美国网络空间安全教育战略计划

■中科院信息工程研究所 / 赵倩 刘峰 林东岱

编者按：教育作为一个国家经济繁荣昌盛的重要条件之一，关乎国家的未来发展，在各个领域中都起着不可忽视的作用。本文从剖析美国关于网络安全教育的国家战略——国家网络安全教育计划出发，结合我国的实际情况，提出五点我国在开展网络安全教育工作时值得借鉴的地方，希望能给我国的网络安全教育工作带来些启迪。

面对与日剧增的网络安全事件，人们不断进行技术创新以寻求解决方案，虽然取得了一定的效果，却难以从根本上解决问题。因此，为保护网络空间安全，提升应对各类突发网络安全问题的应对能力，急需对网络空间进行整治，提升公众的网络安全意识，规范公众的网络行为，培养应对各类网络安全事件的专业技术人才，这是最佳的解决此类问题的重要途径之一。

美国在全国开展了Stop.Think.Connet.活动，旨在增强公众的网络安全意识；设立各种奖学金、组织各种活动鼓励在校学生进行网络安全知识的学习，如美国国家自然科学基金（NSF）设立了服务奖学金（SFS）项目，用于资助美国多所高校的本科生和研究生进行信息保障和网络安全领域的学习；2013年秋天马里兰大学与全球防务商斯罗普·格鲁曼公司花费1100万美元联合启动了网络安全教育计划——针对学生的先进网络安全体验计划（ACES），目的是为格鲁曼公司培养所需的网络安全人才；另外，马里兰大学还组织不同知识水平的学生参加夏季项目和周末研讨会以各种方式学习网络安全知识。英国在2008年制定了《未成年人网络安全计划》将网络安全教育作为中小学课程的必修课程之一；举办公开的网络安全竞赛选拔网络安全人才，设立“网络人才储备库”吸引网络安全领域的专家和专业技术人才；2013年5月英国商务部（BIS）与工程和物理科学研究委员会共同出资750万英镑资助英国牛津大学和伦敦大学合作培养网络安全专家，成立网络安全研究中心，合作培养对抗黑客的网络攻击，保护政府和企业的网络安全。法国在中小学的礼仪与公民教育课程中增加网络安全教育的内容，中小学生需获得信息与网络资格证书。

美国网络空间安全教育计划及推广

美国作为信息技术的源起国，占据着网络空间的绝对技术优势，然而美国的网络犯罪、信息泄露、情报泄露等众多的网络安全事件却频频发生，使美国成为全球网络安全事件发生率最高的国家之一，美国的国民经济和国家安全面临着严峻的挑战。总统奥巴马认为，一项国家教育计划有助于提升整个国家的网络安全意识和数字素养，促进21世纪数字人才队伍的建设。因此，发布一项国家层次的教育计划，有利于指导整个国家网络安全意识的提升、增加网络安全领域的人才储备数和具有全球竞争力的网络安全人才已成为迫切需要。

早在2003年2月14日国土安全部（DHS）发布的《保护网络安全国家战略》中第二、第三和第四个优先任务就提出要“启动国家网络安全意识普及和培训计划”。2008年由布什总统签署，奥巴马总统解密的54号国家安

全总统令/23号国土安全总统令（NSPD–54/HSPD–23，即全面国家网络安全计划CNCI）十二项子计划中的第八条就提出要“推广网络教育”。2009年发布的《网络空间政策评估》报告在构建数字国家的四个目标中前三个目标——“提升公众的网络安全风险意识”、“建立网络安全教育系统”和“增加世界级的网络安全人才的数量，并对网络安全人才进行定义和培训”是与网络安全教育相关的，报告中的十项近期行动计划中的第六项“为增加网络安全，发起全国性的公众常识普及和教育活动”，十四项中期行动计划中的第三项“为保证国家在信息时代经济的竞争力，增加网络安全关键技术教育的力度”和第四项“制定战略来壮大网络安全人才队伍（包括在联邦政府引进和聘用网络安全专家），并对其进行培训”更是给出网络安全教育具体的行动计划。

