创新人才培养模式 建设高素质的网络安全队伍

封化民*

北京电子科技学院 北京 100070

摘 要: 我国是一个网络大国,但还不是一个网络强国。党的十八以来,党中央高度重视网络安全工作,网络安全已成为国家安全的重要组成部分,网络安全建设已成为重中之重的任务。网络安全的竞争归根结底是人才的竞争,而网络安全人才的匮乏是制约我国网络安全发展的瓶颈因素,亟待采取多方面措施全面加强。从国外的经验看,整体规划人才培养方式、充分利用高校资源、创新体制机制、多渠道挖掘与培养网络安全人才都是有效的举措。我们要抓住机遇,因势而动,顺势而为,创新人才培养模式,努力为国家培养高素质的网络空间安全人才。

关键词: 网络空间; 人才培养; 创新; 网络空间安全

中图分类号: G642.0 **文献标识码:** A **文章编号:** 1672 - 464X(2016)3 - 01 - 07

截至 2015 年 12 月底,我国互联网普及率已达到 50.3%,网民规模为 6.88 亿; 手机网民数量为 6.2 亿; 域名".CN"的总数为 1636 万,超过德国国家顶级域名".DE",成为全球注册保有量第一的国家和地区顶级域名。可见,我国是名副其实的网络大国。[1] 但是必须直面的现实是,我国还不是一个网络强国,在网络空间安全方面的自主创新能力还相对落后,尤其是网络空间安全的人才培养方面还存在很多瓶颈,亟待全方位创新培养模式,提升我国网络空间安全的保障能力。

一、创新网络空间安全人才培养模式的迫切性

主要体现在以下三个方面。首先,目前我国的网络空间安全形势非常严峻。我国拥有世界上数量最多的网民,同时也是遭受网络攻击最多的国家,网络安全事件始终处于高发态势,国家安全和网民的利益受到严重损害。仅以 2015 年为例,从 360 互联网中心的报告看,该中心 2015 年全年就截获 PC 端新增恶意程序样本 3.56 亿个; 其网站安全检测平台共扫描各类网站 231.2 万个,扫出存在漏洞的网站 101.5 万个,占比为 43.9%,其中存在高危漏洞的网站 30.8 万个,占扫描网站总数的 13.3%。[2] 中国互联网络信息中心对互联网接入环境的分析也表明,2015 年有 42.7% 的网民遭遇过网络安全问题,其中有 22.9% 的网民发生过账号或密码被盗事件; 有 24.2% 的网民发生电脑或手机中病毒或木马情况,是最为严重的网络安全事件。[3] 由此可见,作为网络大国,我们距离网络强国还有很远的距离,全面加强网络空间安全管理已迫在眉睫,而人才培养显然是其中最为关键的环节。

第二,网络空间安全人才匮乏,亟需创新人才培养模式。2014 年,教育部办公厅、工业和信息化部办公厅对全国信息安全人才培养情况进行了普查,结果显示: 截止到 2014 年 7 月,全国

* 作者简介: 封化民(1963—),男,陕西富平人。计算机博士,教授,北京电子科技学院副院长,教育部高等学校信息安全专业教学指导委员会秘书长。主要研究方向: 网络与信息安全,多媒体智能信息处理。

共有 146 所高校培养信息安全专业人才; 近三年信息安全专业年均招生数 11182 人(含高职高专、本科、硕士、博士) ,另有信息安全专业博士后在站 49 人,分布在 19 所高校中。仅仅从数量上看,目前我国网络空间安全人才培养状况也无法满足相关行业产业的需求,"据不完全统计,国家(含机关、企事业单位) 每年对信息安全人才的需求量达到数十万,而且,随着信息化进程推进,需求量还将继续增长。"[4] 而从人才培养质量上看,目前国内尚未建立起行之有效的网络安全高端人才培养体制,也没有形成助推高水平网络空间安全专家、网络科技领域的领军人才脱颖而出的机制。因此,亟需全方位创新人才培养模式,凝聚各方共识,融合党政军及高校、社会、企业和个人的力量,共同构建我国网络安全人才培养平台。

