

培养复合型高技能网络安全人才改革创新

黎斌

广西职业技术学院

DOI:10.12238/mef.v8i7.12106

[摘要]网络安全作为国家安全的重要组成部分，其领域的快速发展对高技能人才的需求愈发迫切。然而，当前高校网络安全人才培养存在理论与实践脱节、课程设置单一、行业需求响应不足等问题，难以满足社会的多样化需求。为应对这些挑战，本文提出了以培养复合型高技能网络安全人才为目标的改革创新思路。具体措施包括构建涵盖基础、核心和前沿领域的多元化课程体系，强化基于实战场景的实践能力的培养，推进产教融合的校企合作模式，以及利用人工智能与虚拟现实等技术优化教学方法。

[关键词]网络安全；高技能；教育改革；人才培养

中图分类号：G420 **文献标识码：**A

Innovation and Reform of Cultivating Compound and Highly Skilled Network Security Talents

Bin Li

Guangxi Vocational and Technical College

[Abstract]As an important part of national security, the rapid development of network security is facing a more and more urgent demand for highly skilled personnel. However, there are some problems in the current network security talent training in colleges and universities, such as the disconnection between theory and practice, single curriculum, and insufficient response to industry demand, which are difficult to meet the diversified needs of the society. In order to meet these challenges, this paper puts forward the innovative reform ideas with the goal of cultivating compound and highly skilled network security talents. Specific measures include building a diversified curriculum system covering basic, core and frontier fields, strengthening the cultivation of practical ability based on practical scenarios, promoting the school-enterprise cooperation mode of industry and education, and using artificial intelligence and virtual reality to optimize teaching methods.

[Keywords]Network security; High skills; Education reform; Talent cultivation

引言

研究背景

随着信息化社会的不断深化，网络安全已经成为国家安全体系的重要组成部分。近年来，全球范围内的网络攻击事件频发，网络安全威胁呈现多样化、复杂化趋势，不仅对个人隐私与商业数据造成巨大威胁，也对关键基础设施的安全运行带来严重挑战。我国政府高度重视网络安全，在《中华人民共和国网络安全法》《数据安全法》《国家网络安全战略》等政策中，明确了培养高技能网络安全人才的重要性^[1]。

面对信息化发展所带来的问题，高校亟需创新教育模式，通过优化课程体系、强化实践能力培养、深化产教融合与充分利用新兴技术，构建面向复合型高技能网络安全人才培养的教育体系，从而助力国家网络安全人才储备和行业发展。

研究意义

本研究从国家战略需求与教育改革趋势出发，聚焦复合型高技能网络安全人才的培养，具有重要的理论价值与实践

意义。在理论层面，本研究通过分析网络安全教育现状及存在的问题，提出针对性的教育改革策略，为高校课程设置、教学方法优化及校企合作机制提供参考路径。在实践层面，本文的研究成果可为高校网络安全教育转型提供借鉴，有助于提升学生的综合素养和职业能力，满足行业对高技能人才的迫切需求^[2]。

一、网络安全人才培养现状分析

（一）当前网络安全人才培养的主要模式

当前，高校在网络安全人才培养方面普遍采用以理论教学为主、实践教学为辅的模式。在课程设置上，多数高校将网络安全专业课程分为基础课程（如计算机网络基础、信息安全概论）、核心课程（如密码学、网络攻防技术）和选修课程（如区块链安全、云安全）。这一模式较为成熟，在系统化传授网络安全知识方面具有一定优势。然而，这种传统培养模式存在以下显著问题：

1.理论与实践脱节。教学内容往往以教材为主，案例教

学与实战练习较少，学生难以在复杂多变的网络环境中应用所学知识。

2.课程更新滞后。网络安全技术发展迅速，而高校课程体系的更新速度相对较慢，部分课程内容难以涵盖行业最新需求。

3.技能单一化。培养模式多聚焦于单一技术能力，忽视了学生综合素质、跨学科能力及团队协作能力的培养。

（二）当前网络安全人才培养存在的问题

尽管我国高校在网络安全人才培养方面取得了一定成效，但面对行业快速发展的需求，仍存在以下不足：

1.课程体系设计不足。现有的课程体系过于强调基础理论教育，缺乏对前沿技术和实际应用的关注。例如，针对物联网安全、人工智能安全等新兴领域，相关课程在高校中仍属稀缺。此外，课程内容间缺乏系统性与关联性，难以全面提升学生的知识架构和技术能力。

2.实践教学环节薄弱。网络安全作为实践性极强的学科，其教学效果高度依赖实战训练。然而，在高校中，实践课程的学时比例普遍不足，实验设备相对落后，实验场景的复杂性和真实性不足。此外，许多高校的实验项目停留在基础层面，难以涵盖复杂网络环境下的攻防对抗需求^[1]。

