# 创新网络安全人才培养体系 支撑网络强国建设

田志宏

广州大学网络空间安全学院院长、教授

党的十八大以来，以习近平同志为核心的党中央高度重视网信人才工作，提出一系列新思想新观点新论断，为新时代网信人才培养和建设提供了根本遵循。习近平总书记强调，“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”“培养网信人才，要下大功夫、下大本钱，请优秀的老师，编优秀的教材，招优秀的学生，建一流的网络空间安全学院”“要坚持网络安全教育、技术、产业融合发展，形成人才培养、技术创新、产业发展的良性生态”。

当前，网络空间成为大国博弈的关键战场，网络对抗与地缘政治博弈深度交织，网信领域的竞争正在全球展开。网络安全风险激增，新情况新问题新挑战层出不穷，深刻影响着全球经济格局、利益格局、安全格局。网络强国建设迫切需要一支高素质创新型复合型实战型应用型网络安全人才队伍的有力支撑，聚天下英才而用之。要围绕国家网络安全与信息化工作的重大需求，根据网络安全人才特点和质量要求，在目标、机制、平台、生态等方面构建普遍适合我国普通高校的网络安全人才培养有效模式和体系，培养具有国际视野和创新能力的网络安全拔尖人才，在网络空间博弈和人才竞争中赢得主动权。

我国网络安全人才培养体系与能力不断加强

2016年制定出台的《关于加强网络安全学科建设和人才培养的意见》，强化网络安全人才培养宏观指导和政策统筹。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。实施一流网络安全学院建设示范项目，11所高校入选为一流网络安全学院建设示范高校，实现了从本科到硕士、博士的网络安全人才一体化培养。截至2022年9月，国内有60余所高校设立网络安全学院，200余所高校设立网络安全本科专业，每年网络安全专业毕业生超2万人。国家网络安全人才与创新基地建设稳步推进，方滨兴院士网络空间安全实验班（简称“方班”）等一系列网络安全人才创新培养模式探索与实践取得明显成效。网络安全人才奖励激励机制持续完善。设立网络安全专项基金，开展网络安全优秀教材、优秀教师等评选活动，奖励各类网络安全优秀人才近千人。2021年国家网络安全宣传周开幕式上，15个国家网络安全先进集体、29名国家网络安全先进个人受到表彰。2022年首批5家国家网络安全教育技术产业融合发展试验区授牌，探索网络安全教育技术产业融合发展的新机制新模式。当前，我国网络安全人才培养不断加快，技术能力稳步提高，产业体系快速发展，人才培养、技术创新、产业发展的良性生态正在加速形成。

探索网络安全人才培养特色模式，构建网络安全人才培养创新体系

第一，围绕国家战略需求凝聚网络安全人才培养的主题和目标。

网络安全人才培养是关乎国家安全的大事。从国家网络安全战略需求出发，以解决终端普适化、网络泛在化、系统服务化和应用智能化所带来的新的安全问题为人才能力目标，以强化网络安全人才牢牢掌握宿主技术知识的深度、深刻揭示安全问题的伴随性、不断适应动态博弈的复杂局面、培养创新型复合型实战型应用型人才培养为目标，构建具有时效性和实效性的网络安全人才培养新体系，强调人才培养模式的针对性和灵活性，有效缓解我国网络空间安全人才短缺问题，为维护国家网络空间安全提供强有力支撑。从2016年开始研究探索到2018年率先在广州大学正式成立“方班”并实现第一期硕士研究生招生，经过五年的创新发展实践，“方班”已经成为一种有效的高层次实战型网络安全人才培养模式。

广州大学以学生为中心，以互联网技术做支撑，创新性地提出“方班”人才培养“654321”模式，分别是“六个特殊性”（触及法律高风险性、安全保障强技能性、攻防两端不对称性、技能学术弱关联性、宿主技术后伴生性、技能水平难鉴别性）、“五种新机制”（新生强化训练营新机制、后选导师和绩点置换新机制、游戏化课堂教学新机制、评估及量化反馈新机制、网安人才认证新机制）、“四项新计划”（预科计划、名师计划、迭代计划、三创计划）、“三门新课程”（“方班”研讨厅、“方班”前沿秀、“方班”演武堂）、“二级新体系”（技能体系、课程体系）、“一张实验床”（“方班”教学实践平台）（见下图）。

第二，探索网络安全技术创新和人才培养融合发展的新机制。

高校是网络安全人才培养的主体，也是网络空间安全理论与技术创新的核心力量之一。广州大学将理论研究的前沿问题、技术研发的最新挑战以及理论技术成果融入高层次网络安全人才培养，为课程设计、实验实践、选题定向等提供方向指引和素材资源，同时，把成长中的网络安全人才带入前沿理论技术创新活动，从而构建起“三维三工”网络安全技术创新与人才培养融合发展的新机制。该机制把任务型科研项目、能力型发展方向和建设型实验实训资源三个维度相融合，物化形成科研成果向实训资源转化工程、发展能力向实验题目转化工程、实验实训能力对科研发展的支撑工程。创新设计研讨厅机制，院士全程参与教学，为每一名研究生进行点评。课程采用小班制、研讨点评式教学模式，院士、知名专家和专业老师组成教学组，采用“学生演讲、师生质疑、专家点评”的深度翻转课堂形式，以培养学生快速掌握“求源、熵减、思辨”方法，从而培养创新和实践能力（见下图）。

