

网络空间安全人才培养探讨

翁健, 魏林锋, 张悦

(暨南大学网络空间安全学院, 广东 广州 510632)

摘要: 网络空间的竞争, 归根结底是人才的竞争。当前, 世界各国高度重视网络空间安全人才的培养。基于此, 首先介绍了网络空间安全人才培养的现状; 然后分析了网络空间安全人才的需求特点, 并提出了网络空间安全人才培养的若干建议措施; 最后给出了暨南大学在网络空间安全人才培养方面的一些探索。

关键词: 网络空间安全; 人才培养; 人才需求; 人才培养建议

中图分类号: TP302

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2019032

Discussion on the cultivation of cyber security talents

WENG Jian, WEI Linfeng, ZHANG Yue

College of Cyber Security, Jinan University, Guangzhou 510632, China

Abstract: The competition in cyberspace is ultimately the competition of talents. Nowadays, countries around the world pay great attention to the training of cyber security talents. the current situation of cyber security talents cultivation is introduced, the demand characteristics of cyber security talents are analyzed, and some suggestions for cyber security talents cultivation are put forward. Finally, some explorations on the training of cyber security talents in Jinan University are given.

Key words: cyber security, talent cultivation, talent demand, talent cultivation suggestion

1 引言

网络空间目前已成为继陆、海、空、天之后的第五大主权领域空间^[1]。政治、经济、文化、社会、军事等国家重要领域的基础设施与网络空

间联系日益紧密, 网络安全对国家安全牵一发而动全身, 已成为国家安全体系的重要组成部分^[2]。

近年来, 网络空间安全事件频发, 攻击事件所造成的危害前所未有。例如, 2010年, 伊朗核电站遭遇震网病毒的袭击, 致使该国基础设施遭

收稿日期: 2019-05-31; 修回日期: 2019-06-05

通信作者: 翁健, cryptjweng@gmail.com

基金项目: 国家自然科学基金资助项目 (No.61825203)

Foundation Item: The National Natural Science Foundation of China (No.61825203)

论文引用格式: 翁健, 魏林锋, 张悦. 网络空间安全人才培养探讨[J]. 网络与信息安全学报, 2019, 5(3): 44-53.

WENG J, WEI L F, ZHANG Y. Discussion on the cultivation of cyber security talents[J]. Chinese Journal of Network and Information Security, 2019, 5(3): 44-53.

到严重侵害;2015年,乌克兰电网遭黑客袭击,大规模停电严重影响了政府的运转和人民民生;2017年,WannaCry席卷全球150多个国家和地区,直接和间接经济损失数以百亿计。由此可见,现阶段的国际安全形势,已经逐渐向网络空间转移^[3-7]。要贯彻“总体国家安全观”,维护好网络空间这一非传统领域的安全,最关键的要素在于人^[8]。习近平总书记明确指出,人才是第一资源;网络空间的竞争,归根结底是人才竞争。因此,要维护国家网络安全和建设网络强国,必须精心培养一支素质良好的网络空间安全人才队伍。

早在2008年,美国就制定了一个国家级的网络安全人才教育战略,意图启动网络时代的人才革命。2009年,奥巴马在《网络空间政策评估》中强调,需要加强网络安全教育,扩充信息安全人才队伍。2017年,特朗普在13800总统行政令《加强联邦政府网络与关键基础设施网络安全》^[9]中强调需要大力发展网络空间安全人才。2019年5月2日,白宫发布声明称,为了确保美国经济繁荣和国家安全,提高美国在网络安全领域的优势地位,美国总统特朗普签署了一项名为《Executive Order on America's Cybersecurity Workforce》(网络安全人才行政令)的总统行政令,旨在增强美国网络安全人才建设。欧盟国家也陆续开始布局网络空间安全人才的相关政策。例如,英国政府在《国家网络安全战略(2016-2021)》明确将填补网络空间安全人才的缺口作为一项重要目标,并制定专门的人才战略。除此之外,俄罗斯、澳大利亚、日本等诸多国家将网络空间人才战略列为重要的发展核心^[10]。

我国也非常重视网络空间安全人才的培养,出台了一系列相关政策和法律法规用以推进网络空间安全人才的建设。2015年6月,国务院学位委员会、教育部决定增设“网络空间安全”一级