2010年4月，美国国家标准技术研究所（NIST）发布了国家网络安全教育计划（NICE）。NICE作为一个专门的国家教育计划的发布，充分表达了美国对网络安全问题的重视程度及对网络安全问题认识的不断转变。同时，也是落实CNCI和《网络空间政策评估》报告中的近期行动计划的体现。

为开展和有效地实施NICE计划，NIST组织了各种形式的活动，如建设网络安全教育网站国家网络安全职业学习计划（NICCS）的网站（DHS负责），向公众提供免费公开的各种网络安全知识、教育和培训课程等信息；发布指导性战略文件《NICE战略计划》，为NICE的实施提供指导性建议；制定《NICE网络安全人才框架》（美国预算管理办公室OMB负责），定义了网络安全领域的每一种工作岗位所需的知识、技能和能力（KSAs）。这些措施旨在为美国的网络安全教育工作提供必要的工具和方向，确保公众和网络安全人才具有灵活的网络安全知识和技能。

同时，NIST还针对目前主流的对象，发布了一些检测网络安全威胁的工具，如联邦通信委员会（FCC）发布的安全检测器，用于检测智能手机和小型企业中存在的安全隐患，并分别针对智能手机和小型企业的安全保护问题给出了十条建议。2012年10月FCC发布了小型企业网络安全策划者2.0（Small Biz Cyber Planner 2.0）的版本，增加了新的保障网络安全的功能，并对系统在安装新的软件时给出意见，使系统在遇到数据外泄时能远程消除数据或跟踪入侵计算机和移动设备。

此外，为保障NICE计划的有效实施，联邦政府的一些相关部门还发布了一些指南、标准和报告，用于协助美国的网络安全教育活动的实施，如国防部网络安全人员框架和前期培训差异分析（国防部发布）；联邦政府网络安全人员关于网络安全工作能力转换工作组报告（国防部和DHS共同发布）；网络安全能力框架（人力资源管理办公室3发布）；CNCI计划8——扩展网络安全教育活动（DHS和国家安全局共同发布）；ISS LOB Tier 1——安全意识培训计划（DHS发布）；ISS LOB Tier 2——基于角色的培训计划（DHS发布）；基本知识体系（DHS发布）；CNSS教育培训/意识工作组和培训标准（国家安全系统委员会发布）等。

NICE 计划及主要活动

国家网络安全教育计划是由NIST牵头，DHS、国防部、教育部、NSF、国家情报总监办公室、OPM等共同领导，旨在建立一个动态的、可持续的网络安全教育计划，目的是确保各级政府正确使用良好的网络安全实践活动，从而最终提升整个国家的安全态势感知能力。其框架管理结构如图1所示。

作为NICE计划的领导者NIST除了具有协调NICE计划和工作的职责外，还负责维护和更新日常NICE网站的信息、起草计划文件、组织会议促进部门间的讨论和信息交流、代表NICE对外宣布计划的实施情况和已取得的进展等。

NICE计划目标的实现，将分为以下四个部分：

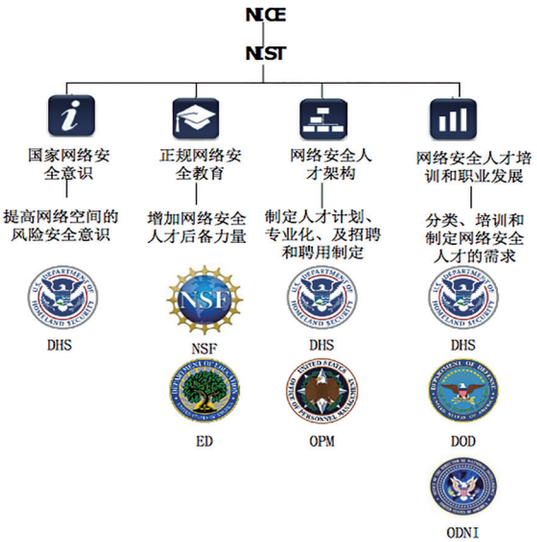

图 1 NICE 计划框架管理结构

第一部分 国家网络安全意识普及——由DHS负责。主要是通过Stop.Think.Connet.活动，增加公众对网络安全威胁的了解，提升美国公众的网络安全意识。此外，NICE还举办一些活动增加美国公众的安全意识，如“活动项目交友活动（Friends of the Campaign program）”、网民论坛等。为确保公众积极参与安全意识普及的活动中，自2010年起，美国总统奥巴马将每年的10月作为国家网络安全意识月（NCSAM）。

