# 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。