

网络空间安全人才培养的规划建议

张宏莉, 于海宁, 翟健宏, 余翔湛

(哈尔滨工业大学计算机网络与信息安全中心, 黑龙江 哈尔滨 150001)

摘要: 网络空间安全竞争的核心是人才的竞争。首先介绍了网络空间安全的内涵和特点, 分析了目前国际上网络空间安全人才的培养现状。然后, 指出了我国网络空间安全人才培养中存在的主要问题。最后, 面向国家在网络空间安全人才建设方面的重大战略需求, 从国家统筹规划、学历教育、职业培训与认证、专才发现与培养等4个方面给出了规划建议, 以探索完善我国网络空间安全人才培养体系。

关键词: 网络空间安全; 人才培养; 学历教育; 职业培训与认证; 专才发现与培养

中图分类号: G643.0

文献标识码: A

doi:10.11959/j.issn.2909-109x.2016.00027

Suggestions on cyber security talents cultivation

ZHANG Hong-li, YU Hai-ning, ZHAI Jian-hong, YU Xiang-zhan

(Computer Network and Information Security Center, Harbin Institute of Technology, Harbin 150001, China)

Abstract: Talent competition is the core content of cyber security competition. Firstly, the definitions and characteristics of cyber security were introduced. Then, the development status of international cyber security talents cultivation were analyzed, and the main problems existing in cyber security talents cultivation were pointed out. Finally, based on national significant strategy, suggestions on cyber security talents cultivation to explore a sophisticated architecture were proposed, which refer to the national overall planning, academic education, vocational training and certification, genius discovery and cultivation.

Key words: cyber security, talent cultivation, academic education, vocational training and certification, genius discovery and cultivation

1 引言

习近平总书记在中央网络安全和信息化领导小组第一次会议上强调,“没有网络安全,就没有国家安全”、“加强网络空间安全人才建设,打造素质过硬、战斗力强的人才队伍”、“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”。

领导小组 2015 年工作要点分工方案中明确提出“建立网络(空间)安全一级学科”。2015 年 6 月,国务院学位委员会、教育部批准增设“网络空间安全”一级学科,学科代码为“0839”,授予“工学”学位^[1]。2015 年 12 月,经学位办批准,我国 29 所高校设立网络空间安全一级学科博士点^[2]。网络空间安全不仅需要研究能力和创新技术,更需要高层次网络空间安全人才的支撑。目

收稿日期: 2016-01-23; 修回日期: 2016-02-12。通信作者: 张宏莉, zhanghongli@pact518.hit.edu.cn

基金项目: 中国工程院咨询研究基金资助项目(No.2016-JY-002)

Foundation Item: The Chinese Academy of Engineering Consulting Project(No.2016-JY-002)

前, 国家政策的支持和网络空间安全一级学科的设立使我国网络空间安全人才培养走上了快车道, 依靠国家政策和一级学科的引领和带动作用, 能够加强跨学科交叉融合、汇聚高素质师资、吸纳优秀学生、加大资源投入, 这为网络空间安全人才培养提供了坚实的基础。

网络空间 (cyberspace) 是所有由可对外交换信息的电磁设备作为载体, 通过与人互动而形成的虚拟空间, 包括互联网、通信网、广电网、物联网、社交网络、计算系统、通信系统、控制系统等^[3]。网络空间与物理空间紧密结合, 成为信息时代社会有机运行的神经指挥系统, 被称为陆、海、空、天之后的第五空间。网络空间安全 (cyber security) 研究网络空间中的安全威胁和防护问题, 即在有敌手 (adversary) 的对抗环境下, 研究信息在产生、传输、存储、处理的各个环节中所面临的威胁和防御措施、以及网络和系统本身的威胁和防护机制。网络空间安全包括传统信息安全所研究的信息保密性、完整性、可用性、真实性和可控性, 以及网络空间的基础设施、信息系统的安全性和可信性。

网络安全学科是在信息技术及其应用的快速发展中逐渐形成的, 针对信息生成、存储、传输、处理和交互的各个环节, 用数学方法刻画和描述其变换的过程和状态, 建立安全控制与管理模型, 进而保障信息及信息系统的高安全性、高可信性和高可用性。网络空间安全学科是综合了通信、电子、计算机、数学、物理、生物、管理、法律等学科, 而发展形成的新兴交叉学科, 它与这些学科既有紧密的联系和渊源, 又具有本质的不同。网络空间安全学科已经形成了自己的内涵、特点、理论、技术和应用, 从而构成了一个独立的学科和研究领域。

