从人才培养体系建设谈实践型网络空间安全人才培养

刘艳东，李　晨
（绿盟科技集团股份有限公司，北京 100089）

摘　要：近年来，我国高度重视网络空间安全人才的培养与体系建设。网络安全的竞争归根结底是人才的竞争，网络空间安全人才体系与机制的建立，对网络安全人才培养至关重要。从美国、欧盟、日本等政府对网络安全人才培养体系进行介绍，并对我国当前网络安全人才培养体系现状进行深度分析，同时给出网络安全人才培养的思路和方法。围绕“培养实践型的网络安全人才”的核心思想，在高校建立网络空间安全靶场，以系统化、实践化方式来培养高质量的网络安全人才。

关键词：网络空间安全；人才培养；网络靶场
中图分类号：TN915.08　　文献标识码：A　　DOI：10.19358/j.issn.2096-5133.2020.09.008
引用格式：刘艳东，李晨. 从人才培养体系建设谈实践型网络空间安全人才培养[J]. 信息技术与网络安全，2020，39(9)：39-43.

Discussing the training of practical cyberspace security talents from the perspective of talent training system

Liu Yandong, Li Chen
(NSFOCUS Technologies Group Co., Ltd., Beijing 100089, China)

Abstract: In recent years, China has attached great importance to the training and construction of cyberspace security talents. In the final analysis, the competition of cybersecurity is the competition of talents. The establishment of a national-level cybersecurity talent system, mechanisms and supporting measures is essential to the cultivation of cybersecurity talents. This article introduces the cyber security talent training system from the US, EU, Japan and other government organizations, conducts an in-depth analysis of the current status of China's cyber security talent training system and puts forward the thought and method of cyber security personnel training. It is suggested that, focusing on the core idea of "cultivating practical cyber security talents", the cyberspace security offensive and defensive range platforms should be set up in colleges and universities to train cybersecurity talents in a systematic and practical way.

Key words: cyberspace security; talent development; cyber range

0 引言

随着全球数字化、信息化的蓬勃发展，网络安全问题也日趋严峻，网络安全已经成为影响全球数字经济发展的重要因素。我国高度重视网络空间安全发展，相继出台《网络安全法》《国家网络空间安全战略》《网络安全等级保护2.0》《密码法》和《网络安全审查办法》等国家安全法律和政策条款，对推动我国网络空间安全强国战略发展，构建网络空间命运共同体具有重要意义，网络空间安全已上升至国家战略高度。

网络空间的竞争，归根结底是人才的竞争。如何培养网络安全多元化、高质量人才，已成为全球各国关注的焦点。体系化的网络安全人才培养体系建立，真实化的网络攻防对抗演练以及常态化的人才培养基础设施建设，已成为大国网络空间安全战略发展的重要举措。

1 各国网络空间安全人才培养体系建设情况

目前，全球各国普遍从管理、立法、政产学研用等方面高度重视网络安全人才培养体系的建设。

1.1 美国：多层次、广覆盖的培养体系

美国高度重视网络安全人才培养建设，相继发布相关网络安全人才培养战略及框架计划：2010年

发布国家网络安全教育计划 NICE；2016 年发布该计划的网络安全人才框架 NCWF[1]；美国政府依托高校建立网络安全人才培养卓越中心，NSA 和 DHS 共同资助国家网络防御学术卓越中心(CAE－CD)计划，专门培养网络安全防御型专业人才。另外，NSA 启动国家网络运营学术卓越中心(CAE－CO)计划，重点培养网络运营型人才；2013 年 2 月，DHS 启动网络安全职业与研究国家计划(NCCS)，目的是开发在线网络安全培训资源[2]。

在学历教育方面，美国高度重视通过正规学校系统教育培养网络安全人才，已经将网络安全教育体系嵌入到不同学龄，甚至是幼儿阶段。同时，加强对青少年网络安全人才的培养和挖掘是网络安全人才的基本理念。高等学校在培养专业人才的同时，注重对网络安全科学研究能力的培养，形成了教学与科研双轮驱动的教育模式。

在社会培训方面，美国政府早在 1998 年就开始实施针对信息系统和网络基础设施安全保障的培训和认证计划，从多方面接入网络安全培训和教育工作。目前，美国社会已经建成面向不同领域的培训体系。

