

网络空间安全人才培养探讨

翁健¹, 马昌社², 古亮¹

(1. 暨南大学网络空间安全学院, 广东 广州 510632;
2. 华南师范大学计算机科学学院, 广东 广州 510631)

摘要: 自从2015年6月网络空间安全正式被批准为国家一级学科, 如何培养符合国家需要的网络空间安全人才成为了学科建设中一个亟待解决的问题。综合分析了国内外培养相关方面人才的现状与网络空间安全的实际人才需求; 结合我国网络空间安全人才培养的特点, 给出了我国网络空间安全人才培养的部分建议。

关键词: 网络空间安全; 人才培养; 学科建设

中图分类号: G643.0

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00031

Discussions on the talent cultivation of cyber security

WENG Jian¹, MA Chang-she², GU Liang¹

(1. School of Information Science and Technology, Jinan University, Guangzhou 510632, China;
2. School of Computer Science, South China Normal University, Guangzhou 510631, China)

Abstract: Cyber security has been formally approved to be the first level discipline in June 2015. How to train the cyber security talents that meet the needs of our country has become an urgent problem to be solved in the discipline construction. Synthetical analysis of the current situation of training related talents at domestic and foreign, as well as the actual demand for the cyber security talents was presented. According to the characteristics of the talent cultivation in cyber security, some suggestions on training the cyber security talents were given.

Key words: cyber security, talents training, discipline construction

1 引言

网络空间(cyber space)是人、机器、信息源之间相互连接而构成的一种虚拟的社会空间^[1], 它作为陆、海、空、太空以外的“第五空间”得到了世界各国的高度重视。网络空间中存储、流动的核心要素是信息。网络空间安全(cyber security)旨在确保网络空间中个人和组织的安全, 保护信息的有效性、完整性、机密性、可靠性和可

用性^[1,2]。

自2001年教育部正式批准开办信息安全专业以来, 我国已经有一百多所高校设置了信息安全类相关本科专业。自2003年起, 一批高校又自行设立了信息安全方面的博士点。目前, 我国已经形成一定的信息安全理论和技术基础。然而, 对于网络空间安全的学科建设和人才培养处于刚起步阶段, 尚有较长的道路需要探索, 还未形成系统、完整的科学研究与人才培养体系^[3]。与发

收稿日期: 2016-01-19; 修回日期: 2016-02-04。通信作者: 翁健, cryptjweng@gmail.com

基金项目: 国家自然科学基金面上基金资助项目(No.61272413, No.61472165); 教育部高等学校博士学科点专项科研基金博导类基金资助项目(No.20134401110011)

Foundation Items: The National Natural Science Foundation of China(No.61272413, No.61472165), The Research Fund for the Doctoral Program of Higher Education of China(No. 20134401110011)

达国家相比,我国的网络空间安全人才培养还存在较大的差距。主要体现在:1) 人才培养的课程体系和计划不完善,缺乏灵活的指导思想和建设思路,多数高校网络空间安全专业从属于计算机或通信专业,在人才培养计划和课程设置上没有独立的指导思想,大部分采用与计算机专业相同的教学体系;2) 网络空间安全尚未建立独立的科学体系,尚未形成完整的人才培养教育体系,目前,我国网络空间安全学科的建设都依托于计算机等学科,很多学校是2个牌子一套人马;3) 缺乏深厚的科研开发和人才培养方面的积累,专业人才数量不足、水平不高。这种情况势必将制约我国网络空间安全学科的发展和高级专门人才的培养。因此,应该加强与国外的交流与合作,进一步提高我国网络空间安全学科教师的理论水平与实际开发能力。

2014年2月27日,中央网络安全与信息化领导小组成立,习近平总书记亲自担任组长,习总书记强调指出“没有网络安全,就没有国家安全;没有信息化,就没有现代化”^[4]。2015年6月,国务院学位委员会、教育部通过了增设“网络空间安全”为一级学科的决定。这给网络空间安全科学的发展带来了机遇,网络空间安全正式开始了独立发展的道路。