学科。2016年6月,中央网信办、教育部等六部委联合印发了《关于加强网络安全学科建设和人才培养的意见》,2016年12月,国家颁布了《国家网络空间安全战略》,首次以国家战略文件形式,要求“实施网络安全人才工程,加强网络安全学科专业建设”“形成有利于人才培养和创新创业的生态环境”。在2017年国家互联网信息办公室发布的《关键信息基础设施安全保护条例(征求意见稿)》中,反复强调了网络空间安全人才对于关键基础设施的重要作用。网络空间安全学科建设和网络空间安全人才培养上升到前所未有的高度^[9]。

但是,我国的网络空间人才培养仍存在诸多不足。首先,人才缺口仍然巨大,这个缺口不仅是人才数量上的不足,还包括高端人才的缺乏和师资力量的薄弱^[11]。其次,网络安全知识体系不能适应行业快速发展需求。第三,网络安全人才实践能力培养过程薄弱^[12]。第四,网络安全能力评价机制尚未有效建立,难以培养出多类型多层次多元化的网络安全人才。针对上述问题,本文从网络空间安全人才的需求角度进行分析,并提出相对应的建议。

2 网络空间安全人才的现状

我国网络空间安全布局较早,但网络空间安全人才现状仍不容乐观。具体来说,有以下问题。

1) 网络空间安全人才缺口仍然巨大,缺乏高端人才。

据统计,目前我国网络空间安全的人才缺口在70万到140万之间,而我国现在信息安全人才总量仅3万人^[13],人才缺口比率高达95%。而我国目前每年仅新增1.5万人的网络空间安全相关人才,远远不能满足我国安全人才的需求。另外,网络空间安全高端人才相对较少。

目前,我国的网络空间安全方面的人才培养主要集中在以本科生为主的基础教育,缺少硕士生、博士生为主的研究人才,更缺少院士、长江学者、国家杰青等领军型高层次人才^[8]。同时,网络空间师资力量不足。由于一级学科成立时间不长,网络空间安全大部分的教师来自于其他专业^[14]。

2) 知识体系不能适应行业快速发展需求。

网络安全人才培养具有多学科交叉、涉及面广等特点,传统的知识体系已经不适应国家战略和行业快速发展的需求。相关专业的课程与知识体系分散,学生在知识结构和实践能力方面存在滞后性。因此现有的网络空间安全方面的培养方案并不完全适用于网络空间安全本身的发展需求^[15]。需要探索基于相关专业知识的网络安全人才培养模式,重构课程与知识体系。

3) 网络安全人才实践能力培养过程薄弱。

网络安全是一门具有很强实践性的学科,传统教学过程对实践能力培养过程薄弱,缺少适应新需求的实践与创新平台^[16],学生工程实践与创新能力不强。高校培养出来的人才在实践能力上缺少足够的锻炼,难以满足社会需要^[17]。因此需要加强实验和实践教学环节,搭建政产学研多元化实践教育体系与平台。

4) 网络安全能力评价机制尚未有效建立。

网络安全人才能力评价具有特殊性,传统人才评价方式偏重于知识考察,网络安全类人才培养质量标准尚未健全^[17]。习近平总书记指出,对于特殊网络安全人才“不要都用一把尺子衡量”。而现在我国对于网络空间人才的培养与评定,还主要停留在“唯学位”“唯论文”的阶段,对于网络空间人才的认定过于局限^[18]。因此需要面向网络安全核心能力,构建多维度评价与持续改进的新机制,保障网络安全人才培养质量。

3 网络空间安全人才的需求特点

下面将对未来网络空间安全人才的需求特点进行分析。具体来说,未来的网络空间安全人才,将具有如下特点。

1) 需要具有交叉学科知识的复合型人才。

网络空间安全是一门高度交叉的学科,横跨理科、工科和管理学等多个门类,涉及数学、物理、生物、计算机科学与技术、通信工程、电子工程、管理科学与工程等多个学科。网络空间安全具有知识基础广博、知识体系庞杂、交叉性高、知识更新快和实践性强的特点。相对于计算机传统学科,网络空间安全学科更关注多个学科和跨界交叉融合情景下的工程创新和实践。

2) 需要网络安全实践型人才。

网络空间安全是一门实践性较强的学科。需要融综合专业实践能力、社会实践能力和创新实践能力为一体的网络空间安全人才。网络安全不能仅靠“动笔”的理论知识学习,还应强调“动手”的技术创新与时间能力,包括渗透、审计、攻防、应急响应等。只有在教育、学习、研究与生产过程中将理论学习与技术实践紧密结合,才能避免“纸上谈兵”与“闭门造车”的情况。