1.2 欧洲：专业教育和全民普及相结合

欧盟 2013 年 2 月发布了《网络安全战略》，并且已制定网络安全人才战略规划。各成员国要在国家层面重视网络安全方面的教育和培训，同时要求学校开展网络安全培训，对计算机科学专业学生进行网络安全、网络软件开发以及个人数据保护的培训，对公务员进行网络安全相关培训。另外，还加强高校对网络安全专家的培养。例如，英国政府为提高网络安全教育质量和教学水平，满足社会对网络安全专家的需求，加强了高校专业认证。另一方面，欧盟注重提升全民网络安全意识。欧盟各成员国在欧洲网络和信息安全局(ENISA)的支持下，从 2013 年起每年组织 1 次私营行业参与的网络安全月活动，以提高用户的安全意识。

1.3 日本：整合政府、企业和高校的资源

日本通过以下几个方面来加强网络空间安全人才培养。首先，日本已通过《网络安全基本法》实现立法保障。日本国内大学开始致力于培养可以应对网络攻击的人才，在大学开设的课程中，介绍对此类法令及企业遭受网络攻击的案例，同时将该课程设为所有入学者必修科目。其次，在专门学校设立网络安全科，在进行网络设计、构造技术学习的基础上，对病毒防治、加密、身份认证等多种信息安全技术进行学习。培养运用高新的技术从黑客以及网络恐怖主义中保护企业以及人民的人才。最后，加强政府、企业、科研机构、高校联合，日本的经济产业省、国立产业技术综合研究所、相关高校都在加强联合培养网络空间安全人才的力度[3]。

1.4 我国：出台相关政策，人才培养体系持续完善

我国在网络空间安全人才培养方面也提出相关政策：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”为一级学科[3]；2016 年，中央网信办、教育部等六部委印发了《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的创新创业的生态环境；2017 年，国家互联网信息办公室发布《关键信息基础设施安全保护条例(征求意见稿)》，反复强调网络空间安全人才对于关键基础设施的重要作用。

2 我国的网络空间安全人才培养体系现状

纵观全球网络强国诸如美国、以色列等国家对于网络安全人才培养的思路和模式，不难看出，国家层面会根据网络空间安全人才需求与发展情况，出台有关人才培养框架和具体实施计划，以推动网络安全人才培养战略的执行与落地。从学校的教育开始，就专门设置完善的网络安全专业相关课程体系和实践活动，并且打通国内网络安全上下游产业，将理论与实践相结合，让专业学生能够到网络安全企业进行实习和锻炼，以充分了解当前网络安全行业和企业对于网络安全人才的实际需求，并接触到最新的网络空间安全前沿热门技术，来拓宽未来网络安全人才的视野和知识。

据相关调研数据显示，每年我国培养的网络安全人才数量在 3 万左右，已经投入社会的安全相关专业人才不足 10 万，而 2020 年，我国的网络安全人才需求缺口将达到 140 万。近些年，随着我国高度重视网络空间安全人才培养，网络安全高等教育建设工作进程也在逐步加快。国家增列“网络空间安全”一级学科博士学位授权点，进一步加快和推进了我国网络安全人才培养的战略规划与部署。目前，我国 40 多所高等院校成立了网络空间安全学

院，实现了网络安全专业人才从本科到博士的一体化教育培养模式。虽然我国网络安全人才培养工作开展得比较早，但整体发展对比世界发达国家较慢，网络安全人才培养速度仍然滞后于我国网络安全产业发展的需要。

2.1 教学师资力量较为薄弱

从院校实际的网络安全专业培养工作来看，很多专业课老师并非是网络安全相关专业科班出身，往往是从计算机专业、通信专业或者是软件工程专业转型而来，老师对原有专业较为熟悉，但对网络安全体系化教学内容并不清晰。网络安全专业是跨学科专业，知识体系也较为复杂，老师很难在较短的时间内将网络安全相关课程体系进行深入理解并教授于人。另外，根据不同区域的教育程度与认知程度的不同，经济较为发达的区域对于网络安全教育投资和人才引进较为重视，偏远的地区受限于教育思想和资金问题的影响，往往在网络安全教育投入方面不足，这就造成了我国不同区域、不同院校对于网络安全人才培养和师资投入的重视程度不同。

