院校“校企合作”网络安全人才培养思考

邢宇航　李敏　王利涛　何玉杰
火箭军工程大学

摘　要：着眼提高网络安全人才新质能力，强化网络安全骨干人才培养条件支撑，紧贴网络空间安全需求，在分析网络安全人才培养基础上，研究“校企合作”人才培养的典型模式，最后详细分析了落实“校企合作”网络信息安全人才培养模式的具体内容和要点。随着网络空间成为新战场，网络空间的对抗愈演愈烈。网络空间安全事件发生的频率更加频繁，破坏程度越来越大，已经严重影响到经济、社会、军事和国家安全。当前的网络空间威胁迫使必须要懂网络、懂安全，否则可能无法适应未来网络环境。网络安全无小事，不能有短板缺项。网络安全能力的提升就是网络安全人才的培养问题。院校是一个特殊的群体，在人才培养方面具有先天优势，如何在院校这个环境中培养网络安全人才是一件迫在眉睫的事情。本文则从网络安全人才培养的现状出发，着重分析院校“校企合作”网络安全人才培养模式现状优劣，探索网络安全人才培养的新模式新方法新举措。

关键词：校企合作；网络安全；人才培养；培养模式
【DOI】10.12252/j.issn.2096-6288.2024.01.016

一、院校网络安全人才培养的特点

没有网络安全就没有国家安全，自从网络安全上升到国家高度，网络安全已逐步得到大家的重视，网络空间安全也发展为一级学科，很多院校也成立了网络空间学院。同时也要看到，还有很多院校没有重视网络安全，在网络安全的投入上还不够，对于提升整体的网络安全素质起到了阻碍作用，究其原因，可能有以下几个方面。

（一）没有专门的系统的专业的培养体系

作为应用型、工程类的院校，专业性强。基础类课程是根据专业需求设计，如果校内没有网络安全专业，相应的基础类网络课程也不会设置[1][2][3]。网络安全知识的获取只能通过自学和非系统化的培训来实现。通过调研发现，重视网络安全的院校网络安全素质较高，一方面是学校有网络空间安全学科和专业支撑，具备专门的知识体系，基础扎实牢固，动手能力强；二是经过基础知识、专业知识和实践课程的系统学习，对网络安全的认识和理解深入，能应对各种网络安全问题和情况。三是长时间的网络安全素养培育，学生都有较高的网络安全意识和素质，从而避免了大部分网络安全问题的发生。网络安全人才培养不是一蹴而就的事，需要专门的系统的专业的培养体系来践行。

（二）没有专门的系统的专业的支撑平台

目前来看，网络安全将是一个永恒的话题，网络安全的未知性、不确定性和潜在风险将影响各个领域。基本的网络安全知识和技能可以回避很大部分的网络安全问题，但不能解决所有的和未知的问题。实践是检验真理的唯一标准，真正提升网络安全能力的最好办法就是实战。通过实战，真正理解整个网络攻击过程中攻防双方的招数，才能在面对实际环境时从容不迫、不慌不忙。从大量的网络攻击案例分析发现，有效的网络空间防御和应急处置，可以大大降低网络空间攻击的破坏程度，挽回很多不必要的损失。大多数人在网络攻击面前束手无策、手忙脚乱，不能有效止损。如果没有网络安全专业，校内也没有专门的实践实训平台，客观上限制了网络安全人才培养。

（三）没有专门的系统的专业的教学团队

如果说硬件资源还可以靠投入来解决的话，没有教学团队更是一个致命的问题。自从国家重视网络安全以来，很多的院校逐渐成立了网络空间安全学科，加大了对网络安全问题的投入和支持，出现了越来越多的专家队伍，甚至院士牵头组建团队，全方位提升了网络安全的能力和水平。但没有认识到网络安全威胁的院校，没办法做到这种程度。网络已与大家工作、学习及生活息息相关，网络安全问题是全覆盖的。如何利用现有的资源，提高网络安全人才的培养质量，首要的就是打造教学团队，没有教学团队的支撑，很难做出大成果来，必须集智攻关，团队协作。

二、院校“校企合作”人才培养模式分析

“校企合作”是比较古老的话题[4][5]，很早就有院校在做，合作的方式更多，但总的来说，大概有以下几种类型。一是技术输出型。一般是院校和企业共同承担一些理论课程，院校为主主理论，企业为辅主实践；二是中心孵化型，表现的主要形式为产业院、实验室和培训中心等。校企共同合作成立一个孵化中心，孵化中心主要是企业产品输出，院校技术输出；三是科研创新型。校企共同合作培养人才，共同攻关科研课题，共同技术创新研究；四是联合共建型。校企形成全面战略合