3) 需要多类型、多层次、多元化人才。

在网络安全人才类型的培养上,既需要具备深厚管理与技术素养的复合型“帅才”,也需要理论与技术功底扎实、文物兼备的“将才”,还需要以培养“尖兵”为目的,包括安全管理人员、安全运营人员、安全运维人员、安全研究人员。需要选拔吸纳各类“偏才”“怪才”,打造一支具备较高技术素养、专业配置适当的多类型、多层次多元化的网络安全人才。

4) 需要德才兼备、持续学习的网络安全人才。

网络安全人才首先要德才兼备,因为网络安全是一个特殊的职业,网络安全知识和技能是一

把双刃剑，它既可以用来维护网络安全，也可以用来制造网络犯罪活动，胜任这一岗位的人选应该具备基本的道德底线，满足“德才兼备”的标准。其次是要具备内生的兴趣和动力，去不断探索。信息技术发展非常快，网络安全人才只拘泥于之前的知识是不够的，只有不断学习和成长，才能迎接快速发展信息技术的挑战。

4 网络空间安全人才培养的建议措施

针对前述的需求特点，本节给出网络空间安全人才培养的几点建议措施。

4.1 交叉学科复合型人才的培养措施

1) 厘清学科关系，建立科学的课程体系。

首先，深入客观地研究网络空间安全与相关交叉学科的内在关系，准确把握网络空间安全学科的内涵和本质，制定符合网络空间安全学科自身特点的学科群系。构建“以网络空间安全理论与技术为核心”的核心学科群，“以信息技术、信息工程和信息管理等理论体系为支撑”的支撑学科群以及“以党和国家网络安全防护为应用方向”的应用学科群。

其次，以建立的学科群系为基础，构建科学的课程体系。针对网络空间安全知识基础广博、知识体系庞杂、交叉性高的特点，必修课程设置应遵循厚基础与宽口径的原则；针对网络安全专业知识更新快和实践性强的特点，选修课程设置要体现实时性、适用性、个性化和多样性的特点；课程实施顺序还应遵循不同知识点之间的前驱与后继关系。

2) 探索基于相关专业知识的网络安全人才培养方式。

对信息技术相关专业但非网安专业的学生，如电子通信、智能科学、信息管理等专业，除了加强典型网安相关知识和技能的培养外，应重点关注其所在学科中网络空间安全相关关键技术和

共性技术，如电子通信专业可以侧重关注物联网安全、智能科学可以侧重关注人工智能安全大数据安全等。对非信息技术相关专业，如生物技术、公共管理、新闻传播等专业，除了培养其网络空间安全基本知识和基础技术外，应重点关注网络空间安全相关理论和技术在其所做专业的典型应用，服务本专业，推进本专业的发展。

4.2 提升学生网络安全实践能力

1) 增加实践教学比重，构建实践平台。

网络空间安全是一门实践性较强的学科。为了培养出具有综合专业实践能力、社会实践能力和创新实践能力为一体的网络空间安全人才，一方面要增加实践教学在总教学计划中的学时和学分，实行理论知识与上机实验的穿插教学，加强学生对理论知识的理解和掌握；另一方面需要结合课程知识自身的特点，构建兼顾网络空间安全基础技术验证、新技术测试和网络攻防演练等多种专业技能训练的仿真模拟演练平台。

2) 组织学生积极参加网络空间安全类竞赛。

基于高校培养的网络空间安全人才和企业的实际需求存在一定差距的事实，积极组织学生参加网络空间安全类的学科竞赛，通过竞赛查不足、补短板、扩眼界，激发学生的学习热情，以学科竞赛带动实践教学工作。学生构思，教师把关，以老带新，将知识渗透到课堂和实践教学过程，充分调动学生的主动性，激发学生的创新能力，制作出更多优秀学科竞赛作品，使学生不仅了解网络空间安全技术发展现状，而且提升网络空间安全对抗能力。

3) 加强校企合作，协同育人。

充分利用校外资源，加强与科研院所和企业事业单位的产学研合作，建立稳定、有序的校企合作协同育人机制，使科研院所和企业参与到高校网络空间安全人才培养的整个过程中，培养目标、

课程设置、教材编制、实验室建设、实践教学、课题研究及联合培养基地等各个环节都要有科研院所和企业的身影。促使学生及时了解网络空间安全现状,把握网络空间安全知识、技能和人才的社会需求,培养学生维护网络空间安全的社会责任感、创新思维和竞争意识,提升学生的社会实践能力,形成网络空间安全人才培养、技术创新、产业发展的良性生态链。