3.校企合作深度不够。尽管产教融合已经成为高校教育改革的重要方向，但网络安全专业的校企合作仍处于初级阶段。高校与企业在人才培养目标上的联动较弱，缺乏长期稳定的合作机制，学生难以通过校企合作获取行业前沿技术经验和实际项目训练机会。

4.新兴技术手段应用不足。近年来，人工智能、虚拟现实等技术在教育领域的应用日益广泛，但在网络安全教育中的应用尚未普及。许多高校未能有效利用这些技术手段优化教学内容和教学方法，导致教学形式较为单一，学生的学习兴趣 and 主动性难以充分激发。

（三）国内外网络安全人才培养的对比

国际上，部分国家在网络安全人才培养方面积累了丰富的经验，其培养模式对我国具有一定的借鉴意义。例如：

1.美国高校强调实践与研究并重。通过与企业、政府和研究机构合作，构建网络安全实验室和攻防演练平台，为学生提供真实的实战环境。

2.以色列重视网络安全教育的系统性。建立了从中小学到高校的分层次培养体系，并通过国家级项目支持高校与企业的合作研究。

3.欧盟通过推出“欧洲网络安全技能框架”等政策。明确了网络安全从业人员的技能需求，并推动成员国高校的课程体系标准化。

与国际先进经验相比，我国网络安全教育在课程体系、

实践教学和校企合作等方面仍有较大提升空间。

（四）网络安全人才培养的行业需求分析

根据行业发展趋势和企业需求，复合型高技能网络安全人才应具备以下能力：

1.技术能力。精通网络安全相关技术，如漏洞挖掘、威胁分析、应急响应等；熟悉前沿领域，如人工智能安全和区块链安全。

2.综合素质。具备跨学科知识，能够在复杂场景中解决多维度的网络安全问题；具有团队协作和沟通能力。

3.创新能力。能够应对快速变化的网络威胁形势，在攻防对抗中设计和应用创新技术。

然而，当前高校毕业生的能力与行业需求之间仍存在一定差距，这一问题进一步凸显了教育改革的重要性和紧迫性。

三、复合型高技能网络安全人才培养核心能力框架

（一）核心能力框架设计的基本原则

复合型高技能网络安全人才的培养需要遵循以下基本原则：

1.实用性原则。核心能力框架应满足行业实际需求，确保学生能够在复杂的网络安全场景中高效解决问题。

2.前瞻性原则。紧跟技术前沿，涵盖如人工智能安全、区块链安全、物联网安全等新兴领域，为学生提供适应未来发展的知识和能力储备。

3.系统性原则。将知识、技能与素养有机结合，构建全面、系统的能力模型，注重学生技术能力、综合素质和创新能力的均衡发展。

4.个性化原则。考虑学生的兴趣与发展方向，提供灵活多样的课程选择和实践机会，以激发学生的学习积极性和潜能。

（二）核心能力要素分析

复合型高技能网络安全人才应具备以下三类核心能力^[4]：

1.技术能力。（1）网络攻防能力：掌握网络攻击与防御技术，如渗透测试、漏洞挖掘、防火墙配置及入侵检测等。

（2）前沿技术应用能力：具备人工智能、大数据、区块链等新技术在网络安全领域的应用能力。

2.综合素质能力（1）跨学科知识整合能力：将法律、管理和经济等多学科知识融入网络安全决策中，能够综合评估安全事件的技术、法律和社会影响。（2）团队协作能力：具备良好的沟通能力和团队合作精神，能够在多职能团队中有效开展工作。（3）项目管理能力：掌握项目管理基本方法和工具，能够规划并执行复杂的安全项目。

3.创新能力。（1）问题解决能力：能够在未知威胁场景下快速分析问题，提出创新性解决方案。（2）研究与开发

能力：具备安全工具和技术的研究开发能力，能够在攻防对抗中开发原创性解决方案。（3）应变能力：适应网络安全环境的动态变化，快速响应并调整策略以应对新的安全威胁。

（三）核心能力框架的构建路径

为构建复合型高技能网络安全人才培养核心能力框架，本研究提出以下路径：

1.明确培养目标。根据行业需求，定义复合型网络安全人才的核心能力目标，确保培养方向清晰。培养目标可细化为以下三个层次：（1）基础能力目标：确保学生掌握网络安全基础知识和技能。（2）拓展能力目标：提升学生的综合素质和跨学科能力。（3）创新能力目标：培养学生在复杂场景中创新思维和技术开发能力。

2.优化课程体系设计。（1）核心课程强化：优化网络安全核心课程内容，增加如网络攻防演练、数据隐私保护、智能安全等方向的课程模块。（2）选修课程多样化：引入如物联网安全、人工智能安全、区块链技术等选修课程，满足学生多元化发展需求。（3）跨学科课程融合：开设网络安全与法律、管理结合的课程，如“网络安全法规与合规管理”“信息安全项目管理”。