网络空间安全学科是信息安全的继承和发展, 与传统意义上的信息安全既有联系又有区别, 研究对象、研究方法、研究内容等内涵和外延更加丰富, 进一步体现国家网络安全重大战略需求, 适应我国网络空间安全的严峻形势、技术趋势和发展形式。网络空间安全学科从研究对象看, 具有一般工科学科不具备的特殊性; 从作用地位看, 具有军地一体、军民融合的特点; 从知识体系看,

具有多学科交叉融合的特点; 从技术体系看, 具有网密一体、攻防兼备的特点; 从学科前沿看, 具有很强的动态发展性特点。

本文从网络空间安全学历培养体系、网络空间安全职业培训与认证体系、网络空间安全专才发现与培养体系 3 个方面切入研究, 针对网络空间安全人才数量奇缺、结构失衡、培养与产业界需求脱节、忽视专才发现和培养等问题, 探索适合我国国情的多层次、多类型的网络空间安全人才培养体系。

2 国际上网络空间安全人才培养现状

2.1 国家战略与计划

国际上, 各国政府都高度重视网络空间安全, 美国、俄罗斯、欧盟、日本、韩国等政府纷纷出台了国家网络安全战略, 制定和实施网络安全人才培养计划^[4]。其中, 美国 2010 年出台的“NICE 战略计划”是比较系统和完善的计划之一^[5]。NICE 计划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。牵头机构为国家标准技术研究所 (NIST, National Institute of Standards), 成员机构包括国土安全部 (DHS, Department of Homeland Security)、国防部 (DoD, Department of Defense)、教育部、国家科学基金会 (NSF, National Science Foundation)、国家情报总监办公室、人事管理局 (OPM, Office of Personnel Management) 等。

NICE 计划由 4 部分组成。第一部分为国家网络安全意识普及, 由 DHS 负责。主要是通过网络安全意识普及活动, 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。第二部分为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, 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、网络安全技能人才和具有网络安全意识的公民; 开展的活动有 NSF 组织的先进技术教育计划 (ATE, advanced technology education), 目的在于增加网络安全人员的数量; NSA 和 DHS 资助的国家卓越学术中心, 旨在促进信息保障领

域的高等教育和研究中信息保障专家的数量等。第三部分为网络安全人才框架,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。第四部分为网络安全人才培养和职业发展,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。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。

2.2 网络安全人才学历培养

为了建立大规模、多层次的网络安全专业人才培养格局,为美国培养网络安全专业人才培养良好的基础,美国国家安全局于 1998 年发起、1999 年开始在高校设立国家信息保障教育卓越学术中心(CAE/IAE)。首批有 8 所高校被授予设立中心的资格,2001 年增至 14 所大学。之后为加强信息安全学历教育,特别是信息安全研究生教育和学术基础研究,又设立了国家信息保障研究卓越学术中心(CAE/R))。截至 2013 年 8 月已有 181 所大学被授予 CAE/IAE 和(或)CAE/R,或 CAE/2Y(面向社区大学,两年学制,2010 年启动)资格,其中,38 所高水平大学具有 CAE/IAE 和 CAE/R,20 所高水平大学具有 CAE/R,91 所大学具有 CAE/IAE,32 所社区大学具有 CAE/2Y。为培养网络作战人才,2011 年,美国国家安全局启动设立国家网络行动卓越学术中心(CAE- Cyber Operation),至 2013 年已有 8 所老牌的信息安全研究强校入选,其中有卡内基梅隆大学和海军研究生院等。同时,对已有的 CAE/IAE、CAE/R 和 CAE/2Y 开展了新的评估。

在教学内容方面,国家安全系统委员会(CNSS, Committee on National Security Systems)制定了 CNSS 课程指南,要求教育卓越中心的教学和课程设置应符合该指南,具体包括:信息系统安全专业人员国家培训标准(NSTISSI-4011)、