2.2 专业课程体系不够完善

网络安全专业是具有跨多学科属性的专业，知识体系也较为复杂，专业知识较强且层次化分明。我国部分地区的网络安全专业的相关课程还采用较早的信息安全教材，且课程内容也已经较为落后，部分课程内容的设置结构不太合理，无法匹配当前网络安全产业的技术发展和人才需求。另外，网络安全专业也是一门实践性要求非常强和知识内容迭代较快的学科，如果将较为陈旧的、脱离实际网络安全技术发展趋势、不结合一定实践操作的课程设置为专业教材，那么院校培养出来的网络安全人才也是不成功的[4]。

2.3 工程实践教学重视不足

网络安全主要就是研究攻防之间的技术博弈和对抗，网络空间安全是一门对技术研究和操作要求较高的专业。我国当前部分院校在网络安全教学时，并没有配套设置相应的技术实践课程，也没有为学生制定工学交替、工程实践的人才培养计划和内容，学生也只是从教材中学习网络安全相关知识理论。网络安全行业和企业不仅需要研究性的技术创新型人才，而且更多的是需要具有丰富实践经验的工程型人才。

3 对网络安全人才培养体系建设的思考

3.1 提升师资队伍能力水平

从国家层面，进一步加强对于网络安全专业师资力量培养的政策与资金支持力度，优化和整合不同区域优质师资教学资源。通过师资优惠政策鼓励师资力量较强的区域将资源向较弱的区域引进和发展；通过线上和线下的网络安全师资培训模式，鼓励网络安全专业教师参加由专业网络安全人才培养企业组织的课外培训，以提升教师自身能力水平；院校方面，可考虑引进一批网络安全企业的技术人员到学校进行教学授课，将当前网络安全行业和企业里的先进技术和人才需求理念传授给教师和学生，真正将网络安全产业和企业的技术与经验转化为网络安全人才培养课程的重要内容之一。

3.2 完善专业课程体系

针对网络安全专业课程知识体系庞杂、交叉性强的特点，国家邀请和组织国内网络空间安全专业高水平的专家、学者和网络安全企业技术人才，对高等院校和高职院校的网络安全专业教材进行系统化、专业化的制定与编写。同时，可以借鉴国外先进的网络安全人才培养教材，将其优质教学内容融入到我国的网络安全专业教材的知识体系中。另外，可以考虑将行业内较为前沿、热门的技术和产业发展动态也编写进专业教材中，让学生可以在实际的专业学习中了解当下行业内比较关注的技术方向和产业发展趋势，而不是在就业时才了解和掌握。

3.3 重视实践性教学

高等院校要加强高质量网络安全人才培养模式的持续创新研究，根据网络安全专业的教学特点，在理论教学的过程中适当增加一定课时的专业实验课程与实践环节，来巩固和提升学生的理论结合实践的专业技能；高等院校与网络安全企业继续深入开展产学合作，不断深化产学融合，进一步加强和推进校企合作工作[4]，建立协同育人项目长效机制，在实践中探索和落地创新性网络安全人才模式。通过开展校企合作项目，让专业学生能够有机会走进企业，了解行业中最新的技术和产品理念，将所学的专业知识在企业的环境中进行实践与验证。

打造“政产学研用”的一体化网络安全创新实践人才培养基地，让学生能够在人才培养基地的环境中锻炼和积累经验，为有意愿进行创新创业的人才提供企业孵化的资源和实践机会[5]。

院校要持续开展或积极参与网络安全攻防竞赛，让学生能够在攻防竞赛中提升自己的网络攻防实践能力，不但可以为院校和企业选拔高质量的攻防型人才，还可以提高院校在国内网络安全专业的知名度，提升网络安全专业招生率和就业率水平。

4 培养具有实践能力的网络安全人才

从网络安全的本质来讲，高质量的实践型网络安全人才包含两类：攻击型人才和防御型人才。培养攻击型人才的目的也是以攻促防，从攻击者视角提出加强网络安全防御体系建设的思路和解决方案，提升企业纵深安全防御水平；防御型人才更是要在持续的企业安全事件应急响应处置的过程中，不断积累安全运营能力和应急处置能力，从企业“守卫者”的视角对企业安全进行技术和运维保障。