第三,党中央高度重视网络空间安全问题,为网络安全学科建设和人才培养创新迎来千载难逢的发展机遇。回顾我国网络与信息安全建设的历史,对人才的关注可以追溯到 2005 年教育部发布的 7 号文件,提出发展和建设我国信息安全保障体系,人才培养是必备基础和先决条件。学科发展的契机是 2012 年的国发 23 号文件,提出大力支持信息安全学科师资队伍、专业院系、学科体系、重点实验室建设,为高校信息安全学科专业建设给予政策支持。2013 年十八届三中全会通过的《中共中央关于全面深化改革若干重大问题的决定》,提出"坚持积极利用、科学发展、依法管理、确保安全的方针,加大依法管理网络力度,加快完善互联网管理领导体制,确保国家网络和信息安全",国家层面的改革由此提到议事日程。2014 年 1 月 24 日,中共中央政治局召开会议决定设置中央国家安全委员会,由习近平任主席,李克强、张德江任副主席。"中央国家安全领导机构负责国家安全工作的决策和议事协调,研究制定、指导实施国家安全战略和有关重大方针政策,统筹协调国家安全重大事项和重要工作,推动国家安全法治建设。"[5] 同年 2 月 27 日,中央网络安全和信息化领导小组成立,习近平担任组长,李克强、刘云山任副组长,"再次体现了中国最高层全面深化改革、加强顶层设计的意志,显示出在保障网络安全、维护国家利益、推动信息化发展的决心。"[6] 在中央网络安全和信息化领导小组召开的第一次会议上,习近平总书记指出,没有网络安全就没有国家安全,没有信息化就没有现代化。并专门就网络安全人才培养作出指示,强调"千军易得,一将难求,要培养造就世界水平的科学家、网络科技领军人才、卓越工程师、高水平创新团队。"[7] 2015 年 6 月 11 日,为实施国家安全战略,加快网络空间安全高层次人才培养,国务院学位委员会、教育部决定在"工学"门类下增设"网络空间安全"一级学科,学科代码为"0839",授予"工学"学位,[8] 这无疑是加快我国网络空间安全人才的培养的一大举措。同年 7 月 1 日,《中华人民共和国国家安全法》公布实施,并在第五章国家安全保障中明确"国家采取必要措施,招录、培养和管理国家安全工作专门人才和特殊人才。"[9] 至此,我国网络空间人才培养的顶层设计已基本完成,网络安全学科建设与人才培养工作获得前所未有的发展机遇。

二、国外网络空间安全人才培养的主要经验

就整体而言,国外网络空间安全的人才培养起步较早、发展较快,内容规划比较成熟、方式十分灵活,主要有四方面的经验特别值得国内借鉴:

第一,整体规划网络安全人才培养方向,通过一系列政策对人才培养进行全过程引导,规范网络空间安全的基本素质。在这方面英国和美国的做法略有不同,英国主要通过人才认证的方式,美国则主要通过制定具体标准的方式来实

