

探索“网安医生”人才培养模式

陈兴蜀^{1,2}, 王海舟^{1,2}, 王文贤², 杨频¹, 阮树骅^{1,2}

(1. 四川大学网络空间安全学院, 四川 成都 610065;

2. 四川大学网络空间安全研究院, 四川 成都 610065)

摘要: 网络安全的竞争归根结底是人才的竞争, 世界各国纷纷将网络安全人才培养放在了国家战略高度。网络空间安全学科作为一门新兴交叉学科, 其学科的内涵外延还在更新发展, 目前缺乏适合网络空间安全人才特点的培养模式及评价机制。根据多年的教学研究, 参考国外的先进培养模式及评价机制, 结合国内实际情况, 提出适合网络空间安全学科特点的“网安医生”培养模式, 该模式覆盖本科培养的全生命周期, 以问题为导向, 培养学生针对网络空间发现和解决安全问题的能力, 高校与产业界、科研机构紧密互动构建人才培养的生态环境。以此提高学生掌握知识、技能和应用能力, 培养学生探索最新前沿科技和核心技术的兴趣和能力, 提升师资力量和教育水平, 同时也有利于企业选拔优秀人才, 提升企业研发能力和市场竞争力。最终实现合作方协同创新, 优势互补, 全面共赢的良好局面, 促进网络空间安全人才培养和学科发展。

关键词: 人才培养; “双导师”制; 网络空间安全; “网安医生”

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2019025

Exploring the talent training mode of “cybersecurity doctor”

CHEN Xingshu^{1,2}, WANG Haizhou^{1,2}, WANG Wenxian², YANG Ping¹, RUAN Shuhua^{1,2}

1. College of Cybersecurity, Sichuan University, Chengdu 610065, China

2. Cybersecurity Research Institute, Sichuan University, Chengdu 610065, China

Abstract: The competition for cyber security is ultimately the competition of talents. Countries around the world have placed cyber security talents at the national strategic level. As a new interdisciplinary subject, the intension and extension of cyber security discipline is still evolving and developing. So far, it lacks a talent training mode and evaluation mechanism suitable for the characteristics of cyber security talents. Based on years of teaching research, with reference to the existing advanced training models and evaluation mechanisms in foreign countries, combined

收稿日期: 2019-03-07; 修回日期: 2019-05-21

通信作者: 陈兴蜀, chenxsh@scu.edu.cn

基金项目: 四川大学新世纪高等教育教学改革工程(第八期)研究基金资助项目(No.SCU8015); 四川省高等教育人才培养质量和教学改革基金资助项目

Foundation Items: New Century Higher Education Teaching Reform Engineering Research Project of Sichuan University (Phase 8) (No. SCU8015), Higher Education Personnel Training Quality and Teaching Reform Projects in Sichuan Province

论文引用格式: 陈兴蜀, 王海舟, 王文贤, 等. 探索“网安医生”人才培养模式[J]. 网络与信息安全学报, 2019, 5(3): 36-43.
CHEN X S, WANG H Z, WANG W X, et al. Exploring the talent training mode of “cybersecurity doctor” [J]. Chinese Journal of Network and Information Security, 2019, 5(3): 36-43.

with the actual situation in China, an innovative training mode of “cybersecurity doctor” suitable for the characteristics of cybersecurity disciplines is proposed. It covers the whole life cycle of undergraduate training. With problem orientation, students are trained to find security problems and solve them in cyberspace. Universities, industry and research institutions are closely interacting. Furthermore, it improves students' knowledge, skills and practical application ability, develops interest and ability to explore the latest advanced and core technologies, improves the quality of our teachers and education, and also helps enterprises select outstanding talents, enhance their research and development capabilities and market competitiveness. In the end, the two sides will achieve synergy and innovation, complement each other, and achieve a comprehensive win-win situation, and promote the cultivation of cyber security talents and the development of disciplines.