2016年2月2日,国家互联网信息办公室网络安全协调局局长赵泽良在中国互联网发展基金会网络安全专项基金捐赠仪式上指出,目前我国网络空间安全相关专业每年本科、硕士、博士毕业生之和仅8 000余人,而我国网民数量近7亿人,网络空间安全方面人才缺口仍然非常大^[5]。我国人口众多,网络发展迅速,已经成为世界网络大国,但仍非网络强国。如何按照国家战略和社会需求培养高素质的网络空间安全人才是我国网络空间安全发展及教育领域的一个重要问题。

2 网络空间安全人才需求

2.1 全球网络空间安全人才需求

美国硅谷和美国国防部对网络空间安全人才的需求最具代表性,近年来,人才需求急剧增加。在全球化的互联网科技推动下,硅谷大量高科技企业的发展日益依赖于网络空间安全人才的保

障。无论是 Tesla 的电动汽车,还是谷歌的全球服务网络,它们对网络空间安全人才的需求都达到了前所未有的高度。为了解决日益严峻的网络安全威胁,这些高科技企业纷纷招募大量优秀的安全人员,组成专业的安全团队,应对各种可能的安全风险。随着美国正式成立网络司令部,大量招募社会上的专业人士,传统部队中的人才已经不能满足军队的需求,这也标志着网络空间安全人才需求的急剧增加。

网络安全公司 Cybersecurity Ventures 发布的2015年《全球网络安全市场报告》报告显示^[6],到2019年全球网络安全的市场规模将超过1 550亿美元;到2018年,美国对信息安全专家的需求将增长53%;到2014年为止,信息安全领域的并购资金首次突破28亿美元大关,而交易还在稳步增长,达到269件交易量;网络安全创业公司加州森尼韦尔(Illumio)提供云及数据中心安全平台,在C轮融资中获得1亿美元投资。美国国土安全局2015年的预算为328亿美元,美国国家情报计划2015年的预算为456亿美元。到2020年,亚太地区在关键基础设施上的安全支出将达到220亿美元。

由此可见,全球信息安全领域投资与并购非常活跃,欧美发达国家在网络空间安全领域的投资与并购加大了全球网络空间安全对高层次人才的需求与竞争。

2.2 我国网络空间安全人才需求

人才是发展我国网络空间安全的关键。一方面,任何网络空间安全产业和技术成果都是人创造的;另一方面,任何危害网络空间安全的事件同样也是人制造出来的。因此,培养大量优秀的网络空间安全人才成为当前我国网络空间安全领域的头等大事。军队、公安、政府、外交等国家重要部门需要大量网络空间安全的专业专门人才;网络空间安全技术和产业的发展也需要大量网络空间安全的专门人才;电子商务、电子政务等应用系统的发展也需要大量网络空间安全的人才。我国专注于网络空间安全领域研究与开发的公司,如蓝盾信息、启明星辰、天融信科技、绿盟信息、知道创宇、深信服等,在2015年均加大了研发投入,需要大量的网络空间安全人才。

中国信息安全测评中心与互联网实验室合作

通过调查问卷、文献研究和专家访谈等方式对我国信息安全从业人员队伍状况进行了调查^[7]，调查的单位包括国有企业、私营企业、国家机关、科研院所、外资企业、合资企业等单位，从业人员包括信息安全工程师、单位中层，信息安全部门经理、项目经理、信息安全助理。收回的1000多份调查显示，信息安全从业人员以本科学历的青年人为主，本科学历占60.9%，研究生学历占24.1%；超过70%的受访者认为组织内信息安全专业人才不足；运维、技术开发与防御类人才尤为紧缺，占比超过50%；各单位和行业对信息安全专业人才的缺口点也各有侧重。

目前，各类单位在信息化建设的进程中基本完成了业务系统的建设。随着搜集及存储的信息越来越多，由信息化建设带来的业务流程的改变使信息安全问题愈发严重，这也使各类单位在信息化建设的进程中越来越重视解决信息安全问题，投入经费越来越多。

我国的IT巨头，如阿里巴巴、腾讯、百度，华为等企业，为了应付日益严峻的网络空间安全的调整，均成立了超过200人的信息安全团队，并且与高校和科研院所建立了稳定的长期的研究机制。中科院信息工程研究所是中科院下属专注于网络空间安全研究的研究机构，成立以来不断加大网络空间安全领域的研究，这显示了我国对网络空间安全的人才有着极大的需求。

