2022

网络安全人才实战能力白皮书

攻防实战能力篇

2022

网络安全人才实战能力白皮书

攻防实战能力篇

编写组织

指 导 单 位：

教育部高等学校网络空间安全专业教学指导委员会

主 编 单 位：

北京航空航天大学

中国科学技术大学

北京永信至诚科技股份有限公司

副主编单位：

西安电子科技大学

东南大学

武汉大学

华中科技大学

上海交通大学

参 编 单 位：

北京电子科技学院

山东大学

四川大学

北京邮电大学

编委会主任： 封化民

编委会副主任： 俞能海

主　　编： 刘建伟

副 主 编： 李　晖　　程　光　　赵　波
邹德清　　刘功申　　蔡晶晶

编　　委：（排名不分先后）

陈鹤影　　陈　凯　　陈晓琳
付　磊　　纪敏智　　刘　飚
李　伟　　孟　魁　　麻治昊
彭海朋　　孙政豪　　童　蒙
魏晶晶　　万　佳　　吴文涛
王小平　　谢　丹　　杨　望
杨　旭　　周　潮　　张　丽
张　倩　　张　意

前言

网络空间的竞争，归根结底是人才的竞争。网络安全人才，赋能千行百业，是数字经济安全发展的基石。网络与信息安全发展，人才队伍建设是关键。

在网络强国战略深入推进的同时，网络安全人才缺口巨大成为了网络安全产业面临的主要问题之一，尤其是实战人才更是严重缺失。数据显示，到2027年，我国网络安全人员缺口将达327万，而高校人才培养规模仅为3万/年。在我国，真正具有实战能力，了解攻击手段和攻击路径的网络安全人才严重缺乏。一方面，仅有8%的企业信息部门、安全部门负责人认为自身团队“各方面攻防实战能力均不欠缺”；另一方面，我国高校人才培养最为现实的问题就是“实习实践”。网络安全人才实战能力建设已经成为亟需解决的时代新命题。

《网络安全人才实战能力白皮书》（以下简称“白皮书”）是业内首份聚焦网络安全人才实战能力的白皮书，基于420场、抽取85761条网络安全竞赛信息，889份调研问卷，结合实战人才供给侧及用人单位需求侧情况，全面呈现我国实战型人才的供需现状、培养现状、评价方式及发展建议。《白皮书》面向党政机关、央企机构、企事业单位及高校等单位，希望能够通过努力为各单位人才战略制定提供详实参考。

《白皮书》主要有以下特色：

（1）基本概念清晰，方法论明确。首次定义了网络安全人才实战能力、网络安全人才攻防实战能力，提出了网络安全人才实战能力“4+3模型”、网络安全人才培养“ASK-P模型”，为网络安全人才实战能力的分类与评价树立了标准。

（2）内容全面，深入浅出。全面对比了国内外网络安全人才发展环境、网络安全人才实战能力供需，全国各地域各行业网络安全人才实战能力，形成大量结论。作者尽量避免使用晦涩难懂的语言描述深奥的理论和技术知识，而是借助大量图表进行表述。

（3）专家力作，内容先进。作者坚守高校的教学和网络安全一线工作多年，在长期的工作中积累了深厚造诣，多位作者还荣获过网络安全优秀教师奖、网络安全优秀人才奖，以及国家技术发明一等奖、北京市科学技术奖一等奖等。他们将深厚的教学理念与实践经验融入了《白皮书》。

《白皮书》由教育部高等学校网络空间安全专业教学指导委员会指导，北京航空航天大学、中国科学技术大学及永信至诚担任主编单位，西安电子科技大学、东南大学、武汉大学、华中科技大学、上海交通大学担任副主编单位，北京电子科技学院、山东大学、四川大学、北京邮电大学参编。

本《白皮书》聚焦攻防实战能力，为《网络安全人才实战能力白皮书》系列之一，未来将陆续对漏洞挖掘能力、工程开发能力、战效评估能力三部分进行发布。由于作者水平有限，加之时间仓促，难免存在疏漏及不妥之处，敬请批评斧正。

目录

CONTENTS

第一章 | 网络安全产业人才状况分析 01

1.1 宏观政策环境 01

1.1.1 国际情况 02

1.1.2 国内情况 03

1.2 人才发展环境 04

1.2.1 院校培养环境 04

1.2.2 单位使用环境 05

1.3 网络安全人才实战能力类别 06

1.3.1 网络安全人才实战能力定义 06

1.3.2 网络安全人才实战能力模型 08

第二章 | 网络安全人才攻防实战能力分析 09

2.1 网络安全攻防实战人才现状 09

2.1.1性别、年龄及学历情况 09

2.1.2地域及行业情况 11

2.2 网络安全攻防实战能力现状 **14**

2.2.1网络安全攻防实战能力技术 14

2.2.2网络安全攻防实战能力情况 14

2.3 网络安全攻防实战经验分析 **17**

2.3.1网络安全竞赛人员参与情况 17

2.3.2 网络安全竞赛经验成果 18

第三章 | 用人单位网络安全人才实战能力需求分析 24

3.1 用人单位的特点及人才需求分析 25

3.1.1 按地域维度分析 25

3.1.2 按行业维度分析 27

3.1.3 按企业性质/规模维度分析 30

3.2 岗位需求 32

3.2.1 岗位基本要求 32

3.2.2 岗位基本需求 34

3.3 岗位与能力匹配分析 36

3.3.1 岗位人才分布 36

3.3.2 岗位能力需求 37

3.3.3 能力提升需求 40

3.4 人员来源分析 44

第四章 | 网络安全人才攻防实战能力提升分析 46

4.1 网络空间安全实战攻防人才培养现状 46

4.1.1 院校网络安全相关专业建设现状 46

4.1.2 社会培训机构发展现状 49

4.1.3 企业内部从业人员培训现状 53

目录

CONTENTS

4.2 人才培养方式分析 55

4.2.1院校培养方式分析 55

4.2.2 社会培训机构培养方式分析 58

4.2.3 企业内部培养方式分析 61

4.3 人才培养效果分析 63

4.3.1 院校培养效果分析 63

4.3.2 培训机构培养效果分析 64

4.3.3 企业培养效果分析 66

第五章 | 网络安全人才攻防实战能力评价分析 67

5.1 网络安全人才攻防实战能力评价现状 67

5.1.1主流评价方式 68

5.1.2 有效评价方式 68

5.1.3 存在问题 68

5.2 网络安全人才攻防实战能力评价分级 69

5.2.1能力分级说明 69

5.2.2 能力评价内容 69

5.2.3 评价标准 71

5.3 网络安全人才攻防实战能力提升与评价方式 73

5.3.1 安全竞赛 73

5.3.2 安全会议 74
5.3.3 培训认证 74
5.3.4 安全众测 75
5.3.5 攻防演练 76
5.4 网络安全人才攻防实战能力提升路径 77
5.4.1 统一的网络安全攻防实战能力框架 77
5.4.2 网络安全攻防实战能力课程/培训认可 79
5.4.3 常态化攻防人才成长通道 80

第六章 | 总结和建议 83

6.1 院校人才培养体系建设建议 83
6.1.1 理论教学体系建设 83
6.1.2 实践教学体系建设 83
6.2 企业单位人才培养建设建议 84
6.3 政府扶持政策建议 85

第一章

网络安全产业人才状况分析

随着新的计算技术、网络技术、通信技术的快速演进，网络空间成为继陆、海、空、天之后的第五大主权争夺空间。网络安全关系到国家安全、社会稳定、经济发展、人民生活等各个方面，为了国家安定与繁荣发展，必须确保我国的网络空间安全，要建设国家网络空间安全保障体系，保护政府、部队、企业等重要部门，以及金融、能源等重要基础设施的网络安全。习近平总书记明确指出，人才是第一资源；网络空间的竞争，归根结底是人才竞争。网络空间安全的核心竞争力在于专业人才，只有培养足够优秀的网络专业技术人才，才能保证国家在未来的网络空间战争中获得优势。因此，世界各国纷纷将网络空间人才培养工作提升到国家战略层次，投入巨量财力物力，建设完备的网络空间安全人才培养体系。

1.1 宏观政策环境

目前，美国是网络空间最强国，网络空间安全人才培养数量和质量优于其他国家，其完备的人才培养体系值得我国借鉴，同时英、法、德、日、韩、俄、以等网络空间强国依托自身国家实际情况培育网络空间安全人才。

在战略层面上，美国先后发布了《网络空间人才计划》(2002)、《美国网络空间安全教育计划》(2010)、《美国网络安全教育计划战略规划：构建数字美国》(2011)、《联邦网络安全人才战略》(2016)、《网络安全人才行政令》(2019)等多个网络安全战略，详尽地规定了从高等院校教育、尖端科技企业培训到社会人才发掘、高中生尖子选拔，再到网络空间安全人才“掐尖”(即以丰厚的条件吸引全球网络空间安全人才)，多层培养网络空间安全人才。

欧盟于2013年2月发布《网络安全战略》，要求各成员国展开网络与信息安全教育。2011年英国发布《网络安全国家战略》，强调要“加强网络安全技能教育”，德国发布《德国网络安全战略》，强调“提高公众对互联网风险的认识，加强专 业人才培养”，法国发布《信息系统防御与安全：法国战略》，提出建立网络防御研究中心，从事专业人才的培训，增加年轻信息安全人才的比重。欧洲各国普遍重视硕士和博士学历教育，并建立了针对在校高学历人才的专业评估授权认证。在专业人才认证方面，建立了CCT和CCP专业认证项目，确定具有专业技能的网络空间安全人才等级并给予相应待遇。

日本自2011年起每年支出约一亿日元用于网络安全人才培养，包括向国外大学输送人才，进入信息安全相关机构进修，参加日美IT论坛。2013 年6 月出台的《日本赛博安全战略》提出培养、发掘掌握创新方法和技术的网络空间安全优秀人才的基本路线。

俄罗斯发布数版《信息安全学说》，指导推进信息安全建设和人才培养工作。信息学是俄罗斯中学阶段的一门核心课程，其内容包括信息技术、网络技术、算法和编程语言，据统计，每年有6万中学生注册参加AP计算机科学考试，为俄罗斯培育了超60 万计算机相关技术人才，这其中就包括了大量的世界知名的黑客。俄罗斯在部队系统内大力培养网络空间安全人才，2015年，国防部设立了IT技术武备学校，用于培养专门的网络部队后备人才。

另外，美、英、韩、俄、以等网络空间安全人才的培养也依托于部队和地方机构的协同合作。美国海军、陆军、空军向大学和研究机构拨付大量资金进行网络攻防技术研发，并将空军研究实验室向后备军官和普通大学生开放；韩国国防部与忠清大学在2014 年设立专业系，为韩国网军培育网络空间安全人才；日本2017年预算七千万日元，用于委托美军进行信息系统人才培养；以色列的网络战部队8200部队更是拥有优先在高中生中招收人才的权利。

1.1.1 国际情况

1999年，美国国家安全局（National Security Agency, NSA）推出了信息保障教育学术卓越中心（CAE in information assurance education, CAE-IAE）计划。1999年，该计划首批认证了七所大学。2004年，NSA与美国国土安全部（Department of Homeland Security , DHS）合作，开展CAE-IAE认证计划。2008年，CAE计划增加了创新和卓越中心研究（Center of Academic Excellence in Cyber Research , CAE-R）认证。2010年，网络空间防御（Center of Academic Excellence in Cyber Defense, CAE-CD）项目启动，面向研究中心、技术学校、政府培训机构，包含三个项目的认证：四年制学士/硕士教育、两年制预科教育和研究中心项目认证。

2010年4月，美国前总统奥巴马启动“国家网络空间安全教育计划(National Initiative of Cyber security Education, NICE)”，期望通过国家的整体布局和行动，在信息安全常识普及、正规学历教育、职业化培训和认证等三个方面开展系统化、规范化的强化工作，来全面提高美国的信息安全能力。

2012年，网络空间操作（Center of Academic Excellence in Cyber Operations, CAE-CO）项目启动，作为NICE框架的一部分，CAE-CO项目是对CAE-CD的补充，特别强调网络操作专业技术。CAE-CO认证面向四年制本科和研究生院校，参与认证的院校必须是已建立计算机科学（Computer Science, CS），电子工程（Electrical Engineering, EE）或计算机工程（Computer Engineering, CE）专业的院系，或拥有同等技术水平的专业院系，或在两个或两个以上的专业之间有所协作的院系。2017年，CAE-IAE指定名称改为网络空间防御教育（Center of Academic Excellence in Cyber Defense Education, CAE-CDE）。2019年10月， CAE-CD项目并入CAE-CO项目。同年，CAE决定强化学术成果产出在评定中的占比，并同时结合其他因素。

截至2020年9月1日，全美共有334所机构获得CAE认证，116所社区学院提供副学士学位课程和学位；48所机构同时拥有CAE-CDE和CAE-R认证；6所机构同时拥有CAE-CDE和CAE-CO认证；2所机构拥有CAE-R和CAE-CO认证；10所机构拥有三种认证。

NCAE项目得到了很多政府相关部门的支持，包括但不限于国防部（DoD），教育部（DoE），国土安全局（DHS），联邦调查局（FBI），NICE，美国网络空间安全司令部（US-CYBERCOM）和美国国家科学基金委员The National Science Foundation（NSF）。

英国政府通信部于2011年底，该国第一个国家网络安全战略起步阶段时启动了一流网络空间安全研究学术中心（Academic Centres of Excellence in Cyber Security Research,ACEs-CSR）建设项目，并于起初的8所大学发展成为2020年19所大学组成的学术联盟，将英国大学的网络空间安全研究体系化。

该计划最初的重要目标是认定英国在网络空间安全领域的一流研究机构，并认定英国研究成果显著的技术领域，这也有助于明确需要加强的研究领域。其愿景是实现对政府和企业的支持。它将协助政府和企业与学术机构进行更有效的互动，以深入了解领先的网络空间安全研究，并利用它为英国创造利益。ACEs-CSR考量的研究领域主要包括以下八大类：密码学、密钥管理及相关协议，信息风险管理，系统工程及安全分析，信息保障方法论，操作保障技术，技术和产品的安全性研究，网络空间安全科学和可信系统的构建。

英国工程与物理科学研究委员会和国家网络安全中心共开展了6次ACE-CSR认证工作。在每次认证过程中，可获认证的机构的数量未做限制。英国政府方面的目标是令所有符合标准的机构都将被邀请加入该计划。2019年（第六轮）认证工作后，ACEs-CSR的认证期限为2022年6月30日。

近年来，在欧盟网络安全局（The European Union Agency for Cybersecurity, ENISA）的规划下，欧盟和欧洲自由贸易联盟国家建立了一个网络空间安全高等教育数据库（Cybersecurity Higher Education Database, CyberHEAD），致力于为所有希望在网络空间安全领域提高知识水平的公民提供参考。这项数据库令年轻的人才对网络空间安全高等教育提供的各种可能性有着更清晰的了解，从而做出更明智的选择。同时，它也帮助大学吸引有志于保障欧洲网络空间安全的学生。

另外，受欧盟地平线2020计划（European Union's Horizon 2020 Program）资助的欧洲网络空间安全研究项目（CyberSec4Europe）调研了欧洲大学的网络空间安全硕士项目。该项目的调研目的之一即为“明确并重视大学教育所需的网络技能”，以及调查现有网络空间安全课程。

1.1.2国内情况

我国也非常重视网络空间安全人才的培养，出台了一系列相关政策和法律法规用以推进网络空间安全人才的建设。2015年国务院学位委员会、教育部发布了《关于增设网络空间安全一级学科的通知》，旨在全面提升网络空间安全学科建设水平。2016年，中央网信办发布了《关于加强网络空间安全学科建设和人才培养的意见》，旨在加强网络空间

安全学院学科专业建设和人才培养。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，加强网络空间安全学科专业建设”、“形成有利于人才培养和创新创业的生态环境”。在2017年实施的《中华人民共和国网络安全法》中强调培养网络空间安全人才。网络空间安全学科建设和网络空间安全人才培养上升到前所未有的高度。

各高等院校在进行网络空间安全相关专业教育过程中，应当以政府政策为支撑点和着力点，加强网络空间安全学科建设和专业设置，合理规划网络空间安全专业课程。国内已有34个高校设立网络空间安全一级学科。2017年，中央网信办、教育部共同组织，确定西安电子科技大学、东南大学、武汉大学、北京航空航天大学、四川大学、中国科学技术大学、中国人民解放军战略支援部队信息工程大学等7所高校作为首批一流网络安全学院建设示范项目。2019年华中科技大学、北京邮电大学、上海交通大学、山东大学4所高校入选第二批一流网络安全学院建设示范项目高校名单。截至2021年，开设网络空间安全专业硕士点（083900）的国内院校共73所。

1.2 人才发展环境

1.2.1院校培养环境

我国网络空间安全人才培养布局较早，但网络空间安全人才培养环境仍不容乐观。据教育部网络空间安全教学指导委员会统计，2019年我国网络空间安全的人才缺口在70万到140万之间，而我国网络安全从业人员约为10万人，人才缺口比率高达93%。而我国目前网络空间安全人才年培养规模在3万左右，远远不能满足我国安全人才的需求。另外，网络空间安全高端人才相对较少。据专业机构测算，2020年我国网络安全从业人员需求数量为155万人，2027年为327万人。当前培养的网络安全人才数量远远不能满足需求。

目前，我国的网络空间安全方面的人才培养主要集中在本科教育，硕士生、博士生为主的研究型人才培养相对不足。网络空间师资力量也不足，由于一级学科成立时间不长，网络空间安全大部分的教师来自于其他专业。

网络空间安全人才培养具有多学科交叉、涉及面广等特点，传统的知识体系已经不适应国家战略和行业快速发展的需求。相关专业的课程与知识体系分散，学生在知识结构和实践能力方面存在滞后性。现有的网络空间安全方面的培养方案并不完全适用于网络空间安全本身的发展需求。需要探索基于相关专业知识的网络空间安全人才培养模式、重构课程与知识体系。

网络空间安全又是一门具有很强实践性的学科，传统教学过程对实践能力培养过程薄弱，缺少适应新需求的实践与创新平台，学生工程实践与创新能力不强。各高校开始普遍重视人才实践能力的培养，在课程设置、实验环境、校企合作等方面开展了不少探索。但是目前高校培养出来的人才在实践能力上缺少足够的锻炼，难以满足社会需要。因此需要加强实验和实践教学环节，搭建政、产、学、研、用多元化实践教育体系与平台。

网络空间安全人才能力评价具有特殊性，传统人才评价方式偏重于知识考察，网络空间安全类人才培养质量标准尚未健全。习近平总书记指出："对待急需紧缺的特殊人才，不要都用一把尺子衡量"。而现在我国对于网络空间人才的培养与评定，还主要停留在"唯学位"、"唯论文"的阶段，对于网络空间人才的认定过于局限。

因此，需要面向网络安全核心能力，构建多维度评价与持续改进的新机制，保障网络空间安全人才培养质量。

1.2.2单位使用环境

近年来，随着全球范围内网络安全事件的日益增加，个人、企业及国家对这一领域的关注程度不断提升，而政企对网络空间安全人才的需求也出现了爆发式增长，网络空间安全人才供不应求，出现结构性短缺。

为应对日益严峻的网络安全威胁，《网络安全法》及一系列配套政策法规的逐步落地实施，国内政企机构对网络空间安全人才的需求也迅速提高。目前从地域上来看，网络空间安全人才的供给和需求都高度集中，北京市、广东省、浙江省、上海市、是网络空间安全人才需求量最大的地域，这四个省市对网络空间安全人才需求的总量占全国需求总量的48%。人才需求数量很大程度上也与国内城市的互联网发展差异及党政机关、大型国企和总部和网络空间安全公司的地域分布有关。