现。2011 年 3 月，英国政府通信总部下属国家信息安全保障技术管理局发布了《信息安全保障专业人员认证》规定，明确了政府部门及其合同厂商的信息保障专业人员的职责和技术能力要求，以及信息保障专业人员招聘、遴选、培训和管理的要求。最新版本是 2015 年 2 月发布的，将信息保障专业人员分为七个类别：认可人员、信息保障审计人员、信息保障架构人员、安全和信息风险咨询人员、信息技术安全人员、通信安全人员以及渗透测试人员。由国家信息安全保障技术管理局指定的认证机构对安全保障人员进行能力评估，判定其是否具备相应资质。[10] 美国早在 1995 年就成立信息安全学术人才中心，并在 1999 年制定了《国家信息安全战略框架》，启动美国国家网络安全教育培训计划。2008 年美国发布《国家网络空间安全全面规划》强调“虽然在保护美国政府网络空间安全的新技术上花费了数十亿美元，但成功与否的关键因素在于具备过硬知识、技能和能够实现这些技术的人，”[11] 因此建议制定专门战略，扩大人员培训，吸引专门人才。这样，到 2010 年，“国家网络空间安全教育计划（NICE）”项目正式启动，并于 2011 年 9 月公布了《NICE 网络空间安全人才队伍框架（草案）》，确立了网络空间安全工作及其人员的通用词汇、分类方法及各种标准。此后，根据形势发展的需要，该框架不断调整完善，最新的网络空间安全领域包括监督与发展、运行与维护、保护与防卫、调查、收集与运营、分析、安全供给七个方面。[12] 围绕上述七大领域，美国国家技术研究院（NIST）明确了网络空间安全所涉及的岗位及人才培养标准，不仅详细列出了每个领域的具体职位、工作任务，而且对每一种任务及其所需要的知识、技术及能力进行了明确的陈述和具体列举。[13] NICE 计划内容规定非常严谨、细腻、精致，值得国内学习借鉴。

第二，借力高等学校培养高端网络空间安全人才。高等学校在培养高端人才方面有着得天独厚的优势，因此，各国都采取各种措施借力高校培养网络空间安全方面的人才。2014 年 8 月 4 日，英国政府通讯总部宣布，授权六所英国大学提供网络安全专业的硕士文凭。这一特殊学位是英国政府 2011 年公布的“网络安全战略”的一部分，旨在通过教育提升英国防范黑客和网络欺诈的能力，同时为政府或商业部门提供未来的网络安全专家。英国内阁办公室大臣弗朗西斯·莫德说，英国政府通讯部与企业和院校合作推出的这一项目是英国经济长期发展计划的“关键部分”，它将有助于英国成为网络交易最安全的国家之一。[14] 目前全英共有 12 个网络安全硕士专业，包括爱丁堡龙比亚大学先进安全和数字取证硕士专业、兰卡斯特大学赛博安全硕士专业、牛津大学软件和系统的安全硕士专业、伦敦大学皇家霍洛威学院信息安全硕士专业、约克大学网络安全硕士专业等。[15] 美国则下大力气加强高校大型网络安全实验室建设，例如卡内基－梅隆大学成立的 CyLab 实验室，是全美规模最大的网络安全研究和教育中心之一，该实验室整合了自身在信息技术领域的全部优势，在信息保障、网络安全技术等领域处于全球领先地位。而海军研究生院成立的信息系统安全学习和研究中心，是全美信息保障专业研究生人数最多的实验室，每年有超过 400 名研究生在这里学习和工作。[16] 与此同时，美国情报部门如国安局、中情局、联邦调查局以及国防部等政府机构，近年对信息安全的人才招聘力度也不断加大，尤其面向美国东海岸知名高校以及开设有优秀信息安全教育项目的大学。美国网络安全专家、防泄密信息应用程序创始人斯塔迪卡认为，这代表网络安全行业的就业趋势变化。斯塔迪卡还发现，一些政府和私人安保机构甚至开始面向高中学生开放实习机会，着眼于向他们灌输兴趣并展示网络安全的就业前景与机会。[17]

第三，通过各类网络安全大赛助推网络安全人才脱颖而出。为了挖掘网络安全方面的精英，

很多国家都举办各种网络安全挑战赛，其中美国国防部高级研究局计划署举办的网络安全挑战赛(CGC)在世界范围有较大影响力。该赛事始于2014年6月，历时两年，总决赛于2016年在拉斯韦加斯举行，正值世界最大型计算机安全会议DEF CON期间，CGC是目前世界上持续时间最长的网络安全夺旗赛，由来自学术界、工业界和安全部门的计算机安全专家组成的35个团队参赛。2015年举办了第一场赛事，其比赛程序与Def Con黑客大会的夺旗模式相仿，要求参赛者分析和利用其他参赛团队系统中存在的薄弱环节，同时保护自己的系统。在2016年的最后一场比赛当中，参赛队伍必须拿出自主创建的安全网络防御，部署补丁和缓解措施，并且监控网络，评估竞争对手的防御机制。综合评分，最后获胜的前三名将获得比较高额奖金。[18] 日本的黑客大赛也吸引了多个国家的大量网络安全人才参与。该赛事由日本网络安全协会主办，由多个政府部门、民营企业、安全机构支持赞助，2014年有7个国家和地区的90名参赛者进入总决赛；2015年有18支队伍进入总决赛。在线预选赛和地方大赛中都采取夺旗赛的方式，出题类型包括计算机取证、网络、编程、Web杂项、逆向分析、密码分析等6种。