3 网络空间安全人才培养现状

3.1 培养目标

作为网络空间安全工作的一般从业人员，应当了解网络空间安全的基础理论和系统的专门知识，了解网络空间安全发展的现状和前沿，能够熟练运用网络空间安全学科的方法、技术与工具，可以从事网络空间安全领域的基础研究、应用研究、关键技术及系统的分析、设计、开发与管理工作的。

作为网络空间安全领域的高层次人才，需要掌握坚实宽广的网络空间安全领域的基础理论和系统深入的专业知识，在熟练运用网络空间安全学科的理论、方法和技术进行研究和实践工作的基础上，善于发现网络空间安全领域中的前沿性问题，

能够深入安全领域中大型复杂系统的设计、开发与管理工作，并在某一领域做出创新性的成果。

3.2 人才培养与就业现状

早期，我国网络空间安全学科没有成为一级学科，网络空间安全挂靠在计算机学科或者通信学科下，没有形成相对完善的培养体系。网络空间安全的从业人员主要由计算机学科及通信学科等相关IT类专业培养，另外由少部分社会机构培养。

据不完全统计，在本科阶段，我国开设计算机专业的高校已经超过1100所，开设网络工程专业的接近200所。截至2014年，教育部批准全国共116所高校设置信息安全类相关本科专业，其中，信息安全专业87个，信息对抗专业17个，保密管理专业12个。25个省（市）的108所高职院校设置了信息安全专业。经过统计，从软件专业代码上统计出来的大约10万人，计算机相关专业毕业生类一年超过100万人。但信息安全专业每年培养的本科生和研究生人数不到1万人，大专毕业生人数约2万人，在校生约0.7万人。

中国信息安全测评中心与互联网实验室的信息安全从业人员培养情况的调查显示^[7]，超过70%的信息安全从业人员在工作期间职位为社会培训和外聘专家培训。超过40%的受访者倾向于社会培训，受访者普遍期望通过培训来获得“网络攻防”专业技能的提升。

这说明网络空间安全的人才培养需要建立立体式的培养，不能仅仅依靠高校培养。

3.3 问题分析

根据中国信息安全测评中心与互联网实验室的调查结果^[7]，结合我国社会对网络空间安全人才的需求，目前人才培养主要存在如下问题。

1) 网络空间安全高端人才稀缺

高端人才是学科发展的重要催化剂。由于信息安全专业的特殊性，全球范围内的信息安全高端人才来华工作的不多，主要靠国内自主培养及引入少量的国际知名华人专家。网络空间安全领域的院士、长江学者、千人计划等高层次人才屈指可数。如何加快网络空间安全高端人才建设不仅关系着学科发展，更关系着国家安全和国际竞争力。

2) 网络空间安全人才培养师资严重不足

大学网上公布了中国“985工程”大学新生

师资力量排行榜^[8], 北京大学的生师比为 1.27, 排名第一, 这意味着 1 个以上教师对应 1 个本科生, 第二名以后高校的生师比均没有达到 1。而网络空间安全方面的老师更是严重缺乏, 由于之前缺乏一级学科, 网络空间安全方向的博士生培养都挂靠在其他学科下面, 导致了博士生的培养数目严重不足。

3) 人才培养方案与社会需求脱节严重

早期的信息安全人才培养集中在硕士、博士阶段, 自 2001 年武汉大学开设本科专业以来, 已经有 80 多所高校开设了本科专业。但是信息安全涉及到多个学科, 存在系统性的挑战, 而且由于 IT 技术的飞速发展, 网络空间安全教师相对较少, 导致了本科人才培养方案及讲授内容更新相对较慢, 导致了人才培养跟不上时代的步伐。

4) 网络空间安全培养的基础设施及平台相对缺乏

网络空间安全属于典型的工科学科, 人才培养除了需要理论支持外, 还需要大量的最新仿真实践环境。据不完全统计, 我国建设的与信息安全有关的国家级实验室有 5 个, 国家级工程中心有 3 个。从学科及人才培养的角度来看, 布局是相对完善的, 但是这些机构在人才培养的过程中, 缺乏真实的实践场景, 这也是我国信息安全人才培养与社会需求脱节的主要因素之一。