4.3 多类型、多层次、多元化网络安全人才的培养

1) 建立多维度的人才培训与评价体系。

打破唯学位、唯论文的思维定式,按照习近平总书记的重要指示,“不拘一格降人才”,发掘和选拔网络空间安全领域的“奇才”和“怪才”。具体来说,可以采取以下 3 点措施:① 建立网络空间安全的特殊人才的发现、培养与认证体系。要因材施教,对于不同层次、不同能力的人才进行有针对性的特殊培养。例如,设立高水平信息安全竞赛,竞赛可以不限学历与年龄,以最大限度发现人才,让人才的能力发挥到最大。② 建立健全符合网络空间安全专业特点的高校教学评估体系。具体来说,在教学评估体系中,不以分数为唯一指标,更加关注从教人员对于学生综合能力的贡献。③ 建立健全网络空间继续教育体系。鼓励开设网络空间安全相关的培训班,增强从业者业务能力的同时,让社会人员参与其中,这样不仅可以从整体上提高全民的安全意识,而且有利于发现错过良好教育机会的“奇才”。

2) 创新网络空间安全人才培养机制。

探索网络安全实验班、特长班的建设,跨专业招收网络安全特长学生;探索校内学习+企业联合培养的网络安全人才培养新模式。推进“翻转课堂”等教学模式,校企联合建设反映前沿技术的在线课程资源。开展国际化联合培养,推进硕博连读和双博士国际联合培养模式。

4.4 德才兼备、持续学习的网络安全人才的培养

1) 建立德育为先、能力为重的育人新模式。

进一步完善网络空间安全人才思想政治教育体系,加大政治类、历史类课程设置,强化政治理论、爱国主义等方面教育,不断提升学生的思想政治修养;探索高校、科研院所和网络安全企业合作培养方式,努力培养一批政治合格、技术精湛的高素质网络安全人才,成为社会主义核心价值观的坚定信仰者、积极传播者和模范践行者,为民族复兴提供有力的网络安全人才支撑。以培养师生树立正确的网络安全观为载体,着力推动建立融合思想政治教育与网络安全法制教育、学生职业发展与规划引导、创新创业热情激发、实践动手能力培养于一体的网络安全学生思政工作新模式。

2) 引导学生关注学术前沿。

要引导学生了解网络空间安全的学术前沿,追踪领域最新热点问题。高校要为学生开展相关的能力培训,培养学生科研检索能力、科研文献阅读能力等,引导本科生阅读能够反映网络空间安全最新进展的国际学术会议(如 S&P、CCS、NDSS、USENIX Security)的论文,培养学生的科研兴趣。

3) 培养学生的逆向思维,打破常规思维。

在碰到理论或者实践中遇到的问题时,鼓励学生用多种方法进行思考;组织网络攻防与网络对抗比赛,参赛双方可以不限制方法,引导学生自己思考;有针对性地开设与网络空间安全相关的逆向思维课程,如软件的逆向工程、反汇编、漏洞测试,让学生从攻击者的角度理解网络空间安全。

5 网络空间安全人才培养探索——以暨南大学为例

暨南大学在 2015 年率先成立广东省首家网络空间安全学院网络空间安全学院,学院目前拥有“网络空间安全”一级学科博士点、网络安全

防护与检测技术国家地方联合工程中心、广东省数据安全与隐私保护重点实验室、广州市数据安全与隐私保护重点实验室、网络空间安全广东省优势重点学科等学科平台。学院在网络空间安全创新实践类人才培养方面进行了诸多探索，形成了多路径多层次复合型的网络安全人才培养模式，如图1所示。

5.1 交叉学科复合型人才的培养——网络空间安全暑假特训营

暨南大学网络空间安全暑假特训营面向全校各专业各类别在读学生，自愿报名，并配备指导老师。特训营分为3个部分。① 网络空间安全基础知识串讲，内容包括网络安全相关基础数学问题、密码学、网络安全相关技术等。通过串讲使不同年级、不同专业学员对网络空间安全知识体系有个整体认识。② 网络安全竞赛分享沙龙，由获得过国内外网络安全重要竞赛的成员分享其实战经验，学员间进行充分技术交流和赛事交流。③ 安全企业