第四，多渠道网罗网络安全人才，普遍加强网络安全培训工作。为解决网络安全人才短缺问题，很多国家都采取了特殊措施，不拘一格降人才。如为招募更多的信息技术和编程专家来扩大防护、培训现有员工，法国国防部在雷恩建设了网络防御人员培训中心，将网络防御尖端研究人员的数量增加三倍，并拓展2012年组建的民间网络防御预备役组织，目的是动员越来越多有能力并值得信赖的人支持国家网络危机管理工作。[19] 俄罗斯方面通过招募“白色黑客”应对网络攻击。俄罗斯联邦委员会在2014年提出这项计划，希望把那些无犯罪前科、能发现系统漏洞、经验丰富的网络专家组成俄罗斯特殊的“网络部队”，对政府机构网站的防护能力进行定期检查，保护包括政府及企业信息资源在内的信息系统，建立预防计算机攻击的检测系统。[20] 英国则主要通过设立专门项目及培训来发现人才。2015年3月24日，英国宣布了一项名为“网络状元”(Cyber First)的新项目，旨在发现网络安全方面的奇才，培养下一代网络安全方面的专家。该项目既网罗那些在校园网络安全挑战赛及国家级的数学竞赛中崭露头角的顶尖人才，也直接提供资金，支持本科生学习与网络空间安全相关的科学、技术、工程和数学课程，还为本科生提供在有关国家安全领域的政府部门或私营部门实践的机会。[21] 韩国方面，主要通过组建网络安全专家团队来维护网络空间安全。该团队成立于2014年3月，由从事保护信息工作5年以上以及大赛获奖者等具有信息通信网络安全相关知识的人才组成，总计约300人，隶属韩国互联网振兴院。韩国政府计划将他们培养成网络安全方面的顶尖人才，以有效防范有关部门和单位发生的个人信息泄漏、遭黑客攻击和感染病毒等。[22]

三、创新我国网络空间安全人才培养模式的建议

相比于国外多样化的网络安全人才培养方式，目前我国网络安全人才培养模式还比较单一，不利于高端人才的挖掘和培养，无法满足信息安全形势的发展需求。因此，应该借鉴国外的成熟经验，结合我国信息安全工作的具体实际，创新体制机制，建立多元化平台，助推高素质网络空间安全人才的脱颖而出。具体建议如下：

第一，制定网络空间安全人才培养规划，发布包括网络空间安全人才应该具备的知识、能力和技术等在内的相关标准。或在划定网络空间安全相关领域的基础上，建立我国网络空间安全人才培养的任务清单、相关职位目录以及所需要

的知识、技术、能力清单，为网络空间安全的人才培养指明方向。或建立统一的认证体系，对网络安全专业人员进行认证，这有利于人才培养质量的提升。

第二，加快网络空间安全学科及专业建设，创新人才培养模式。2016 年 1 月 28 日，国务院学位委员会正式下发《国务院学位委员会关于同意增列网络空间安全一级学科博士学位授权点的通知》，通过新增或调整，共有 29 所高校获得我国首批网络空间安全一级学科博士学位授权点。今后应充分发挥首批院校的引领和带动作用，全方位积极探索专业人才的培养模式，包括培养优质师资队伍、加强实验室建设、推出一批优秀教材、开展课程内容及教学方法改革等; 要积极探索学生培养的多样化途径，通过建立实验班、特长班、跨专业综合班等，吸引相关专业的优秀人才。同时，还要研究缩短本硕博学制的可能途径，扩大实践及实习周期，帮助有网络与信息安全潜力的学生尽快成长; 要加强军民融合，充分发挥军队院校在网络安全人才培养方面的独特优势，鼓励校际、院际师资、学生的流动与交流，鼓励学生的跨学校、跨专业选课，以实现不同院校的优势互补，充分利用一切有利资源，建设一流的网络空间安全学科与专业。