4 网络空间安全人才培养建议

国外发达国家在网络空间安全人才培养上制定了相对完善的制度。如美国国家安全局在 2005 年委托包括卡内基梅隆大学、普渡大学等大学在内的 50 多所教育机构成立了网络安全保障教育和学术中心。美国政府 2012 年发布了国家网络空间安全教育战略计划 (简称 NICE 计划), 该计划建立了从小学到高等院校学生培养、从业人员培训及普通民众教育的人才培养体系, 对全体网民进行网络安全意识培训, 对专业人员进行系统的知识技能教育^[9]。

网络空间安全是一个通过预防、检测和响应攻击来保护信息的过程^[10,11]。在网络空间安全学科建设、人才培养体系、人才评价体系以及人才继续教育等方面有如下建议。

4.1 健全不拘一格体现自身特色的学科建设机制

网络空间安全虽然与数学、计算机、通信等学科有一定的联系, 但它有不同于其他学科的自身特色, 有着符合自身发展的特色道路, 网络空间安全一级学科的建设不应受到其他学科发展的限制, 走一条符合自身特色的道路。不拘一格, 打破传统思维, 依据网络空间安全自身基础来建设学科。实际上, 网络空间学科的发展反过来会促进数学、计算机、通信等相关学科的发展。国际上已经有大约 60 多所大学开始了网络空间安全的硕士学位课程, 包括牛津大学、南加州大学、新泽西理工大学等。作为国内推动网络空间安全建设的参与者, 西安电子科技大学、北京邮电大学、电子科技大学、暨南大学等都迅速地成立了以网络空间安全学科为主体的学院和专业, 从组织架构上保障了学科发展的资源。详细建议如下。

1) 进一步做好一级学科博士点布局

2015 年 10 月, 教育部启动了首批网络空间安全一级学科博士点申报工作, 近 30 所高校及研究机构获批了网络空间安全一级博士点, 这是国家对网络空间安全学科建设的布局, 对网络空间安全的发展起到了积极的作用。在首批申报通知中, 要求申报单位应同时具有计算机科学与技术一级学科、信息与通信工程一级学科、数学一级学科 (或密码学二级学科) 的博士学位授权。网络空间安全虽然与数学、计算机、通信工程等学科有一定的联系, 但是它具有不同于其他学科的自身特色。目前部分高校虽然不具备这 3 个学科的一级博士点, 但是在网络空间安全方面有鲜明的特色, 具有较强的实力。建议国家在下一轮网络空间安全一级学科博士点申报工作中, 鼓励和允许在网络空间安全有特色的院校及科研机构申报, 进一步完善一级学科博士点布局。

2) 布局网络空间安全有关的国家级重点实验室

国家级重点实验室在学科的基础研究及学科建设中具有重要的作用, 主要体现在学科前沿性问题的研究以及重大工程项目的建设上。在 IT 领域, 我国已经建设了数量不少的国家重点实验室, 基于国家战略领域及民生领域的网络空间安全实际需求, 建议进一步增设网络空间安全领域的国

家级重点实验室。

3) 建立国家级网络靶场

在网络空间安全的人才培养过程中, 工程实际至关重要, 如何高质量地仿真实际的网络安全环境是网络空间安全人才培养的主要障碍之一。为解决这个问题, 建议站在国家的层面上, 与国内 IT 巨头联合建立国家级的网络靶场 (cyber range), 并且保持及时更新。

4) 鼓励高校与科研机构联合企业合作进行基础研究

由于网络空间安全的问题实际是一个系统性工程, 与实际需求联系非常紧密, 高校及研究机构具有良好的理论基础, 企业具有良好的工程基础, 二者结合可以很好地解决基础研究中的一些关键问题。譬如 5G 安全问题就需要大企业及高校联合攻关。