高级系统管理员国家信息保障培训标准(CNSSI-4012)、系统管理员国家信息保障培训标准(CNSSI-4013)、信息安全官国家信息保障培训标准(CNSSI-4014)、系统检测认证员国家培训标准(NSTISSI-4015)、风险分析员国家信息保障培训标准(CNSSI-4016)等。同时,NSA 制定了网络行动卓越中心专业课程要求。必修课程包括:离散数学、低级编程语言、软件逆向工程、操作系统理论、计算机网络、蜂窝和移动通信、安全性基本原理、网络空间防护概述、漏洞分析、相关法规等。选修课程包括:计算机体系结构、系统编程、虚拟化技术、大规模分布式系统、可编程逻辑语言、微控制器设计、FPGA 设计、嵌入式系统、SCADA 系统、硬件逆向工程、应用密码学、无线安全、软件安全性分析、安全软件开发、信息系统风险管理、取证和事件响应或介质利用(media exploitation)人机交互/合用性安全、攻击性网络行动等。

在教学方式方面,开设培训课程、组织研讨会是美国高校进行网络安全学历教育的常用模式,游戏教学是近年来备受关注的寓教于乐的教学模式,它能够充分调动学生的积极性,增强教学内容的趣味性和吸引力。不少高校还综合利用上述方式开展网络安全学历教育。

在教学研究方面,NSF 将网络安全教育研究项目完全等同于科研项目进行支持和管理,既强调了教育研究的重要性,同时也加强了对教育研究的科学性的高要求,对促进和鼓励开展网络安全教育研究有很好的作用。自 2012 年起,美国国家科学基金发布了安全和可信网络空间的项目指南(NSF 12-596 和 NSF 13-578),项目在 2014 年的资助经费总额达到 7450 万美元,其中 240 万美元专项资助 8 项网络空间安全教育项目。NSF 发出了加强网络空间安全教育研究的意向通告信,考虑将通过“NSF 早期概念的探索性研究”项目进一步资助网络空间安全教育研究。NSF 继续加大对“网络军团服务奖学金”的支持力度,2014 年新增资助经费总额达 1 967 万美元。据美国《商业周刊》网站 2014 年 4 月 15 日的报道,已有 1554 名学生获得该奖学金毕业,另有 463 名学生在校。

在办学模式方面,大胆探索应用型人才培养

新模式, 强化实践能力培养。对于国家急需的网络安全人才, 特别是政府相关部门需要补充的专业人员, 美国采取了由其信息安全主管部门授权的方式, 鼓励和支持大学开展网络安全领域的专业教育, 并由用人单位主导, 预先确定培养方案, 包括具体的主要课程和教学内容, 这样就能够准确地指导高校为学生提供与实际需求紧密结合的知识体系和能力训练, 解决了大学教学与实际应用相脱离的问题; 美国需要大量的网络安全专业人士, 美国政府通过网络安全竞赛发现懂得攻防的下一代“网络战士”。美国国家安全局与卡内基梅隆大学联手举办“高中黑客大赛”旨在挖掘有潜质的青少年人才; 设立富有竞争力的研究项目和薪酬吸引高素质的人才。

2.3 网络安全人才培养

在网络空间安全人才培养方面, 美国政府、高校及科研机构、专业组织和各大公司都投入到信息安全的培训和教育中, 提供相应的课程、开展各类研讨会并颁发各种培训证书, 基本上形成了规模化的信息安全继续教育与培训产业。

美国国家政府许多机构都向他们的工作人员提供信息保证和安全方面的培训, 形成大批量的培训需求。美国的网络安全教育与培训要求研究机构美国国家标准技术研究所(NIST, National Institute of Standards and Technology)根据NISTSP800-16N定义教育和培训的基本内容, 测试和评估课程内容符合信息安全工作的实际需要, 行业协会(IFIP\ISACA\ASTS等)负责组织教育和培训工作, 最后由国家安全代理机构INFOSEC建立对信息保障培训的评估程序, 旨在评估研究机构、大学等学校在提供培训方面的等级是否符合NSTITSSL标准。

目前, 国际网络空间安全认证和培训体系具有较高的权威性和认可度, 例如, 国际信息系统安全认证联盟(ISC)²的注册信息安全师(CISSP, certified information systems security professional)认证、注册软件生命周期安全师(CSSLP, certified secure software lifecycle professional)认证、注册网络取证师(CCFP, certified cyber forensics professional)认证等^[6]; 信息系统审计与管控协会ISACA的注册信息系统审计师