Key words: talent training, dual-mentor system, cyber security, cybersecurity doctor

1 引言

当今世界,各国政府都高度重视网络空间安全,美国、俄罗斯、欧盟等纷纷出台了国家网络安全人才战略,制定和实施网络安全人才培养计划。美国于2010年开始施行《国家网络安全教育计划》(National Initiative for Cybersecurity Education,简称NICE计划)^[1],将网络安全人才培养上升到国家战略高度,该计划建立了多层次、连续性和终身性人才培养机制,系统化、规模化、体系化的网络安全教育和培训体系。英国发布了《网络安全国家战略》,将网络安全视为英国历史上重要的安全政策,充分发挥企业、高校及科研机构的优势,提升网络安全专业人才培养水平。随着国家信息化进程的推进,网络空间安全问题越来越受到重视。尤其是斯诺登事件之后,世界各国纷纷将网络安全放在了国家战略高度。

2015年,习近平总书记在第二届世界互联网大会上指出,技术和人才是互联网产业突破性发展、建设网络强国的关键。网络空间安全人才日渐成为国家网络安全建设的核心资源,其数量、质量及结构是国家网络安全软实力和竞争力的重要标志。因此,我国建设网络强国,需要制定国家网络安全人才培养战略,明确网络安全人才培养目标,设计网络安全人才培养发展路线,部署网络安全人才培养具体措施。

契合网络强国战略,近年来,我国从顶层到地方政府制定了一系列政策措施,2015年正式设立了网络空间安全一级学科,2016年六部委联合发文《关于加强网络安全学科建设和人才培养的意见》(中网办发文[2016]4号),2017年启动了一流网络安全学院建设示范项目(中网办秘字[2017]573号)。我国在近4年时间里,密集出台了一系列加强网络空间安全人才培养的法律法规、制度及专项工作,为网络安全人才培养提供了良好的机遇,使我国网络空间安全人才培养走上了快车道。

然而,综合来看,网络空间安全学科作为一门新兴交叉学科,其学科的内涵外延还在更新和发展。国内与国外的学术界与产业界,以及政府和各行业都在关注网络安全人才培养的相关问题,不同背景的专家、学者也给出了具有学科特点的人才培养模式的创新思路。

本文针对网络空间安全学科特点,提出了网络安全人才应能解决网络空间安全问题,鉴于网络空间安全学科与临床医学人才培养的同性,提出了面向四年制本科教育阶段的“网安医生”人才培养模式。

2 人才培养现状

2.1 国外现状

网络安全的竞争归根结底是人才的竞争。国

际上的网络强国（如美国、英国等）非常重视网络空间安全人才的培养。网络安全关系到国家安全、社会稳定、经济发展、人民生活等各个方面，政府、军队、公安等国家重要部门，以及金融、电力、能源等重要基础设施都需要大量优秀的网络安全专门人才。

网络安全公司 Cybersecurity Ventures 分析指出，2019 年全球网络安全人才缺口是 100~200 万人，到 2021 年这一数字将增加到 350 万^[2]。网络安全岗位需求增长加剧了网络安全人才短缺态势。由美国 NICE 计划发起的一项调查表明，美国当前网络安全人才为 71.57 万人，职位空缺约为 31.37 万人^[3]。到 2020 年，印度网络安全人才缺口将达到 100 万人。网络安全求职者远不能满足市场需求，网络安全人才短缺已成为一个世界性难题。

网络安全人才需求增加原因主要来自于全球网络安全市场规模的快速增长。Cybersecurity Ventures 公司调查显示^[4]，预计到 2021 年，全球网络犯罪损失将达到 6 万亿美元，包括数据丢失、知识产权盗用、个人金融数据盗窃、网络诈骗、窃听数据的恢复和删除费用等。网络犯罪数量将急剧增加，迫使各大公司不得不投入巨额资金来维护网络安全。微软每年投资 10 亿美元用于网络安全研发领域，美国摩根大通银行将其用于网络安全的年度预算从 2.5 亿美元上调到 5 亿美元。2017 年，美国白宫声明将在国会年度预算中投入超过 190 亿美元用于网络安全领域^[5]。据统计，2019 年全球网络安全市场规模预计 1 600 亿美元，将保持年均 10.2% 的增长率，预计到 2023 年，将达到 2 480 亿美元规模^[6]。

