

网络空间安全学科人才培养之思考

李晖, 张宁

(西安电子科技大学 网络与信息安全学院, 陕西 西安 710071)

摘要: 网络空间安全已被正式批准列为一门一级学科, 该学科的人才培养与已有学科的联系与区别值得深入探讨。分析了该学科和信息与通信工程、计算机科学与技术等相关一级学科的关系, 给出了网络空间安全学科的知识体系, 将其分为网络空间安全基础理论、物理安全、网络安全、系统安全、数据和信息安全等5个大的学科领域。借鉴基于产出的教育模式, 提出了该学科硕士和博士研究生的培养标准, 并提出了涵盖5个方向的模块化参考课程体系。最后, 给出了对网络空间安全学科人才培养的一些建议。

关键词: 网络空间安全; 人才培养; 培养方案; 学科

中图分类号: G643.0

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2015.00003

Suggestions on cyber security talents cultivation

LI Hui, ZHANG Ning

(School of Cyber Engineering, Xidian University, Xi'an 710071, China)

Abstracts: Cyber security has been approved to be the first level discipline by Academic Degrees Committee of the State Council. It is important to figure out the curriculum of this new discipline and make it clear what is the difference between this new discipline and existed ones. The relationship between cyber security discipline and other disciplines such as information and communication engineering, computer sciences and technology, etc was analyzed. The cyber security was divided into 5 research areas, including fundamental theory, physical security, network security, system security, data and information security. Based on a given knowledge framework, the cultivation standard for master and Ph.D. students, as well as a reference curriculum of cyber security discipline was proposed. Finally, some suggestions were given for training talents of cyber security.

Key words: cyber security; talent cultivation; curriculum; discipline

1 引言

网络空间 (cyber space) 是人、计算机和各种物理设备通过泛在网络连接在一起所形成的虚拟空间, 网络空间中存储、流动的核心要素是信息。美国国家标准技术研究所 (NIST, National Institute of Standards Technology) 推出的《增强关键技术设施网络空间安全框架》给出的网络空间

安全的定义是: 通过预防、检测和响应攻击, 保护信息的过程。随着网络技术与计算技术的不断发展, 网络空间与物理空间呈现加速融合的趋势, 成为人们生活的第二空间。

网络空间安全对于国家安全和人民日常生活都是至关重要的。美国等发达国家特别重视网络安全人才的培养。美国国家安全局 (NSA, National Security Agency) 和国土安全部 (DHS, Department

收稿日期: 2015-09-07; 修回日期: 2015-09-27。通信作者: 李晖, lihui@xidian.edu.cn

基金项目: 中央网信办网络安全人才培养试点基地建设基金资助项目

Foundation Item: Project of Cyber Security Talent Cultivation Based on Office of Central Leading Group for Cyberspace Affairs

of Homeland Security) 针对网络空间安全设立了网络空间防御 (CAE-CD, national centers of academic excellence-cyber defense)^[1] 和网络空间操作 (CAE-CO, national centers of academic excellence-cyber operation) 的学术优秀计划^[2]。

CAE-CD 的目标是通过提升网络防御方面的高等教育和研究, 为国家培养具有网络防御专长的专业技术人才, 以降低国家信息基础设施的脆弱性。

CAE-CO 的宗旨是支持美国网络安全教育国家行动 (NICE, national initiative for cyber security education), 目的是建设数字国家并且扩大能够支撑网络安全国家的技术人才池, 是 CAE-CD 计划的补充, 是一个主要建立在计算机科学、通信工程和电子工程之上的跨学科深入的高等教育计划, 重点放在特定的网络操作上, 包括信息的收集、分析和响应, 这些对于美国的情报、军事和执法部门采取相关行动都至关重要。

这两个培养计划规定了从事网络空间防御和运行人才培养所需要具备的知识单元。美国的教育机构都可以申请开设相关专业, 政府机构对这些专业要进行认证以保证确实达到了这些知识单元的要求。同时, NSA 对申请开办网络安全这两个专业方向的学术机构设定了严格的学术与科研