(CISA, certified information systems auditor)认证、注册信息安全经理(CISM, certified information security manager)认证、企业信息科技管治(CGEIT, certified in the governance of enterprise IT)认证、风险及信息系统监控(CRISC, certified in risk and information systems)认证等^[7]; 国际电子商务顾问局EC-Council的道德骇客(CEH, certified ethical hacker)认证、安全分析师(ECSA, EC-council certified security analyst)认证、授权渗透测试员(LPT)认证、首席信息安全官(CCISO, certified chief information security officer)认证等^[8]。

综上所述, 发达国家致力于制度的建设, 以较为完备的法律法规和国家标准引导行业协会和组织建立信息安全的教育和培训机构, 引领网络安全人才培养的健康发展。

3 我国网络空间安全人才培养存在的主要问题

网络空间安全一级学科的设立为我国网络空间安全人才的学历培养提供了坚实的基础。经过多年发展, 我国初步形成了网络空间安全职业培训和认证体系, 例如CISP认证和相关授权培训。然而, 综合来看, 目前我国网络空间安全人才培养体系并不完善, 难以满足国家关于“加强网络空间安全人才建设”的战略需求, 存在的主要问题如下。

1) 亟待加强国家级顶层设计, 统筹规划网络空间安全人才教育与培训工作

网络空间安全防护能力高低与信息系统的的设计、实现、维护、管理、使用过程中每个人的防护能力密不可分, 需要唤起全社会各年龄段人们的安全意识, 尤其IT从业者更应具备基本的防护和应对能力。目前, 仅在部分高校设立信息安全类本科专业和网络空间安全一级学科尚不能达到以上目的, 同时缺乏必要的、规范的高标准的培训。国家和社会需要进一步回答“谁需要”、“谁培训”、“培训谁”、“培训什么”、“培训得怎么样”等一系列问题。

2) 网络空间安全人才需求迫切, 数量奇缺

根据高校信息安全人才培养情况调查统计(教高厅函[2014] 4号), 信息安全研究生年均就

业率不小于 97%，本科生年均就业率不小于 95%，远高于其他专业。截至 2013 年，教育部批准全国共 96 所高校设置信息安全类相关本科专业，其中信息安全专业 85 个，信息对抗专业 17 个，保密管理专业 12 个，每年培养毕业生约 1 万人，累计不超过 8 万人，我国网络空间安全的人才缺口已超过 50 万人。美国的 ISACA 协会公布的 2015 年全球网络空间安全状态的报告，网络空间安全人才的缺乏率达到了 86%。随着我国信息化建设的不断推进，网络安全专业人才需求将持续增长，并呈逐年递增趋势，预计到 2020 年，我国网络空间安全人才需求数量将超过 140 万人。具体原因有以下 2 点。

① 网络空间安全的学历培养体系不完善，导致招生数量较低，培养能力不足。② 网络空间安全的职业培训制度建设滞后，导致培训市场秩序差，认可度低；专业培训机构数量少，培训规模有限；培训机构能力参差不齐，培训质量有待提高。在当前网络空间安全人才培养体系下，很难在短期内培养出大量优秀的网络空间安全人才。

3) 网络空间安全人才结构失衡，高端创新型人才极度匮乏

从我国网络空间安全人才教育程度来说，本科学历的信息安全人才占据较大比重，高达 61.8%；硕士研究生以上学历的约占 9.6%；大专约占 25.2%；其他约占 3.4%。高学历人才相对较少。网络空间安全学科综合了通信、电子、计算机、数学、物理、生物、管理、法律等学科，是一门新兴的交叉学科，其涉及众多领域知识和技术。目前，我国具备卓越的网络空间安全知识和技术的核心技术攻关型人才和高端战略型人才十分匮乏，且梯队化培养机制尚未形成。其原因包括：① 本科生培养过程中忽视交叉学科间的相互融合，导致网络空间安全人才缺乏多学科的基础知识；② 研究生培养过程中忽视分类指导，因材施教，降低了深入钻研、创新研究的兴趣，导致网络安全人才缺少“高难度对抗”的能力；③ 现有的网络空间安全人才学历培养更注重理论学习，实战方面的培养力度不足。在当前网络空间安全人才培养体系下，很难在短期内培养出高质