从网络安全人员的不同职能属性进行分类，可以分为战略型人才、研究型人才、服务型人才和工程型人才。战略型人才要具备丰富、全面的战略规划、组织管理、技术保障等综合能力和经验，从企业信息化建设的顶层设计角度出发，对网络安全技术体系、管理体系和运行体系进行统一规划和设计，其战略规划的科学合理性将影响企业未来的战略发展；研究型人才肩负着对网络空间安全技术创新和理论研究的重任，在研究过程中往往要分析大量的恶意代码和异常文件样本，研究攻击者的战术、技术和过程，从而提出应对新型或高级网络攻击的有效防御手段和产品方案，研究型人才对网络安全产业技术发展具有很强的推动作用；服务型人才为企业提供渗透测试、安全咨询、等保测评、风险评估、应急响应等服务，他们往往具有丰富的理论知识和实践型项目经验，是实践技能要求较高的一类人才；工程型人才是企业安全保障体系的构建者，通过实践化的一线工程经验，为企业提出合理、可靠、安全的工程实施方案，并根据企业面临的新的安全风险，提出优化改进建议和技术方案[6]。

5 实践型人才培养基础设施平台建设

网络靶场作为网络安全人才培养的重要基础设施，融合云计算、虚拟化、SDN、NFV、容器和虚实结合等技术，构建了“学习、竞赛、演训、测评、科研”一体化的实践型人才培养平台。

5.1 网络靶场平台架构

网络靶场利用灵活的网络编排管理、弹性的虚拟化部署和柔性的虚实结合等场景仿真技术，结合攻击、防御、流量仿真、数据采集与评估等能力组件，构建从学习、竞赛到训练、测评、研究的综合性人才培养解决方案，可以满足用户对理论学习、攻防竞赛、攻防演训、测试评估、技术研究等不同方面的业务需求。网络靶场采用大数据分析、行为分析、态势理解、机器学习、ATT&CK 和 Killchain 杀伤链等技术与对抗研究模型，对靶场数据进行深度理解、推理和关联分析，利用 3D/2D 动态可视化模型，可实时呈现攻防训练和对抗态势，并进行效果和效能评估。用户还可以对攻防数据进行复盘分析，以总结实践性经验和技术方法推演。网络靶场系统设计架构如图 1 所示。