要求, 以保障人才培养的质量, 专业认证的有效期为 2~4 年不等。我国博士和硕士研究生教育是按学科组织的^[3,4], 信息安全的研究生教育一直分设在不同的一级学科之下。2015 年 6 月 11 日, 国务院学位办正式批准网络空间安全成为一级学科, 这对我国网络空间安全人才的体系化培养起到极大的促进作用。如何建设好这个一级学科, 培养出高水平的网络安全人才成为摆在我们面前的一个重要课题。

2 网络空间安全学科与相关一级学科的关系

从网络空间安全的内涵分析, 它和信息与通信工程、计算机科学与技术、军队指挥学、电子科学与技术、软件工程、控制科学与工程、物理、数学、生物学、管理、法学等都有关联。在网络空间安全学科设立以前, 相关一级学科也都在培养相关安全的人才。但各自学科培养的安全人才基本是研究各自学科的问题, 而网络空间安全作为一个整体, 并不是将各自学科安全问题进行简单集合, 而是以跨学科凝练的安全基本理论体系和方法论体系, 来指导各个学科内的安全问题的研究。

网络空间安全学科的知识体系如图 1 所示,

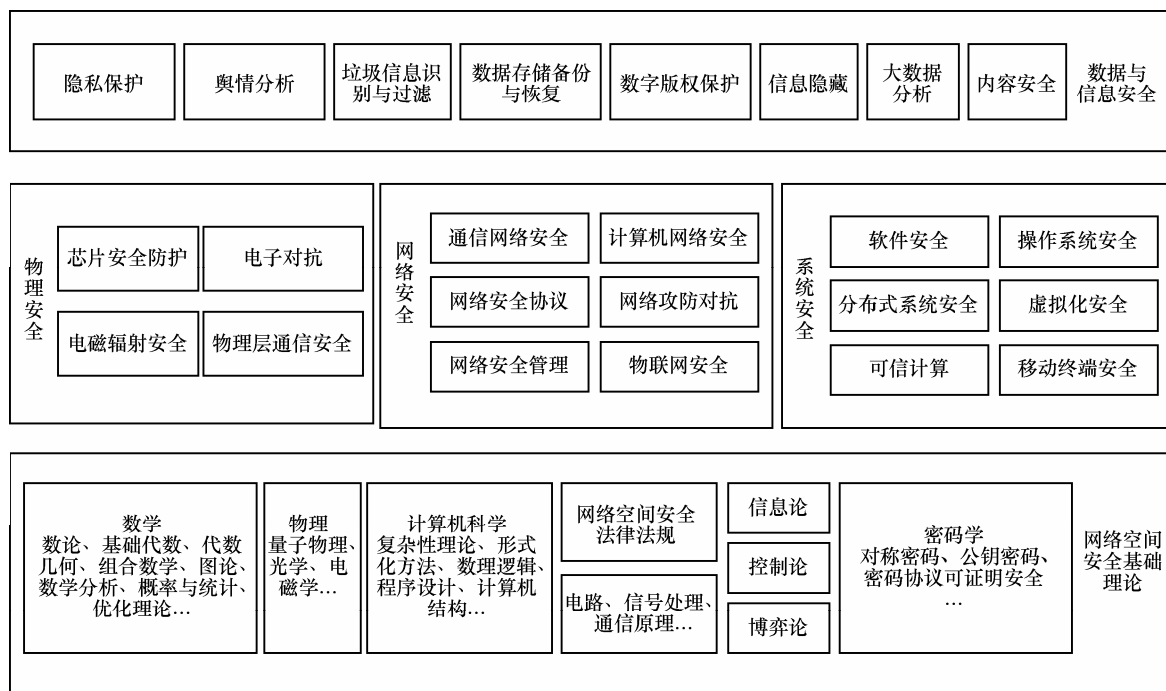


图 1 网络空间安全学科的知识体系

包括网络空间安全基础理论、物理安全、网络安全、系统安全、数据与信息安全。

其中,网络空间安全基础理论包括从事网络空间安全研究工作所需要的数学、物理、电子学、计算机科学与技术、信息论、控制论、博弈论、密码学理论、网络空间安全法律法规等基础理论;物理安全包括芯片安全防护、电子对抗、电磁辐射的安全、物理层通信安全等方面的理论与技术;网络安全包括各类无线通信网络、计算机网络、物联网等的安全协议、对抗攻防、网络安全管理、取证与追踪等方面的理论与技术;系统安全则包括软件安全、操作系统安全、分布式系统安全、虚拟化安全、可信计算、移动终端安全、工业控制系统安全等方面的理论与技术;数据与信息安全则包括隐私保护、数据存储与恢复、数字版权保护、舆情分析、垃圾信息识别与过滤等方面的理论与技术。