据调研统计，当今我国网络安全产业，具备网络安全实战能力的人才，"本科"群体依旧是行业的主力军，占比为68.0%，其次是"硕士"，占比17.5%、"大专/高职"学历的人群占比为9.4%，"高中"与"中专"学历的人群占比总和不到5%。而从企业角度分析，用人部门在招聘时最关注的是网络安全实战能力（60%），其次才是网络安全专业知识（45%）。这说明在网络安全领域，学历并不是用人企业最为看重的因素，企业需要的是具有实际操作能力，能够解决实际问题的安全技术人员，而不是只有学术能力，缺乏动手能力的人。

据统计，网络安全领域，求职者期望的平均月薪约为14013.2元，而政企机构提供给相关岗位就职者的平均月薪约为　11554.8元，用人单位提供薪资水平实际上明显低于求职者的期望。但就目前来看，网络安全市场上有经验的人才较少，预计未来3-5年内，具备实战技能的安全运维人员与高水平的网络安全专家，将成为网络安全人才市场中最为稀缺和抢手资源。

我国当前网络空间安全人才供给在量和质这两方面的缺失。在量的方面，企业要发展壮大，在内部员工培训的同时，还要不间断地引进优秀的网络安全人才。相对于传统开发人员，网络安全人才供给明显不足，即使给出高于行业平均标准的薪资，也难以引进足够数量的人才。在质的方面，企业需要实用型人才。引进人才缺乏相应的动手和解决问题的能力，需要企业再对其进行深入的实践培训才能胜任工作。这样又会增加企业人才引进成本，也与人才引进的初衷相背离。

网络空间安全人才认定工作思路较窄，需求方在招聘时通常会强调所需要的人才具有网络空间安全专业背景，甚至部分网络安全人才认证机构在进行人才认证时也要有专业背景或工作经验。不过社会当中有很多人是靠自学成为网络空间安全人才的，所具备的网络空间安全知识、技能足以应对一部分实际问题。因此，如果一味强调专业背景、从业经

验，很多优秀网络空间安全人才可能被埋没。同时某些传统企业，内部更重视产品生产，对网络安全重视程度不高，网络空间安全工作人员很少有再培训提高的机会，在岗位中加深、拓宽安全知识机会较少，缺少晋升通道。

1.3 网络安全人才实战能力类别

网络安全人才是典型的复合型人才，要构建以基本资历结构、知识结构、技能结构和职业素养为主的网络空间安全人才能力结构模型。

1.3.1网络安全人才实战能力定义

网络安全人才实战能力是人才培养的重要目标。

从业务场景需求出发，网络安全人才实战能力可以归纳为“攻防实战能力”、“漏洞挖掘能力”、“工程开发能力”、“战效评估能力”四种类型。

1. 攻防实战能力指的是，在真实业务环境下利用网络空间安全技术和工具开展安全监测与分析、风险评估、渗透测试事件研判、安全运维、应急响应等工作的能力。能力高低的决定因素包括攻防业务技术水平、前沿技术和产业动态了解情况、业务模式和服务场景掌握程度等。

2. 漏洞挖掘能力指的是，综合应用各种技术和工具，发现网络和系统中潜在漏洞的能力。该能力对安全人员的理论实践、工具运用、工作经验和漏洞信息掌握情况有较高要求。

3. 工程开发能力指的是，网络安全产品和工具的研发、网络安全系统的集成能力。能力的高低取决于人员自身对业务场景的理解程度、安全知识和工具的掌握应用程度以及产品的工程化能力。

4. 战效评估能力指的是，具备安全防御体系顶层设计、战略规划，具备突发网络安全事件作战指挥、协调保障，以及对使用网络安全武器装备完成规定任务的作战效能进行评估的能力。

在全国信息安全标准化技术委员会(SAC/TC260)提出的《信息安全技术　网络安全从业人员能力基本要求》(征求意见稿)中将网络安全工作类别分为5类，包括：网络安全管理、网络安全建设、网络安全运营、网络安全审计和评估以及网络安全科研教育，如表1-1所示。

表1-1 工作类别及工作任务

序号	工作类别	承担的工作任务
1	网络安全管理	网络安全需求分析 网络安全规划和管理 网络数据安全保护 个人信息保护 密码技术应用 网络安全咨询

序号	工作类别	承担的工作任务
2	网络安全建设	网络安全需求分析 网络安全架构设计 网络安全开发 供应链安全管理 网络安全集成实施 网络数据安全保护 个人信息保护 密码技术应用
3	网络安全运营	网络安全运维 网络安全监测和分析 网络安全应急管理 网络数据安全保护 个人信息保护 密码技术应用
4	网络安全审计和评估	网络安全审计 网络安全测试 网络安全评估 网络安全认证 电子数据取证
5	网络安全科研教育	网络安全研究 网络安全培训

该征求意见稿详细列出了网络安全从业人员完成工作任务应具备的通用知识和通用技能，给出了承担相应工作类别的从业人员应具备的基本专业知识和技能要求。因不同组织对工作角色的划分存在不同，还给出了工作类别、工作角色与国家网络安全职业设置的映射关系。网络安全人才实战能力贯穿于各个岗位中，不同类型的岗位对实战能力的要求不同。

安全管理岗：具备规划安全战略、协调安全资源、设计网络系统、规划保障体系、风险管理及预判、设计防御体系、设计应急响应体系能力；

安全建设岗：具备设计安全架构、配置部署安全产品、安全基础测试、调度安全保障资源、设计安全检测计划、识别评估安全风险能力；

安全运营岗：具备维护网络设备运行、管理威胁情报、编制预案、组织应急演练、排除监控议程、安全应急响应、入侵溯源追踪能力；

测试评估岗：具备脆弱性渗透测试、数据风险评估、编制网络安全审核计划、网络安全评估及审计、合法合规审查、电子溯源取证能力；

科研教育岗：具备前沿技术研究、未知漏洞挖掘、武器库开发、制定培训计划、设计培训方案、实施培训考核、评价及改进培训内容能力。

1.3.2网络安全人才实战能力模型

实践是检验网络安全实战能力的有效标准。近年来，我国在网络安全人才检验的模式、体系和机制方面做了很多有益探索。从实践实训的模式逐步加强，到引入网络安全竞赛作为技能检验评定的一种模式，再到社会各界广泛参与的实战演练和众测活动，都是以“技术应用场景”的模式来检验和督促人员进步，现已经取得了显著成效。

综上所述，围绕网络安全人才实战的四种能力和三种验证方式，我们推出网络安全人才实战能力“4+3模型”，如图1-1。

图1-1 网络安全人才实战能力4+3模型

本白皮书的后续部分将对网络安全人才实战能力中的“攻防实战能力”做出详细的分析论述。

第二章

网络安全人才攻防实战能力分析

随着数字化进程的加速，网络边界逐步消失，网络攻击暴露面无限扩大，给网络空间乃至国家安全造成了严重威胁，各企事业单位面临的防御压力与日俱增，攻防实战能力作为最直接也是最前线的重要能力成为了企事业单位重点关注的网络安全人才能力之一，在网络安全人才缺口严峻的背景下，网络安全攻防实战人才成为了重点关注对象。

网络安全攻防实战能力指的是，在真实业务场景中，人才在技术应用、协同配合、应急反应等方面，在网络攻防对抗条件下实际产生效能的潜力和水平。

具体来说，攻防实战能力需要网络安全人才掌握各类安全标准的落地实践经验，可以熟练使用网络安全技术和工具，为具体业务开展风险评估，提供安全落地规划指导和建议。同时，网络安全人才还应具备一定的调查取证能力，能够在受到攻击后收集、处理、保存、分析并呈现计算机攻击相关证据，为后续的攻击溯源或案件侦查提供帮助。

网络安全竞赛具有强实践性、创新性、对抗性的特点，经过近些年的蓬勃发展，已成为了全面检验和提升攻防实战能力的重要方式之一，发现、培养、选拔了大量网络安全一线人才。“以赛促学、以赛代练”理念也已贯彻落实到了各网络安全实践工作中，网络安全竞赛参与者在各项网络安全工作发挥着越来越重要的作用。

本章节，将以近三年的85761条网络安全竞赛数据为样本，重点对我国网络安全人才攻防实战能力做出详细刻画。样本覆盖全国（港澳台除外）31个省（自治区、直辖市）及新疆生产建设兵团，通信、交通、金融、医疗卫生、政法、政务、能源、电力、高校/职校、互联网、网络安全等重点行业均有覆盖。

2.1 网络安全攻防实战人才现状

2.1.1性别、年龄及学历情况

通过数据分析，目前网络安全攻防实战人才在性别比例上悬殊较大，总体呈现“男性群体居多”的分布情况，女性群体仅占16%，如图2-1。

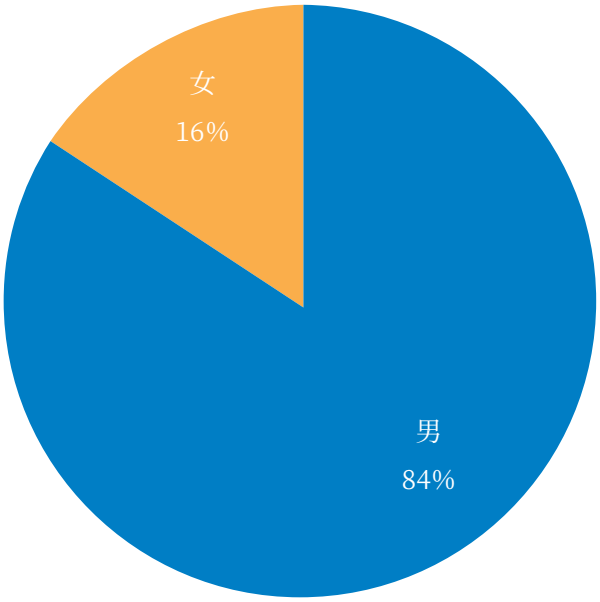


图2-1 网络安全攻防实战人才性别分布

数据显示，网络安全攻防实战人才的年龄主要集中在“18-35岁”这一年龄段，其中，“20-25岁”的群体占比最高，为40%，“25-30岁”与“30-35岁”的群体占比较为接近，分别为22%和20%，“20岁以下”的人群也占据了10%的比例，如图2-2。

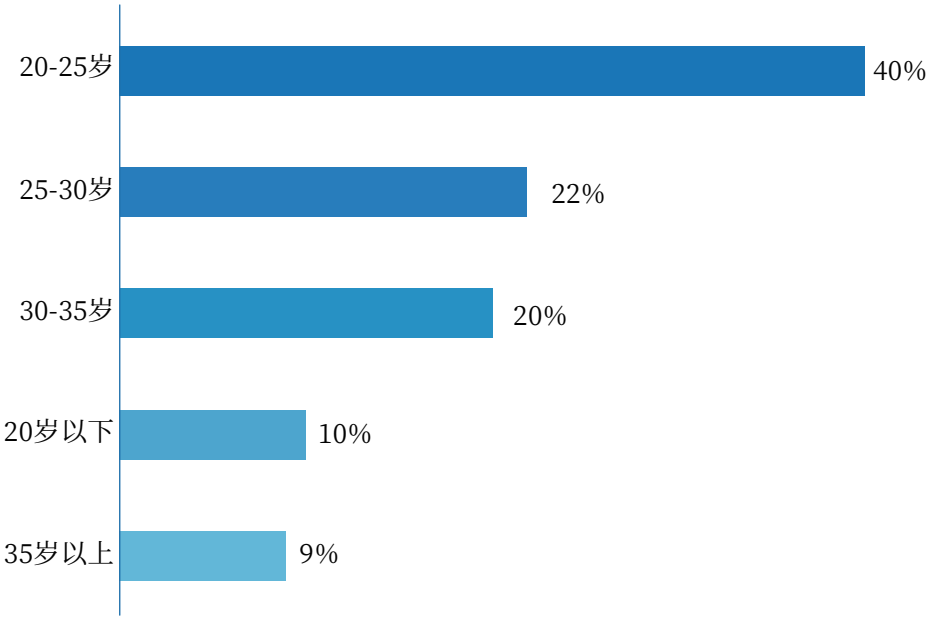


图2-2 网络安全攻防实战人才年龄分布

进一步分析数据可知，“18-25岁”的群体中学生居多，占95%如图2-3。学生群体越来越大的现象，一方面反映出目前院校及相关专业的培养对攻防实战的重视度越来越高，途径更加广泛；另一方面也可以看到，未来网络安全行业的储备力量正在逐渐扩大；年龄区间在“25-35岁”的群体中“学生”与“从业人员”占比则完全不同，这一区间中基本以从业人员为主，占比高达94%，如图2-3。

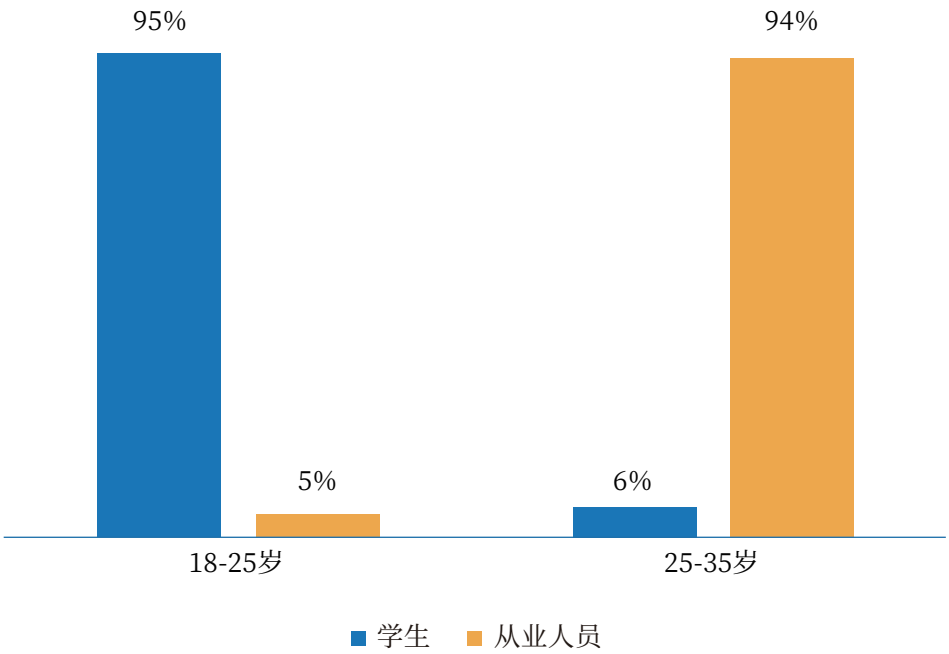


图2-3 不同年龄群体属性分布

分析网络安全攻防实战人才的学历现状可以发现，“本科”群体依旧是行业的主力军，占比为68%，其次是“硕士”，占比18%、“大专/高职”学历的人群占比为10%，“高中”与“中专”学历的人群占比总和不到5%，如图2-4。

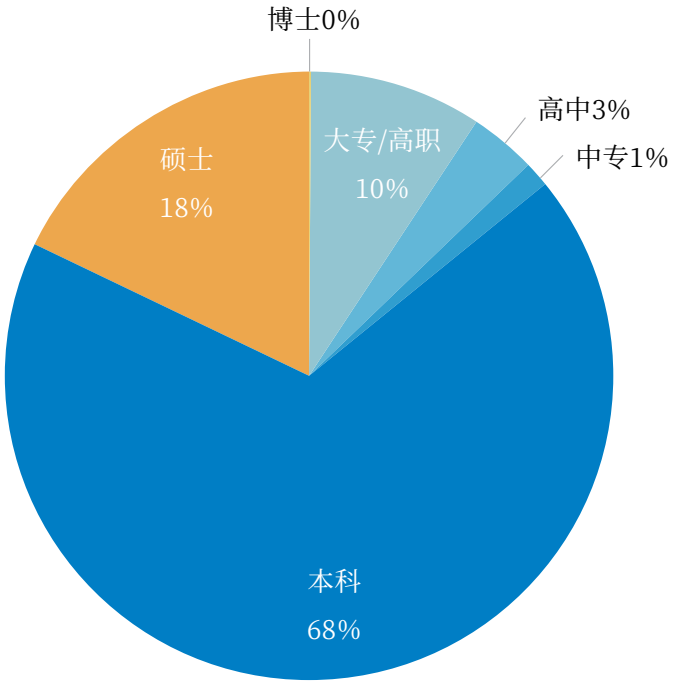
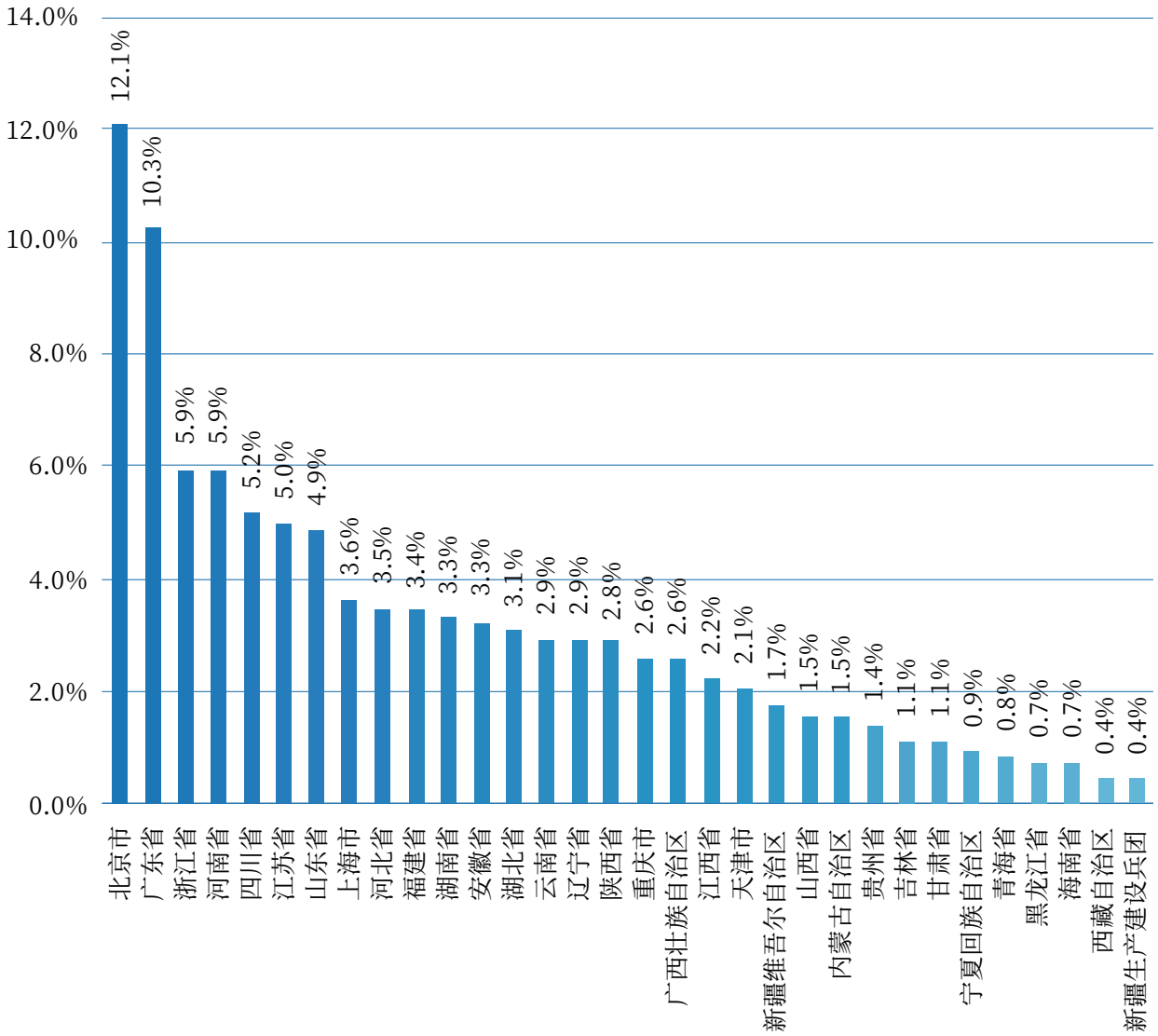