参观，通过参观让学员了解企业对网络空间安全相关人才的职业知识和技能要求，为其下一步制定学习目标（尤其是技能训练目标）打下基础。

5.2 网络安全实践能力的提升——网络空间安全寒假特训营及“世安杯”网络安全大赛

暨南大学网络空间安全暑假特训营面向全校大一至大三本科生和全体研究生开展。特训营学习内容分为3个部分。① 网络空间安全竞赛训练，由暨南大学网安战队现役或退役的核心队员担任授课教师，利用学院已有实验环境或自行搭建环境，通过现场演示与讲解带领参训的学员进行实战训练，并全程指导学员亲自进行实操，旨在带领学员入门某一竞赛实战领域，具体包括Web安全、二进制分析、移动安全等。② 校外竞赛团队经验分享，主要邀请在网络安全相关竞赛中获奖的战队分享竞赛经验，从而开拓学员的知识面与竞赛思路，积累竞赛经验。截至目前，训练营已邀请了国内在代码审计、漏洞利用分析等

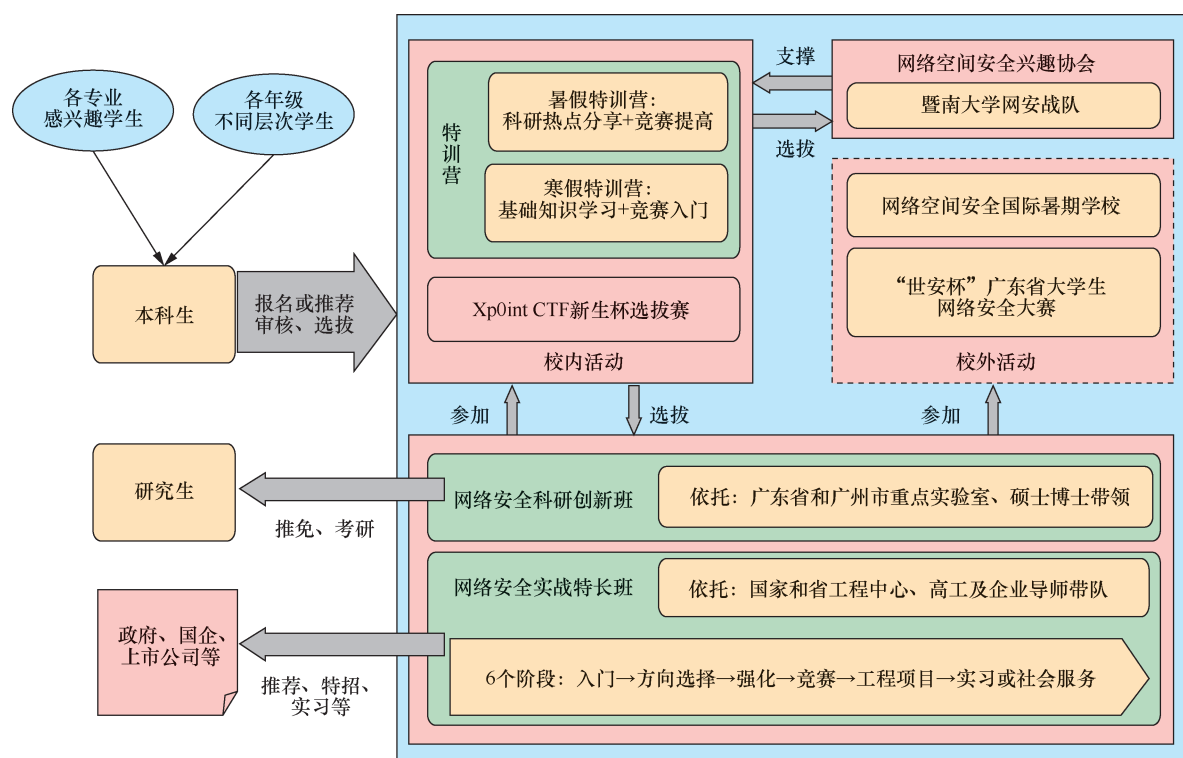


图1 暨南大学网络空间安全多路径多层次复合型创新实践人才培养模式示意

领域竞赛成绩突出的多支战队进行了经验分享。

③ 安全企业访问,通过到安全企业学习交流,加深企业与学员间的互相了解,促进学员赴企业实习或进行创新训练的机会。寒假特训营与暑假特训营的对比如表 1 所示。

同时,通过举办“世安杯”来锻炼学生的实践能力。广东省大学生网络安全大赛由广东省科技厅指导,广东省网络安全检测与防护工程技术研究开发中心主办,暨南大学网络空间安全学院/信息科学技术学院承办,是面向广东省大学生的大型网络安全大赛。通过竞赛辅助教学的形式,将理论与实践相结合,激发广大青年学子的创新意识、提高实践能力,强化专业技能,自 2014 年以来已经成功举办了 4 届,大赛参赛高校超过 100 所,参加大学生超过 2 000 人,在广东高校大学生中具有较强的影响力。