3.加强实践教学环节。（1）建立仿真实验平台：开发虚拟化网络攻防实验平台，模拟真实攻击场景，为学生提供实践机会。（2）引入企业项目：通过校企合作引入企业真实项目，让学生在实战中提升技能和解决问题的能力。（3）举办创新竞赛：鼓励学生参与CTF比赛和创新创业项目，激发其探索新技术的兴趣和能力。

4.深化校企合作模式。（1）联合培养基地：与企业共建网络安全人才培养基地，为学生提供实习和就业机会。（2）双师型师资队伍：聘请行业专家作为兼职导师，提升教学的实践性与行业适应性。（3）行业认证支持：与企业合作引入国际网络安全认证课程，提升学生的职业竞争力。

5.应用新兴技术手段。（1）智能教学平台：开发基于人工智能的教学辅助工具，个性化推荐学习资源。（2）沉浸式学习环境：利用虚拟现实（VR）和增强现实（AR）技术，为学生提供沉浸式安全攻防演练场景。（3）数据驱动教学优化：通过学习数据分析，优化教学设计和学生能力评估。

四、培养复合型高技能网络安全人才的具体措施

为了应对网络安全行业对复合型高技能人才的迫切需求，高校需要在课程体系、实践教学、校企合作、教学方法以及师资建设等方面进行全面改革，以实现理论与实践并重、学科交叉融合的人才培养目标^[5]。

（一）课程体系优化

1.构建模块化课程体系。按照基础、核心和拓展三个层次进行设计，涵盖从基础理论到核心技术应用再到前沿技术

探索的内容，满足不同学生的学习需求。

2.增加跨学科课程。将法律、管理、社会学等领域的知识融入网络安全教育，培养学生多维度的思维能力和综合素质。

3.实施分层教学模式。针对不同水平的学生，设计差异化的教学目标与内容，通过分组教学、分层作业等形式，确保学生在学习过程中获得充分的成长和发展。

（二）实践教学强化

网络安全是一门实践性很强的学科，加强实践教学是培养人才的关键环节。

1.建设高水平仿真实验平台。开发虚拟化网络攻防实验平台，模拟真实的网络环境和攻击场景，使学生能够在逼真条件下进行实战训练。引入人工智能和大数据技术，构建智能化实验平台，动态调整实验难度，满足学生不同实践需求。

2.开展项目式学习。结合企业真实需求，引入实际项目案例作为教学内容，让学生在解决具体问题的过程中学习知识、培养能力。例如，通过开发企业安全监控系统、设计数据加密方案等项目，帮助学生积累实战经验。

3.举办竞赛激发兴趣。鼓励学生参与CTF比赛、网络攻防演练以及创新创业大赛等活动，提升其动手能力和创新意识。同时，学校可组织校内安全竞赛，通过团队协作形式模拟复杂安全场景，锻炼学生的综合能力。

（三）教学方法创新

在教学方法上，探索多元化和互动式教学模式，激发学生学习兴趣和主动性。

1.应用案例教学法。将真实案例融入教学过程，通过实际问题引导学生思考并动手实践，提升其分析和解决问题的能力。

2.引入沉浸式教学。利用虚拟现实和增强现实技术，构建虚拟网络攻防场景，为学生提供沉浸式学习体验，增强其对复杂网络安全问题的感知和理解。

3.数据驱动教学优化。通过学习分析技术收集学生学习行为数据，动态调整教学策略。例如，利用人工智能技术分析学生的学习弱点，有针对性地推荐学习资源和练习内容，提高学习效率。

五、结语

培养复合型高技能网络安全人才是高校教育改革中的重要任务。通过构建多元化课程体系、强化实践教学、推进校企合作及利用新兴技术手段优化教学，可以有效弥补高校人才培养与社会需求之间的差距。高校应持续探索与优化网络安全人才培养模式，为国家网络安全战略提供高质量的人才支撑。

[参考文献]

[1]班海琴.网络安全与执法专业计算机网络实验课程教学改革研究[J].电脑知识与技术,2024,20(22):133-136.

[2]李煜民,李曦.网络攻防课程教改视角的网络安全人才培养[J].福建电脑,2020,36(10):63-65.

[3]潘赞,陈双喜,傅新杰,等.专项任务与课程学分互换研究——以信息安全技术应用专业为例[J].职业技术,2024,23(10):70-78.

[4]施江勇,陈颖文,付绍静,等.面向岗位胜任力培养的网络防御综合实践课程建设[J].软件导刊,2024,23(08):43-48.

[5]李文朋,杨新涛,陈青钦,等.数字中国信息安全在新时代的机遇与挑战[J].软件,2024,45(09):88-90.

作者简介：

黎斌（1981-），男，汉，广西梧州，教师/副教授，研究生，单位：广西职业技术学院，研究方向：网络安全

基金项目：

广西科技发展专项资金（广西重点研发计划）“面向关键信息基础设施保护的网络安全大模型应用与技术示范”，项目编号：2024AB33303