5) 鼓励国内高校、科研机构与国外知名高校联合培养博士生

对于网络空间安全高端人才的培养, 无论是导师还是学生都面临生源问题, 相关部门及主管机构鼓励高校或科研机构联合国外知名高校联合培养博士生。

6) 如何处理好新建学科和原有学科之间的关系, 是发展网络空间安全学科建设必须重视的另一个重要问题

一方面, 原有的计算机科学、软件工程、网络工程、数学等学科都已经具有很好的基础, 可以作为丰富和发展网络空间安全学科的出发点。另一方面, 通过充分发展网络空间安全的学科体系, 发现和发掘其独特的科学问题, 在推动其自身体系发展的同时, 可以促进与其他学科, 如电子商务、信息管理与信息系统等的融合。

因此, 网络空间安全学科的发展应该既以原有相关学科为基础, 又必须走一条符合自身特色的道路, 逐步完善网络空间安全学科建设。

4.2 健全与时俱进的立体人才培养体系

建立网络空间安全知识更新机制, 使学生了解最新的网络空间安全状态, 激发学生学习最新的网络空间安全技术。依据网络空间安全的实时需求, 建立基础研究、系统研发与运维、社会大众的立体人才培养体系。通过网络空间安全学科

的培养, 使学生掌握密码和网络空间安全基础理论和技术方法, 掌握信息系统安全、网络基础设施安全、信息内容安全和信息对抗等相关专门知识, 并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、企事业单位和行政管理部门网络空间安全方面的科学研究、技术开发及管理工作。

首先, 人才培养目标不但要涵盖网络空间安全基础知识和技能, 更要体现网络空间安全的“新”意, 与其他学科不同, 网络空间安全具有实时性, 这种实时性体现在网络攻击的日新月异, 导致了网络安全知识需要实时更新。因此, 各网络安全人才培养单位要有正确的渠道让学生了解到网络空间安全的最新动态, 建立网络空间安全知识更新机制, 教会网络空间安全人才做好不断学习新知识的思想准备。

其次, 基础研究方面, 考虑到基础研究是学科创新的根本源泉, 能极大地带动学科建设与人才培养, 尤其是对高端人才的培养具有不可替代的作用, 针对网络空间安全基础研究培养体系, 建议国家有关部委设立网络空间安全的重大专项。美国自然科学基金资助项目从 2011 年开始就大力度地支持了一系列有关可信网络空间 (trustworthy cyberspace) 的项目。通过这几年的积累, 在一系列高校和科研机构中汇聚和培养了一大批网络空间安全的优秀人才, 并推动了一系列关键问题的研究, 例如如何在不可信的计算环境中保护应用和用户数据的安全^[12]。美国国防部高级计划研究署 (DARPA) 从 2003 年到 2008 年大力支持 CALO 项目^[13], 最初的目的是推动人工智能技术的发展, 以期能够为美国军方提供智能的系统, 然而现在 CALO 最为著名的成果是大家在苹果手机上所广泛使用的 Siri 语音识别系统。此外, 基于 CALO 项目这 5 年的强力支持, 美国教育和科研机构培养了一大批人工智能领域的高层次人才, 为近年来在全球范围内迅速发展的大数据相关方向奠定了基础。因此, 国家有关部委针对网络空间安全的基础研究, 设置一些重大专项, 可以有效地培养网络空间安全领域的高端人才。

再次, 针对网络空间安全高端人才缺乏的问

题,建议国家有关部门在网络空间安全领域设立一项人才计划。国家发布了千人计划等一系列的人才计划,但在网络空间安全领域引入的高端人才相对较少,建议国家有关部委针对网络空间安全的实际需求,面向海内外选拔一批网络空间安全的学科带头人。

最后,完善网络空间系统开发与运维人才的培养体系。IT技术经过几十年的发展,已经开发了大量的信息系统,由于早期没有过多地关注安全问题,这些系统或多或少存在安全漏洞,同时由于物联网技术及移动互联网技术的高速发展,网络空间中还将建设大量的信息系统,这需要大量的人才,如何培养这部分的人才,需要建设完善的网络空间系统开发与运维培养体系。具体建议如下。

