和计算机安全的概念和规范，将其作为实现核安保目标的基本要素。《核安保丛书》为在核设施中实施网络知情工程方案安排国家资源以及制定行业法规和概念提供了导则。

作为促进最佳实践和知识共享的国际标准组织，电工委员会与原子能机构密切合作。根据电工委员会与原子能机构之间的谅解备忘录，与电工委员会合作的科学家和专家制定了关于通过具体计划和工程要求实施原子能机构导则的标准和技术报告。这些要求可用于设计和开发当前和未来的数字系统，而这些系统可根据符合原子能机构导则的监管模式进行认证。核工业拥有执行电工委员会标准经验的专家然后可以支持原子能机构导则的未来迭代发展。

科学家和专家自愿助力电工委员会的工作，我们随时欢迎更多的志愿者参与电工委员会工作。核领域的计算机安全专家群体相对较小，即使在全球范围内也是如此。助力电工委员会的工作，为构建可在全球范围内用于支持全球核工业的标准提供了机会。

随着气候变化和能源安全等全球问题变得更加紧迫，许多国家在寻求利用新型和创新型核技术作为生产低碳能源的一种方式，这使得标准化对于维护核设施的安全和安保更加重要。

—国际电工委员会Tighe Smith

国际原子能机构“行为准则”放射源安全和安保20年进展

在会外活动“性别平等和包容以及《放射源安全和安保行为准则》：20年进展”上的发言人员。（图/国际原子能机构W. Wawrzuta）

2023年5月，来自128个国家和4个国际组织的270多名法律和技术专家在奥地利维也纳召开会议，审查在放射源安全和安保方面取得的进展，并解决需要改进的领域。

放射源在许多领域发挥着不可或缺的作用。在医学方面，它们有助于治疗癌症。在农业方面，它们使科学家能够开发改良作物品种，以适应气候变化和解决粮食安全问题。在艺术和考古方面，它们有助于保护无价的文化遗产。但这些放射源必须以适当的安全和安保措施来处理。

为了帮助各国应对风险，保护人和环境免受意外辐射照射或涉及放射源的未经授权的故意行为的影响，原子能机构制定了《放射源安全和安保行为准则》（“行为准则”）。该“行为准则”于2003年获得原子能机构理事会核准，今年正值其20周年。

“‘行为准则’获得核准20年来，我们在改善世界各地放射源的安全和安保方面取得了稳步进展，”原子能机构总干事拉斐尔·马里亚诺·格罗西在分享各国执行《放射源安全和安保行为准则》信息的技术和法律专家不限成员名额会议开幕式上说，“但必须进一步努力，以实现更多的政治承诺，并分享可持续、安全和可靠管理这些放射源的全球最佳实践。”

会议为期五天，为全球专家交流各国执行“行为准则”及其两个补充导则文件的实践提供了一个平台。此类会议每三年举行一次，使各国能够分享经验、交流教训以及确定在实施“行为准则”方面存在的现有和未来挑战。

在整个一周的时间里，与会者深入探讨了各种主题，包括核安全和核安保的演变、法律方面、国际合作、未来发展和“行为准则”的影响。讨论涉及的挑战和优先事项包括：为放射源的安全和安保建立适当的监管框架、放射源寿期管理、放射源的进口和出口规定以及当这些放射源被宣布为废弃源时应如何管理。至关重要的是，这次

会议为与会者提供了交流各自有效执行“行为准则”规定的方法的机会。

为安全可靠的未来提供重要导则

会议联合主席、加拿大核安全委员会执行副主席兼首席监管运营官Ramzi Jammal在开幕式上发言时强调，实施“行为准则”对于确保保护环境、公众和工作人员至关重要。“我们的最终目标是确保放射源整个寿期内的总体安全和安保，以避免发生意外辐射照射，并防止放射源被恶意使用。这是一项持续的合作努力。”

在介绍关于“行为准则”历史的特别会议时，美国核管理委员会副处长Theresa Clark也作为联合主席向与会者致辞：“在反思和庆祝这二十年的过程中，我们希望从法律和技术角度对‘行为准则’的背景达成共识，以便我们能够分享经验、最佳实践，并相互学习，以改进‘行为准则’在全球的实施。”

该“行为准则”详细说明了各国如何确保放射源从最初生产到最终处置的安全和安保。它包含了国际考虑因素，并对国家政策、法律和法规的制定、协调和实施以及国家之间的合作提出了建议。尽管它是一个没有法律约束力的文书，但自2003年理事会核准该“行为准则”以来，已有146个国家表示在政治上支持执行该“行为准则”的规定。

该“行为准则”有两个补充性导性文件。《放射源的进口和出口导则》阐述了在确保放射源进口和出口安全和安保方面的作用和责任。《弃用放射源管理导则》为弃用放射源的管理提供了导则，规定了放射源寿期结束后的管理方案，如再循环和再利用、长期贮存和处置以及归还供应商。该导则还鼓励制定国家政策和战略来管理弃用放射源。

“‘行为准则’及其补充导则文件为国家和国际辐射安全和核安保带来了实实在在的好处，使我们能够充分利用放射源来实现可持续的未来。”阿联酋联邦核监管局辐射安全主任、联合主席Aayda Ahmed Al Shehhi总结道。

原子能机构与各国密切合作，确保对放射源进行统一、安全和可靠的管理。它支持各国实施“行为准则”的原则，并提供广泛援助，帮助制定实施“行为准则”的战略和行动计划；改进许可证审批、检查、执法和管理系统；以及根据原子能机构安全标准、核安保导则和国际最佳实践加强国家监管机构的能力。