2.2 国内现状

我国网络安全起步较晚，据腾讯安全发布的《2017 年上半年互联网安全报告》^[7]，截至 2016 年 12 月，我国网民规模达 7.31 亿。但与此相对应，

中国互联网安全人才却极度匮乏，现状急需改善。我国只有 126 所高校设立了 143 个网络安全相关专业，仅占 1 200 所理工院校的 10%，高校教育培养的信息安全专业人才仅 3 万余人，而网络安全人才总需求量则超过 70 万人，缺口高达 95%。作为国内顶级互联网企业，阿里巴巴安全部门员工约为 2 000 人，占员工总数的 4% 左右；百度安全部门员工人数为 1 000 人，占员工总数的 2.5%；华为安全部门员工占比为 0.6%；腾讯安全部门员工占总人数的 0.25%。

党的十八大以来，以习近平为总书记的党中央高度重视国家网络安全人才培养问题，明确指出，“网络空间的竞争，归根结底是人才竞争。建设网络强国，没有一支优秀的人才队伍，没有人才创造力迸发、活力涌流，是难以成功的”。2015 年，国务院学位委员会正式批准，在工学门类下增设网络空间安全一级学科，加快网络空间安全高层次人才培养。2017 年 6 月 1 日起正式实施的《网络安全法》首次以法律条款的形式对网络空间安全领域的人才问题进行规定，充分体现出国家对网络安全人才的重视。

在人才培养方面，文献[8]专题分析和研究了近年来我国在网络安全人才培养方面的创新成果和热点问题。文献[9]提出了多元化、多层次的网络空间安全人才培养模式。文献[10]探究了一套完善的网络安全人才培养实践思路。文献[11]提出建立网络空间安全人才教育工程和“网络医院”的培养模式^[12]。文献[13]分析了网络安全人才培养模式创新的 4 条途径。文献[14]从网络空间安全人才价值的培养、价值的实现、价值的评估、价值的发展 4 个维度提出了网络空间安全人才价值体系。文献[15]提出了符合现实需求的实战型网络空间安全人才培养框架。文献[16]提出了建立我国网络安全实用型人才培养模式的具体措施。

然而，在面临机遇的同时，网络安全人才的

知识体系具有知识面广、学科交叉、知识更新快、难度大等特点,使当前培养的网络安全专业学生存在知识深度不够、系统性不强、综合分析能力不强、学科交叉知识不足、动手能力不强等现象,亟需建立一种创新的网络安全人才培养模式。

3 “网安医生”人才培养模式

3.1 借鉴临床医学学生的培养理念

临床医学学生的培养已经有长久、系统的经验,而相关的人才培养也会随着技术、社会的需求进行调整和完善。2014年6月30日,教育部等六部门以教研[2014]2号印发《关于医教协同深化临床医学人才培养改革的意见》,它在深化院校教育改革,提高人才培养质量中明确:建立临床医学人才培养与卫生计生行业人才需求的供需平衡机制;深化临床医学专业五年制本科生培养改革。要求加大教学改革力度,加强医学人文教育和职业素质培养,推进医学基础与临床课程整合,完善以能力为导向的评价体系,严格临床实习实训管理,强化临床实践教学环节,提升医学生临床思维和临床实践能力。

临床医学专业是一门实践性很强的应用科学专业。在临床医学人才的培养中,除了注重专业主干学科和主要课程外,还非常重视实践教学和第二课堂。结合专业教育,会开设早期实践课程;在各课程教学过程中,加强实验、见习,强化实践技能培训和实践能力培养;在专业实习中,强调综合运用各学科知识,增强分析和解决实际问题的能力。此外,基础技能的培训是完成医疗工作的必备能力,医学生在国家严格考核的规范化培训基地参加培训,有更多参与实践的机会,能够面对更全面的疾病病种,能够接触最先进的医疗技术,经过培养可以最大限度地提高技能。