1) 以创新思维建设网络空间安全的本科人才培养。网络空间安全作为一级学科,应该从安全的角度重新调整培养计划,理论内容应该包括数学、通信、编程等方面的内容,实践内容应该包括硬件安全、操作系统、网络安全、数据库安全、云安全等方面的内容,这些内容不能简单地升级为现有计算机学科或者通信学科的内容,而是需要重新定义这部分的内容。

2) 强化计算机学科或者通信学科的网络空间安全知识体系。经过计算机学科或者通信学科培养的本科、硕士人才有相当部分会从事信息系统的开发,如何开发高质量的安全的代码是目前计算机学科或者通信学科的人才培养体系中欠缺的。譬如可以开设《安全编程》等类似的课程,主要讲述在开发过程中如何保证存储安全、通信安全等内容。

3) 设立各种类型的网络空间安全人才培养项目。建议开设网络空间安全专业的高校引入业界领先的安全攻防平台,这样可以极大地促进工程类型人才的培养。建议开设网络空间安全专业的高校与国家知名高校合作,开设网络空间安全暑期学校(summer school),向学生介绍网络空间安全最前沿的理论及产品。建议通过校企结合解决高校和企业人才能力培养与需求不对等问题,高校及时与企业合作,收集企业在安全领域的实际需求,结合安全领域的理论与产品,及时

更新培养计划与内容。建议加强法制建设,培养学生法律意识,培养德才兼备的网络空间安全人才。

4.3 健全科学合理的人才评价体系

针对高端人才的评价问题,建议有关部门学会建立符合网络空间安全自身特色的高端人才的评价体系。首先,网络空间安全人才评价不能唯SCI论,更不能唯影响因子论。实际上,网络空间安全领域更注重在顶级国际会议上发表成果,统一地用SCI论文来评价网络空间安全人才是不公平的。建议采用同行评议的方式来评价网络空间安全人才质量。

其次,网络空间安全人才评价不能唯CCF A类期刊论,目前,由于此前网络空间安全学科附属计算机学科或者通信学科,导致现有的对网络空间安全高端人才的评价直接引用计算机学科或者通信学科,这是有缺陷的。譬如,有些高端人才并没有在CCF A类期刊上发表太多的成果,但在Crypto、Eurocrypt、IEEE S&P等顶级会议上发表了开创性的成果,如果沿用计算机学科或者通信学科的评价体系是不合适的。在密码学领域,中国密码学会制定了推荐学术刊物和国际会议目录,供国内高校和科研单位作为学术评价的参考依据,这一做法值得推广。

最后,网络空间安全人才不能唯论文和项目论,社会上许多优秀的信息安全人才具有很强的工程实践技能,他们是黑客或者红客中的佼佼者,他们是工作在第一线的网络安全工作者,他们也是网络空间安全的掌控者和安全事件的制造者。给这部分人才合理的评价有助于社会的公允,有助于鼓励更多优秀的人才进入网络空间安全领域。

因此,在计算机学科或者通信学科评价体系的基础上需逐步改进和完善网络空间安全学科评价体系。由于现实条件的制约,现有科研评价体系主要侧重如何量化和可操作性,这相对于原来的没有标准已经是很大的进步。但是,如何让科研评价体系回归促进科学发展的原本目的,还需要进一步的探索和改进。建立科学合理的网络空间安全人才评价机制,是网络空间安全学科发展的前提,也是人才建设的必备环节。

4.4 健全网络空间安全继续教育体系

由于信息技术的飞速发展, 网络空间安全面临的问题变化多端, 网络空间安全从业人员的知识需要及时更新。对于这部分已经离开高校的网络空间安全从业人员如何进行继续教育也是网络空间安全人才培养体系必须解决的问题。

建议国家有关部委通过市场化运作方式, 联合有特色的高校及企业建立网络空间安全再学习平台。譬如尝试建设网络空间安全 Mooc 平台, 部分高校引入的攻防平台可以对外开放, 建设完成的国家级网络靶场可以尝试对外开放。

