网络安全视域下安全防御人才培养机制探索

张植豪

郑州信大先进技术研究院 河南 郑州 450001

【摘　要】针对我国高校网络安全防御人才培养过程中的突出问题深入剖析新环境形势下人才培养的困境，提出一种网络安全视域下安全防御人才培养方案，从“以点带面，深入挖掘网络安全事件折射出来的网络安全知识元素，构筑知识完整、难度适宜的课程体系”、“以课程为基石，以虚拟化前沿技术为依托，构建场景还原度高、简洁易用的网络安全教学一体化平台”两个方面探索网络安全防御人才培养机制，为全球数字化背景下我国网络空间安全体系的高素质人才队伍建设提供参考。

【关键词】网络安全；安全防御；人才培养

1.新环境形势下人才培养的困境

2021 年 7 月 CNCERT 发布的《2020 年中国互联网网络安全报告》指出，安全漏洞、数据泄露、网络诈骗、勒索病毒等网络安全威胁日益凸显，有组织、有目的的网络攻击形势愈加明显，为网络安全防护工作带来更多挑战。[1] 调查研究发现，网络安全事件频发且对国家的政治、经济等产生了严重威胁，如“供应商被黑，日本政府大量敏感数据泄露”事件、“网络攻击致使英国邮政巨头中断国际寄件服务”事件、“针对中文用户，黑客利用谷歌搜索广告传播恶意软件”事件等。

专业人才培养模式中，成功的人才培养模式应该能够全方位提升人才综合素质和技能，如图所示。

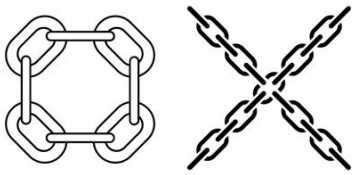

图 成功的人才培养模式示意图

在“成功的人才培养模式示意图”中，“教-学-用”各环节紧密连接，形成一个完整的知识体系闭环；“校-企”深度融合，多维度培养理论扎实、实操经验丰富的实战型人才。

但相比较于网络空间安全严峻的态势，我国针对网络安全防御人才的培养显得有点滞后。[2,3]调查结果显示，实际中的网络安全防御人才培养效果如图所示。

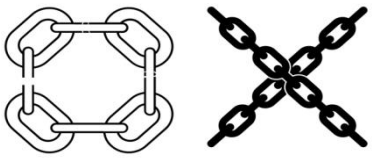

图 网络安全防御人才培养现状

从图“网络安全防御人才培养现状”中不难推出，在我国高校的网络安全防御人才培养方面，人才培养的突出问题体现在：知识体系复杂，融会贯通能力差；实战情境脱节，“看似融合，深度不足”，知识技能转化率低；设计情境过分依赖于传统课程体系，知识掌握的广度和深度发展受限。

进一步分析发现，成功的人才培养模式与网络安全防御人才培养现状的矛盾的原因主要体现在以下几个方面：①课程内容较为滞后：与频发的安全攻击事件相比，现有的知识体系中某些内容已经过时，僵化、滞后的课程设置阻碍了网络安全防御人才培养体系的完善；②实训课程缺乏针对性：纵观现有模式，很多高校、企业等都设计开发了相应的实训课程，但这些课程仍是以教材为参照，对人才综合能力提升有限；②缺乏清晰的学情分析：由于人与人之间认知度、敏感度等方面的差异性，学生对网络安全领域知识的掌握与运用程度不同，导致实训课程设计与目标对象不匹配。

基于此，需要将网络安全专业基础知识与综合实际运用有机融合，实现理论、实训、创新等能力的渐进式提升，真正从多维度锻炼、提升我国安全防御人才的综合素质。

2.网络安全视域下网络安全人才培养机制

为切实提升我国网络安全防御转业技术人才的网络安全理论基础、技能实操本领，本文基于“从热点事件驱动思方向”、“从单位用工需求询架构”两方面探究新形势下需要什么样的人才。从发生频率愈来愈高、态势愈演愈烈的网络安全事件可知，网络空间安全严重制约着经济的发展、社会的安定；基于问卷调查与单位用工需求的统计分析，在人才能力需求方面呈现出“各个城市阶层对网络安全方向人才需求量大”、“弱化学历，追求能力”的特点，且在能力需求方面要求从业人员能够全面感知网络安全体系并融会贯通，能够快速感知与定位网络安全风险，做到“来之即战，战之必胜”。