图2-4 网络安全攻防实战人才学历情况

2.1.2地域及行业情况

以地域维度进行人员划分时可以发现，网络安全攻防实战人才在全国（港澳台除外）31个省（自治区、直辖市）及新疆生产建设兵团均有分布。其中，“北京市”的网络安全攻防实战人才占比位居第一，共计12.1%。其次是“广东省”占比为10.3%、“浙江省”占5.9%，如图2-5。



2-5网络安全攻防实战人才地域分布情况

整体可以看到，“华东地区”的网络安全攻防实战人才占比最高，为28.3%，“华北地区”占比为20.7%，“华南地区”、“西南地区”、“华中地区”整体差异较小，网络安全攻防实战人才占比分别为13.6%、12.5%、12.3%，如图2-6。

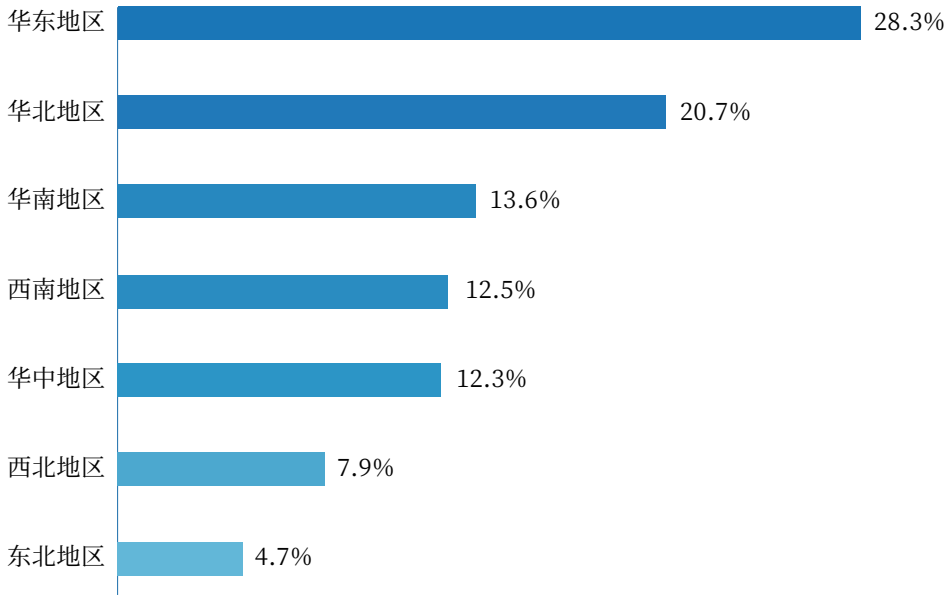


图2-6 网络安全攻防实战人才区域分布情况

进一步分析网络安全攻防实战人才所处行业数据后可以发现，来自“高等院校”的网络安全人才占比远高于其他行业，整体占比高达28%，可见，学生群体对网络安全实践能力提升的参与性与积极性都较高。

位于“高等院校”之后的是以“金融”、“通信”、“能源”、“交通”等为代表的关键信息基础设施行业，各行业的网络安全攻防实战人才占比均较为接近，分别是：“金融”11%、“通信”10%、“能源”9%、“交通“9%；其中“互联网企业”的攻防实战人才占比达到了7%，“网络安全企业”的人才占比也达到了4%，如图2-7。各行业的人才占比在一定程度上也反映了其对网络安全攻防实战人才的需求情况。

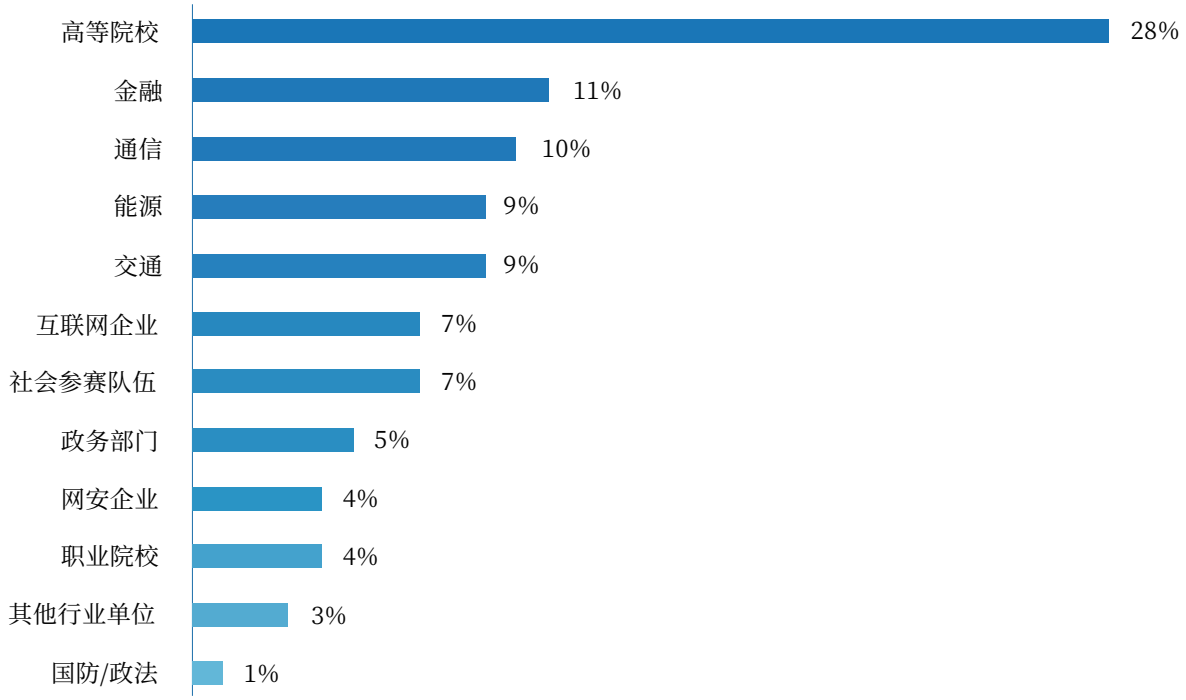


图2-7 网络安全攻防实战人才行业分布情况

2.2 网络安全攻防实战能力现状

2.2.1网络安全攻防实战能力技术

为了更直观的检验网络安全人才的攻防实战能力，通常从技术方向上划分为 “Web安全”、“二进制漏洞挖掘与利用”、“逆向工程”、“密码研究”、“其他类别（也叫杂项）”五个方面。

Web安全技术方向主要涉及情报收集、追踪溯源、资产梳理、安全管理、风险评估与发现、应急响应、安全运维、安全开发、中间件安全、数据库安全、静态代码审计等攻防实战技术能力；

密码研究技术方向主要涉及可信计算、区块链、加解密算法研究、密码算法实现等攻防实战技术能力；

逆向工程技术方向主要涉及逆向分析、防御加固、安全开发、操作系统安全、病毒与木马分析、移动安全、自动化逆向分析等攻防实战技术能力；

二进制漏洞挖掘与利用技术方向主要涉及漏洞发现与利用、安全开发、操作系统安全、IoT安全、防御加固、自动化漏洞挖掘等攻防实战技术能力；

其他类别（也叫杂项）技术方向主要涉及情报收集、追踪溯源、资产梳理、电子取证、流量分析、协议分析、5G安全应用、AI安全应用等攻防实战技术能力。

2.2.2网络安全攻防实战能力情况

数据显示，网络安全人才按照技术方向专长划分，呈现不同的分布。

在网络安全攻防实战人才中，擅长Web安全的人员比例最多，为29%，其次是逆向工程，比例为22%，杂项占比为20%，擅长密码学领域的人才占比为19%，而仅有10%的人才在二进制漏洞利用与挖掘方面专长，如图2-8。

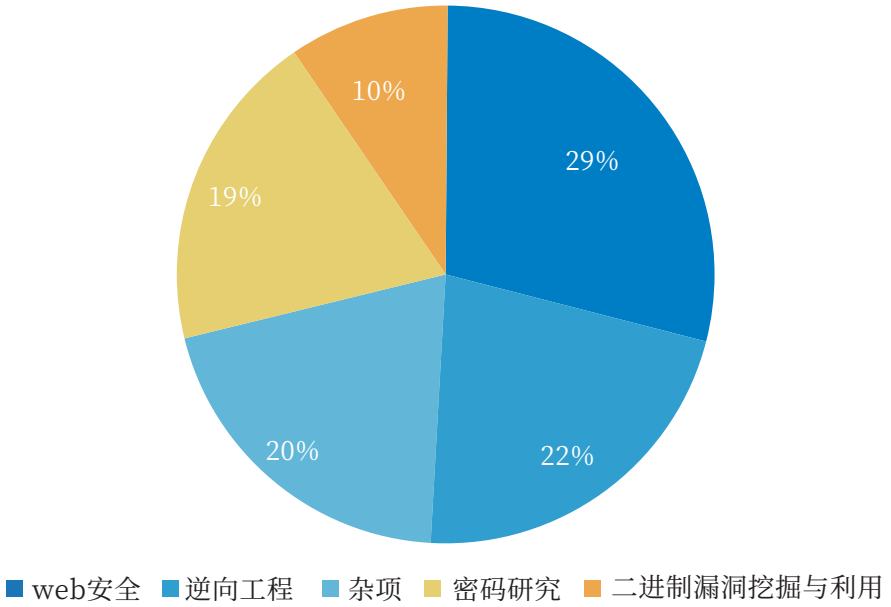


图2-8 专业人才能力分布

从人才能力专长方向种类来看，70%的攻防实战人才拥有单项专长，15%的人才会有两种专长方向，而拥有3种能力特长的多面手则占到了10%，4种能力均具备的人才仅为4%，而擅长所有能力方向的人才更是凤毛麟角，仅占1%，如图2-9。

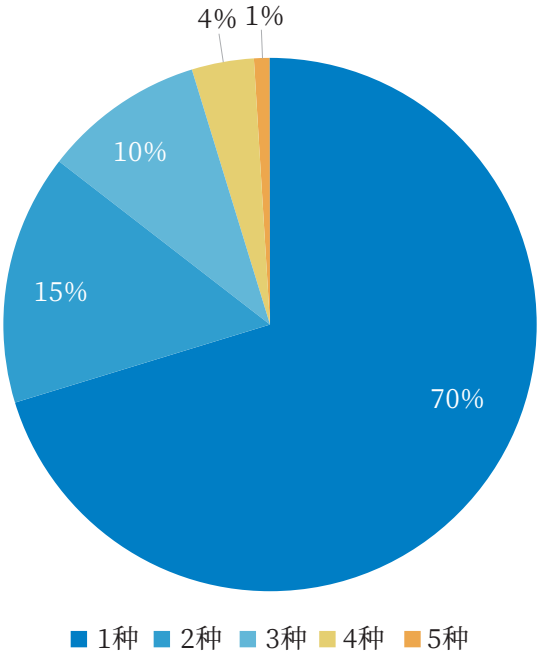


图2-9实战攻防人才能力种类覆盖

数据显示，从各行业维度进行统计分析，网络安全人才的攻防实战能力分布如下：

（1）Web安全人才和密码研究型人才在行业分布中，以高等院校/职业院校居多，比例为33%和38%，在通信行业和能源行业的占比均超过了10%，如图2-10、2-11。

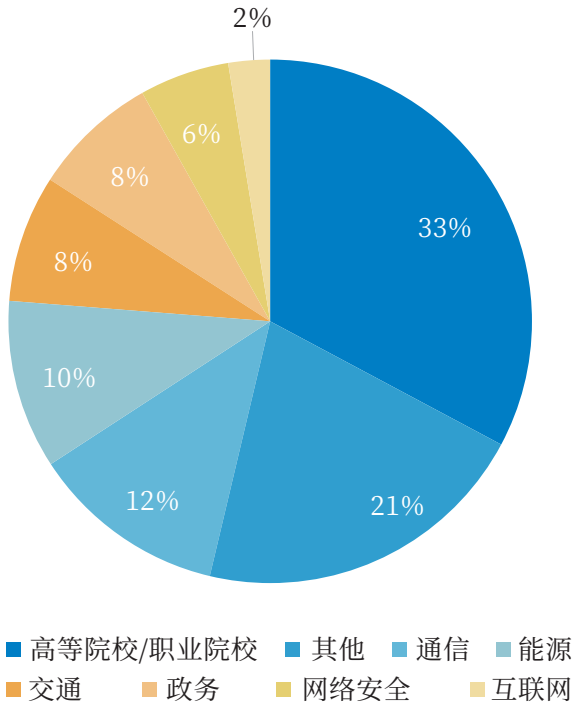


图2-10 Web安全人才行业分布

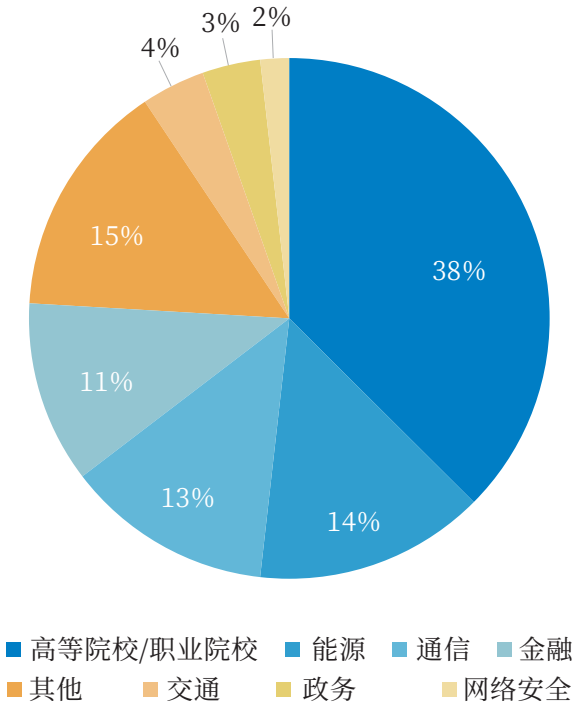


图2-11 密码研究人才行业分布

(2)杂项人才行业分布中,以通信行业居多,比例为28%,其次为能源行业,比例为18%,第三为金融行业,比例为12%,如图2-12所示。

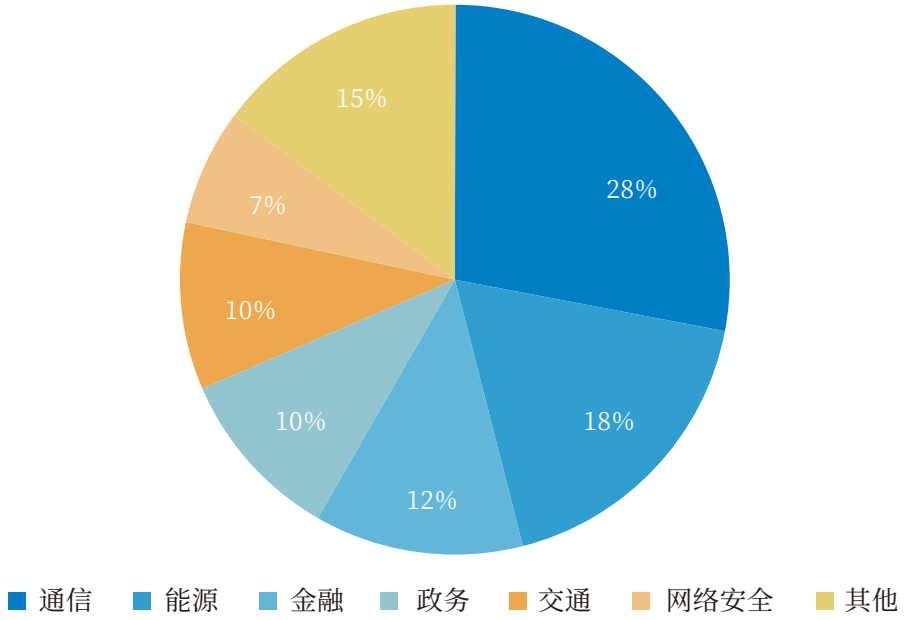


图2-12 杂项人才行业分布

(3)二进制漏洞分析与利用型人才,以高等院校/职业院校居多,比例为31%,其次为能源行业,比例为15%,第三为金融行业,比例为9%,如图2-13。

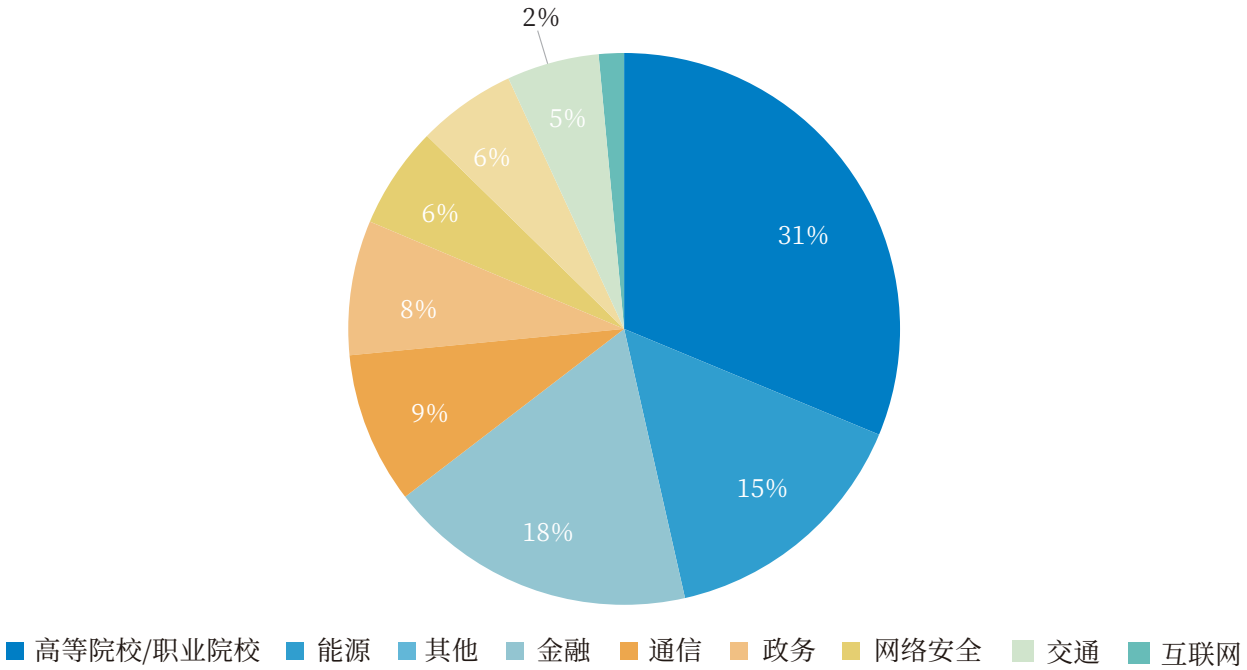


图2-13 二进制漏洞挖掘与利用人才行业分布

(4)逆向工程型人才,以高等院校/职业院校居多,比例为46%,其次为通信行业,比例为9%,第三为政务行业,比例为6%,如图2-14。

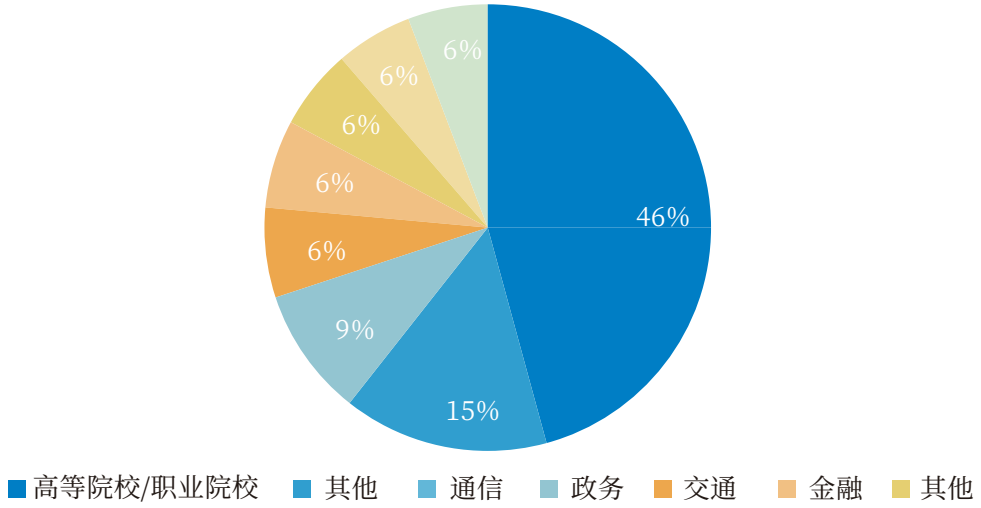


图2-14 逆向工程人才行业分布

由此可见，高等院校/职业院校非常重视学生的实战能力提升，各种维度的实战竞赛均有涉及且广泛参与，通信、能源等行业在Web安全、密码研究、逆向工程、杂项等方向积累较多，能源行业和金融行业在二进制漏洞利用与挖掘方向较为重视，政务行业对逆向工程、杂项方向更为看重。