作，在共同领域进行深层次的技术合作和技术支撑，互为补充，相互促进。下面分情况具体分析“校企合作”人才培养的几种模式。

（一）技术输出型“校企合作”人才培养模式

这种合作模式相对比较简单，校企双方的自由度高，各自做好各自的工作即可，校企双方提前沟通好负责的内容，在特定的时间内把对应的内容落实。而且根据双方情况随时调整，只要能够达成一致，这种培养模式就可以落地。这种方式的优势是利用校企双方的长处。一般地，院校在理论授课方面有优势，企业在实践教学方面有优势。院校可以调动校内资源把课上好，企业可以利用企业资源，做好实践课程配套。同时，可以把最新的资源融入实践课堂，保持创新性。这种方式的劣势是模式单一，如果理论与实践衔接不好，容易产生矛盾，会产生理论与实践相脱节的问题。同时，无法限制固定的授课人员，也会造成培训效果打折扣的问题。当然，如果准备充分、沟通充分，可以回避上述问题。

（二）中心孵化型“校企合作”人才培养模式

院校涌现了很多这种类型的成功案例，但对于很多院校来说，无法发挥出这种方式的优势。主要原因在于，一是管理规定问题；二是运维问题。成立一个新的部门或者中心，需要相应配套的管理、运维等岗位，需要专门的人员来操作。同时，企业作为产品输出售后的方式参与教学管理，会限制知识内容的更新效率，这种响应式的保障方式无法满足教学效果。这种模式如果贯彻落实的好，可以形成规模，具有示范效应，增大中心的影响力，从而促进中心的快速发展。弊端是需要投入大量的人力和财力，基础条件建设投入大，需要专门有人进行管理和运行。

（三）科研创新型“校企合作”人才培养模式

这种模式在院校也非常常见，从效果来看，活力好，发展潜力大。实际上，网络安全是一个不断发展演变的事物，从技术到产品再到人才培养，只有不断创新和研究，才能不断发展，进而适应新的网络安全形势。从技术角度看，这种模式非常适合采用，一方面可以促进网络安全教学队伍的发展和能力提升。另一方面可以持续保证技术的前沿性和先进性。另外，还可以快速提升人才培养的质量。但这种方式的起点较高，首先必有一定的基础和相应的技术储备，才能保证在科研创新合作中提升实力。其次，也必须有专门从事网络安全的人参与进来，否则很难达到想要的效果。这种方式的劣势是高技术层次的合作，对于不同层次的网络安全人才培养缺乏针对性，需要加以区分对待。

（四）联合共建型“校企合作”人才培养模式

这种模式是一种灵活多变且合作覆盖多个层次的方式，它最显著的特点是没有基础条件要求，可以通过双方需求达到共赢的目的。合作可以落在技术探讨、技术研究及创新，也可以落在教学支撑上，企业可以定期为院校做网络安全形势分析、网络安全前沿知识普及等，还可以是共同申报教学课题、科研课题等方式。而双方可以通过类似挂牌、战略合作合同、人才交流等方式来维系。所以说，这种方式最灵活，形式多样，可以把企业作为院校实践基地，把院校作为企业网络安全技术及产品推广普及的单位，达到互惠互利的目的。这种方式的优势明显，弊端少，完全是根据各自所需进行合作，效益好可以深入合作，效益差可以调整合作方式。总之，是发挥两者的优势，实现最大的效益。

前面分析了“校企合作”的不同模式，每种模式都有成功的案例可以借鉴，根据各自的特点，可以针对性的选择合作方式，目的就是发挥大家优势，集智提升网络安全人才培养的质量。

三、院校“校企合作”人才培养模式内容要点

从当前网络安全发展来看，企业在网络安全技术层面把院校远远地抛在了后面。院校的网络安全人才培养想快速赶上、超近路，应该借用企业的力量。通过合作，提升网络安全人才培养的质量，增强整体网络安全防御能力和水平。而落实“校企合作”这种培养模式的话，应该如何实施，从哪些方面入手呢，下面具体分析“校企合作”落地几个方面的考虑。

（一）“校企合作”网络安全人才培养体系

真正落实合作，要从人才培养的顶层设计出发，需要建立人才培养方案，涉及培养目标、需求、原则及内容等方面具体要求。网络安全因其技术复杂性，不能一概而论，一个标准，可能造成调子高，达不到目的。要分析培养对象，就是分析其能力需求，从能力需求出发，确定要学习的内容及要求。比如一个本科生，本人已有网络基础知识及其相关的网络工具使用技能，还可以熟练配置网络防御系统等，他的培养方案定位就是高层次网络安全能力提升，可以直接跨过基础知识的学习，直接进入网络配置、网络夺旗竞技实战、渗透测试等阶段，甚至直接参与网络对抗演练等提升环节。如果是网络零基础的人，本人对网络知识的学习和了解比较困难，那么就要侧重网络安全意识的提升环节。如果对网络安全感兴趣，但之前没有基础，可以从系统培养的角度出发，从基础知识、能力培养、动手实践和综合训练的逐级提升的方案来设计。网络安全防护必须不能留漏洞，千里之堤毁于蚁穴，只有提升整体的水平，才能真正避免大部分的网络攻击。