第三，建立多样化网络空间安全人才选拔机制，为人才成长提供充足机会与空间。从国外的经验看，举办各种挑战赛是发现和选拔有潜质人才的一个重要途径，目前国内虽然也有类似的竞赛，但是赛制设计、赛事规模及影响力均有待提升。应该大力加强国际交流与合作，通过不断完善竞赛过程及规则，提升竞赛质量，吸引更多优秀人才参赛。除竞赛外，还可以通过建立网络平台，统筹国内的优质资源，包括在军民融合背景下，利用军地网络安全资源，实现军民优势互补、融合发展。同时，还应积极鼓励校企合作，使相关企业能深度参与高校的网络安全人才培养工作，使人才培养能够切实满足企业的现实需求。最后，还应积极发挥科研院所、行业协会在人才培养方面的积极作用，促进其与高校的协同合作，建立创新发展中心、培训中心、研究中心，为人才成长提供充足空间。

第四，创新网络空间安全人才培养的激励制度，创造宽松的人才成长孵化环境。网络空间安全人才培养既包括对从事相关专业在职人员的再教育，也包括发现挖掘新人尤其是年轻人，对这两类人员的培养方式应该有所差别。对于从事网络空间安全的在职人员，开展培训及继续教育是最重要的手段，同时要建立有效的激励机制，例如建立卓越工程师项目，设立千人培养计划、万人培养工程等; 同时，还可以通过各种评比活动如国家网络安全优秀人才奖、表彰奖励活动激发在职人员的工作热情。但对于初出茅庐的年轻人，吸引他们的最好方法是激发他们的研究兴趣。谷歌在创立之初曾通过一道非常复杂的数学题，吸引了成千上万的专门人才敲开了公司招聘的大门，这些人甚至都不知道这是一则招聘广告，仅仅凭着对数学题的浓厚兴趣齐聚谷歌麾下，成就了谷歌的辉煌。而 2016 年 3 月，美国国防部甚至发起了一项“攻击五角大楼网络”活动，邀请经过审查的外部黑客对国防部的一些公开网址进行测试，预计届时将有数千名合格的人员参加试验计划。[23] 特别需要强调的是，对待年轻人的成长，宽松包容的孵化环境非常重要。因此，创新活动方式与创造宽松包容的孵化环境对培养年轻人同等重要，是激发年轻人网络安全兴趣必不可少的外部保障。

总之，网络空间安全事关国家安全，而人才培养是网络空间安全保障体系的关键环节。我们要把握住时代的发展机遇，群策群力，按照习近平总书记的指示，把人才资源汇聚起来，建设一支政治强、业务精、作风好的强大队伍，为建设网络强国而奋斗。

参考文献

[1] CNNIC. 第 37 次中国互联网络发展状况统计

报告[R]. 北京: 中国互联网络信息中心,2016 -01 -22.

[2] 360 互联网安全中心. 2015 年中国互联网安全报告[R]. 北京: 360 互联网中心,2016 -02 -29.

[3] 刘畅. 2015 年全球网络安全行业面面观[N]. 人民邮电. 2016 -1 -11(006).

[4] 封化民. 人才培养: 网络空间安全保障体系的关键环节[J]. 信息安全与通信保密,2014(5):24.

[5] 中华人民共和国国家安全法,第一章第五条,2015 -07 -1.

[6] 中央网络安全和信息化领导小组成立,习近平任组长,强调创新发展,把我国建设成为网络强国[N]. 人民邮电. 2014 -03 -03(1).