2.3 网络安全攻防实战经验分析

2.3.1网络安全竞赛人员参与情况

基于网络安全竞赛数据统计分析发现：

近三年参赛次数超过2次的人员中，4%的人员参赛次数超过了10次，属于极少数。11%的人员参赛次数为5-10次，参赛次数为3-5次的人员占比为16%，参赛次数为2次的人员最多，占比为49%，如图2-15所示。

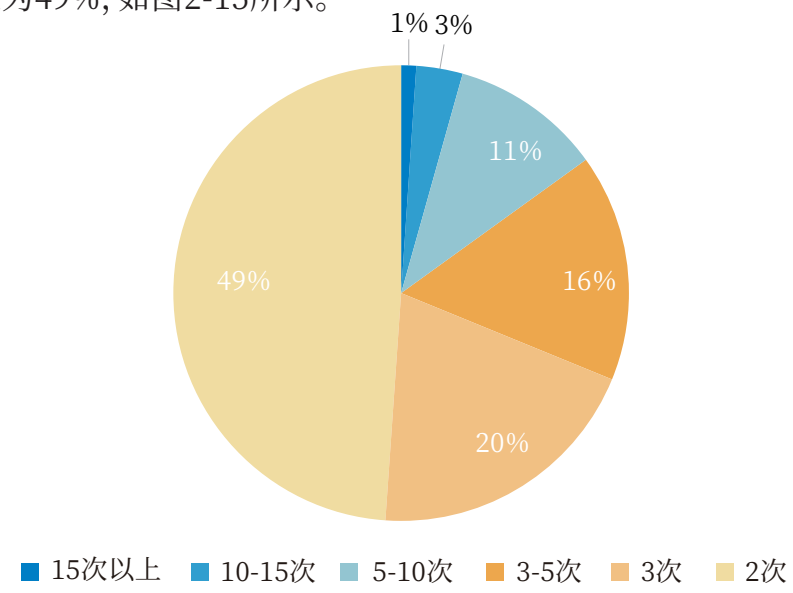


图2-15 选手参赛次数

在所有参赛次数为两次及以上的人员中，超过半数来自院校（58%），如图2-16所示。

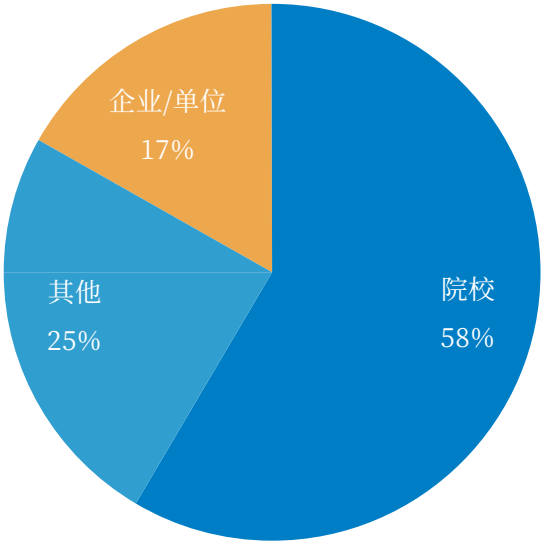


图2-16 参赛选手所在单位（2次及以上）

参加5次以上的人员仍然以高校居多，占比达到73%，来自企业/单位的人员占13%；参赛次数在2-5次区间中，各大企业/单位职工占比上为17%，如图2-17所示。可见，学生群体相比其他的企事业单位职工而言，在各大赛事中均有较高的参与度与积极性。

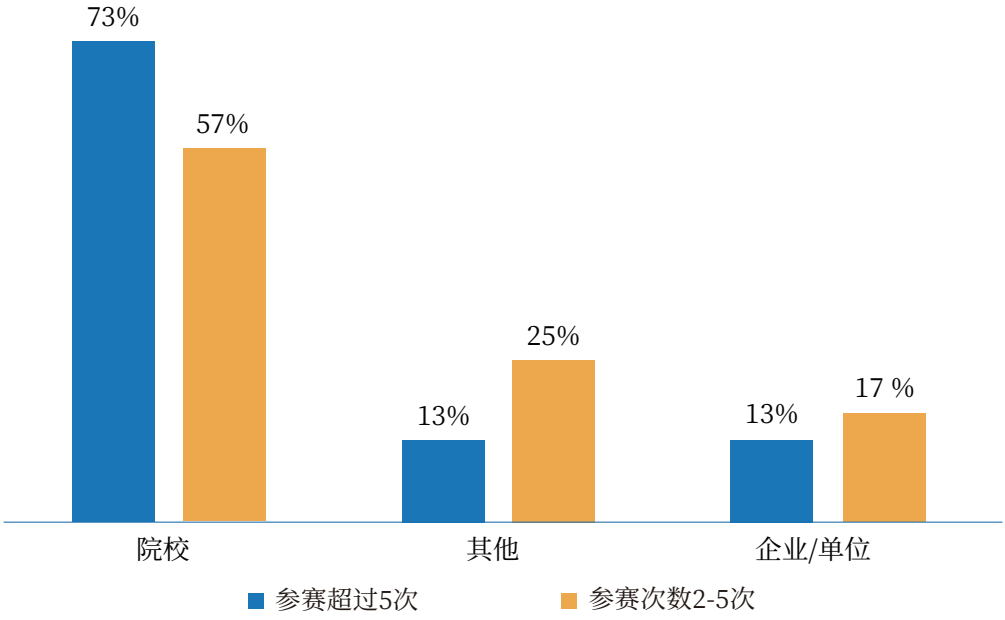


图2-17 参赛选手所在单位（2-5次、5次以上））

2.3.2网络安全竞赛经验成果

经过三十余年的发展，网络安全竞赛已风靡全球并在中国得到了蓬勃发展。国际上知名的赛事有以DEF CON为代表的CTF大赛，以Pwn2Own为代表的破解赛，参与者不乏我国知名战队。在我国，各部委、各行业、各地域均举办了很多网络安全赛事，为网络安全人员实战能力的选拔、评价、提升提供了舞台。比如全球最大规模的国家级赛事“网鼎杯”、中央网信办指导的国家级网络安全赛事“强网杯”等国家级综合大赛；国

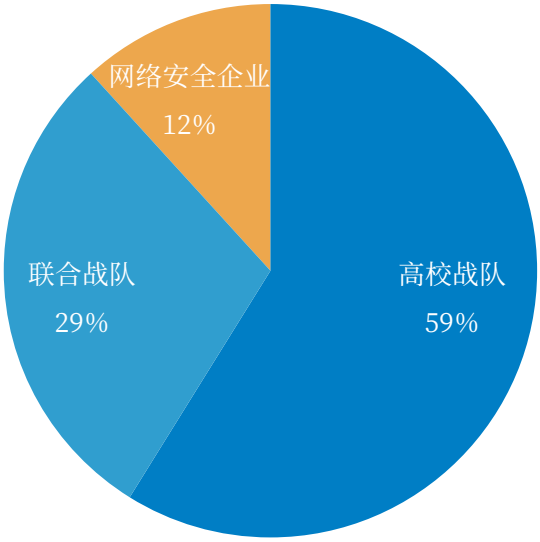
内最大规模工业互联网网络安全大练兵的“护网杯”、国家卫健委主办聚焦医疗行业的“卫生健康行业网络安全技能大赛”、聚焦数据安全领域的国家级赛事“全国数据安全大赛”、面向全国高等院校的高规格赛事“大学生信息安全竞赛创新能力实践赛”、面向全国警院学生的高水平网络安全赛事“蓝帽杯”等行业品牌赛；全国首个“以防为主”国家级网络安全赛事“陇剑杯”、全国首个城市级靶场演习的“巅峰极客”、聚焦华南地区的“红帽杯”、东北地区的“祥云杯”、京津冀地区的“长城杯”等区域品牌赛。

从技术切磋到技能训练，网络安全大赛正在走进各行业，走向全国各省市，持续提升网络安全人才攻防实战能力。国家可以以此来选拔人才，各个战队所属组织间也能通过技术切磋进行交流，而参赛选手们也通过竞赛可以学到很多新技巧，掌握新技术，对个人发展起到积极作用。

然而通过参赛数据分析，还发现了一些潜在问题：

第一，多数参赛选手来自于院校，企业/单位虽人员基数较大，但参赛人数和次数并不多，参与程度有待加强。这其实是与院校相关专业的人才培养目标以及宣传力度与覆盖方向是密切相关的。许多院校会将一些竞赛与学生个人考核评优指标关联起来，因此院校的领导教师们也会对其学生进行竞赛等活动的宣传。

第二，多数排名靠前的战队来自于高校，近三年来两次排名进入前10的战队，高校占比为59%，其次是联合战队，占比为29%，第三为网络安全企业，占比为12%，如图2-18所示。



2-18两次排名进入前十的战队所在行业

第三，对于参赛次数超过2次的人员为基础进行统计发现，网络安全竞赛的人员流动性较大，参加多次竞赛的“老玩家”较少，且多为院校学生。通过问卷调查发现，这与网络安全竞赛的技术门槛较高、对新手不是足够友好是有一定关联的。

第四，从行业维度上看，高水平网络安全攻防实战人才分布较为集中：

通过对各个技术专项能力TOP100人才合并统计分析，我们发现网络安全行业人才占比最高，为20%，其次为高等院校/职业院校，比例为15%，通信为第三，比例为13%，能源、政务、交通、互联网分别为11%、11%、7%、5%。可见从个体分析，网络安全行业、高等院校/职业院校、通信均涌现了一批高水平人才，如图2-19所示。