（二）“校企合作”网络安全人才培养课程体系

从多年的教学经验来看，人才培养是一个系统工程，但网络安全人才的培养在不同的环境中，是可以走捷径的，首要的是打造一些精品课程。让一个网络零基础的人去自学或者选择上什么课，肯定是盲目而不得法。因为网络上的资源太多，狂轰乱炸下来，对初学者来说，太难选择了[6]。需要打造几门精品课程来引导学生学习。这里讲课程而不是教材，一门课程可以选择多个教材，需要花些功夫根据不同层次的目标来设计。利用院校和企业的资源，定制化打造精品课程，使得学习者更容易上手。比如，针对初学者，可以打造一门网络入门课程，它系统介绍网络基础知识、网络配置、网络工具使用、网络安全系统设置等。针对网络防御的学习者，可以打造一门安全防护系统构建配置的课程；针对网络攻防学习者，可以打造一门网络攻击案例复盘的课程，让其真正的感受实战过程。课程打造需要一个积累过程，一门课程可能涉及很多的知识，需要进行大量资料整理和逻辑推理工作。可以徐徐推进，但从长远来看，培养不同层次的人，必须要努力打造精品课程。

（三）“校企合作”网络安全人才培养支撑平台

如何提高网络安全人员的实战能力和水平，理论学习是远远不够的，需要大量的实践实战。从调研情况看，企业在各种网络靶场的构建和技术创新上有无可比拟的优势，环境条件比较充实和丰富。而院校偏理论教学和课程实验，且内容的更新速度也比不上企业。但院校定制的特殊场景则是企业没有的，需要二者协作配合来完成。建议依托企业的技术力量，基于院校环境条件，共同打造符合实战场景的支撑平台，让学生可以在一个类真实环境的情形下训练，从而快速提升实战能力。而打造这样一个支撑平台需要充分论证，设置什么样的科目、构建什么样的场景、网络攻防做到什么程度、模拟什么样的攻击等，需要校企双方充分对接和共同运维。只有这样的平台，才能真正的把学生的学习动力调动起来，才能真正向实战靠拢，而不是纸上谈兵。

（四）“校企合作”网络安全人才培养评估系统

作为院校，传统的对学生的考核基本都是理论考试+实践考核+形成性考核。理论考核就是试卷的形式，实践考核就是动手操作，形成性考核就是平时表现或者大作业。这种考核方式从面上体现了对这门课程学习的学习效果。但网络安全人才的培养不能停留在这个层面，需要的是学生解决实际问题的能力，否则等于没学。大量网络安全案例表明，网络攻击的颠覆性是人所共知的，来不得半点马虎。把理论知识真正转化为实战能力是网络信息安全人才培养的关键，而这个转化的关键就是不断的实战。因此，实战是判断评估学习效果的唯一标准。但这个环节如果仅凭院校完成是非常难的，校内很难组织大规模的实战对抗，必须联合企业，甚至走到更大的平台上去，到省级或者全国的平台上去。如果做不到，校企合作共建一些实战科目，通过科目积分来完成学生的学习效果评估。旨在检验网络安全的实际能力和水平。考核组由企业和院校共同组成，参照工信部的网络安全认证标准来衡量，真正的把人才培养起来。

（五）“校企合作”网络安全人才培养创新平台

“校企合作”人才培养模式不能停留在表面上，最好是深度合作，从课程讲授到课程实践，这只是已有成果传授，是浅层次合作。共同进行教学、科研、学术的深度合作，才是深层次的。一方面，深度合作可以快速的提高院校的人才培养质量；另一方面，深度合作可以促进企业改进产品，推动企业发展；再者，成果的推广也可以提高两者的影响力和知名度，可以促进二者的更快发展和合作深度拓展。把研究成果反哺教学，才能保持合作的可持续性和新鲜性。网络安全的未知性和不确定性，一直都是其显著特征，只有不断更新和探索，才能真正强大。

结束语

“校企合作”不是一个新名词，但作为院校，由于缺乏对网络安全的重视，造成巨大损失的案例比比皆是。网络安全人才培养来说，非常适合这种模式，而且是互惠互利的一种合作模式。采用哪一种方式、合作到什么程度，可以根据各院校的实际情况。当前网络安全形势非常严峻，探讨院校“校企合作”网络安全人才培养也是重视网络安全的一种具体表现，浅层次的是提高大家的网络安全意识，深层次的是为培养适合未来网络空间合格人才做准备。

参考文献

[1]王晓凡.1998年以来我国高等教育研究进展及反思[D].导师：马力.湖北大学，2022.

[2]李玉枝.我国高等教育发展方式转变研究[D].导师：赵庆年.华南理工大学，2021.

[3]赵丽华.我国高等教育第三方评估机构运作模式研究[D].导师：王彦才.海南师范大学，2021.

[4]李欣悦.基于DEA-Malmquist组态的我国高等教育投入产出效率及影响因素探析[D].导师：杨俊青.山西财经大学，2021.

[5]赵劲，侯丽朦.“变轨超车”：互联网发展对我国高等教育的影响及应对[J].浙江树人大学学报（人文社会科学），2021，（02）：94-99.

[6]刘丽丽.公共价值视角下我国高等教育慕课政策研究[D].导师：闵辉.华东政法大学，2021.