[7] 习近平主持召开中央网络安全和信息化领导小组第一次会议[N]. 人民日报. 2014 -02 -28(1).

[8] 国务院学位委员会,教育部. 国务院学位委员会 教育部关于增设网络空间安全一级学科的通知(学位[2015]11 号)[EB/OL]. 教育部网站.(2015 -06 -11)[2016 -07 -18].
http://www.moe.edu.cn/jyb_xxgk/moe_1777/moe_1778/201511/t20151127_221423.html.

[9] 中华人民共和国国家安全法,第五章第七十四条,2015 -7 -1.

[10] 王星. 英国网络安全人才队伍建设体制研究[J]. 中国信息安全,2015(11):102.

[11] 张文贵,彭博,潘卓. 国家网络安全综合计划(CNCI)综述[J]. 信息网络安全,2010(9):70.

[12] Interactive National Cybersecurity Workforce Framework[CP/OL].
https://niccs.us-cert.gov/training/tc/framework.

[13] Information Systems Security Operations (Information Systems Security Officer)[CP/OL].
https://niccs.us-cert.gov/training/tc/framework/spec-area-detail/28。

[14] 英国情报机构推出“网络间谍”硕士专业[N]. 信息时报. 2014 -08 -04.

[15] 王星. 英国网络安全人才队伍建设体制研究[J]. 中国信息安全,2015(11):103.

[16] 刘金芳. 国外网络安全人才建设的经验及启示.[EB/OL]. 网易.(2014 -11 -27)[2016 -07 -19].
http://gov.163.com/14/1127/16/AC2RGTK600234IG8.html.

[17] 孙宝云. 全球网络部队建设、网络安全人才培养与网络安全教育: 2014 年新动向[J]. 北京电子科技学院学报,2015(1):70 -71.

[18] 小朗. 美军方将举办全球首届“黑客大赛”[N]. 扬子晚报. 2014 -06 -05.

[19] 法国“很忙”: 扩编网络部队 订购攻击核潜艇新型加油机[EB/OL]. 深圳广电集团.(2014 -02 -23)[2015 -01 -03].
http://www.s1979.com/a/20140223/23114675923.shtml.

[20] 俄联邦委员会拟利用“白色黑客”应对网络攻击[N]. 环球时报. 2014 -01 -26.

[21] Cyber First: improving cyber skills in the UK, Cabinet Office. 24 March 2015. https://www.gov.uk/government/news/cyber-first-improving-cyber-skills-in-the-uk.

[22] 徐悦、李小飞. 韩拟建一支 300 人网络安全队伍 防黑防毒防诈骗[EB/OL]. 环球网.(2014 -02 -26)[2016 -08 -11].
http://world.huanqiu.com/exclusive/2014 -02/4861201.html.

[23] 美国防部邀请黑客攻击五角大楼网站[EB/OL]. 观察者网.(2016 -03 -03)[2016 -07 -20].
http://www.guancha.cn/america/2016_03_03_352813.shtml.

Innovating Training Model and Constructing High-quality Network Security Team

Feng Huamin

(Beijing Electronic Science and Technology Institute, Beijing 100070, China)

Abstract: China is a cyber giant but not a strong cyber power. After the 18th National Congress of the Communist Party of China, the CPC Central Committee attaches great importance to network security. Network security became an important component of national security, and the building of network security has become a priority task. Cybersecurity competition in the final analysis is the talent competition, and the lack of network security professionals becomes the bottlenecks to restrict the development of China's network security. Correspondingly, a variety of measures to comprehensively strengthen the building of cybersecurity should be taken into consideration. Experiences from abroad like overall planning of talent training mode, making full use of university resources, innovation of institutional mechanisms, multi-channel mining and cultivating talents are effective measures to strengthen network security. We must seize the opportunity and strive to cultivate high-quality national cyberspace security talent.

Keywords: Cyberspace; Talent Cultivation; Innovation; Cyberspace Security

(责任编辑: 李波洋)