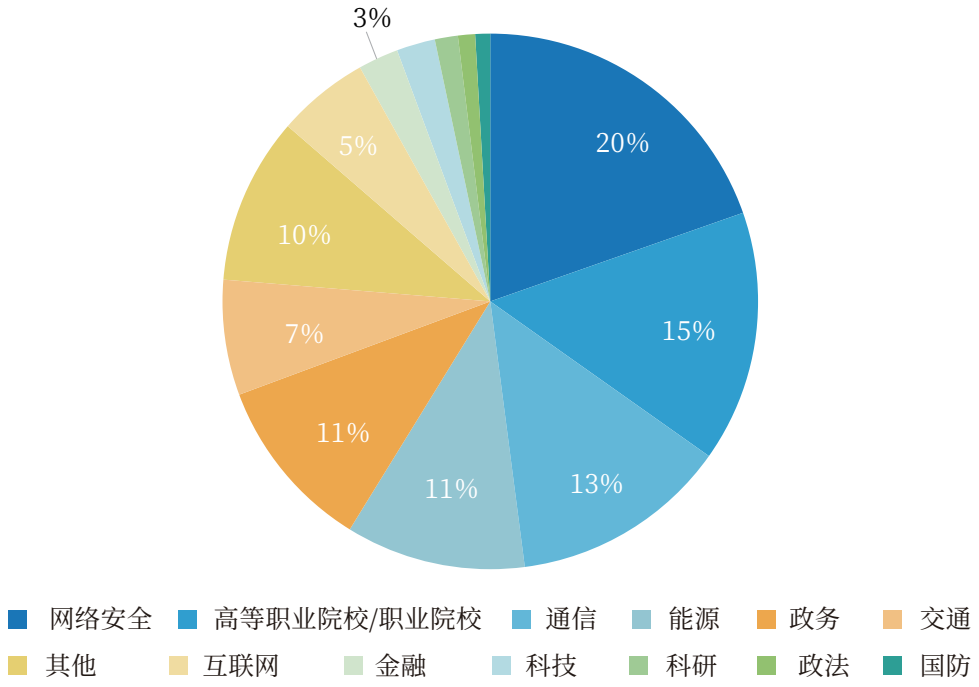


图2-19 TOP100人才行业分布

对各专项技术能力方向TOP100人才分析，所在行业分布呈现以下现状：

Web安全技术方向，26%的顶尖人才分布在高等院校/职业院校，其次为能源行业，比例为21%，第三为网络安全，比例为12%，如图2-20所示。

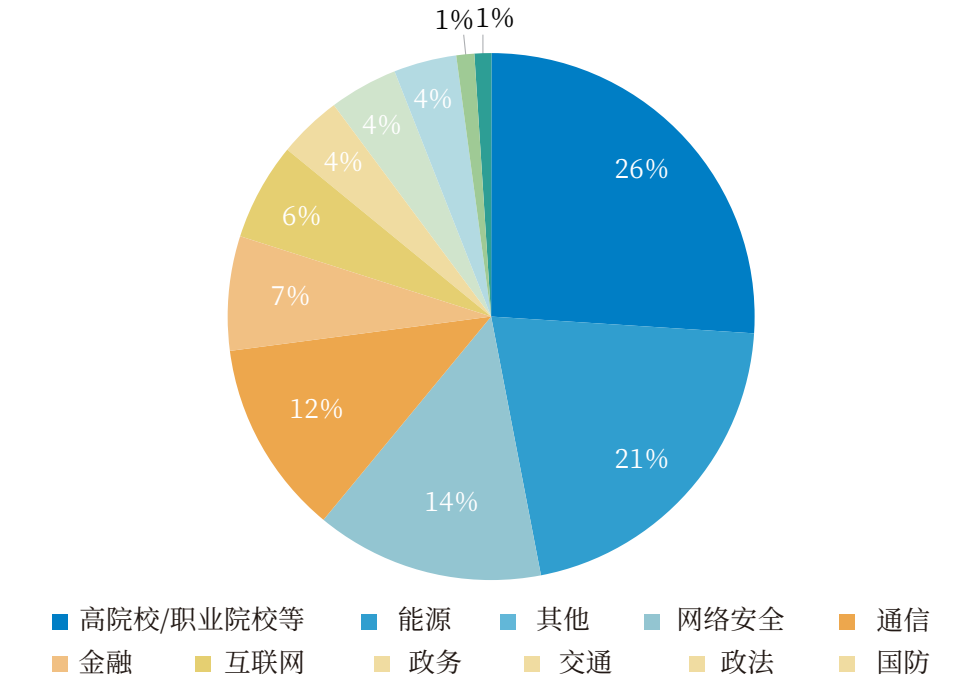


图2-20 Web安全TOP100人才行业分布

杂项技术方向，34%的顶尖人才分布在网络安全行业，其次为高等院校/职业院校，比例为19%，第三为互联网，比例为12%，如图2-21所示。

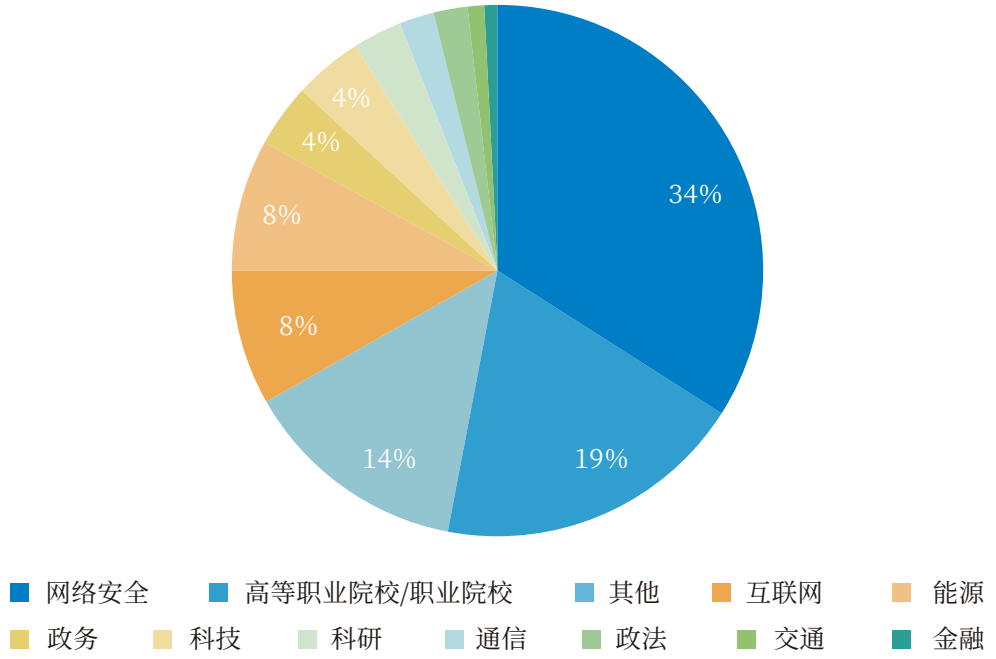


图2-21 杂项TOP100人才行业分布

密码研究技术方向，19%的顶尖人才分布在网络安全行业，其次为通信行业，比例为18%，第三为高等院校/职业院校，比例为16%，如图2-23所示。

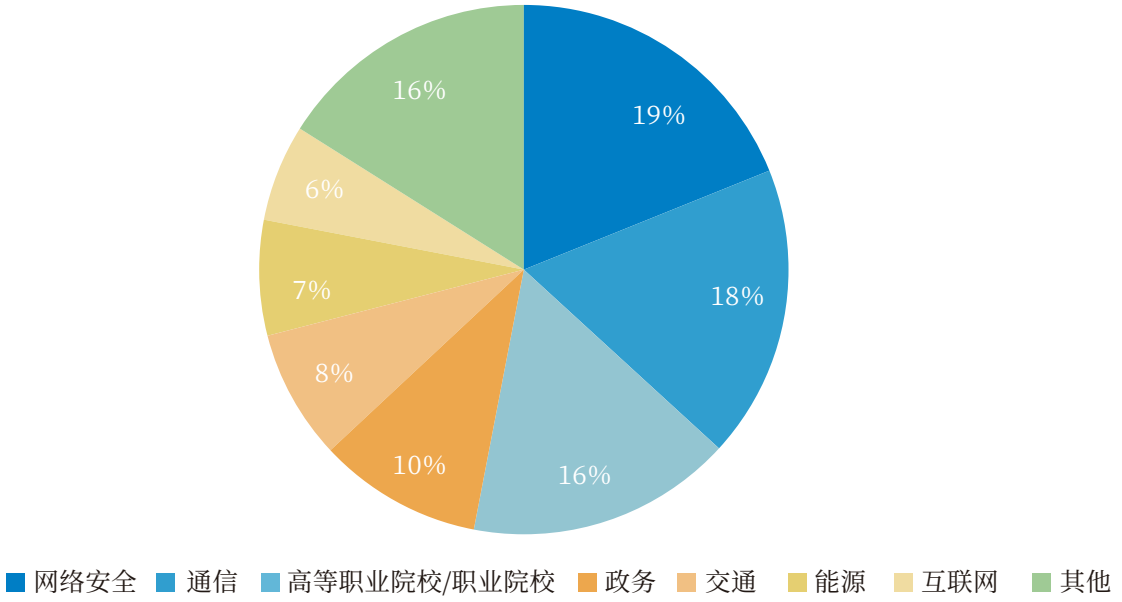


图2-22 密码研究TOP100人才行业分布

二进制漏洞挖掘与利用技术方向，28%的顶尖人才分布在网络安全行业，其次为通信行业，比例为19%，第三为高等院校/职业院校，比例为15%，如图2-23所示。

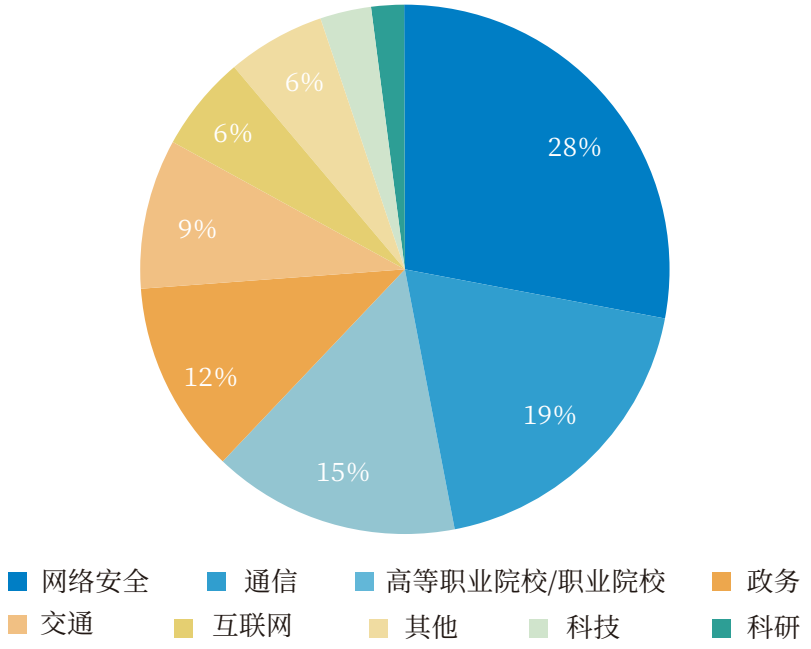


图2-23 二进制漏洞挖掘与利用TOP100人才行业分布

逆向工程技术方向，政务行业与通信行业的顶尖人才最多，比例均为20%，其次是能源行业，比例为18%，如图2-24所示。

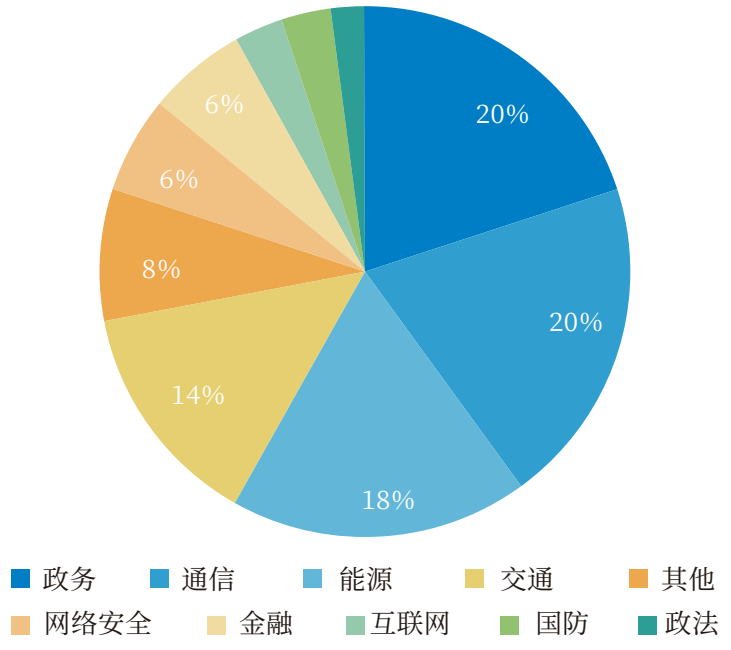


图2-24 逆向工程TOP100人才行业分布

通过统计分析，不难得出人才的攻防实战能力的基本特征：

首先从基本信息、实战技能、领域需求三个维度刻画了网络安全实战人才分布现状。从基本信息维度分析，我们发现网络安全人才以年轻人作为主体，其中学生居多且持续

性增长，这与高校等科研机构的教育投入，以及学生本人的专业选择是密不可分的。其次，网络安全人才的性别比例是显著不均衡的，整个人才群体以男性居多。未来可考虑吸引更多女性群体加入网络安全相关的工作。另外，在地域分布上，网络安全人才在全国分布较广，其中北京市和广东省人才占比名列前茅。在区域分布上，华东华北地区明显更受网络安全人才的偏爱，这显然与技术先进性以及经济优越性是有一定关系的。

从实战技能维度分析，擅长Web安全及逆向工程的人员比例最大。以后应加强对其余三个方向尤其是二进制漏洞利用与挖掘方面人才的培养。不同方向的人才分布存在一定差异，整体而言各方向大多以高等院校/职业院校人才占比居多，一定程度上反映出高等院校/职业院校非常重视学生的实战能力提升，各种维度的实战竞赛均有涉及且广泛参与，社会行业大多专注于特定领域。

从领域需求维度分析，整体上网络安全攻防实战人才呈短缺态势，其中高水平人才短板明显，且大多分布在网络安全行业和高等院校/职业院校。对于不同实战方向，顶尖人才集中分布较为不同。值得注意的是，大部分网络安全攻防实战人才仅拥有单项专长，全项人才十分短缺。这提醒我们未来应强化多维度高水平人才培养，关注网络安全实战人才的全面发展。

习近平总书记反复强调，没有网络安全就没有国家安全。网络安全人才作为国家人民军队之外的另一道防线，其实战能力的重要性不言而喻。在飞速发展的当今社会，网络安全实战能力的形成与强化也愈发重要。路靠人开，钢用铁炼，从有到优的实战能力，也需要通过各界的共同努力逐渐锤炼出来。唯有革故鼎新的魄力、锐意进取的决心，我们才能在这个千帆竞渡的时代挺立潮头，牢牢立于不败之地。

第三章

用人单位网络安全人才实战能力需求分析

当前，随着数字经济的加速发展，数字化技术更加深入的应用到企业生产经营的方方面面，随之带来更为复杂、隐蔽的网络安全风险，因此，各行业新场景、新技术也对网络安全防御提出了新的要求。《网络安全法》、《关键信息基础设施安全保护条例》、《数据安全法》等法律、法规密集发布，网络安全作为国家安全的重要部分，被提升到国家战略的高度。“网络空间的竞争，归根结底是人才的竞争”，人是安全的核心已成为各行业、单位的共识。特别是对于正处在数字化转型关键时期的政企单位来说，人才匮乏成为迫切需要解决的难题，尤其是实战型人才短缺的问题，正在成为掣肘政企单位网络安全能力和水平提升的一大瓶颈。

《关键信息基础设施安全保护条例》要求，“鼓励网络安全专门人才从事关键信息基础设施安全保护工作；将运营者安全管理人员、安全技术人员培训纳入国家继续教育体系。”

《关于进一步加强中央企业网络安全工作的通知》（国资厅发综合[2017]33号）中要求：“加大人才培养力度，改进人才培养机制，加强工作人员的技能培训和考核，开展网络安全关键岗位人员资格认证，提高网络安全人才的配置能力。”

“十四五”规划中强调，“国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。”

在国家相关法律法规的指引下，各行业在网络安全人才培养模式、体系方面都做了很多有益探索，网络安全人才培养工作加速推进，积极建立网络安全人才培养机制，从实践实训的模式逐步加强，到引入网络安全竞赛作为技能检验评定的一种模式，再到社会各界广泛参与的实战演练和众测活动，都对网络安全人才攻防实战能力提升有着重要的促进作用，并取得了显著成效。

然而，网络安全人才依然面临严重缺口。从用人单位角度来讲，很多用人单位的网络空间安全专业岗位设置数量与人员数量还远远不够，甚至大部分用人单位仍然是“兼职干部”挑大梁，很多网络安全岗位职责是由其他信息化相关岗位人员兼任。与安全业务开展不匹配的资源、编制、培训配置也成了用人单位网络安全人才引进的制约因素。不仅如此，用人单位整体攻防实战能力的提高，既依赖高精尖的专业技术人才，也与运维、研发等相关岗位人员安全能力水平息息相关，因此，如何有效建立完善的人才体系，形成科学合理的人才培养和评价机制是促进企业持续、稳定开展生产经营的重要支撑。同时，用人单位的人才应用机制在一定程度上限制了网络安全领域专才、奇才的涌现，这也是用

人单位对于实战型人才需求的困惑点。

针对以上背景和现状，用人单位已经开始在根据自身业务特点，积极组织力量培养实战型网络安全人才。接下来，本章节围绕用人单位的性质特点、岗位需求等维度进行了相关梳理、统计与分析，力求客观呈现用人单位在网络安全人才攻防实战能力需求方面的真实情况。

3.1 用人单位的特点及人才需求分析

3.1.1按地域维度分析

通过对不同地域划分的用人单位网络安全人才特点及情况进行分析，各省（自治区、直辖市）及新疆生产建设兵团的用人单位人才需求统计如图3-1所示。

从地域分布上来看，目前网络安全人才的需求量高度集中在北上广等一线省市，其中北京对网络安全人才需求量达全国需求量的18%，广东紧随其后，需求量占比为15.2%，浙江对网络安全人才的需求量为10.2%，相比较起来，上海对网络安全人才的需求量有所降低，位列第四。北京、上海、广东、浙江网络安全人才需求之和接近全国需求量的一半，这也跟这几个地区是大型政企机构的聚集地有关，同时网络安全企业总部也大多在一线省市。

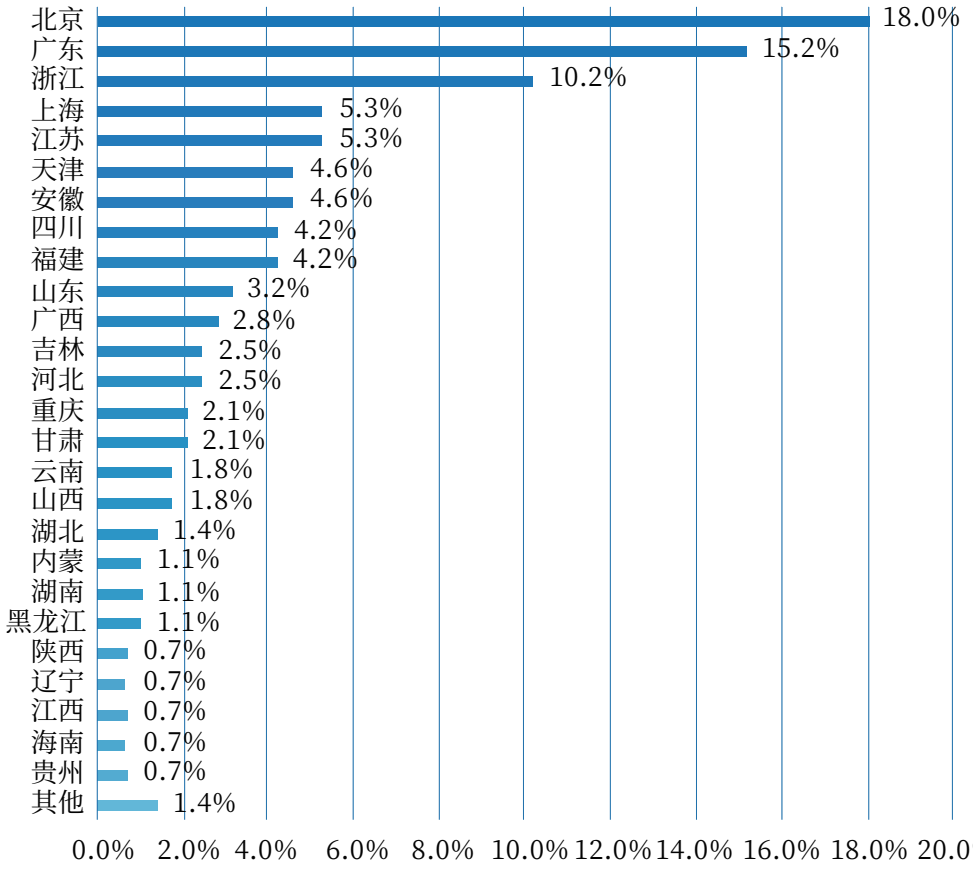


图3-1用人单位区域分布统计

在对北上广浙地区用人单位的网络安全人才技术能力需求分析发现，渗透测试方向人才的需求最为明显，占比达36%。其次是逆向分析方向、漏洞发现与利用方向，占比分别为32%、26%。同时，我们发现，近年来随着各行业对网络安全攻防实战的重视，安全运维成为了一个独立的岗位，正在从网络运维工程师中分离出来，并且影响力越来越大。如图3-2所示。

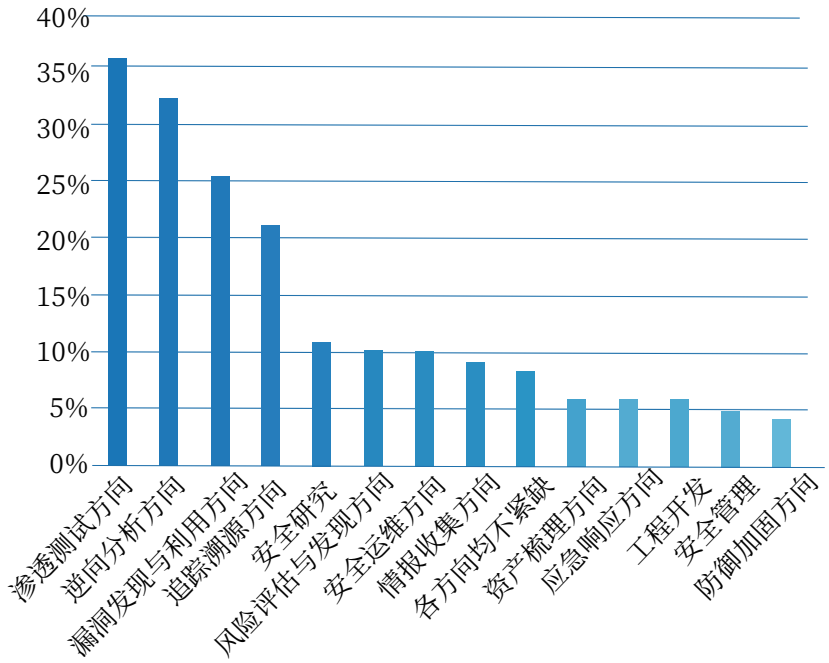


图3-2北上广浙人才需求方向占比情况

从整体上看，长三角、珠三角、京津冀等一线地区对于人才需求既有共性，又各具特点。如下图3-3所示，各地区对渗透测试、漏洞挖掘、分析和利用及逆向分析方向网络安全人才均有较大需求，其次是对病毒与木马分析、Web安全；京津冀对于Web安全方向人才需求较高；珠三角相较于其他地区而言，更需要具备追踪溯源能力，及云、5G、AI、区块链等新兴安全领域能力的人才。

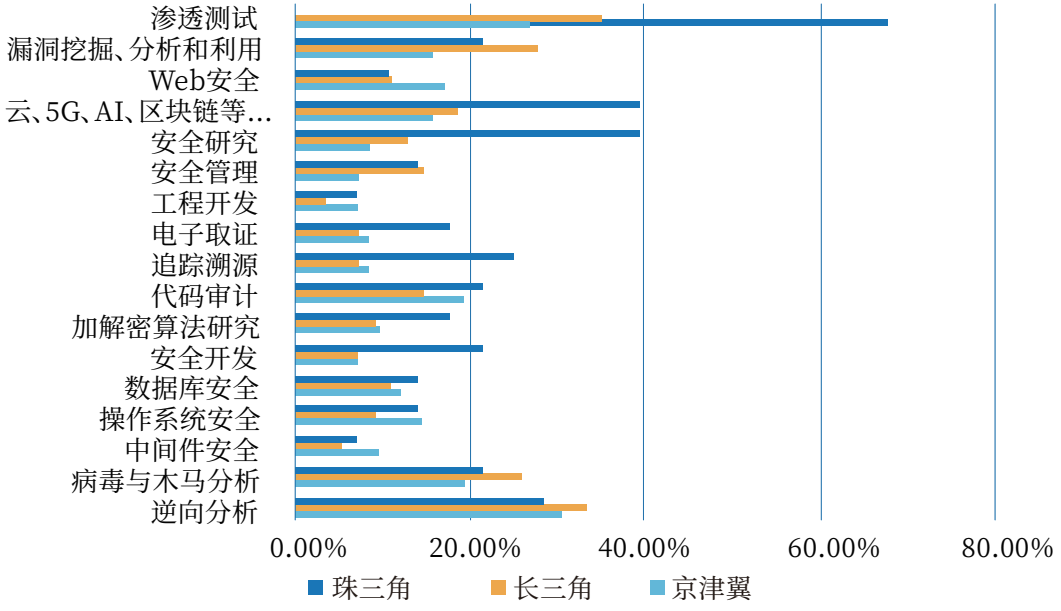


图3-3 三大区域人才能力需求占比情况

3.1.2按行业维度分析

无论是宏观背景下，国家对网络安全各项政策的导向指引，还是微观背景下，以个体为单位的每一位公民，其潜在安全意识的提升，都在很大程度上体现了网络安全的重要性与必要性。于企业而言，对网络安全人才的实际需求也因其所处行业领域、单位性质以及人员规模的不同而有所差异。

通过现有数据对各行业的网络安全人才需求进行分析后发现，能源行业的需求量位列第一，在细分行业中其人才需求占比为21%，其次是通信、政法、金融、交通，网络安全人才需求量占比分别为16%、14%、9%、7%。