加强核领域的多样性和包容性

在会议间隙，加拿大核安全委员会主办了题为“性别平等和包容以及《放射源安全和安保行为准则》：20年进展”的会外活动。120名与会者参加了这次活动，讨论如何促进和加强女性在核领域的参与，包括在核安全和核安保领域的参与，并为所有人提供平等机会，不分性别。

加拿大核安全委员会主席兼首席执行官Rumina Velshi表示，“参与会议讨论的代表多样性，有助于增加质疑的态度，继而促进组织进一步强化安全文化。性别平等不仅仅是女性的问题，而是一个需要所有人面对的社会问题”，并补充道，对人力资源日益增长的需求使得确保在核领域为女性提供更多机会成为当务之急。

“核安全和核安保依赖于质疑和学习的态度、对建设性反馈持开放态度，以及综合不同观点和调动不同专业知识的能力。在这方面，包括性别多样性在内的多样性是一笔真正的财富。当我们拥抱多样性并鼓励我们的员工发表意见时，我们会更强大和更高效，”原子能机构副总干事兼核安全和安保部部长莉迪·埃夫拉尔在活动中表示。

原子能机构副总干事兼管理部部长玛格丽特·多恩表示：“加强女性和来自不同背景人员在核相关部门的参与，对任何组织都至关重要。”她强调了原子能机构关于改善性别平等的举措，包括旨在让更多女性进入核领域的玛丽·斯克洛多夫斯卡-居里进修计划和莉泽·迈特纳计划。

阿联酋联邦核监管局局长Christer Viktorsson就这一主题表达了自己的看法：“阿联酋联邦核监管局集中开展了促进性别平等的活动。领导层的承诺和支持至关重要，包括对我们如何提高包容性和公平对待所有员工的调查。同样重要的是，要有适当的包容性框架和有效的实施。”

文/ Artem Vlasov

阿拉伯语国家讨论核安保计划

参与最近突尼斯地区会议人员分享在制定和实施“核安保综合支助计划”方面的经验。（图/国际原子能机构Z. Hassan和阿拉伯原子能机构）

阿拉伯核监管人员网成员国最近在突尼斯举行会议，交流与在各自“核安保综合支助计划”框架内实施核安保活动有关的最佳实践、挑战和机遇。会议强调了提高监管和运行能力的地区方案的重要性，这些方案是原子能机构核安保计划的一部分。

“通过地区视角处理核安保问题，可以改善国际合作，促进原子能机构核安保计划的实施。”原子能机构核安保司司长Elena Buglova说，“与阿拉伯核监管人员网等地区网络的合作，进一步加强了‘核安保综合支助计划’支持机制的有效性，为确定和讨论地理位置相近的国家或语言相同的国家之间的共同需求和挑战创造了机会。”

会上，来自14个国家的28名与会者提供了关于其国家“核安保综合支助计划”实施情况的信息。特别关注的领域包括：与核安保立法和监管框架有关的活动；国家威胁和风险评定；实物保护制度；涉及脱离监管控制的核材料或其他放射性物质的犯罪行为和未经授权行为的探查；涉及脱离监管控制的核材料或其他放射性物质的核安保事件响应；以及国家核安保制度的维护。

黎巴嫩目前是利用“核安保综合支助计划”作为加强国家核安保基础结构的机制的国家之一。“会议使我们能够分享我国实施‘核安保综合支助计划’的经验，并讨论了我国核安保挑战以及应对这些挑战的可能方法。”黎巴嫩原子能委员会负责授权、检查和监管部门负责人Hassan Basat说，“最重要的成果是确定了需要在阿拉伯核监管人员网成员中进一步加强的‘核安保综合支助计划’共同优先领域。”

目前，在22个阿拉伯核监管人员网成员中，有19个成员拥有经批准的“核安保综合支助计

划”。在全球范围内，92个国家已批准“核安保综合支助计划”。

“在地区层面上，我们共享边界，也共享特定挑战。”巴林最高环境委员会辐射防护局物理分析部门负责人Shaima Khalid AlJanahi说，“会议促进了经验和知识的分享，希望随后能够采取切实行动，改善和加强该地区的核安保。”

这次会议由阿拉伯原子能机构主办，得到欧盟的财政支持。

“核安保综合支助计划”支持机制

原子能机构应请求协助各国制定“核安保综合支助计划”。“核安保综合支助计划”为制定以下一种系统而全面的方案提供框架，该方案用于确定国家核安保需求并进行优先排序，以及制定在国家层面实施核安保改进计划。通过“核安保信息门户”网站向感兴趣的国家提供自愿开展的自评定工具，补充“核安保综合支助计划”。

“核安保综合支助计划”及其相关实施计划使各国能够满足其最迫切的需求，并确定可以在国内解决的领域以及需要寻求国际社会援助的其他领域。

一旦确定每个国家的需求，原子能机构即可开始为定向援助打基础工作，例如，通过国际实物保护咨询服务工作组访问和国际核安保咨询服务工作组访问提供援助。

国际原子能机构与阿拉伯核监管人员网的合作

阿拉伯核监管人员网是2010年在国际原子能机构全球核安全和核安保网框架下建立的地区网络。阿拉伯核监管人员网促进、提高、加强和协调参与国的辐射防护及核安全和核安保监管基础结构框架，发挥着分享和交流监管经验和实践论坛的作用。

文/ Vasiliki Tafili

在线阅览本期和其他各期《国际原子能机构通报》：
www.iaea.org/bulletin

更多了解国际原子能机构及其工作，请访问网址：
www.iaea.org

或通过以下方式关注我们：

ISSN 1011-257X 23-01968