量的核心技术攻关型和高端战略型网络空间安全人才。

4) 网络空间安全人才培养与产业界需求脱节，匹配度不高

产业界经常抱怨高校网络空间安全毕业生无法快速适应实际岗位工作需求，高校毕业生与网络空间安全用人单位岗位匹配度较低。高校毕业生往往需要用人单位进行一年甚至更长时间的二次培训才能适应实际工作需求。主要有如下 3 个原因。① 教育界和产业界人才供需对接的不匹配导致安全人才学历培养与产业界需求脱节。教育界按照一级学科内涵和边界“自顶向下”地确定学科的研究方向、研究内容、理论体系和知识体系，制定相应的课程体系和培养方法，进而全面系统地培养“创新和实用符合型”人才。产业界不关心一级学科的边界，只在乎“实用型”人才的某些实用技能，期望按照实际需要“自底向上”地构建网络空间安全的学历培养体系。② 长久以来，教育界和产业界共同呼吁产学研合作联合培养人才，然而，实际执行效果不佳，企业倾向于“掐尖”网络空间安全专业毕业生，缺少针对性的实习、实训培养体系。③ 随着新兴技术的快速发展，网络空间安全技术和应用领域快速更新，安全风险层出不穷，网络攻击和防护的对抗日益激烈，更加剧了网络空间安全人才培养与实际需求的脱离。在当前网络空间安全人才培养体系下，很难在短期内修复网络空间安全人才培养与产业界需求的脱节。

5) 缺少网络空间安全专才的发现和培养体系，难以保障专才的产生、发现、成长和成功

相比于理论基础坚实、成果丰硕的“学院派”网络空间安全人才，网络空间安全的“奇才”和“怪才”对网络空间安全技术有着强烈的兴趣和热情，他们一般非科班出身，实践经验丰富，实战成果丰硕，通过高难度对抗解决实际安全难题，他们“剑走偏锋”的技术往往成为网络空间安全对抗中的杀手锏。目前，我国对网络空间安全专才的选拔和培养投入不足，尚未建立针对性的发现和培养体系以及认可机制。网络空间安全专才无法完全为国家网络空间安全事业所用，甚至其中一些人成为了危害国家网络空间安全的潜在因

素。其原因包括：①“黑客”是一把双刃剑，如果才能用反了方向，对国家、社会和个人都不利，人们总是担心“培养出太多的黑客”；②国内外的事实证明，按常规的学历培养体系，很难培养出顶级的“黑客”，许多顶尖“黑客”偏科严重，考试不及格，被认为是“差生”，他们缺少社会的认可，才能往往被埋没。在当前网络空间安全人才培养体系下，无法保障网络空间安全的“奇才”和“怪才”的产生、成长和成功。

综上所述，我国迫切需要认清当前网络空间安全人才培养存在的问题，最终从国家顶层设计角度，打破传统人才培养方面的限制，探索适合我国国情的、多方合作的、多层次、多类型的网络空间安全人才培养体系，加快我国网络空间安全人才队伍培养步伐，支撑网络强国建设。

4 建议与措施

为了促进网络空间安全人才数量和质量的快速提升，需要对网络空间安全人才培养的国内外现状、发展态势等进行综合分析，进而凝练出人才培养的关键问题，并提出合理可行的人才培养体系。网络空间安全人才的培养规划建议主要包括3个方面：“研究网络空间安全的学历培养体系，以学历教育为主渠道，为我国网络空间安全建设提供素质全面的人才”；“研究网络空间安全的职业培训与认证体系，以职业培训为辅助渠道，快速灵活地为我国网络空间安全建设提供满足实际工作岗位技能要求的人才”；“研究网络空间安全的专才发现与培养体系，以专才的发现与培养为特殊渠道，为我国网络空间安全建设提供道德黑客”。具体规划建议如下所述。

4.1 国家网络空间安全人才的统筹规划

网络空间安全人才最终要服务于国家和社会网络空间安全保障事业之所需。因此，首先需要加速国家网络安全战略的制定，从国际竞争、国家安全保障的角度，理清保卫网络主权的基本原则和核心策略，界定各网络主体在网络安全管理中的责任权利，进而明确对网络空间安全人才的具体需求。根据我国网络空间安全的发展现状，

定义我国网络空间安全工作的岗位分类法及其通用词汇，并对每种岗位的职责标准，以及从业人员所需的“知识、技能、能力”进行详细的描述。一方面，引导行业和用人单位部署内设机构、设置相应岗位、确定人员编制，推动网络空间安全岗位体系的建立，为网络空间安全认证和培训提供市场需求。另一方面，指导完善我国网络空间安全人才培养体系，明确人才培养和培训目标，保障人才培养有的放矢。基于此，进一步制定培养和培训内容、质量认证标准、培训机构资质、培训组织与实施过程、专业人才库等一系列规范和标准。