值得注意的是，网安企业与医疗卫生的人才需求占比也进入了前10，均为6%。而对教育行业（此处不包括学生群体）的网络　安全从业者进行筛选分析后，数据显示其对网络安全人才的需求占比仍有2%，如图3-4所示。

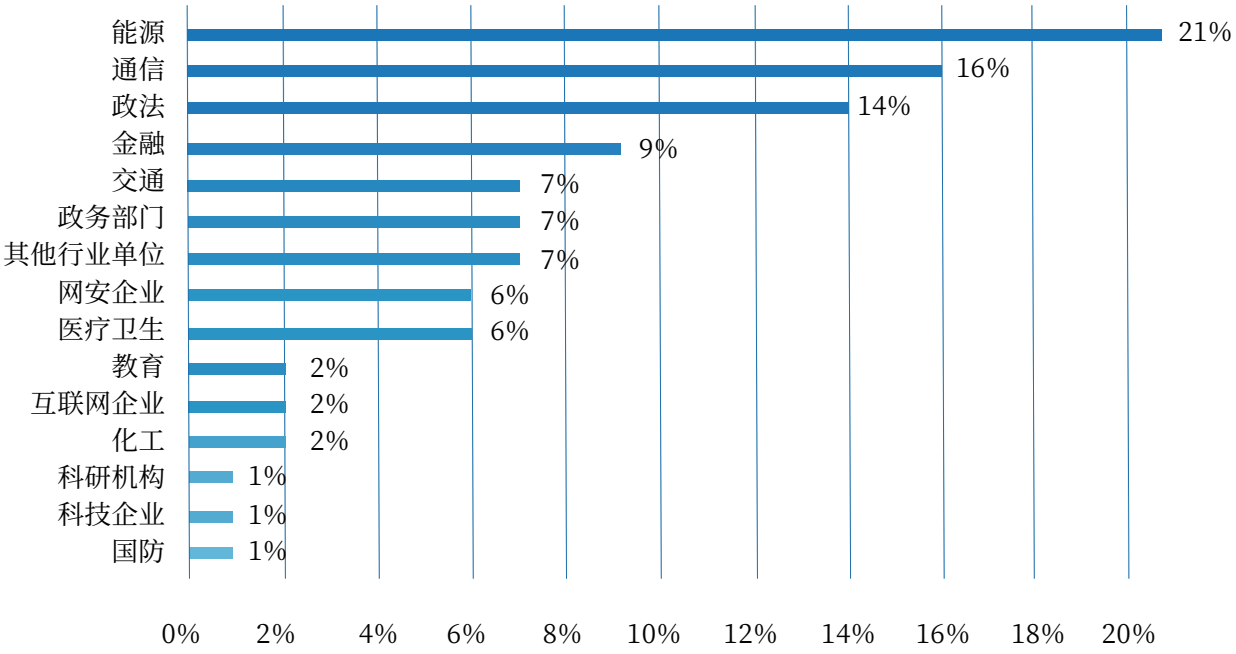


图3-4行业需求分布

金融、能源、电力、通信、交通、医疗卫生等作为关键信息基础设施，是经济社会运行的神经中枢，是网络安全的重中之重，同时，作为经济实力较强，对于业务连续性要求高的行业领域，已在多年前开始建设网络安全人才梯队。在满足用人单位自身安全工作需求的同时，以体系化的规模参加安全竞赛、攻防演练、风险评估等工作，激发、带动行业安全人才的培养。

以下以金融、通信、医疗卫生、教育、互联网五个行业为例，分别对其人才能力需求进行分析。

（1）金融行业人才需求

根据调查数据分析，金融行业对渗透测试方向、逆向分析方向网络安全能力需求最为明显，占比均达30%，对Web安全、代码审计、漏洞挖掘、分析和利用方向网络安全能力也有较高需求，如图3-5所示。

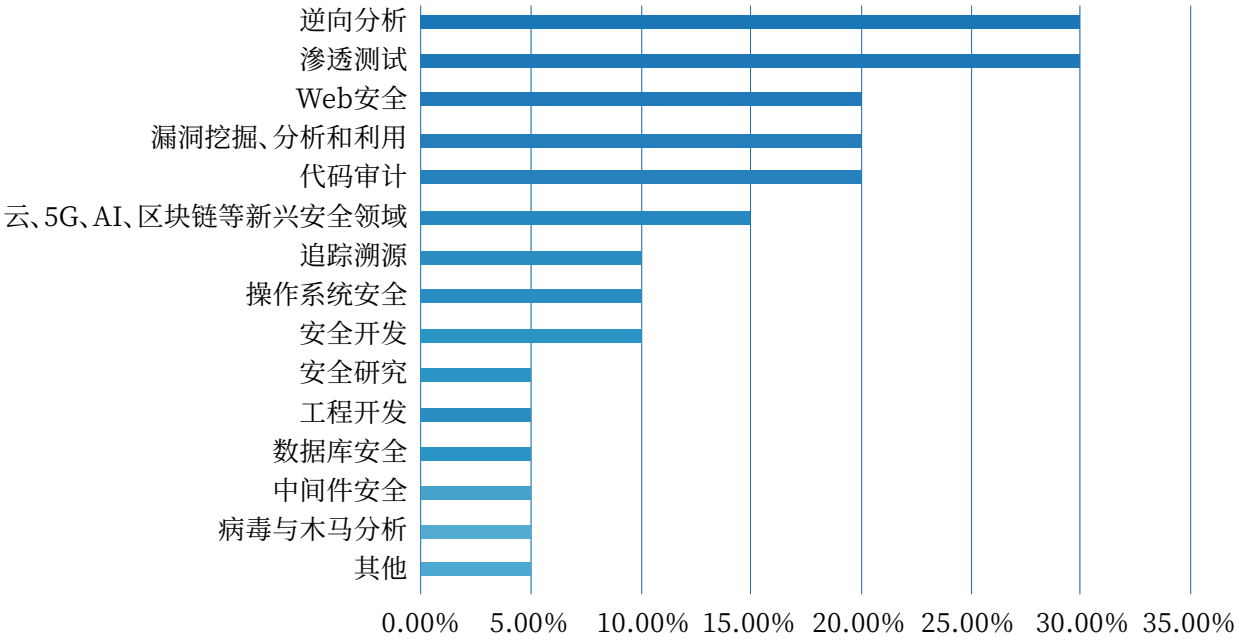


图3-5金融行业人才能力需求占比情况

(2)通信行业人才需求

根据调查数据分析,通信行业对逆向分析能力需求最为明显,占比32%;对代码审计、病毒与木马分析能力需求占比均超过了25%,同时对云、5G、AI、区块链等新兴安全领域网络安全能力有较高需求,如图3-6所示。

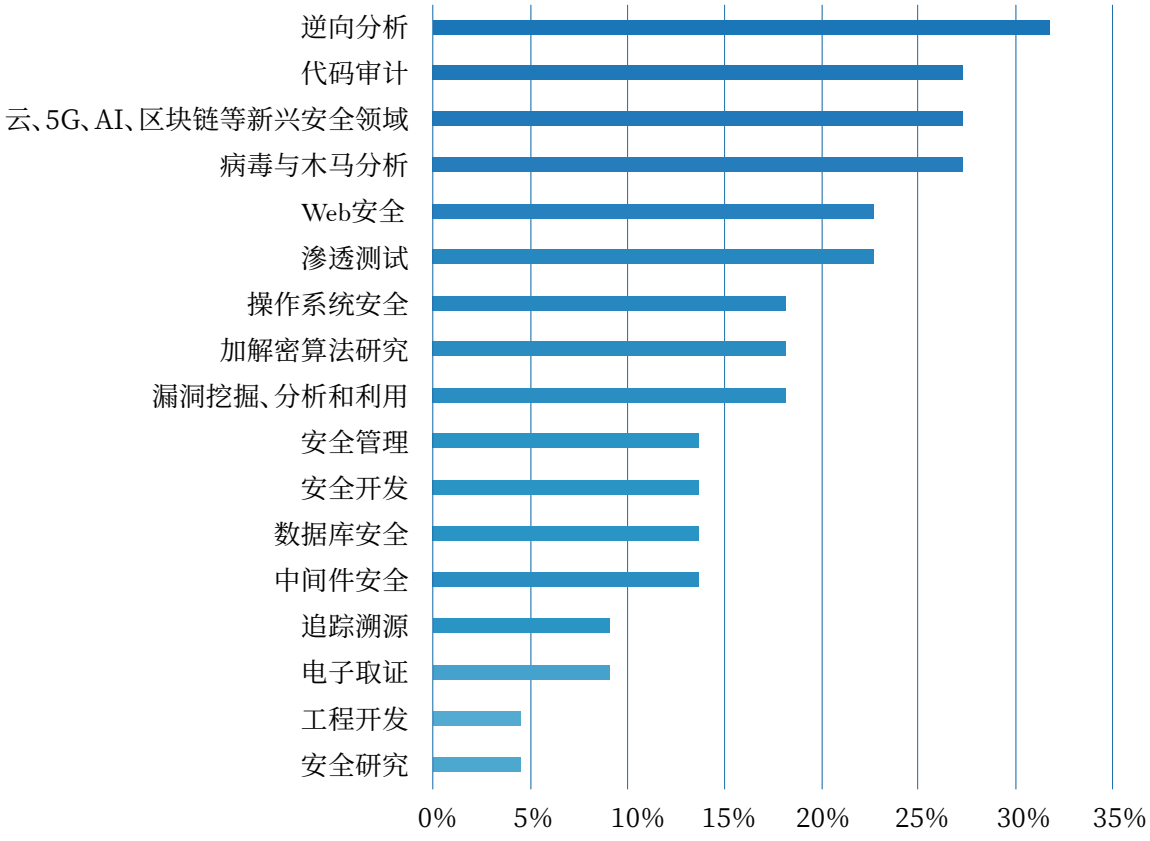


图3-6通信行业人才能力需求占比情况

(3)医疗卫生行业人才需求

根据调查数据分析，医疗卫生行业57%的单位对渗透测试方向网络安全能力需求最为明显，逆向分析方向、Web安全方向、数据库安全方向网络安全能力也有较高需求，如图3-7所示。

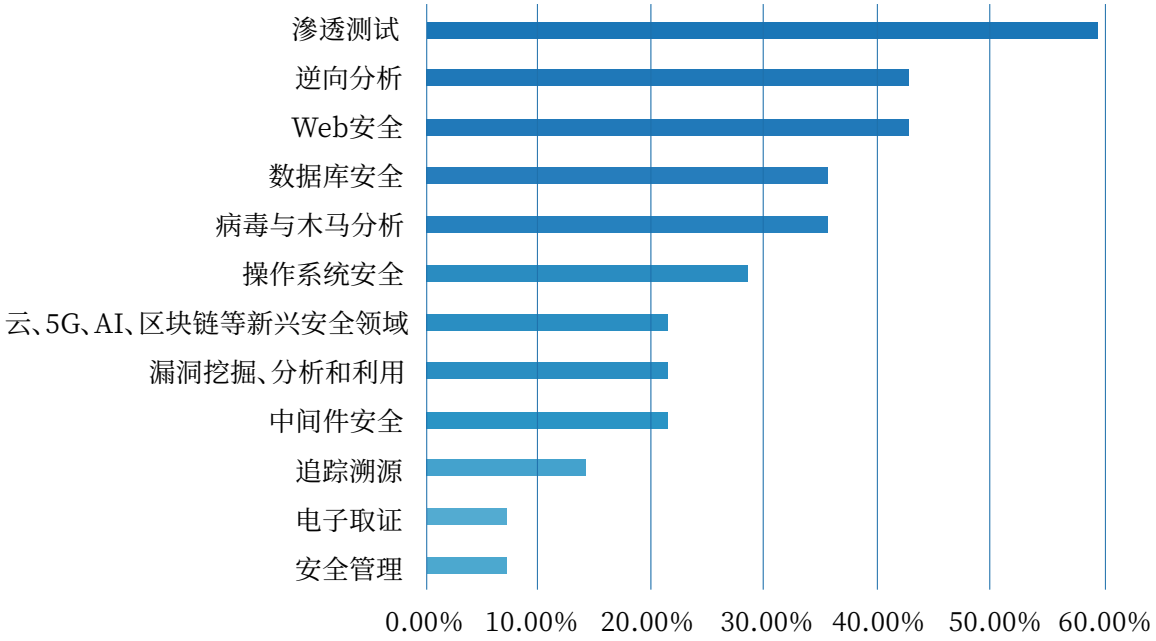


图3-7医疗卫生行业人才能力需求占比情况

(4)教育行业人才需求

根据调查数据分析，教育行业对病毒与木马分析、渗透测试方向网络安全能力需求最为明显，均占比38%，对漏洞挖掘、分析和利用，逆向分析，Web安全方向网络安全能力也有较高需求，占比均超过了30%，如图3-8所示。

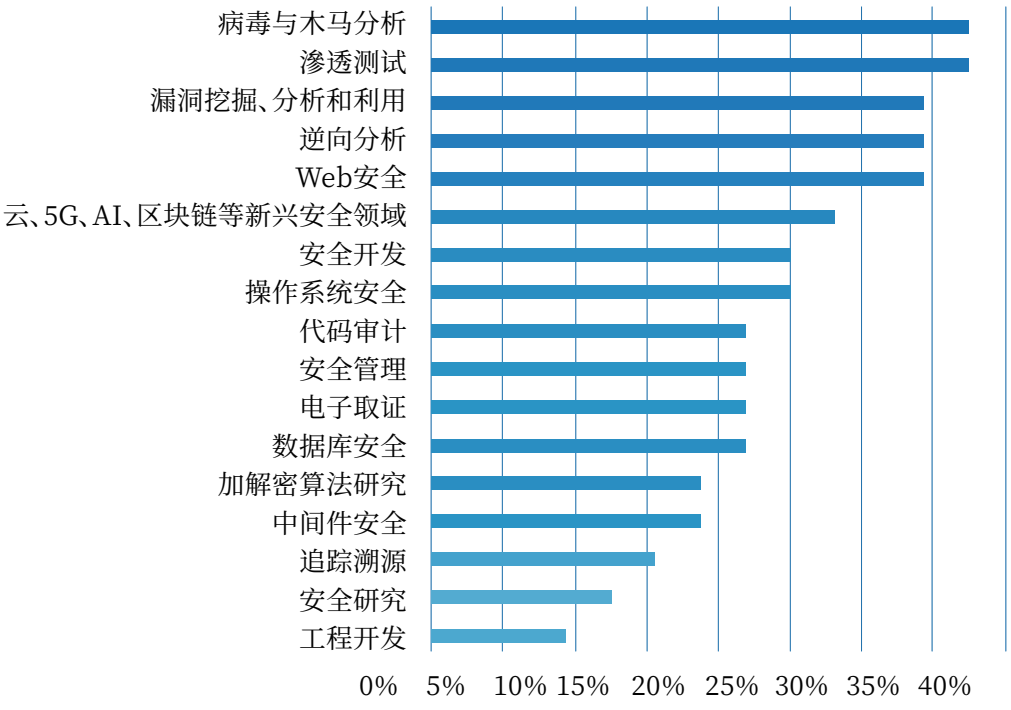


图3-8 教育行业人才能力需求占比情况

(5)互联网行业人才需求

根据调查数据分析,互联网行业36%的单位逆向分析方向网络安全能力需求最为明显,渗透测试方向紧跟其后,占比33%,如图3-9所示。

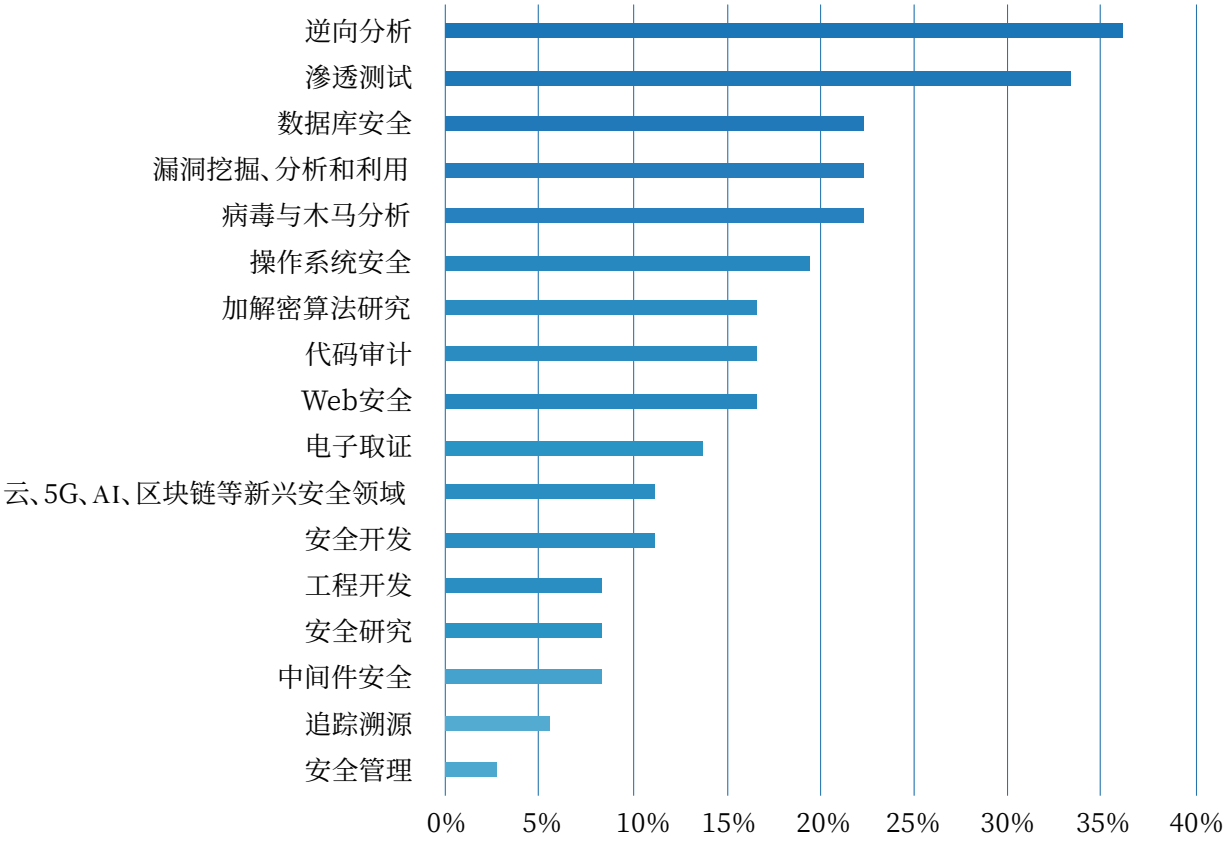


图3-9互联网行业人才能力需求占比情况

根据调查数据,可以看到金融、医疗卫生、教育等行业均在网络安全渗透测试方向有明显需求,对Web安全方向能力、逆向分析能力等均有较高需求,这也与当前APT攻击持续走高导致这几个行业成数据泄露重灾区有关;通信行业、互联网行业的网络安全实战能力需求则主要体现在逆向分析方向,这与通信网络、互联网面临的网络对抗、信息泄露、数据完整性破坏、非授权使用和抵赖等安全需求有关。此外,相较于其他行业而言,通信行业对代码审计方向,云、5G、AI、区块链等新兴安全领域方向,病毒与木马分析方向能力提出了较高需求。

3.1.3按企业性质/规模维度分析

从企业性质维度来看不难发现,“民营企业”对网络安全人才的需求量占比最高,为45%,“央企/国有企业”占比为18%,紧随其后的是“国家行政机关”、“事业单位”、“高校/科研院所”,其网络安全人才需求占比均为9%,如图3-10所示。

