普杰立：网安局本月展开

保护人工智能系统技术指南公众咨询

卫生部兼通讯及新闻部高级政务部长普杰立医生说，在过去几年中，人工智能迅速普及，并被广泛应用于各个领域，这极大地影响了网安威胁格局。

赵世楚 报道
zhaosc@sph.com.sg

新加坡网络安全局这个月将针对“保护人工智能系统技术指南”展开公众咨询，新指南将为本地系统所有者提供可用以应对潜在风险的实用措施。

资讯通信专才协会（Association of Information Security Professionals，简称AiSP）星期三（7月3日）举办首届人工智能安全峰会。

卫生部兼通讯及新闻部高级政务部长普杰立医生出席峰会致辞时宣布，网安局将于7月为“保护人工智能系统技术指南”（Technical Guidelines for Securing AI Systems）展开公众咨询。

普杰立说，在过去几年中，人工智能迅速普及，并被广泛应用于各个领域，这极大地影响了网安威胁格局。

他举例说，美国麻省理工学院的研究人员曾让人工智能将一只三维打印的乌龟误认为是一支步枪。

他指出：“人工智能的快速发展和应用给我们带来了许多新的风险，包括对抗性机器学习，它能让攻击者破坏模型的功能。”

广邀人工智能业界所有成员为指南提供改进建议与反馈

对抗性机器学习（adversarial machine learning）是一种机器学习方法，它通过输入欺骗性信息，来干扰与欺骗原本的机器学习模型，从而导致人工智能产生分类错误。

为应对不断变化的网安威胁，这项新指南旨在为现有的人工智能安全资源提供支持，并为本地系统所有者提供可用来应对系统和用户潜在风险的实用措施。

普杰立提到，当局邀请人工智能生态中的所有成员，包括AiSP成员和国际合作伙伴，就如何改进指南提供建议与反馈。

他也指出，政府清楚人工智能在广泛环境中应用，并涉及多种应用实例。“我们希望确保这些指南切实有用。”

他提醒，人工智能也容易受到数据隐私威胁，尤其是人工智能的广泛应用导致数据暴露、外流或损坏的可能性增加。

卫生部兼通讯及新闻部高级政务部长普杰立医生星期三在资讯通信专才协会举办的首届人工智能安全峰会上致辞时宣布，网安局将于7月为“保护人工智能系统技术指南”展开公众咨询。（李奕仪摄）

接下来几周，网安局将发布有关公众咨询的更多详细信息。

资讯通信专才协会成立兴趣小组供交流经验

同时，资讯通信专才协会也在现场宣布启动人工智能特别兴趣小组（AI Special Interest Group），为成员提供一个讨论人工智能发展的平台，让专业人士交流关键见解、洞察与经验。

普杰立也说，成员可以使用这个平台讨论网安部门如何在与人工智能共存的同时，继续确保数码领域既可信又安全。

他也提到，如果使用得当，人工智能也可以帮助防御者以更快速度、更大规模和更高精度识别风险，从而更快地应对风险。“越来越多的应用案例利用机器学习算法来检测异常情况，或对潜在威胁做出自主响应。”

人工智能侦测网安威胁 解决身份冒用等问题

黄俊恒 报道
wongjunheng@sph.com.sg

人工智能的应用日益广泛，不仅可帮助科技公司及时侦测网络威胁和入侵行为，还能有效打击身份冒用等问题。

为促进业内交流，资讯通信专才协会（Association of Information Security Professionals，简称AiSP）邀请五家科技公司，参加星期二（7月2日）举行的首届人工智能安全峰会，分享最新的人工智能科技。

以参与峰会的SailPoint为例，这家网络安全科技公司通过人工智能，让企业客户更全面地掌握员工的访问权限。例如，后台管理系统会根据员工职务安排适当的使用权限，并在员工离职时，提醒雇主取消权限。

SailPoint东南亚地区执行总监江翊铭受访时说，九成的数据泄露事件，是因身份被冒用所致。他说：“现在的大型企业聘请许多非正式员工和外包员工，他们的入职和离职程序须更加完善，以避免公司机密外泄。”

为应对不法分子日益复杂的招数，国际科技公司思科（CISCO）使用人工智能侦测网络入侵行为，并为这些威胁标上危险系数，同时自动生成相应的解决方案。

思科网安工程师纳德瓦特（Avinash Naduvath）带领的团队，开发了具有上述功能的聊天机器人（chatbot）。“人工智能可以帮助我们更及时地发现和解决问题，同时也可以马上关闭被入侵的相关网络领域，防止进一步泄密。”

包括SailPoint和思科在内的五个科技公司，是AiSP的人工智能特别兴趣小组成员。昨天的峰会也是小组首次为业界人士提供交流平台。

领导人工智能特别兴趣小组的AiSP助理秘书黄潭（Tam Huynh）说，已开始筹备下一场峰会，届时将邀请前线的网安从业员分享人工智能如何提高工作效率，预计在10月前举行。