

·科学共同体推介·

英国皇家学会发布 《网络安全的现状和研究》报告

互联网是人类20世纪最伟大的发明之一,互联网正在改变并将继续改变人们的世界。它引领了信息技术的高速发展,同时带来了社会生产的变革,是人类继农业革命、工业革命后的又一重大产业技术革命。互联网产生的数字技术极大提高了人类认识世界、改造世界的能力,从社交网络到自动驾驶汽车,数字技术正深刻地改变人们工作、交流和生活方式。

但是随之而来的信息安全等问题也不容小觑。互联网具有匿名性和全球性等特点,利用互联网进行网络监听、网络攻击、网络恐怖主义等已成为全球公害。加强全球网络安全合作,已成为国际社会一项重要议题。

英国正处在互联网高速发展的情况之下,政府对于这一产业投入了大量的支持,并出台多项支持性政策。对于科学研究及创新产业发展来说,英国也有着很强大的实力将互联网变革带来的益处展现给民众。但另一方面,互联网的风险也仍然存在,对于大多数基于互联网的组织来说,网络安全滞后于现有的技术发展水平,针对互联网的攻击与日俱增,而这些会带来个人和组织的重大损失,从而破坏了互联网的潜在益处。

因此,英国皇家学会在2013年成立了一个专家指导小组,公开征集调查网络安全相关的数据,持续关注英国的网络安全问题及解决方案。在2016年7月,发布了《网络安全的现状和研究》,突出了新兴的网络安全存在的问题及挑战,以及在未来5~10年,应对这些挑战所需要的政策框架(图1)。



图1 网络安全的现状和研究——为英国撑起一个适应性强和值得信赖的系统
(报告来源 <https://royalsociety.org/topics-policy/projects/cybersecurity-research/>)

报告分为5个章节,分别探讨了网络安全与数字社会(cybersecurity and the digital society)、信任(trust)、适应性(resilience)、研究(research)、转化(translation);对网络安全的影响。

报告中指出,信任是增加和维持数字社会民众参与度所必

不可少的。互联网组织需要通过建立可靠且安全的系统,带有尊重地对待人们及其隐私和数据,提供可靠和易于理解的信息来帮助人们了解他们的安全状况,从而赢得人们的信任。加密是支撑数字计算安全性的关键技术。随着数字技术日益成为人们生活的核心部分,加密就变得更加重要。各国政府必须承诺维护端到端加密的稳健性,并敦促其广泛使用。现代数字系统面临着一系列的风险和威胁。如果有包含明确标准和正确做法的循证指导,将有助于企业和其他组织在这个危险的环境中保护自己。

此外,适应性作为在压力下或冲击面前发挥功能、适应、成长、学习和变换的能力,将帮助企业提供可靠和安全的系统。适应性强的组织可以更好地保护自己的客户,提供更有用的产品和服务,并获得人们的信任。适应性将有赖于企业和其他组织有机会获得高质量、值得信赖的建议和标准,以及由其他人共享的早期信息等。这些都依赖于公共部门机构,这将需要专家和透明度,并且有明确的职权范围和目标。政府正迈出可喜的一步,将其网络安全管理职能整合到一个机构当中(新的国家网络安全中心),还承诺对英国未来的网络安全需求进行独立审查,以确定长期所需的体制结构。因此需要快速推进,同时企业需要更大的激励来提高他们的网络安全,并助力他人的安全。企业和公共部门组织应定期报告网络安全实践标准的稳健性,并且应鼓励它们分享信息,帮助他人。

英国始终把研究和创新作为持续发展的动力。在网络安全方面,工业界和学术界的研究和创新将继续推动建设一个适应性更强和可信程度更高的数字环境。研究可以整合不同学科、行业和全球的见解,阐明如何最佳地建立、评估和改善数字系统。在目前的进展速度下,研究的发展不够迅速,未来将无法具备应对网络攻击者的网络安全防御能力。为实现网络安全能力的跃升,英国应当引入一个新的、以挑战为导向的研究资助机构。网络安全是一个跨学科、全球性、跨部门的独特领域。这些特性使英国利用跨国界、跨学科、跨部门研究人才进行研究和实践显得十分重要,包括通过同行评议和协作。

最后,创新研究思想和方法的转化可以催生出可靠、成熟的解决方案。人们需要这种多样化的工具和解决方案,来解决一些难以预料的网络安全风险问题,而这些工具和解决方案需要通过最大化那些有产品潜力的创新的多样性和数量才能最佳地实现。政府应通过其采购活动,以及资助那些具有潜在巨大溢出效益、但通过其他途径难以获得资助的理念,帮助创新走出学术界,面向市场。大学的技术转让办公室应注重商业化机会的数量,目的是更容易吸引到研究人员来商业化他们的想法。这将为社会带来更大的长远利益,而不是着眼于大学短期的财务回报。政策、实践和研究都需要顺应改变,以使得人们能够在不影响安全性的前提下享受到数字系统的益处。建立一个值得信赖、自我改进和适应力强的数字环境,应在面临预测不到的威胁时可以持续成长,并获得人们对它的信任。

编译/田恬(《科技导报》编辑部)