在现有学科体系下,网络空间安全人才培养具有一定的局限性。突出表现为知识体系不够完整和全面。计算机学科背景下人才强于网络和系统安全,但对密码学及其之上的信息安全原理了解不够;而密码学出身人才的系统安全知识都相对缺乏。网络空间安全需要的是具有综合安全能力和素质的人才,是具有从全面的视角来发现、分析和解决安全问题能力的人才。

网络空间安全学科有其独特的方法论,与数学或计算机科学等学科的方法论既有联系又有区别,包括观察、实验、猜想、归纳、类比和演绎推理,以及理论分析、设计实现、测试分析等,综合形成了逆向验证的方法论。网络安全保障体系是一个复杂巨系统,必须从复杂系统的观点,采用从定性到定量的综合集成的思想方法,追求整体效能。从系统工程方法论的观点出发,网络空间安全不能简单地采用还原论的观点处理,必须遵循“木桶原理”,注重整体安全。

3 网络空间安全学科的研究生培养

3.1 网络空间安全学科的培养目标

网络空间安全学科人才培养属于实践性极强的工程教育范畴。基于产出的教育模式(OBE, outcomes-based education)^[5]当前已成为美国、英

国、加拿大等国家教育改革的主流理念。美国工程教育认证协会(A-BET, Accreditation Board for Engineering and Technology)全面接受了OBE的理念,并将其贯穿于工程教育认证标准的始终^[6]。基于OBE来引导网络空间安全学科的人才培养也具有现实意义。

依据OBE的理念,网络空间安全学科人才培养首先应该确定学生在毕业时应达到的能力要求,也就是培养目标,并依据这一目标来组织教学过程,包括课程和实践环节。网络空间安全人才培养应达到如下目标:培养适应网络强国建设需要的,具有学术创新能力和国际视野的德、智、体全面发展的高层次创新型专门人才。热爱祖国,遵纪守法,具有良好的职业道德,具有高度的事业心和追求真理、献身科学的敬业精神,具有高尚的科学道德和创新精神,具有良好的体魄与素养,能积极为社会主义建设服务;掌握坚实的网络空间安全基础理论,在密码学、网络安全、系统安全、应用安全中的特长方向具有系统的专门知识,具有较高网络空间安全综合专业素质、较强的实践能力和创新能力,能够承担科研院所、企事业单位或行政管理部门网络空间安全方面的科学研究、技术开发或管理工作。

3.2 网络空间安全学科硕士研究生的知识能力标准

网络空间安全学科的硕士研究生可来自信息安全、信息对抗、电子信息类、计算机科学类以及数学类的本科毕业生,应当已经具有如下知识和能力:

- 1) 高等数学、线性代数、复变函数、概率与数理统计方面的知识;
- 2) 力、热、光、电磁、近代物理等普通物理方面的知识;
- 3) 高级程序语言的编程能力;
- 4) 电子线路的基础知识和设计、调试能力;
- 5) 计算机系统结构、计算机网络方面的基础知识;
- 6) 具备解决复杂工程问题的初步能力;
- 7) 具备持续自我学习的能力;
- 8) 获取文献的能力;

9) 可较熟练的应用外语进行交流的能力。

通过网络空间安全学科的研究生阶段学习，其应具有的知识能力如下：

1) 掌握信息论、博弈论、数学基础、安全法律法规等网络空间安全基础理论与知识；

2) 密码学基础知识和应用能力；

3) 一定的软件逆向工程能力；

4) 网络安全理论、技术与一定的攻防能力；

5) 密码学、网络安全、系统安全、应用安全的一个或多个方向上较好的设计开发或运维管理能力；

6) 具备良好的使用外语获取信息、写作和口语交流能力；

7) 良好的持续学习和追踪技术前沿的能力；

8) 良好的解决复杂网络空间安全工程问题的能力。

3.3 网络空间安全学科博士研究生的知识能力标准

博士研究生应当在网络空间安全硕士研究生的基础上进一步发展在某一学科方向上深入研究的能力。如果博士生的硕士专业不是网络空间安全，则应该补充学习相关知识。博士毕业生应达到的能力如下：