通过寒假特训营及“世安杯”比赛的承办,暨南大学学生在网络空间安全实践能力方面得到了较大提升,近年来在各级网络空间安全竞赛中

成绩斐然。例如,获得了 2017 全国高校网安联赛(X-NUCA'2017)“企业安全众测”靶场挑战赛冠军、2018 年普华永道 PWC 全国高校网络安全黑客大赛决赛冠军、2018 年全国高校网安联赛总决赛(X-NUCA'2018)全国第 6 名、2016~2017 赛季全国信息安全铁人三项总决赛二等奖和总决赛个人赛单项亚军、2017 年第十届全国大学生信息安全竞赛一等奖、2015 年广东省首届“强网杯”网络安全大赛高校组冠军、2017 年广东省第二届“强网杯”网络安全大赛高校组冠军、2017 年全国信息安全铁人三项华南赛区冠军、2018 年第二届广东省“红帽杯”网络攻防大赛高校组冠军、2016 年第三届“世安杯”广东省大学生网络安全大赛一等奖、2017 年第四届“世安杯”网络安全大赛一等奖等多项奖励。

5.3 多类型、多层次、多元化人才的培养——“网络安全科研创新班”和“网络安全实战特长班”

“网络安全科研创新班”依托暨南大学建设的“广东省数据安全与隐私保护重点实验室”等多个

表 1 竞赛暑假特训营与寒假特训营方案对照一览表

	暑假特训营（重理论）	寒假特训营（重实践）
相同点	招生范围	全校在读各专业各类别学生,包含研究生
	设置时长	一周,设置在假期结束前一周
	预备知识	均需要在开营前假期内进行预备知识和技术的自学
	企业参观	均安排安全企业参观交流学习
不同点	内容设置	网络空间安全基础知识串讲 网络安全竞赛分享沙龙
	训练目的	网络空间安全竞赛训练 校外竞赛团队分享
	训练目的	拓展学员该领域的知识面,追踪该领域最新热点问题 激发学习该领域知识和技术的热情 与具有参赛经验的学员进行充分交流,扩展知识面与思路 快速入门网络空间安全竞赛相关赛事内容
	录取	对网络空间安全领域具有浓厚的兴趣
	关注点	关注学员储备知识和热点追踪能力 自学能力强,学习努力 竞赛分享沙龙要求学员获得国内外重要网络公开赛事奖项 希望提升该领域技术水平
	训练方式	网络空间安全基础知识串讲以学员面授为主,指导老师评分评价 网络空间安全竞赛训练和校外竞赛团队分享以技术、工具讲解,结合竞赛内容演示和实操演练 竞赛分享沙龙以经验交流、分享和实操为主,自由交流
	授课教师	每个参与者自己既是学员又是分享者,每个人分享内容不同 校内教师、校内战队现役或退役核心队员、校外竞赛团队、校外教师、企业安全高级工程师等

省、市重点实验室开展人才培养工作，重点培养学生在网络空间安全领域的创新能力。每年根据学校教务处相关规定，经学生自愿申请，面向全校大二学生选拔对网络空间安全感兴趣且在该领域有所特长的学生转入“网络安全科研创新班”就读。网络空间安全学院投入专门力量对创新班学生进行重点培养，结合本科生导师制与重点实验室团队合作制，向学生开放多元化的研究方向与研究资源，对学生进行网络空间安全领域科研能力的培养。在此期间，除了完成本科生常规课程任务，科研创新班学生还需要参与导师和重点实验室团队的科研任务，经过3年的培养，多数学生可获得保研或硕博连读资格，成为网络空间安全专业的研究生后备力量。