网络安全学科与临床医学的共同之处如下。

1) 以问题为导向。网络安全人才需要解

决网络空间的安全问题,而临床医学专业人才需要具备临床诊疗及预防能力,实现基于器官系统的病情诊疗。

2) 知识面广,实践性强。两者涉及的知识面都非常广,都是实践性非常强的学科,强调科学理论与实践相结合。

3) 强调人本主义与道德教育。网络空间安全涉及国家安全,需要学生具备国家使命和责任;临床医学需要将医学人文精神、职业素养渗透到课程中。

4) 学科发展快,强调终身教育。基于两者在人才培养的共同之处,现借鉴“临床医学”人才培养模式,结合国内实际情况,本文提出产业界、高校及优秀人才全程融合的“网安医生”创新培养模式。

3.2 培养目标

“网安医生”的人才培养目标包括知识要求、能力要求、素质要求3个部分。

(1) 知识要求

网络安全专业人才应具备坚实的网络空间安全基础知识结构和专业思维,用于指导未来的学习和网络空间安全实践;宽厚的管理、法律及人文社科知识,充分认识网络空间安全涉及的各方面问题,包括网络空间安全国际关系及政治影响,网民社会行为及心理因素对互联网环境安全的影响等;扎实的网络安全基础知识,能够理解网络上存在的各种安全威胁及安全攻击问题;与数学、管理、法律、新闻等学科的交叉融合思维。

(2) 能力要求

网络安全专业人才应具备较强的实践能力,能为进入行业打下坚实基础;较强的科研能力,能够独立开展科研,具有良好的科研思维;较强的学习能力、认知能力、思辨能力、实践能力和外语应用能力。

(3) 素质要求

网络安全专业人才应具备良好的职业素

养,包括职业道德和敬业精神,尤其是能够抵御黑色产业链中的巨大诱惑;应具备批判性思维、开拓创新精神和严谨求实的科学态度;应具有良好的身体素质和较强的心理适应能力;应具有国际视野和跨文化交流能力。

3.3 培养方案及流程

3.3.1 培养方案

“网安医生”培养模式针对四年制本科教育阶段,遵循以下培养理念。

1) 以解决问题为导向的理念。把解决网络空间安全问题的理念和能力融入本科教育培养计划中。

2) 将网络安全的使命和责任感培养渗透到课程中。开始网络空间安全的法律、法规和伦理道德课程,将网络空间安全肩负国家使命和社会责任感融入教学内容中。

3) 重视网络空间安全思维和解决问题的能力培养。尽可能早地让学生在低年级接触网络空间安全的实践课程,产生感性认识;在不同的年级融入不同难度、不同目的的实训课程,提升学生解决问题的能力。

4) 加强课堂教学的过程考核,提升课堂教学质量。通过翻转课题、课程设计、课堂各环节的学生参与和考核等提升教学质量,吸引学生积极参与课堂教学。

5) 加强实训课程、基地的建设。加强与产业界的合作,明确实训任务和目的,建立高质量的实习基地,加强学生实训成效的考核和监督。

3.3.2 培养流程

针对网络空间安全学科特点,建立覆盖本科生培养全生命周期的“网安医生”培养模式,通过与知名企业、科研院所紧密合作,形成高校、产业互动的人才培养模式。根据学生所处年级的不同,采用差异化培养方案,并将整个“网安医生”培养模式融入学生学习的各个阶段,培养流程如图1所示。

(1) 本科一年级学生

培养地点在大学校园,将邀请企业界的专家来高校做专题报告,让学生初步了解企业的文化和最前沿的技术;利用学术型社团(如网络空间安全协会)对学生进行网络空间安全知识的普及,引导学生对网络空间安全专业的兴趣和热爱。