5.2 典型应用

5.2.1 教学实训/科目训练

(1)理论与实践结合的进阶式安全技能学习体系，满足信息安全方向的理论学习和实验实操；

(2)安全技能考核，对学习效果进行量化评判；

(3)安全意识培养，从人的因素强化安全意识思维。

5.2.2 攻防竞技

提供在线理论答题、在线 CTF、攻防兼备 AWD、竞速夺旗 CFS 等竞赛模式，使参与者在竞技对抗中提升网络攻防技能水平。

5.2.3 攻防演训

(1)红蓝对抗，红蓝双方进行高逼真化的攻防对抗演练，以攻促防；

(2)从攻击维度，训练网络攻防技能，并对训练结果进行量化评估；

(3)从防守维度，针对突发的入侵威胁和安全事件，进行应急响应和处置的技能训练和提升；

(4)基于 APT 仿真环境，红蓝双方进行 APT 仿真对抗演练和技能提升。

5.2.4 测试评估

(1)利用自动化攻击组件或人员进行模拟攻击或渗透测试，对目标系统进行安全风险和脆弱性检测，以验证纵深防御体系的安全防御能力是否有效；

(2)对系统或产品进行性能指标测试和漏洞检测。

5.2.5 技术研究

(1)网络空间安全技术创新研究；

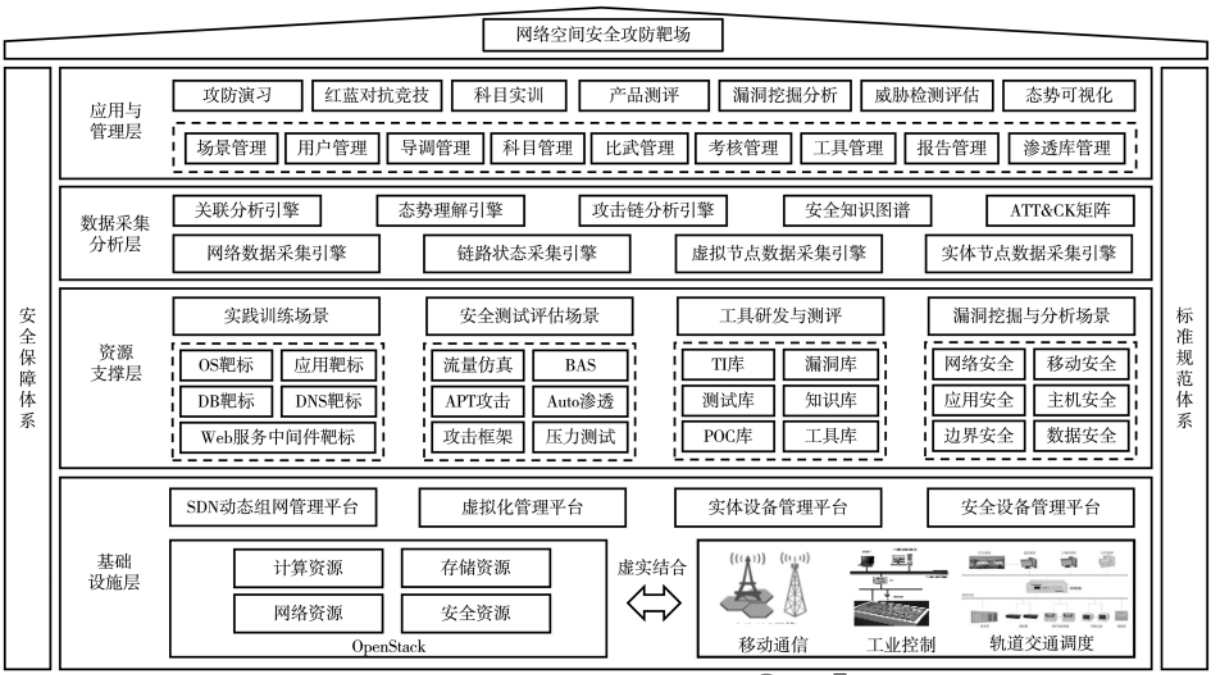

图 1 网络靶场系统设计架构

(2)对安全漏洞进行分析与研究。

5.3 关键技术

(1)大规模虚实结合节点的快速构建与弹性部署;

(2)低损耗的带内/带外全数据采集[7];

(3)高逼真的用户行为、应用和流量仿真模拟;

(4)基于大数据流式处理架构的事件理解解析;

(5)基于知识图谱、图计算、攻击链模型、机器学习算法的智能事件推理、关联分析;

(6)基于安全态势的分析与量化评估[8];

(7)基于任务标签和访问控制的安全隔离技术。

5.4 行业应用

网络靶场作为网络空间安全攻防演训、测试评估与人才培养的重要基础设施,可应用于教育、能源制造、运营商、金融等行业领域。

6 结论

加强与完善网络空间安全人才培养体系建设,对我国网络安全人才发展战略有重要的推动与指导意义。网络靶场,是培养实践型网络安全人才重要的技术支撑平台,加快建设网络靶场,对我国培养高质量的网络安全人才将有积极的促进作用。

参考文献

[1] 张文贵,彭博,潘卓.美国《国家网络安全综合计划(CNCI)》综述[J].信息网络安全,2010(9):69-72.

[2] 蔡军,于小红.美国网络安全人才培养机制[J].国防科技,2018,39(1):64-69.

[3] 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.

[4] 常利伟,李春雪,刘畅,等.网络空间安全人才培养体系现状分析与建设途径[J].信息安全研究,2018,4(12):1083-1088.

[5] 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.

[6] 李勇,田霞,吴春花.网络安全人才培养应"实战化"[J].信息安全研究,2018,4(12):1062-1065.

[7] 方滨兴,贾焰,李爱平,等.网络空间靶场技术研究[J].信息安全学报,2016,1(3):1-9.

[8] 周芳,周正虎.国外信息保障靶场建设[J].指挥信息系统与技术,2013,4(1):1-4,12.

(收稿日期:2020-07-06)

作者简介:

刘艳东(1985-),男,高级安全顾问,主要研究方向:网络靶场、边缘计算安全、工业互联网安全。

李晨(1983-),男,绿盟科技集团副总裁,主要研究方向:脆弱性检测技术、风险评估、应用安全、云安全。

版权声明