截至2023年7月，广州大学已开展136期“方班”研讨厅，培养广州大学研究生476名。除此之外，还专门开设面向全国高校的“方班拓展班研讨厅”，现已开展64期，先后有来自北京航空航天大学、北京邮电大学、南开大学、南京邮电大学、哈尔滨工业大学、西北工业大学、电子科技大学、山东大学、东南大学、中山大学、澳门城市大学等28所高校441名研究生参与教学培养，大部分参加高校以“创新与思辨”课来计入学分。全国共有29所高校的182位教师参与研讨厅教学模式，并成立相关的教学研讨组及教学指导委员会。同时，还积累大量实验实训资源，来自国内40余所高校师生访问量超过10万次。“方班”200名硕士研究生参与科研项目任务和科研方向拓展，支撑20多项省部级以上科研课题研究，孵化出6个学生创业企业。

第三，构建网络安全人才培养和产业融合发展的创新平台。

安全分析和攻防对抗是网络安全人才实战实践能力的集中体现，同时也是高校培养学生实战能力的切入点。将“使用”网络安全人才的产业实体与“生产”网络安全人才的高校教育主体有机融合，构建校企联合教育平台，不仅可以打通供需通道，还可以实现网络安全企业在实战型师资资源与高校在教学师资资源的优势互补。广州大学围绕“方班”网络安全人才培养这个核心，与国内20多个网络安全企业建立不同方向的联合实验室，形成“以优势互补为抓手，以人才培养为目标”的产教融合体系。同时，依托联合实验室，创新性设计“演武堂”机制，由网络安全企业冠名教学班，把企业实战专家请进课堂，将企业的实战能力与高校的教学方法进行有机结合，以培养学生快速掌握“分析、验证、工程”方法，锻炼实战实践能力。“方班”为构建校企联合、产教融合提供了一个行之有效的实践案例。截至2023年7月，“方班”演武堂已开设32期教学活动，受益研究生165名，绿盟科技、海康威视、天融信、安天、任子行等五家网络安全企业参与“方班”演武堂课程的教学班冠名，派出企业导师合计超过1000人课次；参与支撑包括2022年北京冬奥会、中国进出口商品交易会、中国（深圳）国际文化产业博览交易会、“粤盾”、“护网”等大型活动安保任务和演练任务40多次。

第四，打造产学研创一体化的网络安全人才培养新生态。

教育教学不应该是一个封闭的环境，我国网络安全人才的培养需要一个集产业、教育、科研和服务等一体化的生态环境。产业是未来网络安全人才需求的主要源头，也是反哺网络安全人才教育的重要源泉；承担教育使命的高校是培养网络安全人才的主体，也是科研创新的核心力量之一；服务是连接网络安全人才供需两端、科研创新产用两侧的关键，是构建网络安全人才培养新生态乃至网络空间安全产学研创生态的关键。广州大学从打造我国网络安全人才培养生态的初心使命出发，作为发起单位之一和首任秘书长单位，于2018年成立中国网络空间安全人才教育论坛（即“网教盟”）。截至目前，成员单位包括国内网络安全教育高校、网络安全龙头企业、各类网信科研机构等200余家，形成以服务网络安全人才培养为中心、促进网络安全产学研创融合的生态体系。产学研创一体化的网络安全人才培养生态逐渐显现。

深化网络安全人才培养改革支撑网络强国建设

党的二十大报告指出，“教育、科技、人才是全面建设社会主义现代化国家的基础性、战略性支撑。必须坚持科技是第一生产力、人才是第一资源、创新是第一动力，深入实施科教兴国战略、人才强国战略、创新驱动发展战略，开辟发展新领域新赛道，不断塑造发展新动能新优势”“我们要坚持教育优先发展、科技自立自强、人才引领驱动，加快建设教育强国、科技强国、人才强国，坚持为党育人、为国育才，全面提高人才自主培养质量，着力造就拔尖创新人才，聚天下英才而用之”“加快建设国家战略人才力量，努力培养造就更多大师、战略科学家、一流科技领军人才和创新团队、青年科技人才、卓越工程师、大国工匠、高技能人才。加强人才国际交流，用好用活各类人才”。要深入学习贯彻落实党的二十大精神，始终坚持以习近平新时代中国特色社会主义思想特别是习近平总书记关于网络强国的重要思想为指导，全面贯彻党的教育方针和总体国家安全观，进一步聚焦育人方式改革这一人才培养的核心问题，深化网络安全人才培养理念、培养模式、教学内容及方式方法等方面的改革，着力搭建创新平台，积极打造创新载体，努力形成有利于创新人才成长的育人环境，培养造就世界水平的科学家、网络安全领军人才、卓越工程师和高水平创新团队，奋力开创网络安全人才培养工作新局面，为推进国家网络安全体系与能力现代化提供有力的人才保障，有力支撑网络强国、数字中国建设，助力中国式现代化，护航中华民族伟大复兴。

中国网信2023-09-14