5 结束语

网络空间安全一级学科点的设立体现了这一科学领域的重要性和国家对相关人才的迫切需求。然而, 作为一门新兴学科, 其在如何培养符合国家、市场需求的专业人才上仍有很多需要摸索、探讨的地方。本文从人才的需求培养以及学科的建设方面给出了一些个人见解。真正符合网络空间安全专业要求的技术人才仍然十分短缺, 为此, 既需要结合已有学科基础, 了解国家和社会需求, 建设好教师队伍和研究方向; 也需要建设合理的培养体系, 通过产学研、教学形式改革等多种手段培养高水平的各层次人才。本文见解还比较粗陋, 需要在实践中验证。希望能抛砖引玉, 吸引更多的讨论, 促进网络空间安全学科的发展, 为国家网络空间安全的科研和产业提供优秀人才。

参考文献:

- [1] Information technology-security techniques-guidelines for cybersecurity[EB/OL].http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44375.
- [2] Overview of cybersecurity[EB/OL]. <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136>.
- [3] 积极构建网络空间安全创新人才培养体系[EB/OL]. http://news.xinhuanet.com/politics/2015-06/04/c_127879542.htm.
Building talent cultivation system for cyber space security[EB/OL]. http://news.xinhuanet.com/politics/2015-06/04/c_127879542.htm.
- [4] 习近平: 把我国从网络大国建设成为网络安全强国[EB/OL]. http://news.xinhuanet.com/2014-02/27/c_119538788.htm.
XI Jin-ping: transform network in China from big to strong[EB/OL]. http://news.xinhuanet.com/2014-02/27/c_119538788.htm.
- [5] 3 亿元支持网络安全人才培养, 中国首个网络安全专项基金成立[EB/OL]. <http://news.sina.com.cn/o/2016-02-02/doc-ifxnzpkx>

5831276.shtml.

300 million funding for cultivating network security talents, the foundation of the first network funding in China[EB/OL]. <http://news.sina.com.cn/o/2016-02-02/doc-ifxnzpkx5831276.shtml>.

- [6] 2015 网络安全市场报告[EB/OL]. <http://www.freebuf.com/news/special/66278.html>.
2015 network security market report[EB/OL]. <http://www.freebuf.com/news/special/66278.html>.
- [7] 张晓菲, 李斌, 王星. 2014-2015 年度我国信息安全从业人员现状调查[J]. 中国信息安全, 2015(11):67-72.
ZHANG X F, LI B, WANG X. 2014-2015 survey on personnel of information security in China[J]. China Information Security, 2015(11):67-72.
- [8] 2012 年中国大学师资力量排行榜[EB/OL]. <http://news.china-10.com/307813.html>.
2012 Chinese university ranking on teachers and students[EB/OL]. <http://news.china-10.com/307813.html>.
- [9] 网络空间安全人才须系统培养[EB/OL]. http://news.xinhuanet.com/politics/2014-11/27/c_127258023.htm.
Talent cultivation system for Cyber space security[EB/OL]. http://news.xinhuanet.com/politics/2014-11/27/c_127258023.htm.
- [10] 李晖, 张宁. 网络空间安全学科人才培养之思考[J]. 网络与信息安全学报, 2015, 1(1):18-23.
LI H, ZHANG N, Suggestions on cyber security talents cultivation[J]. Chinese Journal of Network and Information Security, 2015, 1(1): 18-23.
- [11] 马建峰, 李凤华. 信息安全学科建设与人才培养: 现状、问题与对策[J]. 计算机教育, 2015(1): 11-14.
MA J F, LI F H. Construction of information security discipline and talent cultivation: state of art, problems and strategies[J]. Computer Education, 2015(1): 11-14.
- [12] BONEH D, GUPTA D, MIRONOV I, et al. Hosting services on an untrusted cloud[C]//The 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, 2015: 404-436.
- [13] CALO[EB/OL]. <https://en.wikipedia.org/wiki/CALO>.

作者简介:



翁健(1976-), 男, 广东茂名, 暨南大学教授、博士生导师, 主要研究方向为密码学与信息安全。

马昌社(1972-), 男, 湖南武冈人, 博士, 华南师范大学教授, 主要研究方向为物联网体系架构和安全技术。

古亮(1982-), 男, 四川隆昌人, 博士, 暨南大学研究员, 主要研究方向为系统软件、系统安全。