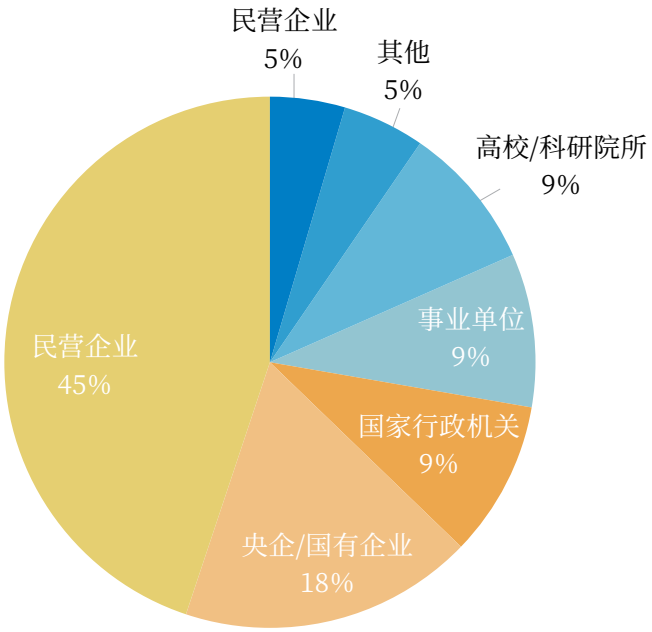


图3-10企业性质统计情况

同时，进一步分析企业人员规模对网络安全人才需求的变化时可以发现，人员规模在“1000人以上”的企业对网络安全人才的需求量最大，占比为29%，其次是“101-300人”的中小企业，其网络安全人才需求占比为18%，人员规模在“301-500人”与“501-1000人”的企业对网络安全人才需求相差不大，分别为13%、12%，如图3-11所示。

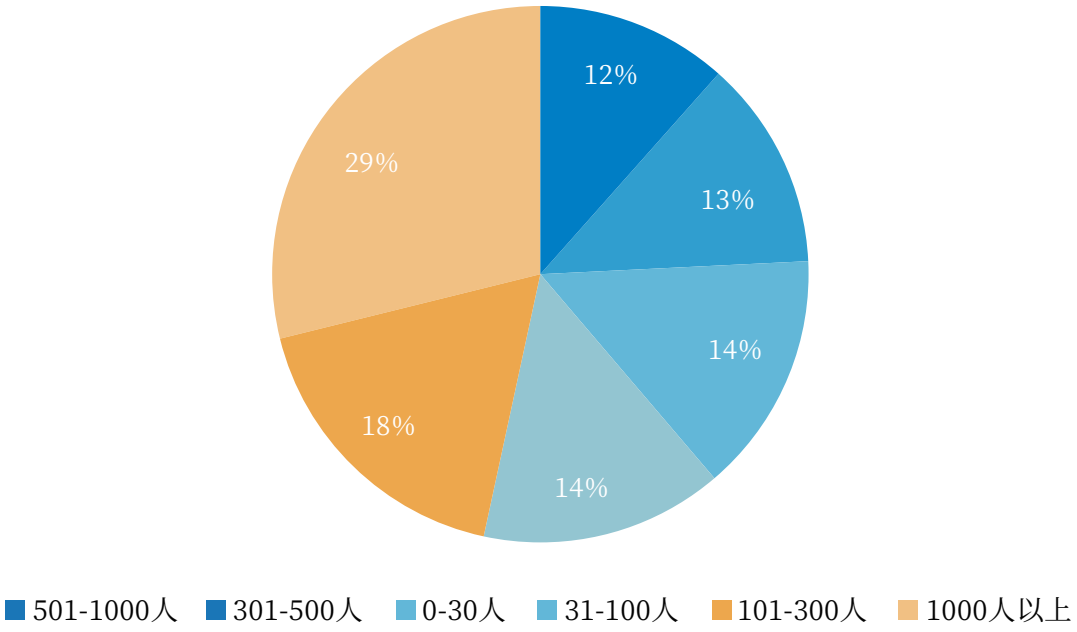


图3-11企业规模统计情况

3.2 岗位需求

3.2.1岗位基本要求

从网络安全攻防实战人才的年龄需求分布情况看，35岁以下（含35岁）人员占比为84%，表明从事网络攻防实战的人员以年轻力量为主。根据统计分析可知，28-35岁这一年龄段的人员更具挑战精神，抗压能力和学习能力更强，更受用人单位的青睐，同时也说明国家培养了更多的网络安全新生力量，如图3-12所示。

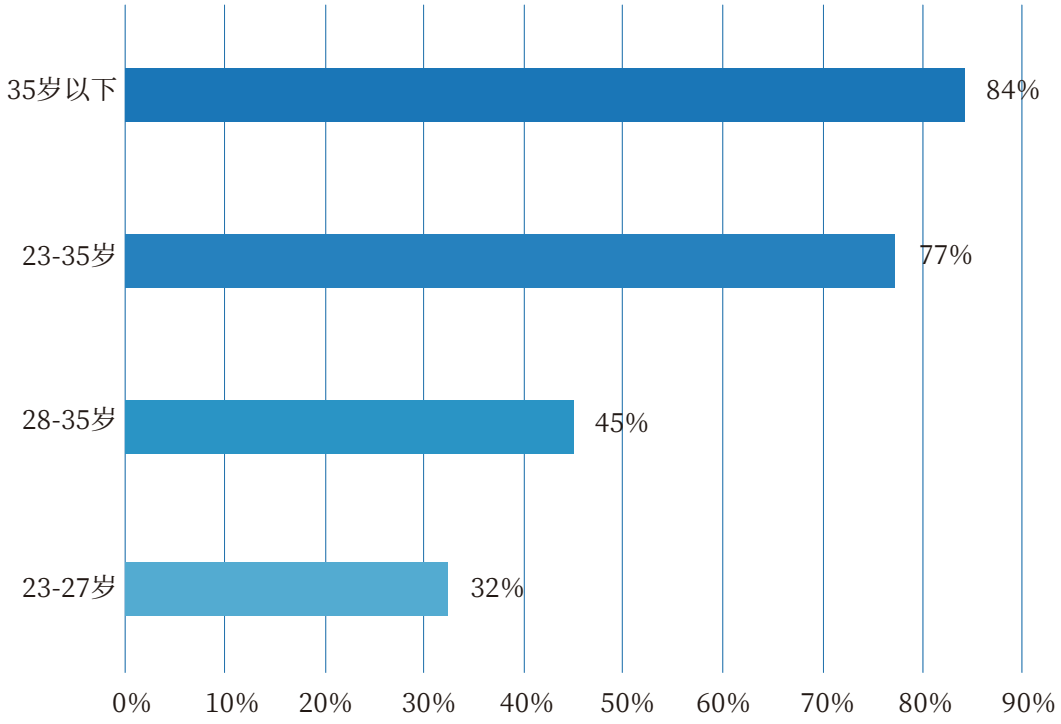


图3-12网络安全人才年龄分布

从网络安全攻防实战人才的学历需求分布情况看，本科占比64.5%。表明现阶段本科学历是大多数用人单位招聘攻防实战人员的基本要求，对于攻防实战人才更注重攻防工具、方法的应用。用人单位将对攻防实战人才的网络安全能力提出更高要求，未来一段时间，用人单位对于具备对抗博弈理论、战略战术研究方面人员需求将会有所上升，随之网络安全教育会进一步深入，为用人单位提供更多高学历的人才，如图3-13所示。

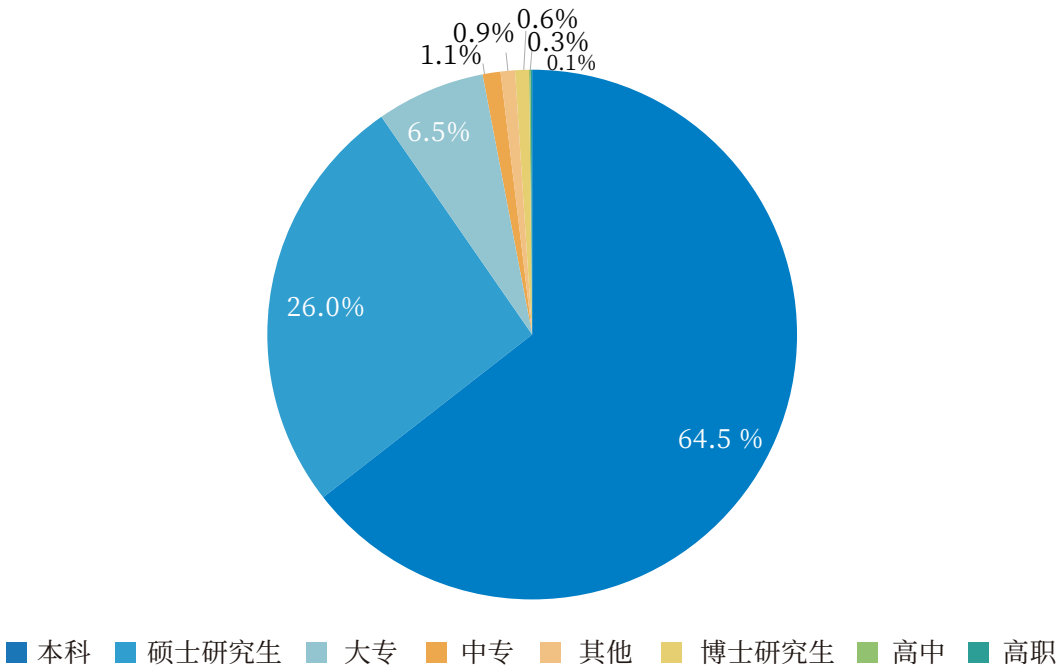


图3-13网络安全人才学历情况

从网络安全攻防实战人才工作年限需求分布情况看，拥有5-10年经验人才需求量最大，占比为25%。其次工作年限为1-3年和3-5年的人才，占比为20%。工作年限10年以上的占18%。工作年限1年以内的占比17%。上述数据说明，用人单位对于5-10年的实战经验的人才更为青睐。由于从事网络安全攻防工作5-10年的人员，对网络安全有深入的理解，同时具有丰富的攻防实战经验，熟练使用渗透测试工具、密码算法以及逆向分析工具，更能满足用人单位的用人需求，如图3-14所示。

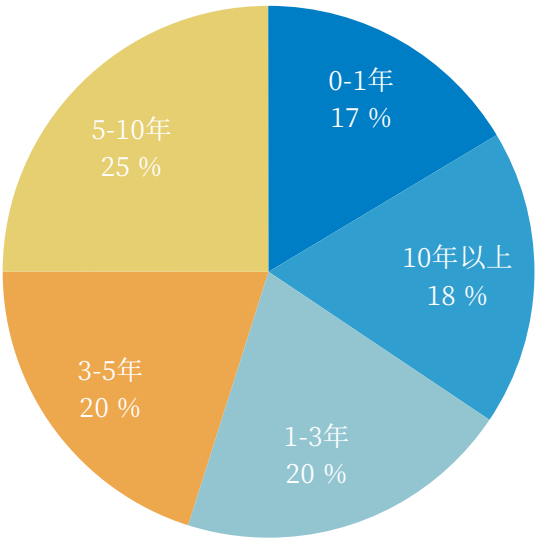


图3-14网络安全人才工作年限情况

从网络安全攻防实战人才技能需求分布情况看，渗透测试方向的技能与能力更受用人单位青睐，而这与渗透测试能力可以较为全面的体现人才的综合实战能力紧密相关。该类人才不仅在重大活动保障、重大项目技术推进、攻防演练、应急处置，还是在日常安全测试等方面都能够发挥作用，对于提升整体安全防护的各方面都能发挥作用。

此外，网络安全领域权威证书作为网络安全攻防实战人才能力的认证，证明网络安全人才具备系统化信息安全知识和一定的实操能力，24%的用人单位在遴选优秀人才的时候会作为标准之一。取得网络安全领域权威证书的人员，更有机会从众多候选人中脱颖而出。同时表明用人单位对安全人员学习能力、综合运用以及实战化方面提出了更高要求，如图3-15所示。

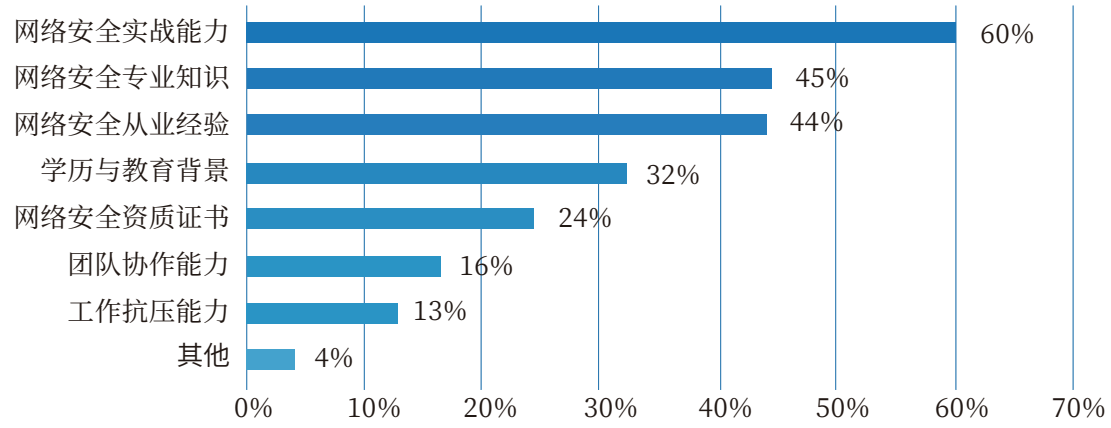


图3-15 用人单位招聘网络安全人员看重的方面

3.2.2岗位基本需求

对用人单位网络安全人员编制情况分析，82%的用人单位设置了网络安全专职岗位。只是在这些用人单位中，岗位编 制符合实际情况、员工各司其职的占比仅为32%，大部分单位的人员还是不能满足需求的，其中有安排编制，但人员招募困难的占比15%；编制不足，存在一人多职情况的占比25%；编制严重欠缺，员工普遍一人多职的占比也达到了11%。

分析上述数据发现，在关基保护和等保2.0的安全防护要求下，用人单位更加重视信息系统的安全建设与维护，更多的用人单位倾向于设置专职安全岗位负责业务系统安全保障。同时，在后疫情时期，为了个人能力的持续沉淀积累，网络安全人才更倾向于长期、稳定的专职岗位，如图3-16所示。

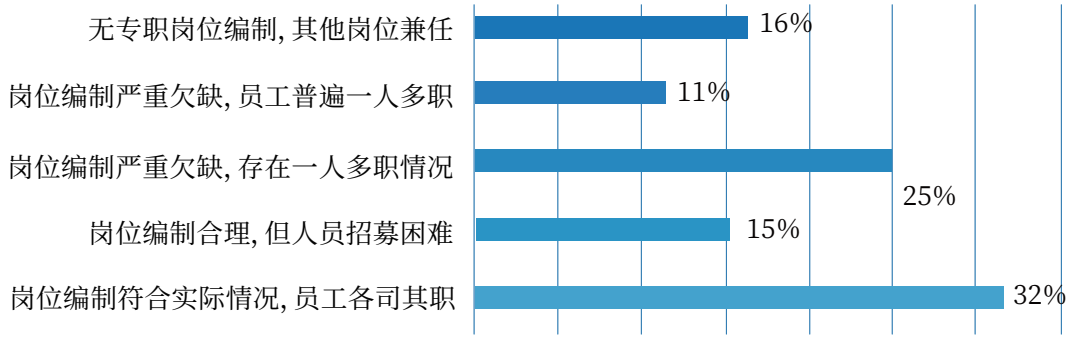


图3-16岗位编制情况

从关键信息基础设施单位的专职人员队伍规模来看，70%的关键信息基础设施单位，网络安全队伍规模不足10人。其中27%的单位无专职人员，29%的单位在1~5人，15%的单位在6~10人，如图3-17所示。

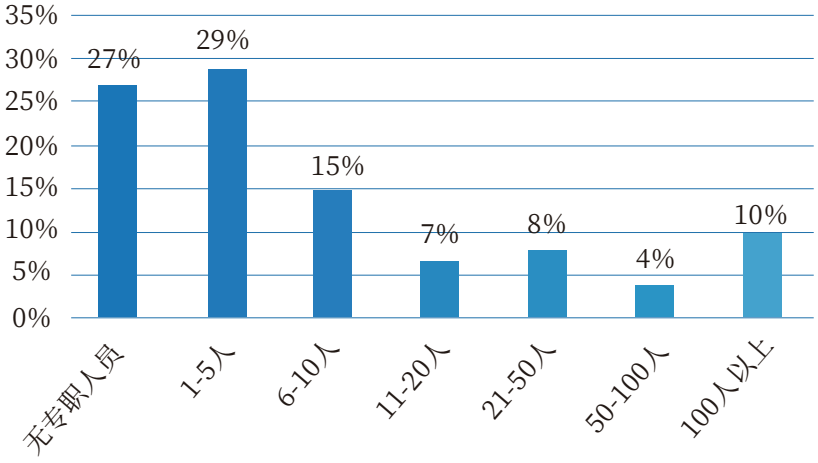


图3-17关键信息基础设施单位安全队伍建设规模占比

从总体用人单位专职人员队伍规模来看，安全团队规模两级分化比较明显，在1~5人的占比最高，达23%，100以上规模的占比也达到了18%，中间规模的团队占比比较集中，在10%左右，如图3-18所示。

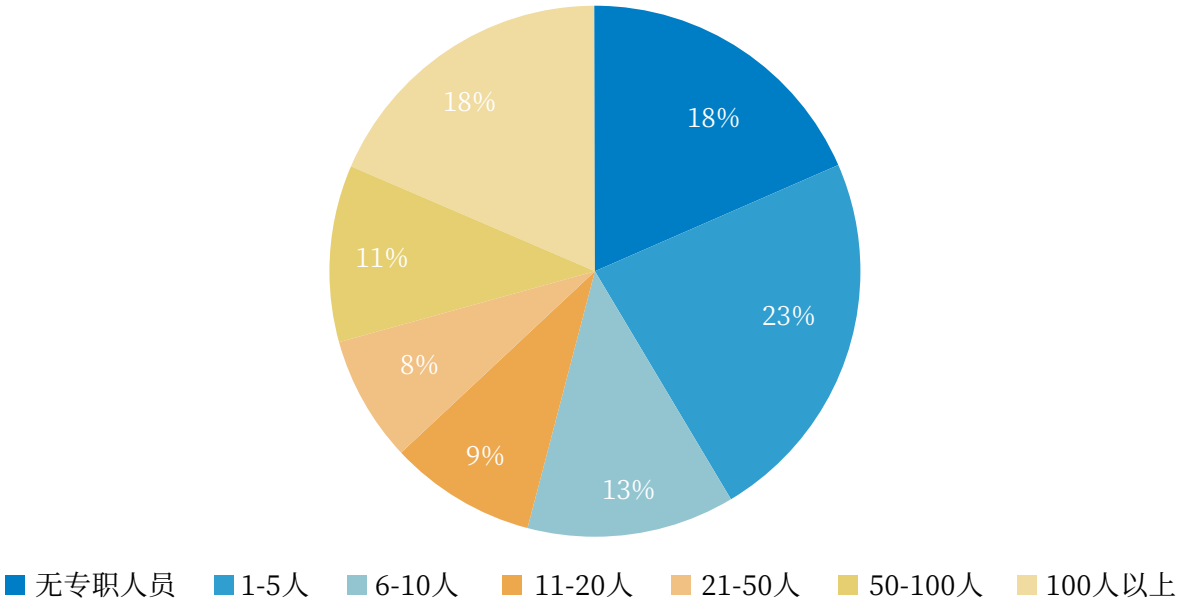


图3-18网络安全专职队伍规模

从用人单位最紧缺的网络安全攻防实战人员调查情况看，渗透测试、漏洞发现与利用和逆向分析技能缺口较大，分别占比40%、33%和32%，如图3-19所示。具备上述技能的人才对用人单位来说炙手可热。由于具有丰富渗透测试经验的人员擅长全面检验信息系统，发现信息系统的脆弱点；具有丰富逆向分析经验的人员可通过反编译手段分析程序的执行逻辑，挖掘应用程序存在的逻辑缺陷；有丰富漏洞发现与利用经验的人员可全面评估信息系统面临的安全风险，以及在遭受攻击时产生的后果及代价。

