

# 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。