“网络安全实战特长班”依托暨南大学建设的“网络安全检测与防护国家地方联合工程研究中心”开展人才培养工作，面向社会和产业需求，重点培养学生解决实际工程问题的能力。实战特长班学生的选拔面向全校所有专业，入选学生在原专业继续就读的基础上参加实战特长班的培养。该班以“工程项目管理制度和校外企业导师制度”相结合的方式对学生进行网络安全实践能力培养，具体的培养路径如下。① 技术入门阶段：学生在暨南大学网络空间安全在线实验中心进行自学（配备指导老师全程答疑），历时3个月完成所有实验、实操课程，达到技术入门水平。② 方向选择阶段：通过在暨南大学网络空间安全综合实验室进行为期一个月的学习，选择自己的兴趣方向（可选方向包括Web安全、移动安全、漏洞挖掘与利用、APT攻防、社会工程学等实战领域），利用暨南大学网络安全靶场系统题库（SCR系统）进行所选方向的强化训练。③ 技能强化阶段：由不同方向的学生组成战队，利用暨南大学网络攻防实战系统（NRT系统）与其他线上平台进行为期一个月的攻防对抗强化训练。④ 竞赛实战阶

段：组建战队参加省级以上高水平网络安全竞赛，通过竞赛查漏补缺，从多方面提升实战能力。⑤ 工程项目实践阶段：在企业网络安全高级工程师的带领下，参与工程中心的具体项目（为期10个月），包括渗透测试、漏洞挖掘与分析代码审计、攻防对抗、补丁研发等内容。⑥ 企业实习和安全教育阶段：根据学生的擅长技术，推荐其到业内知名公司进行实习，或加入工程中心对外安全服务团队，为政府部门和企事业单位提供安全服务，为网络安全公开平台（如国家漏洞库发布平台、广东省网络安全应急响应平台漏洞盒子）贡献技术力量。

5.4 德才兼备、持续学习的人才培养——协同育人新机制及网络空间安全国际暑期学校

学院构建了从课程、教材、科研、实践、管理到文化、服务、组织、心理、资助“十育人”体系，组建了专业教师、思政教师、辅导员、班主任、导师、管理干部到行业特殊辅导员、家长以及学生自身的育人“组团”，搭建了全员全过程全方位的深度协同思政育人新机制。

通过网络空间安全国际暑期学校引导学生接触学术前沿。暨南大学从2016年开始每年举办一届网络空间安全国际暑期学校，暑期学校历时一个月，面向全球网络空间安全领域的青年学者、博士后和优秀的博士生、硕士生。暑期学校邀请了国际上网络空间安全领域学术水平较高的青年才俊担任授课教师，授课内容主要是国际上网络空间安全领域最新研究热点，为我国乃至国际网络空间安全学子提供了较好的科研和创新交流平台。例如，2016年第一届暨南大学网络空间安全国际暑期学校吸引了包括美国纽约州立大学布法罗分校、清华大学、香港中文大学、香港城市大学、中国科学技术大学在内的国内外36所大学的95名青年教师、博士研究生、硕士研究生报名参加。

6 结束语

网络空间安全人才的培养,是我国重点战略布局。本文首先分析了我国在网络空间安全人才培养方面所面临的问题与不足。针对这些不足,结合未来的人才需求,提出了一系列的规划与建议。本文认为,要想满足网络空间安全的发展战略,必须从顶层设计,在各个层次上填补人才缺口。首先,改进培养方案,培养交叉学科的复合型人才。其次,加强网络安全实践能力的培养。第三,培养多类型多层次多元化的网络安全人才。最后,培养德才兼备持续学习的网络安全人才。具体的措施包括探索基于相关专业培养网络安全人才的模式,构建网络安全课程体系。同时,增加实践学比重,鼓励学生参加各类竞赛,加强校企合作。进一步地,多维度地建立健全我国在网络空间安全人才评价体系。同时,通过多与国际交流合作的方式,引导学生接触学科前沿,培养德才兼备的持续学习能力。暨南大学进行了诸多实践探索,可以为高校人才的培养,提供参考和借鉴。

参考文献:

- [1] 王世伟, 曹磊, 罗天雨. 再论信息安全、网络安全、网络空间安全[J]. 中国图书馆学报, 2016, 41(5):4-28.
WANG S W, CAO L, LUO T Y. Further discussion of information security, network security, and cyberspace security[J]. Journal of Library Science in China, 2016, 41(5):4-28.
- [2] 沈昌祥. 以科学的网络安全观加快网络空间安全学科建设与人才培养[J]. 信息安全研究, 2018,4(12):1066-1067.
SHEN C X. To Accelerate the discipline construction and talent cultivation of cyberspace security with scientific cyber security concept[J]. Journal of Information Security Research, 2018, 4(12): 1066-1067.
- [3] 戴方芳, 刘凯. 网络武器泄露威胁全球网络空间安全事件简析[J]. 现代电信科技, 2017, 47(4):11-13.
DAI F F, LIU K. Analysis on leakage of cyber weapon and its threat to global cyberspace security[J]. Modern Science & Technology of Telecommunications, 2017, 47(4):11-13.
- [4] 金伟新. 网络空间面临的战争威胁和应对策略[J]. 中国信息安全, 2015(11): 113-115.
LIU W X. The war threat and countermeasure of cyberspace[J]. China Information Security, 2015(11):113-115.
- [5] 沈昌祥. 建好网络空间一级学科加快安全可信体系建设[J]. 中国信息安全, 2016(12): 50-51.
SHEN C X. Establishing the first-level discipline of cyberspace and accelerating the construction of secure and credible system[J]. China Information Security, 2016(12): 50-51.
- [6] 张焕国, 王丽娜, 杜瑞颖, 等. 信息安全学科体系结构研究[J]. 武汉大学学报(理学版), 2010, 56(05): 614-620.
ZHANG H G, WANG L N, DU R Y, et al. Research on information security discipline[J]. Journal of Wuhan University (Natural Science Edition), 2010, 56(05): 614-620.
- [7] 杜瑞颖, 张焕国, 王丽娜, 等. 创建信息安全专业培养体系引领信息安全专业建设[J]. 中国信息安全, 2015(11): 79.
DU R Y, ZHANG H G, WANG L N, et al. Establishing the training system of information security talent and leading the construction of information security specialty[J]. China Information Security, 2015(11):79.
- [8] 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.
- [9] 保障国家网络空间安全, 筑牢人才根基是关键[EB/OL]. <https://baijiahao.baidu.com/s?id=1597640207451812250&wfr=spider&for=pc>.
The key to guarantee the national cyber security is to make a firm talent foundation[EB/OL]. <https://baijiahao.baidu.com/s?id=1597640207451812250&wfr=spider&for=pc>.
- [10] 王星. 美国网络安全人才政策综述[J]. 信息安全与通信保密, 2018(08):69-76.
WANG X. An overview of the US' cybersecurity workforce development policies[J]. Information Security and Communications Privacy, 2018(08): 69-76.
- [11] 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.
- [12] 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(05): 22-25.
FENG H M. Talent training: key link of the cyber security system[J]. Information Security and Communications Privacy, 2014(05): 22-25.
- [13] Counting the cost: cyber exposure decoded, Lloyd's of Lon-

don[EB/OL]. <https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/countingthecost>.

- [14] 网络安全人才荒已成全球性问题[EB/OL]. <https://aq.tencent.com/news/newslst4.html>.

The shortage of cyber security talents has become a global problem[EB/OL]. <https://aq.tencent.com/news/newslst4.html>.

- [15] 翁健, 马昌社, 古亮. 网络空间安全人才培养探讨[J]. 网络与信息安全学报, 2016, 2(2):1-7.

WENG J, MA C S, GU L. Discussions on the talent cultivation of cyber security[J]. Chinese Journal of Network and Information Security, 2016, 2(2):1-7.

- [16] 刘金芳. 探索我国网络空间安全人才培养新模式[J]. 信息安全与技术, 2017, 8(Z5):15-18.

LIU J L. Design and implementation of a unified authorization management system[J]. Cyberspace Security, 2017, 8(Z5):15-18.

- [17] 李晖, 张宁. 网络空间安全学科人才培养之思考[J]. 网络与信息安全学报, 2015, 1(1):18-23.

LI H, ZHANG N. Suggestions on cyber security talents cultivation[J]. Chinese Journal of Network and Information Security, 2015, 1(1):18-23.

- [18] 马建峰, 李风华. 信息安全学科建设与人才培养现状、问题与对策[J]. 计算机教育, 2005(1):11-14.

MA J F, LI F H. Current situation, problems and countermeasures of information security discipline construction and talents training[J]. IT Education, 2005(1): 11-14.

[作者简介]



翁健(1976—),男,广东茂名人,博士,暨南大学教授、博士生导师,主要研究方向为密码学与信息安全。



魏林锋(1983—),男,湖北黄冈人,暨南大学高级工程师,主要研究方向为人工智能安全、云计算安全和网络空间安全检测与防护。



张悦(1990—),男,陕西榆林人,暨南大学博士生,主要研究方向为信息安全与智能移动端安全。