Source: *Lianhe Zaobao,* p9
Date: 15 November 2025

AI代劳测试安全漏洞　国大与安信合作提高网安效率

郑智浩　报道
zhteo@sph.com.sg

网络威胁日益复杂，新加坡国立大学借助代理式人工智能，让系统自主完成搜集情报到生成安全漏洞报告的整个流程，以便网安人员把精力投在价值更高的任务上。

国大与安信资讯安全公司合作，接下来一年将验证代理式人工智能（agentic AI）进行安全漏洞评估与渗透测试方面的可行性。

安信资讯安全公司咨询部开发运营负责人郭明宏受访时说，渗透测试（penetration testing）旨在提前识别应用或网站的安全漏洞，以便尽快修复。这往往依赖人工操作，耗时耗力；有了代理式人工智能可大规模全天候运作，也不必担心测试人员水平参差不齐，造成评估结果不一致。

他指出，人工智能可试着像人类一样思考，收到指令后推理，不再只是个数学模型，可媲美应届毕业生或中级测试人员，进行初步分析。

“举例来说，绕过登录等安全漏洞可轻易找到，测试人员可腾出时间，专注创造新方案或进行复杂工作。没预算的小企业也能购入这套系统测试，保障最低的安全水平。”

新加坡国立大学数据科学研究所副所长黄思强教授说，网安的未来趋势可能是人工智能之间的对抗，或是人工智能与人类的联合攻防，因此须提前找到提高效率的解决方案，未雨绸缪。

今年网络安全局共拨1600万元资助业界

网络安全创新日星期五（11月14日）举行，上述项目是18个获选的提案之一，新加坡网络安全局今年共拨出1600万元资助业界。

数码发展及新闻部兼卫生部高级政务部长陈杰豪致开幕辞时指出，数码技术是经济重要引擎，融入日常生活，但也伴随威胁，特别是对关键信息基础设施和基本服务的干扰。“在这场网络空间保卫斗争中，仅靠政府是不够的。我们得利用学术界和私营部门的想法和人才。”

政府2023年宣布投入1亿1000万元，与南洋理工大学联合设立新加坡网络安全研究项目办公室（CyberSG R&D Programme Office，简称CRPO），也与国大合作设立网安人才、创新与增长合作中心（CyberSG Talent, Innovation and Growth Collaboration Centre，简称CyberSG TIG），加强本地网络安全生态系统。

陈杰豪说，CRPO迄今有22个研究项目获得总额达4000万元的资助，一些项目已进入试点阶段；CyberSG TIG支持的网络安全企业至今获得3700万元投资。

另一获选的科技方案来自Betterdata公司，旗下平台能把真实数据转化成可屏蔽敏感内容的合成数据，方便银行、医药和公共机构等客户提取其他有用信息。

网络安全创新日公布18个获选的科技方案，包括新加坡国立大学数据科学研究所黄思强教授（左起）和安信资讯安全公司咨询部开发运营负责人郭明宏，以及Betterdata联合创办人兼首席执行官贾维德分别主导的两个项目。（陈斌勤摄）

公司联合创办人兼首席执行官贾维德（Uzair Javaid）受访时说，人工智能发展依赖于数据的输入，但涉及个人身份、交易等重要信息受法规保护，也无法随意调取，平台可生成一套供企业安心分享和使用的合成数据。

贾维德说，没有任何数据的新公司，也可利用这项技术模拟数据，构建人工智能应用。目前有多家机构和公司使用Betterdata的平台，包括美国国土安全部和日本的鹿岛建设株式会社。