第二部分 正规的网络安全教育——由ED和NSF共同负责。任务是增加正规的网络安全教育计划活动（如图 2所示），这些活动主要侧重于STEM（Science, Technology, Engineering, Mathematics）领域，目的是增加政府和私营企业的专业技术人才储备，为国家培养网络安全研究人员、网络安全专业人才、网络安全技能人才（cybersecurity capable workforce）和具有网络安全意识的公民。其中，网络安全技能人才不仅包括计算机科学、信息保障、信息技术和信息安全领域里的专业人才，而且还包括关心网络安全问题的学生和工作人员。开展的活动有NSF组织的先进技术教育计划（ATE），目的在于增加网络安全人员的数量；NSA和DHS资助的国家学术卓越中心，旨在促进信息保障领域的高等教育和研究，帮助增加整个学科中IA专家的数量等。

第三部分 制定网络安全人才框架——由DHS负责统一领导，成员来自联邦部门（由OPM负责领导）、政府（非联邦）部门（由DHS负责领导）和私营企业（由DOL和NIST共同负责领导）中的网络安全人才，主要侧重于网络安全专业人才的管理。目的是评估工作人员的专业化水平，为预测未来网络安全需求推荐最佳的实践活动，为招募和挽留人才制定国家策略。

第四部分 网络安全人才培训和职业发展——由ODNI、DOD、DHS共同领导，协调学术界、工业界和各级地方政府，共同制定国家网络安全人才所需的网络安全培训和职业发展过程（培训和发展过程如图 2所示）。目的是建立和维护一个具有全球竞争力的网络安全专业人才队伍。

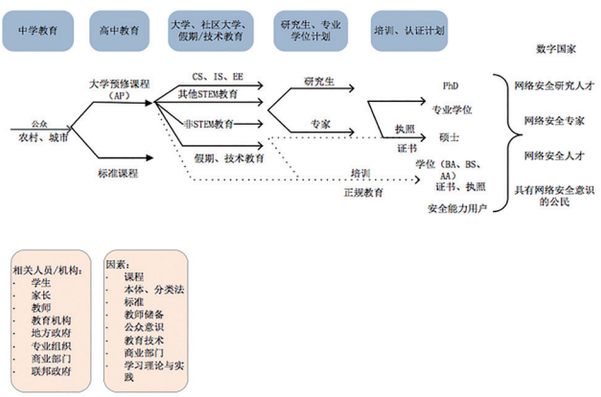

图 2 网络安全人才培养路线

NICE计划目前还在继续实施过程中，截止到目前为止，NICE的代表性活动主要有三项，一是创建国家网络安全职业学习计划网站，二是发布《国家网络安全教育战略计划》，三是发布《NICE网络安全人才框架》。这些活动为实现增强网络空间风险的国家安全意识、增加网络安全

领域的人才储备数、培养具有全球竞争力的网络安全人才的目标提供方法和路径，以保证美国具有维持经济继续繁荣和国家安全的能力。

思考与建议

目前美国集合联邦政府之前的所有工作，与学术界、工业界及私营部门一起，共同促进美国的网络安全教育计划，以促进和保障美国在21世纪的经济繁荣和国家安全。纵观整个NICE计划，联邦政府负责指导整个计划，并制定活动准则；州和各级地方政府负责在建设和达成共识方面，鼓励各界积极参与；学术界和工业界则负责积极进行参与合作，并保障最佳实践活动的进行，鼓励共同使用或超越现有技术。

作为国际上的科技强国，美国面临着网络漏洞、个人隐私泄露等众多网络安全问题，严重威胁着美国的经济发展和国家安全，而对各个方面都在发展中的中国而言，已经遇到或者即将遇到这些安全问题，NICE计划的出台与实施对我国保护网络空间安全具有积极的借鉴意义。