4.2 网络空间安全的学历培养体系

针对不同类型、不同层面、不同技术领域的人才设立系统化的培养目标。以本科生“厚基础、宽方向”和研究生“分类指导、分轨培养”为指导方针设定培训内容。采用以高校为主导的“校际合作、校企联合和政府支持”的方式，制定产学研合作的、包容多模式、多轨道的培养方法。建立完善的网络空间安全的学历培养体系涉及到4个关键要素：外部资源环境、师资队伍、科学研究、人才培养。师资队伍和外部资源环境为人才培养和科学研究提供基础支撑，人才培养和科学研究形成良性的相互促进关系，因此，构建学历培养体系要围绕着这些要素系统化地规划，打破学科边界，打开产学研的藩篱，通力合作培养理论和实践并重的网络空间人才。具体建议如下。

1) 师资队伍的建设。全面加强师资队伍建设和持续提升师资水平是提高学历培养质量的根本。以网络空间安全一级学科为牵引，进一步吸引国内外高水平科研、教学人员，甚至产业界高端人才，扩充网络空间安全学科教师队伍。

2) 多模式培养机制的构建。为学生提供多种类型培养方案，学生根据自身的能力、兴趣和未来规划自由的选择培养方案，给学生充分的自由度，让他们充分发挥自己的特长。各个培养方案之间相互联系，侧重点互补。

3) 科研与实践能力的提升。坚持服务国家目标与鼓励自由探索相结合的科研模式，培养

学生发现前沿性问题和探索新的方法解决问题的能力，科研与教学相结合提升学生科研实践能力。

4) 产学研的通力合作。教育界和产业界深度合作，通过联合实验室、科研项目合作、联合课程建设、学生实习实训等手段积极探索产学研共育网络空间安全人才的机制，实现高校人才培养与产业界需求的无缝衔接，不仅向产业界提供高质量的实用型人才，还提供核心技术攻关型和高端战略型人才。

4.3 网络空间安全的职业培训与认证体系

网络空间安全的职业培训与认证是我国网络空间安全人才建设的重要组成部分。相比与网络空间安全的学历教育，网络空间安全职业培训具有以下特点。1) 针对性和实用性。体现在培训目标和课程等根据岗位实际需求和执业认证标准确定。2) 灵活性和多样性。体现在培训形式多样，培训时限弹性，培养对象不受限制，教学形式灵活。3) 技术性和技能性。体现在培训方法强调理论与实践操作相结合。4) 连续性和持久性。体现在职业培训周期短，能够应对网络空间安全领域不断涌现的新知识、新技术和新产品。这些特点决定了建立职业培训与认证体系能够快速壮大网络空间安全人才队伍，持续提升网络空间安全人才的技术水平和实践能力。

针对我国网络空间安全职业培训与认证存在的主要问题，建立相关政策和制度；建立政府、认证机构、培训机构、高校及科研院所、企业多方协作的认证和培训模式；规范我国认证机构和培训机构的认可授权制度，完善我国认证的知识体系和培训的课程体系；加强我国认证机构和培训机构的基础设施和师资队伍建设；积极推动我国认证和培训的全球标准化进程，夺取网络空间安全认证和培训的国际话语权。进而初步构建自我发展、良性循环的网络空间安全职业培训与认证体系。具体建议如下。

1) 由行业协会牵头，面向行业岗位需求制定培训标准

面向国家和社会的实际需求，制定规范的网络安全人才知识体系和能力体系标准，明确网络空间安全人员应该具有的“知识、技能、能力”，

为网络空间安全职业培训提供市场需求，确保各培训渠道的培养有的放矢；为了提高国家整体网络防护能力，规范关键网络基础设施单位用人制度，关键岗位从业人员必须具备相应资质能力，持证上岗；制定培训机构资质认定标准、培训过程认证标准、人才资质评价与认证标准。