1) 掌握信息论、博弈论、数学基础、计算机科学相关理论等网络空间安全前沿基础理论；

2) 全面的密码学理论和应用能力；

3) 较好的软件逆向工程能力；

4) 密码学、网络安全、系统安全、应用安全的具体方向具有较强的创新研究能力；

5) 优秀的解决复杂网络空间安全工程问题的能力；

6) 具备熟练使用外语获取信息并开展学术交流的能力，具有广阔的网络空间安全国际化视野；

7) 优秀的持续学习和追踪技术前沿的能力；

8) 较好的提出问题并解决问题的能力。

3.4 模块化的培养方案

网络空间安全学科本身具有跨学科的属性，对于网络空间安全学科的研究生，其本科的专业背景可能是电子信息类专业、计算机类专业、数学类专业或信息安全类专业，其知识背景的不同给网络空间安全学科的培养方案制定和培养过程带来了比较大的挑战。

为应对这一挑战，兼顾网络空间安全覆盖面宽的客观现实，在培养方案的制订原则上，应采用模块化的结构。在对学生进行必要的网络空间安全专业基础教学的基础上，根据不同方向安排模块化的课程，方便学生根据兴趣特长更好地发展。

课程和教学环节的设计应使学生能够达到相应的培养标准。网络空间安全学科博士和硕士的参考课程体系如表1所示。

在课程体系之外，还应设置相关的教学环节使学生得到标准要求的能力训练。

表1

网络空间安全学科博士和硕士的参考课程体系

公共基础课		英语、政治课程、信息安全法律法规
专业基础课		信息论、控制论、博弈论、计算复杂性理论、数学（基础代数、数论、组合数学）、现代密码学、现代机器学习理论、形式化方法、软件逆向工程
专业方向	密码学	专业课 可证明安全理论、密码分析、现代编码理论
		任选课 现代公钥密码与应用、对称密码设计理论、量子密码理论
	物理安全	专业课 现代信号处理、网络信息论
		任选课 宽带无线通信与物理层安全、网络编码
	网络安全	专业课 复杂网络理论、网络安全理论与技术、安全协议理论
		任选课 无线网络安全技术、网络攻防概论、物联网安全
	系统安全	专业课 可信计算、操作系统安全、代码安全与漏洞分析
		任选课 数据库安全、Web 安全、移动终端安全、安全管理与风险评估、数字取证、虚拟化安全
	数据与信息安全	专业课 隐私保护技术、信息隐藏、数据挖掘与知识发现
		任选课 大数据分析技术、云计算数据安全、内容安全技术

1) 学术活动。要求听取学术报告、做学术报告,并参加国际学术会议至少1次。

2) 科研实践。参加纵向、横向科研项目,或者在企业工作岗位上工作1年以上并解决实际工程问题。

3) 学术论文。在网络空间安全相关领域学术会议和学术期刊上发表得到同行评议认可的学术论文。

4) 学位论文。学位论文是博士生培养的重要环节,论文选题应为本学科前沿,对国民经济、科学技术发展具有重要的理论意义和实用价值,鼓励博士生选择富于开拓性和创新性的课题。

4 多方协同培养网络空间安全人才

在制订科学的培养方案基础上,网络空间安全学科的人才培养还应根据学科特点和要求,采取特殊的措施。

1) 不拘一格,吸引网络安全生源

国家主管部门组织面向中学生、本科生、研究生的全国性网络安全竞赛,以选拔有特长的网络安全特殊人才,在本科入学阶段,可通过“少年班”等方式对有专长的中学生保送进入本科学习,或者制订特殊的自主招生政策,对拥有网络安全特长的中学生降分录取;在本科培养阶段,创办“实验班”,从各专业在校学生中选拔有志于网络安全的优秀学生进行培养,也可允许有网络安全特长的学生在规范的方式下转学进入网络安全人才培养能力强的学校;针对研究生选拔,可以根据学生在网络安全领域的特长,制订特殊的免试推荐标准,比如在各类网络安全竞赛获得高级别奖励的学生可以获得推免,在研究生考试时设置多种专业课吸引不同专业背景的学生等。