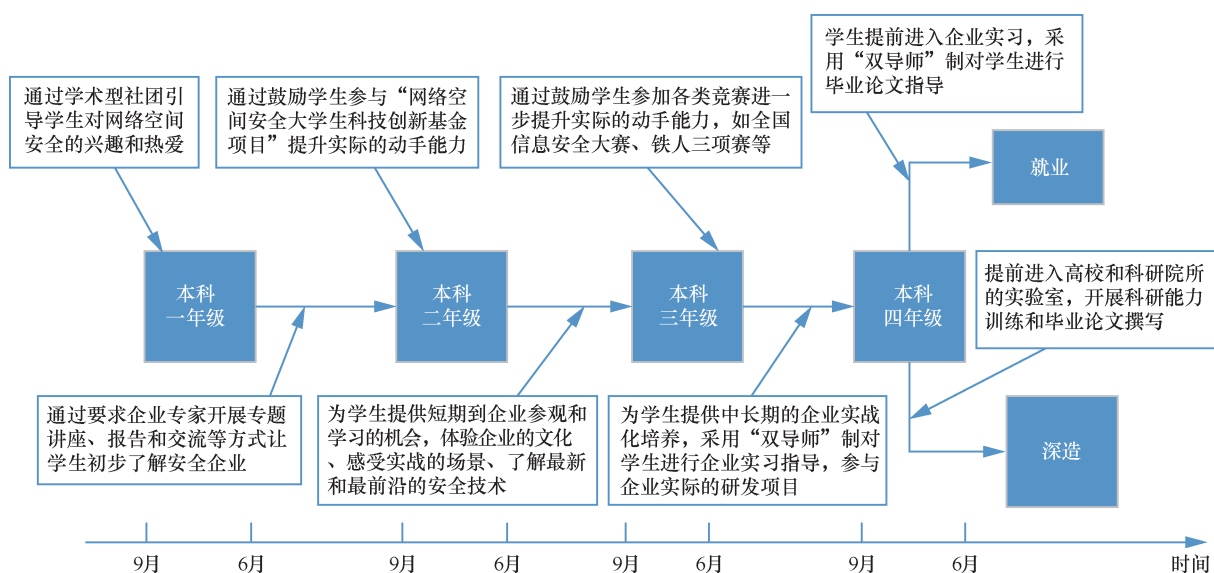


图1 “网安医生”人才培养流程

(2) 本科二年级学生

培养地点集中在大学校园,同时提供学生到企业短期交流和学习的机会。例如,在本科二年级下学期的假期为学生提供不超过2周的企业实习机会,让学生体验企业的文化、感受实战的场景、了解企业最新和最前沿的安全技术;此外,为学生提供“网络空间安全大学生科技创新基金项目”的支持,鼓励高低年级的搭配,每一个项目由一位专职教师进行指导。

(3) 本科三年级学生

培养地点集中在企业,安排学生到企业进行为期1~2个月的实习,采用“双导师”制对学生进行企业实习指导,参与企业实际的研发项目,真正进行实战化培养。

(4) 本科四年级学生

培养地点分散在企业、高校和科研院所,对于有意向深造的学生提前进入高校和科研院所的实验室开展科研训练和毕业论文撰写,对于有意向到公司就业的同学则可提前进入企业实习,采用“双导师”制对学生进行毕业论文指导。

3.4 培养方式

(1) 探索“双导师”人才培养新机制

实行学术导师和实践技能导师共同指导学生的“双导师”制,学术导师由学校教授担任,企业导师需由具备“实战经验”的企业研发带头人担任,对学生实行学术、实践齐头并进的教导方式。企业、高校导师和学生全程参与项目。在“双导师”制下,由导师为每位学生定制适合各自特点的专业规划,并指导学生开展相关科研训练和实践。

强化本科生创新意识和实践能力的培养。采取理论教育与应用实践教育相结合的方式,在校内进行基础理论的学习与研究,在校外企业进行应用实践研究。学生各主要课程设计和独立开设的“三性”课程等主要实践环节(含校内外实践)采用“工程项目驱动”培养方式,即采用企业现