2) 建立网络空间安全认证机构和培训机构的认可制度

根据国际标准《ISO/IEC 17024-2012 合格评定人员认证机构通用要求》，建立我国网络空间安全认证机构的认可制度。认证机构的认可制度有利于推广我国认证机构所提供的特有资格和专业知识和技能，保护认证的信誉，增进用人单位和公众对本土认证和持证者的信心，推动跨国、跨行业的人才流动。认可制度的建立将加快我国网络空间安全认证的全球标准化进程，为持证人提供更广阔的发展机遇。培训机构的认可授权制度用以明确职业培训机构的资质认定标准，确定授权培训机构的职能，规范授权培训机构的审批、考核和管理。培训机构的认可授权制度有利于规范我国网络空间安全培训市场秩序，推动培训机构师资队伍、课程体系和配套实验环境的建设，进而提升网络空间安全职业培训质量。

3) 大力支持网络空间安全职业培训的发展，加快基础设施建设，实施讲师培训工程

国家和各级政府在融资、开业、税收、咨询等多方面出台优惠政策，支持网络空间安全培训机构的创立和发展，逐步形成覆盖全国的职业培训网络，使职业培训“人人可学，处处可学，时时可学”。对于获得认可授权的执业培训机构，按照其年度培训人数、培训人员获得认证的级别等指标给予资金奖励。对创新培训模式、部署实时仿真教学实验平台，且培训质量显著提升的培训机构给予资金奖励，并协助其推广先进培训经验和成果。实施网络空间安全培训讲师的培训工程，委托高校或网络空间安全协会制定培训的知识体系，设置培训课程，开展培训工作。每年定期统一举行培训讲师认证考试，对考试合格的申请人授予网络空间安全培训讲师执业资格。网络空间安全培训讲师

持证上岗, 强制要求培训机构聘请具有执业资格的培训讲师授课。根据上岗年限、培训人数和通过率等指标制定培训讲师的等级晋升制度, 并建立培训讲师人才库。

4.4 网络空间安全专才的发现与培养体系

针对网络空间安全领域的“奇才”和“怪才”, 要特殊对待, 绝不能按常规出牌, 遵循“因材施教”、“早发现、早培养、早锻炼”的原则, 要鼓励学生“剑走偏锋”。为建立我国网络空间安全专才发现与培养体系, 特别是青少年专才的发现与培养体系, 吸引青少年学习网络空间安全知识, 尽早发现青少年专才, 专门培养青少年专才成长、成才, 提出如下建议。

1) 举办全国青少年网络空间安全竞赛, 选拔网络空间安全青少年专才, 提高竞赛奖励力度, 防止专才流失

我国举办的青少年网络空间安全知识竞赛和青少年信息学奥林匹克赛, 均缺少网络空间安全实战对抗的元素, 青少年专才参加这类竞赛难以获取实战对抗的成就感。目前, 我国青少年专才缺少一个兴趣驱动、重实践、高水准、公平公正的网络空间安全竞技对抗的舞台来尽情展示自身的网络空间安全技艺。鼓励主办全国青少年网络空间安全竞赛, 旨在发现网络空间安全青少年人才, 激发青少年对网络空间安全技术的兴趣, 为我国网络空间安全人才队伍建设提供青少年人才储备。青少年网络空间安全竞赛相比于国际黑客竞赛在竞赛形式、考察重点、参赛人员、题目难度和知识范围等方面存在较大区别。青少年网络空间安全竞赛经验不丰富、心智还未完全成熟。因此, 题目难度应有所降低, 达到一个合适青少年年龄段的程度。尤其在预赛中, 针对一个方向的一道题目一般可只设置 1~2 个考点, 而设置 3 个以上的连环考点对于他们来说就相当困难, 会导致竞赛选拔失效。青少年网络空间安全竞赛具有兴趣驱动、注重实践、公平、高水平的特性, 通过竞赛, 能够解决传统网络空间安全青少年人才选拔过程中的弊端。此外, 应加大青少年网络空间安全竞赛的奖励力度, 防止青少年专才流失, 保障青少年专才成长。

