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）