2) 政产学研协同,全链条创新网络空间安全人才培养

与党政机关、研究机构和产业等用人单位紧密协同,根据不同单位对网络安全人才的不同需求,联合制定培养方案,灵活本科、硕士和博士培养模式。对本科可以采用3+1模式(即3年校内加1年校外实习)或2+1模式(即每学年2学

期在校内加1学期在校外实习);对研究生可以采用1+X培养模式(即1年在校学完专业课程,最后在实际工作岗位上完成论文工作),学校与相关企业共建实践基地,联合完成对研究生的指导。在学校课程教学中,也应聘请业界的资深专家和工程师承担一定比例的教学任务,使人才培养更有针对性。

3) 建立学术与网络安全工程能力并重的教师评价体系

灵活用人机制吸纳人才,应打破高校传统的教师聘任方式,不唯学历和学位,聘用确有特长的人员作为高校的专职教师。

除专职教师外,从国内企业、研究机构和海外高校聘请高水平专家担任兼职教师和客座教授,向学生传授业界和学术界最前沿的技术,兼职教师比例应达到25%~30%。

教师晋升与评价不唯学术论文,对于解决网络安全国家重点工程问题、网络安全技术成果转化等都应给予积极合理的评价,为这些人才提供上升通道,从而引导教师的科研为国家急需服务。

4) 改变片面重视论文的学科评价体系

建立符合学科特点和国家需求的网络空间安全学科评价体系,引导学科建设面向国家重大需求和理论技术前沿。在学科评估中,对服务于国家的人才培养、服务于国家需求的研究项目与成果以及有影响的学术前沿成果加强权重。

5) 改革教学方式和评价方法

在教学过程中改革授课方式和考核机制。应积极采用翻转课堂、任务教学等方式,激发学生主动学习,发挥特长。改革课程考核的方式,淡化期末考试考核,增加课程过程中形成性评价考核方式,以考核为导向引导学生注重解决问题能力的培养。

5 结束语

网络空间安全学科的设立为网络安全人才培养提供了更为宽阔的平台,然而网络空间安全的研究培养标准、知识和课程体系、培养方法还亟待深入研究。推出的一些见解还非常粗浅,是否合理也有待商榷。希望能够抛砖引玉,通过充

分的讨论，形成符合我国特色、行之有效的网络安全人才培养体系，为网络强国建设提供人才保障。

参考文献：

- [1] National centers of academic excellence-cyber defense[EB/OL]. <http://www.nsa.gov/academia/ncae-cd/index.shtml>.
- [2] National centers of academic excellence-cyber operations[EB/OL]. http://www.nsa.gov/academia/nat_cae_cyber_ops/index.shtml.
- [3] 国务院学位委员会第六届学科评议组. 学位授予和人才培养一级学科简介[M]. 北京：高等教育出版社，2013.
The Sixth Discipline Appraisal Group of the State Council Degree Committee. Introduction to the degree granting and talent training of first-level disciple[M]. Beijing: High Education Press, 2013.
- [4] 国务院学位委员会第六届学科评议组. 博士、硕士学位基本要求[M]. 北京：高等教育出版社，2014.
The Sixth Discipline Appraisal Group of the State Council Degree Committee. Basic requirements in PhD, master's degree[M]. Beijing: High Education Press, 2014.
- [5] WILLIAM S. Outcome-based education: critical issues and answers [M]. Arlington: Va American Association of School Administrators, 1994.

- [6] 李志义. 解析工程教育专业认证的成果导向理念[J]. 中国高等教育, 2014(17): 7-10.
LI Z Y. Analytical engineering education professional certification results oriented concept[J]. High Education Press, 2014(17): 7-10.

作者简介：



李晖（1968-），男，河南灵宝人，博士，西安电子科技大学教授、博士生导师，主要研究方向为密码学、无线网络安全、云计算安全、信息论与编码理论。



张宁（1979-），女，陕西宝鸡人，博士，西安电子科技大学副教授，主要研究方向为公钥密码学、应用密码学、无线物理层安全、信息安全法。