2) 创立道德黑客学校和培训班, 规范办学制度和学员审查制度

建立严格、完善的道德黑客学校的办学制度和学员审查制度。道德黑客学校或培训班是一把双刃剑, 如果没有把握好, 就会培养出一些恶意黑客。所以, 需要规范制度, 指导道德黑客学校和培训班把握好培养道德黑客准则的尺度。而对于黑客学校的开办, 要严格监管和控制, 包括道德黑客学校和培训班开办的必要条件、学员的准入条件、技术合法应用协议等。道德黑客学校根据网络空间安全态势, 灵活地制定以实战对抗为导向的课程体系和教学模式, 并部署配套仿真实战环境。道德黑客学校开设不同技术层次的课程, 由简单到复杂, 由泛化到具体, 使学员能够由浅到深地掌握网络空间安全技能, 稳步地提升实战能力。鼓励国内高校和网络空间安全企业以其深厚的技术实力为青少年开办夏令营、冬令营等网络空间安全技术培训班, 为青少年提供相对系统的技术培训。

3) 设立网络空间安全青少年发展基金, 以资助网络空间安全青少年专才发现和培养

建立网络空间安全青少年发展基金, 规范发展基金管理办法。发展基金的设立旨在营造网络空间安全青少年专才成长的良好环境, 构建青少年专才发现和培养的长效机制, 具体资助项目包括: 青少年网络空间安全竞赛的举办, 青少年黑客技术的培训, 以及网络空间安全青少年专才的奖学金。发展基金的主要来源包括政府资助、企业捐赠和资源众筹 3 个渠道, 由地方政府负责监管, 每年报告基金使用情况、资助项目执行情况及资助作用发挥情况。

5 结束语

网络空间安全人才的培养是一个系统工程, 按照系统工程的思想, 建议建立网络空间安全人才的培养体系, 覆盖各类网络安全人才的各培养阶段, 进而打通“学历培养”、“职业培训与认证”和“专才发现与培养”3 条渠道, 源源不断地输送网络空间安全人才。构建以高校为主导的包容多模式、多轨道的网络空间安全的学历培养体系, 以此作为主渠道提供素质全面的人才; 初步构建

自我发展、良性循环的网络空间安全人才的职业培训与认证体系，以此作为辅助渠道提供实用型的人才；建立网络空间安全的专才发现与培养体系，初步构建竞赛驱动的专才发现体系，激发兴趣、因材施教的专才培养体系，以此作为特殊渠道提供对抗型的人才。

参考文献：

- [1] 教育部关于增设网络空间安全一级学科的通知[EB/OL]. http://www.moe.gov.cn/jyb_xxgk/moe_1777/moe_1778/201511/t20151127_221423.html.
Notice about adding network space safety level of discipline[EB/OL]. http://www.moe.gov.cn/jyb_xxgk/moe_1777/moe_1778/201511/t20151127_221423.html.
- [2] 关于开展增列网络空间安全一级学科博士学位授权点工作的通知[EB/OL]. http://www.moe.gov.cn/jyb_xxgk/moe_1777/moe_1778/201511/t20151127_221424.html.
Notice about adding cyber security level discipline doctored degree authorized units[EB/OL]. http://www.moe.gov.cn/jyb_xxgk/moe_1777/moe_1778/201511/t20151127_221424.html.
- [3] 方滨兴. 从层次角度看网络空间安全技术的覆盖领域[J]. 网络与信息安全学报, 2015, 1(1): 1-6.
FANG B X. A hierarchy model on the research fields of cyberspace security technology[J]. Chinese Journal of Network and Information Security, 2015, 1(1): 1-6.
- [4] The comprehensive national cyber security initiative[EB/OL]. <https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative>.
- [5] Strategic plan for the national initiative for cyber security education(NICE)[EB/OL]. <http://csrc.nist.gov/nice/>.
- [6] (ISC)² [EB/OL]. <https://www.isc2.org/>.
- [7] ISACA[EB/OL]. <https://www.isaca.org/Pages/default.aspx>.
- [8] EC-Council[EB/OL]. <https://www.eccouncil.org/>.

作者简介：



张宏莉（1973-），女，吉林榆树人，博士，哈尔滨工业大学教授、博士生导师，主要研究方向为网络与信息安全、网络测量与建模、网络计算、并行处理等。



于海宁（1983-），男，黑龙江鹤岗人，博士，哈尔滨工业大学助理研究员，主要研究方向为物联网体系结构、物联网安全搜索等。



翟健宏（1968-），男，山东临沂人，哈尔滨工业大学副教授、硕士生导师，主要研究方向为网络信息安全等。



余翔湛（1973-），男，黑龙江哈尔滨人，哈尔滨工业大学研究员、博士生导师，主要研究方向为网络容灾、信息安全、物联网安全等。