第一，根据我国的实际情况，出台具有全国性的网络安全教育政策，用于全局指导我国的网络安全教育工作，为提高全民网络安全意识和培养网络安全专业人才做统筹安排。同时根据政策的出台，制定有效地措施或机制，确保各种措施的有效实施和整个国家的资源得到充分的利用，如建立专门的机构用于统一管理、监督或评估政策的实施情况等。

第二，充分利用新兴媒介（如网络、媒体等）的传播、宣传和教育作用，提高公众对网络安全重要性的认识。虽然网络安全事件频繁发生，但是公众对保护网络安全的重要性并不是很了解，多数公众的隐私保护观念淡薄，对个人的网上行为有可能带来的潜在危险并不清楚，甚至认为保护网络安全是政府的事情，与个人无关。因此，政府部门除了广泛开展网络安全的宣传工作外，还应加大力度建立诸如NICCS、Stop.Think.Connet.之类的网站，为公众获取网络安全知识提供开放、便捷的环境。同时，大力鼓励各机构组织内容丰富、形式多样的网络安全意识教育活动，吸引更多的公众参与。

第三，扩充网络安全领域的教师队伍，适当地在小学、中学和大学中开设相应的网络安全领域的课程。随着计算机进入千家万户，许多人在童年时代就接触到了网络，在一些城市的小学教育中开设一些提高网络安全意识的课程，使公众在小学就接触到网络安全知识，从小培养公众的网络安全意识，该项课程的实施范围可随着生活水平的提高逐渐进行扩大。另外，政府或教育部应该鼓励开展形式多样的安全教育活动，如夏（冬）令营、公开赛、设立奖学金等，使更多的学生接触并了解网络安全知识。

第四，大力支持非正规教育机构组织的网络安全知识培训活动，充分发挥网络安全机构的专业培训作用，实现政府、企业、教育科研机构的多方合作与交流。目前国内虽然也有一些网络安全领域的培训机构，但大多是面向企业，且数量不多。另外，由于学校教育传授的只是网络安全的理论知识，培养出来的学生很少既能掌握计算机硬件和系统知识，又熟悉实际的网络安全知识和技能，需要在实战中进行大量的研发和创新活动，才能真正了解高端的网络安全威胁和对抗技术。重点发挥国家实验室、专业培训机构、企业等的专业培训作用，开展对本科生、研究生的网络安全实习计划，使更多的公众有机会参与到实践中。

第五，制定有效措施，加强网络安全研究人才的选拔、聘用和培养工作。创新的人才选拔机制、优厚的聘用条件和良好的发展空间是国内外吸引人才永不变的真理，要想确保国内网络空间的安全，需要大量网络安全领域的专业人才，只有具有良好的人才选拔、聘用和培养机制才能为国家吸引和留住更多优秀的人才。

（本栏责编：袁胜）

网络安全挑战

信息技术令企业发展如虎添翼，云时代移动办公日益普及，企业办公环境更为开放；与此同时，网络应用快速增长，并呈现移动化、Web化发展趋势，为各类威胁快速侵入网络创造了更加便捷的途径，在新的环境下，如何精准感知威胁，获取更可靠的安全保护？

华为USG6000下一代防火墙 悉您所需 为您所用

以精准感知能力全面保障您的网络安全

迈入云时代，网络边界日渐模糊，网络环境愈加复杂，企业需要更加可靠的安全屏障。华为USG6000下一代防火墙，基于ACTUAL全局环境感知，具备业内领先6000+应用识别能力和500万威胁识别能力、8种用户认证手段和全业务虚拟化技术，提供精细高效的业务隔离和安全防护，全面保障网络安全。

- 基于ACTUAL（应用，内容，时间，用户，攻击、位置）的环境感知体系实现业务环境的全局感知，提供真正面向业务的安全管控
- 6000+应用识别，500万威胁防护，30+文件内容感知提供了精准的访问控制能力
- 全新的硬件平台和引擎设计，实现了应用层性能的大幅提升，提供万兆级的全威胁防护能力，满足大型企业网络防护

更多详情，敬请访问：**enterprise.huawei.com**

华为USG6000下一代防火墙

扫描二维码
查阅解决方案
详情

扫描二维码
查阅官方微博

使用微信
扫一扫
二维码添加
官方微信

HUAWEI