因此，网络安全防御人才的培养要以现实为基础并服务于现实。

2.1.构建以热点网络安全事件为依托的课程体系

目前，网络安全防御基础理论知识体系的相对稳定性与现实复杂多变的网络安全防御态势相冲突，因此要广泛深入推进校企联合，要从增强学生学习沉浸式、获得感方面着手，对人才培养实际情况进行深入调研。教师最贴近学生、最了解学生的知识深度且最熟悉教材、最理解经典知识体系全貌，企业具有深耕于网络安全一线的资深教学培训专家、专注于网络空间安全靶场构建的技术专家。因此校企深度合作，以热点网络安全事件为依托，深入剖析安全事件诱因；以网络安全某一剖面，挖掘适合学生掌握的知识点；以点带面，挖掘事件折射出来的网络安全知识元素全面评估；精细规划，构筑真正面向学生难度适宜的网络安全课程体系。

本文以“全球关键半导体厂商因勒索攻击损失超 17 亿元”热点事件为例，以点带面，深入挖掘网络安全事件折射出来的网络安全知识元素，构筑知识完整、难度适宜的课程体系。面向网络安全实际问题解决的完善的课程制作流程如图所示。

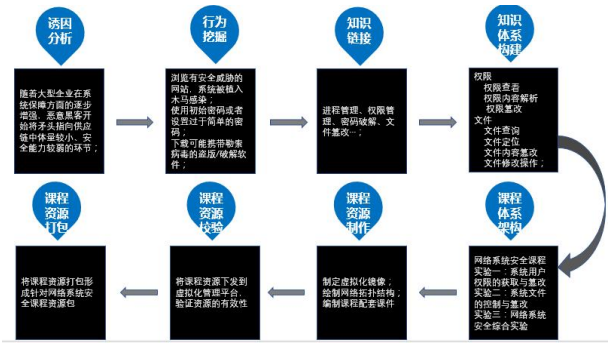

图 以热点网络安全事件为依托的课程体系构建过程

2.2.构建以课程为基石的网络安全教学一体化平台

网络安全教学一体化是一种实现理论、实训渐进式学习的较好实践，其专注网络场景的逼真模拟，依据掌握的目标网络指纹信息，通过虚拟环境与真实设备的结合、网云融合一体化协同、网络安全数据中心管控，建立可扩展、高可靠、高逼真的网络空间环境，从而为网络空间安全治理赋能。

根据对市场网络安全教学产品的调研，本文提出以课程为基石，以虚拟化前沿技术为依托，构建场景还原度高、简洁易用的网络安全教学一体化平台，以实现与以热点网络安全事件为依托的课程体系的深度融合。如图所示。

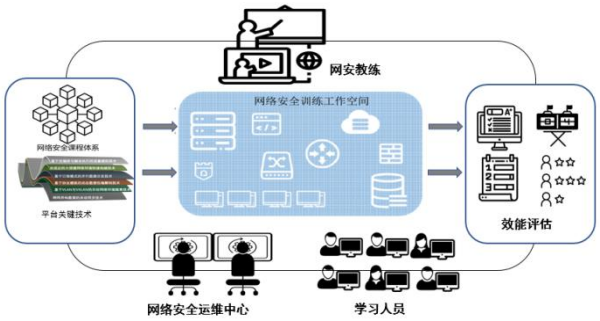

图 以课程为基石的网络安全教学一体化平台

如上图，借助于包编排与脚本执行的流量模拟、自适应的大规模网络环境快速构建、跨网异构数据的自动同步等技术将“以热点网络安全事件为依托的课程体系”导入平台，通过网安教练的导调为学习人员提供网络安全训练工作空间，并通过效能自动化评估机制实现对受训人员的学习效能全面评估，从而有效提升网络空间安全防御专业技术人员的知识储备能力、业务技能、实操本领。

3.结语

基于人才培养的困境从“以点带面，深入挖掘网络安全事件折射出来的网络安全知识元素，构筑知识完整、难度适宜的课程体系”、“以课程为基石，以虚拟化前沿技术为依托，构建场景还原度高、简洁易用的网络安全教学一体化平台”入手，形成了网络安全视域下网络安全防御人才培养的闭环，为我国网络安全防御人才培养体系的进一步完善提供了参考。

【参考文献】

[1]国家互联网应急中心 CNCERT. 2020 年中国互联网网络安全报告.中华人民共和国国家互联网信息办公室.2021-07-21.http://www.cac.gov.cn/2021-07/21/c_1628454189500041.htm

[2]闫桂勋,王超.产学研融合发展的网络安全人才培养机制研究.科技中国[J],2022.11(10),54-59.

[3]闫玺玺,冯苏伟,张静.新工科背景下网络空间安全专业人才多维联动培养模式探索.高教学刊[J],2023.02(05),157-159.