有的典型工程项目,使用企业现有的工程实验设备,使教学内容与工作实际接轨。校企双方将根据人才市场的需求和产业发展趋势共同制订人才培养具体方案。

与企业合作已取得了一系列成果。例如,四川大学与阿里云共建“云计算安全”的课程与教材,通过四川大学教师与阿里云企业专家多轮商议,共同制定授课内容和教材提纲,并共同编写教材,完成课堂教学任务。该课程以学生为中心、以问题为导向、以应用实践和创新发展的目标。虽然云计算安全涉及的面非常广,课程难度大,通过课堂授课与实际云平台上的课后实践相结合,学生能更好地理解授课内容。首次开课时,阿里云公司承担了6周的授课任务,从杭州总部安排专家直接上讲台,深受学生欢迎。

(2) 构建“网络安全附属医院”新平台

建立高校与科研院所、行业企业联合培养人才的“实习基地”新平台——“网络安全附属医院”,着力提升学生的网络空间安全工程实践能力和岗位适应能力,实现以人才培养为核心、校企双方共赢的人才联合培养合作新局面。

依托“网络安全附属医院”安排学生、教师进行实践教学活动,培养学生的实践创新能力,丰富教师的实践教学经历,此外通过结合课程、结合项目、结合科研、共建本科生人才培养合作模式,共同打造横跨“产学研用”的创新生态系统。

企业对与高校合作建立“网络安全附属医院”(即新型的实习基地)具有很高的积极性,四川大学已经与天融信、中国网安、成都404、西普教育等建立了实训基地和联合实验室。学生参加互联网+竞赛、大学生创新创业项目、网络安全竞赛等,取得了良好的成果。例如,学生参加各级大创项目50余项,参加人数占学生总数的93%;项目申请国家专利5项,软件著作权近10项,发

表论文 10 余篇; 获得省级以上奖励近 10 项。

(3) 探索交叉学科人才培养新机制

打破学院建制壁垒, 整合网络空间安全学院、计算机学院、数学学院、文学与新闻学院(新闻学院)、公共管理学院、法学院、临床医学院等优势科研团队, 建立跨学院、跨学科的交叉科研创新平台。制定交叉学科科研团队管理、评价、激励机制, 针对网络空间安全的核心、关键问题开展攻关, 带动学校多学科交叉融合。

通过跨学科、跨学院的科研平台的建立, 探索招收网络空间安全方向的工学、理学、法学、管理学等学科门类的学生, 制定和完善跨学科、跨学院的网络空间安全人才培养方案, 探索网络空间安全战略型、管理型、学术型、技术型等复合型人才的培养方案。

目前, 在跨学科复合型人才培养方面, 主要是在研究生阶段开展探索。网络空间安全学院从 2018 年开始, 每年拿出 20% 左右的硕士研究生招生指标, 由网络空间安全学科的导师与其他学科(如新闻学、医学、国际关系等)的导师联合培养研究生, 培养其具有网络空间安全基础理论和技术能力, 同时具有其他学科背景, 能够解决如网络舆情分析和研判、网络空间安全国际形式分析、医疗大数据隐私保护等关注的热点问题。

4 结束语

为贯彻落实网络强国战略, 推进实施中央网信办等六部委《关于加快网络安全学科建设和人才培养的意见》, 中央网信办、教育部决定在 2017 年~2027 年期间实施一流网络安全学院建设示范项目。四川大学作为首批实施一流网络安全学院建设示范项目的高校之一, 积极探索网络空间安全人才培养创新机制。本文从网络空间安全人才培养面临的实际需求和问题出发, 通过调研国内外网络安全相关人才培养模式、其他专业创新人才

的培养经验, 借鉴临床医学专业学生培养模式, 探索网络安全人才实践技能培养创新模式, 通过建立科学的网络安全人才培养目标、培养流程、培养手段, 以期形成可复制、可推广的“网安医生”人才培养模式。

参考文献:

- [1] NIST. NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)[EB/OL]. <https://www.nist.gov/itl/applied-cybersecurity/nice>.
- [2] Cybersecurity Ventures. Cybersecurity jobs report[R]. 2018.
- [3] Cybersecurity supply/demand heat map[EB/OL]. https://www.cyberseek.org/heatmap.html?tdsourcetag=s_pctim_aiomsg.
- [4] Cybersecurity Ventures Official. Cybercrime damages \$6 trillion by 2021[EB/OL]. <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>.
- [5] The White House. FACT SHEET: cybersecurity national action plan[EB/OL]. <https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>.
- [6] Markets and markets, cybersecurity market size global forecast to 2023[EB/OL]. <https://www.marketsandmarkets.com/MarketReports/cyber-security-market-505.html>.
- [7] 腾讯电脑管家. 2017 年上半年互联网安全报告[R]. 2017. Tencent Computer Housekeeper. Internet security report for the first half of 2017[R]. 2017.
- [8] 封化民. 网络空间安全人才培养专题概要[J]. 信息安全研究, 2018, 4(12): 1071-1072.
FENG H M. Introduction to the issue of cultivation of cyber security talents[J]. Journal of Information Security Research, 2018, 4(12): 1071-1072.
- [9] 李建华. 多元化多层次网络空间安全人才培养创新与实践[J]. 信息安全研究, 2018, 4(12): 1073-1082.
LI J H. Innovation and practice of pluralistic and multi-level cyber security personnel training[J]. Journal of Information Security Research, 2018, 4(12): 1073-1082.
- [10] 莫雯希. 高校网络安全人才培养需求分析与实践思路探索[J]. 中国新通信, 2018, 20(3): 155.
MO W X. Requirements analysis and practice exploration of cybersecurity talents training in colleges and universities[J]. China New Communication, 2018, 20(3): 155.
- [11] 陈钟, 陈兴蜀, 王文贤, 等. 网络空间安全人才培养的机遇与挑战[J]. 中国信息安全, 2015(11): 75-78.
CHEN Z, CHEN X S, WANG W X, et.al. Opportunities and challenges of training cybersecurity personnel[J]. China Information Security, 2015(11): 73-78.
- [12] 陈兴蜀. 建立科学的人才培养创新模式[J]. 中国信息安全, 2015(12): 56.

CHEN X S. Establishing scientific innovation of personnel training mode[J]. China Information Security, 2015(12): 56.

- [13] 李旻, 余大为, 周海鹏, 等. 新时代高校网络安全人才培养与机制创新[J]. 网络空间安全, 2018, 9(02): 90-93.

LI Y, YU D W, ZHOU H P, et al. Innovative cybersecurity talent cultivation mechanism of higher education in the New Era[J]. Cyberspace Security, 2018, 9(2): 90-93.

- [14] 王坤, 伍军. 构建网络空间安全人才价值体系的高校责任[J]. 信息安全研究, 2018, 4(12): 1093-1097.

WANG S, WU J. The responsibilities of university to build the value system of cyberspace security talents[J]. Journal of Information Security Research, 2018, 4(12): 1093-1097.

- [15] 张镇, 贺新朋. 实战型安全人才培养框架设计[J]. 信息安全研究, 2018, 4(12): 1119-1123.

ZHANG Z, HE X P. Practical information security personnel training framework[J]. Journal of Information Security Research, 2018, 4(12): 1119-1123.

- [16] 樊佳, 李阳, 杨学敏. 建立网络信息安全实用型人才培养模式[J]. 信息安全研究, 2018, 4(12): 1127-1129.

FAN J, LI Y, YANG X M. Building the cultivation of practical talents in network information security[J]. Journal of Information Security Research, 2018, 4(12): 1127-1129.

[作者简介]



陈兴蜀（1968-），女，四川成都人，博士，四川大学教授、博士生导师，主要研究方向为大数据安全、云计算安全、网络安全、舆情及情报分析。



王海舟（1986-），男，四川南充人，博士，四川大学副教授，主要研究方向为网络安全、内容安全、社交网络、舆情监控。



王文贤（1978-），男，福建晋江人，博士，四川大学讲师，主要研究方向为网络安全、情报分析。



杨频（1967-），男，四川武胜人，博士，四川大学教授，主要研究方向为网络安全、软件安全。



阮树骅（1966-），女，浙江绍兴人，四川大学副教授，主要研究方向为云计算及大数据安全。