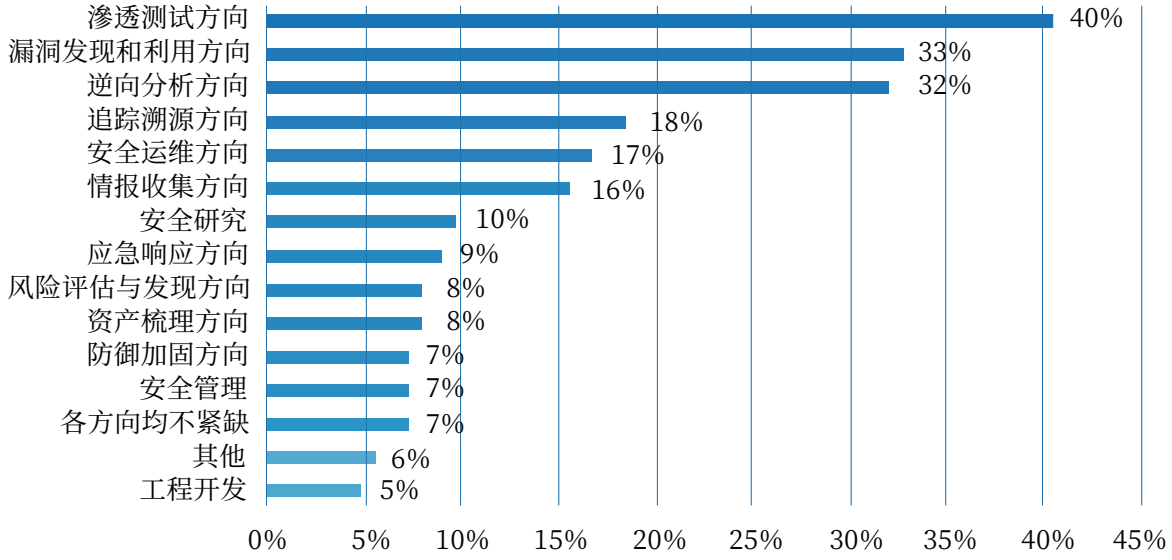


图3-19用人单位紧缺的实战人员技能方向

我国的网络安全发展与攻防实战人才培养的速度仍然存在较大差距。同时攻防人才发展存在明显的专业倾向性，从长远来看，复合型人才将占据更大比重，复合型攻防人才将是未来人才培养的重要方向。

3.3 岗位与能力匹配分析

3.3.1岗位人才分布

从统计数据上来看，网络安全岗位类别主要分为安全管理岗、安全建设岗、安全运营岗、测试评估岗、科研教育岗五种类型，具备网络安全人才攻防实战能力的人群以安全运营岗与测试评估岗居多，其余三种从人数上来看相对较少，如图3-20所示。

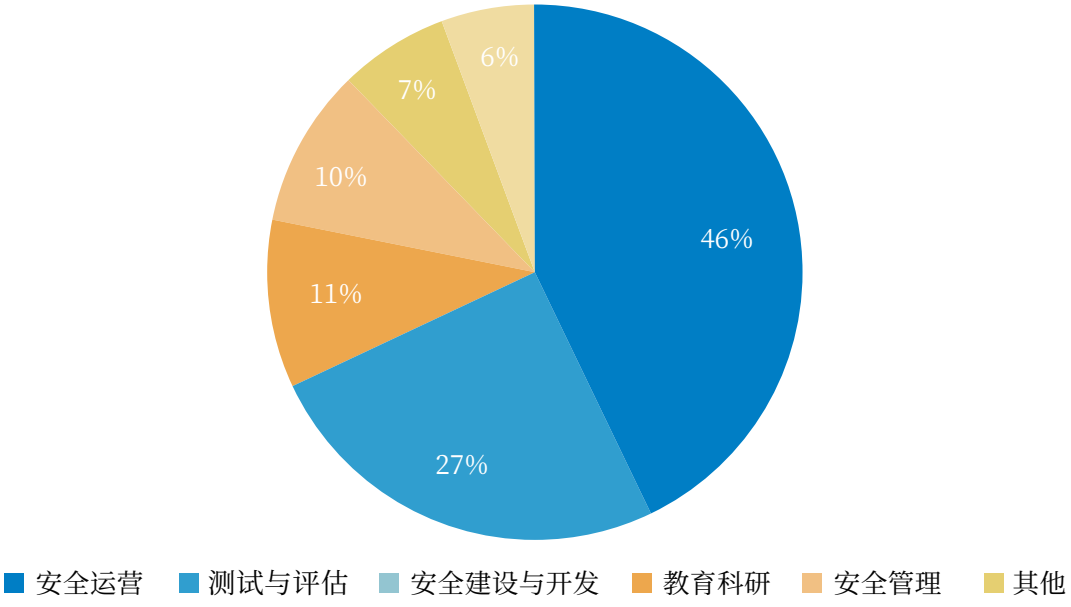


图3-20岗位类型分布

从统计数据来看，网络安全行业岗位名称很多，各用人单位会根据自身情况有不同的叫法，归纳整理来看，具备攻防实战能力的岗位主要集中在运维工程师、安全服务工程师、安全运营工程师、渗透测试工程师等。其中，运维工程师数量最多，占比达26%，排名第二的是安全服务工程师，紧随其后的是安全运营工程师，如图3-21所示。

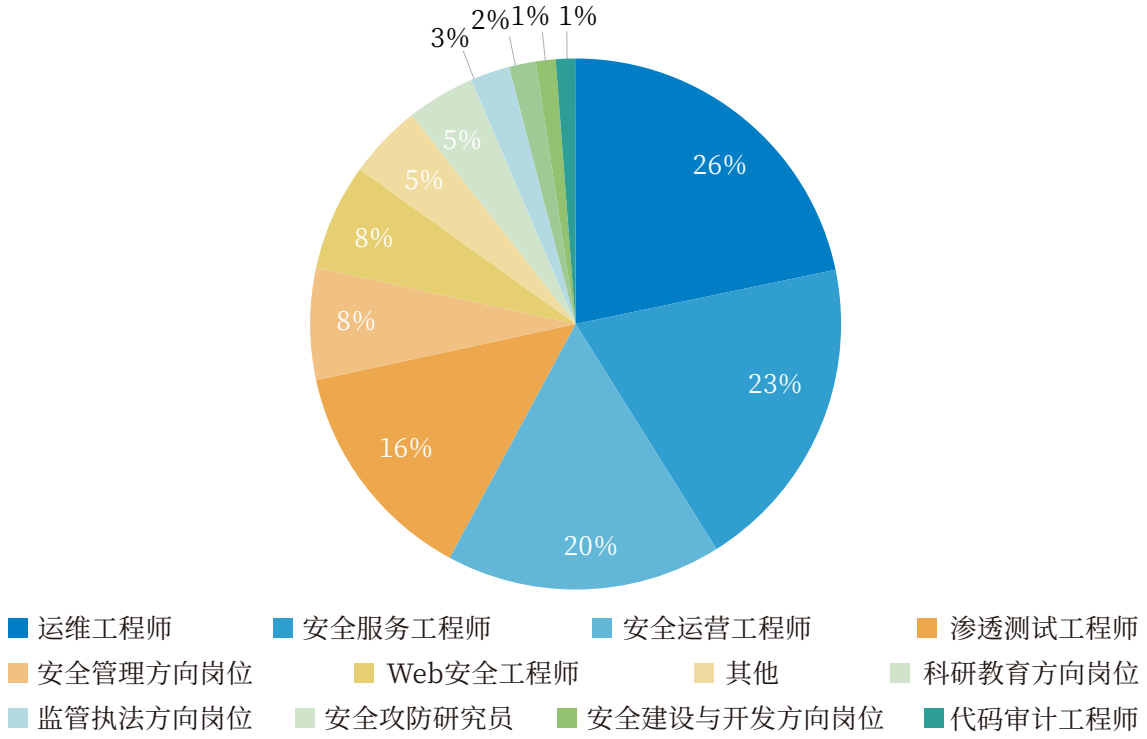


图3-21岗位分布

3.3.2岗位能力需求

根据调查数据分析，在岗员工主要的安全实战能力方向体现在：渗透测试、漏洞发现与利用、安全运维、应急响应、风险评估与发现、资产梳理、追踪溯源、情报收集、安全研究、防御加固、逆向分析等，如图3-22所示。

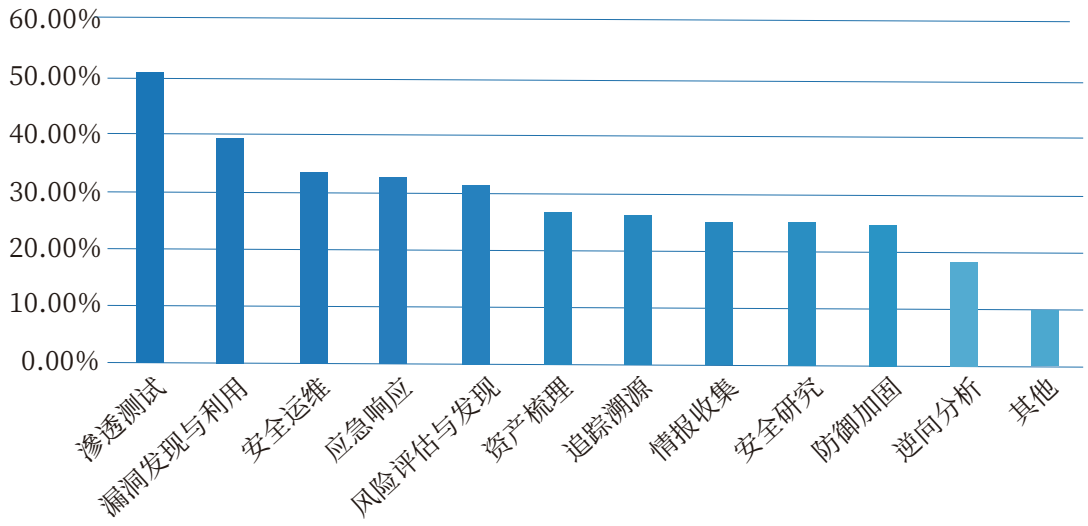


图3-22主要实战方向

其中，Web安全工程师更为看重渗透测试方向网络安全能力，其次是逆向分析能力、Web安全能力。Web安全工程师岗位目前亟需提升的网络安全能力中，渗透测试能力占比65%，逆向分析能力占比48%，Web安全能力占比39%，如图3-22所示。

渗透测试工程师更为看重渗透测试方向网络安全能力，其次是代码审计和逆向分析，对云、5G、AI、区块链等新兴安全领域方向网络安全能力也有较高需求。渗透测试工程师岗位目前亟需提升的网络安全能力中，渗透测试能力占比58%，代码审计能力占比50%，逆向分析能力占比42%，云、5G、AI、区块链等新兴安全领域能力占比38%，如图3-22所示。

运维工程师对渗透测试、Web安全、安全管理方向网络安全能力需求最为明显。运维工程师岗位目前亟需提升的网络安全能力中，渗透测试能力占比54%，Web安全能力占比42%，安全管理能力占比38%，如图3-22所示。

安全服务工程师岗位对渗透测试方向网络安全能力需求最为明显，对漏洞挖掘、分析和利用，病毒与木马分析，Web安全方向网络安全能力也有较高需求。安全服务工程师岗位目前亟需提升的网络安全能力中，渗透测试能力占比59%，漏洞挖掘、分析和利用，病毒与木马分析，Web安全能力均占比38%，如图3-22所示。

安全运维工程师岗位对漏洞挖掘、分析和利用方向网络安全能力需求最为明显，对渗透测试，云、5G、AI、区块链等新兴安全领域方向网络安全能力也有较高需求。安全运维工程师岗位目前亟需提升的网络安全能力中，漏洞挖掘、分析和利用能力，渗透测试能力均占比58%；云、5G、AI、区块链等新兴安全领域能力占比53%，如图3-22所示。

安全运营工程师对渗透测试方向网络安全能力需求最为明显。安全运营工程师岗位目前亟需提升的网络安全能力中，渗透测试能力占比44%。安全攻防研究员岗位对漏洞挖掘、分析和利用方向网络安全能力需求最为明显，对病毒与木马分析、中间件安全方向网络安全能力也有较高需求，如图3-22所示。

安全攻防研究员岗位目前亟需提升的网络安全能力中，漏洞挖掘、分析和利用能力占比73%，病毒与木马分析能力占比47%，中间件安全能力占比40%，如图3-22所示。

安全管理方向岗位对安全管理方向网络安全能力需求最为明显，对渗透测试、安全研究方向网络安全能力也有较高需求。安全管理方向岗位人才目前亟需提升的网络安全能力中，安全管理能力占比61%，渗透测试能力占比57%，安全研究能力占比35%。

监管执法方向岗位对逆向分析方向网络安全能力需求最为明显，对渗透测试、病毒与木马分析安全研究方向网络安全能力也有较高需求。监管执法方向岗位人才认为目前亟需提升的网络安全能力中，逆向分析能力占比78%，渗透测试能力、病毒与木马分析能力均占比67%，如图3-22所示。

科研教育方向岗位对逆向分析，操作系统安全，数据库安全，云、5G、AI、区块链等新兴安全领域方向网络安全能力需求最为明显。科研教育方向岗位人才认为目前亟需提升的网络安全能力中，逆向分析，操作系统安全，数据库安全，云、5G、AI、区块链等新兴安全领域方向能力均占比43%，如图3-23所示。

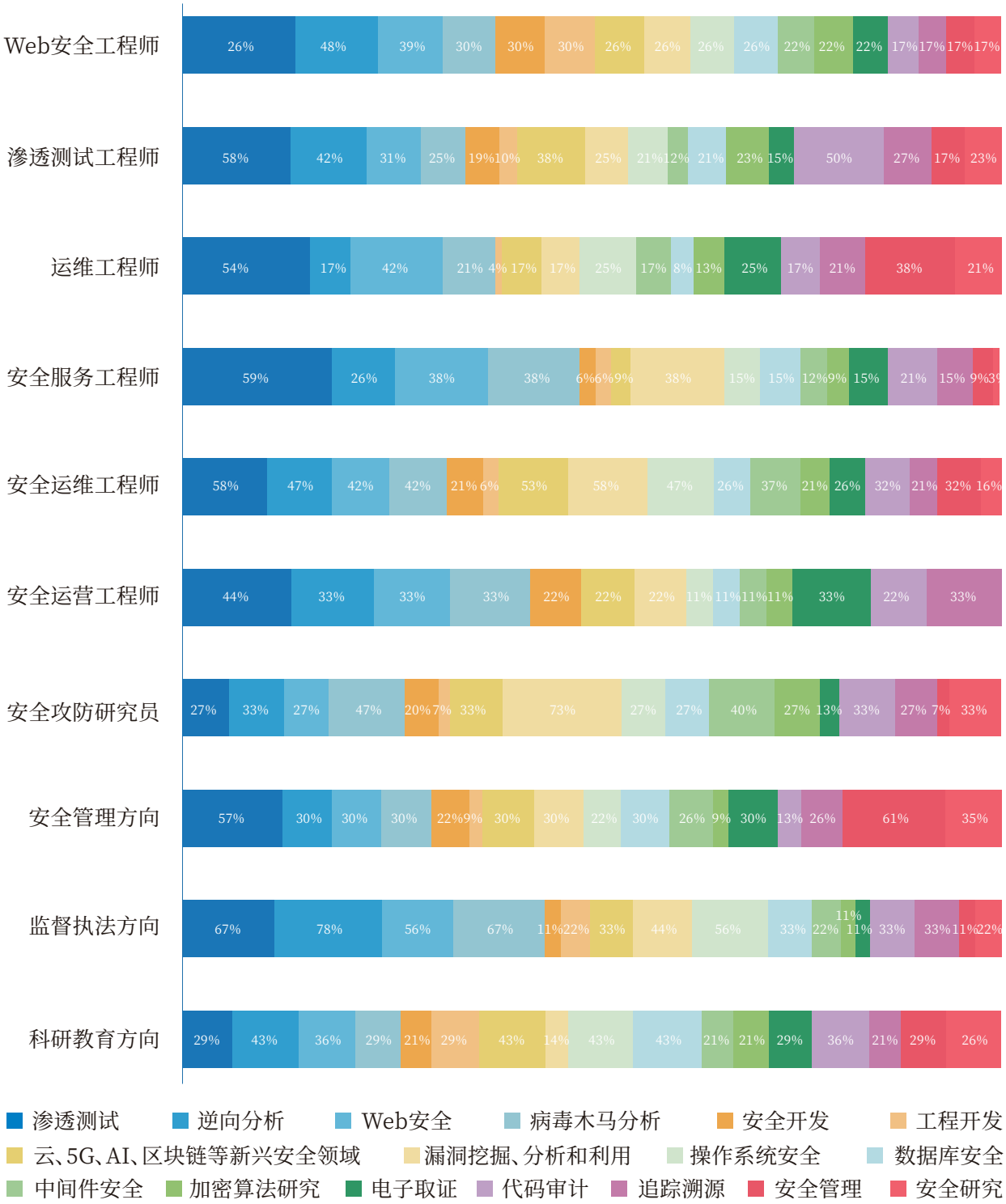


图3-23各岗位专业能力需求情况

根据调查数据，可以看到Web安全工程师、安全服务工程师、安全运营工程师、渗透测试工程师均对渗透测试方向网络安全能力需求最为明显；安全攻防研究员、安全运维工程师均对漏洞挖掘、分析和利用方向能力需求最为明显；安全管理方向岗位、运维工程师均对安全管理方向网络安全能力需求最为明显；监管执法方向、科研教育方向岗位均对逆向分析方向网络安全能力需求最为明显。

此外，Web安全工程师、渗透测试方向岗位均对逆向分析有较高需求；安全管理方向岗位、安全运维工程师、监管执法方向岗位均对渗透测试方向网络安全能力有较高需求；Web安全工程师、安全服务工程师、运维工程师均对Web安全方向网络安全能力有较高需求；安全服务工程师、安全攻防研究员、监管执法方向岗位均对病毒与木马分析方向网络安全能力有较高需求；安全运维工程师、科研教育方向岗位、渗透测试方向岗位均对云、5G、AI、区块链等新兴安全领域方向网络安全能力有较高需求。

相较于其他岗位而言，安全攻防研究员岗位对中间件安全方向网络安全能力有较高需求；安全管理方向岗位对安全研究方向网络安全能力有较高需求；科研教育方向岗位对操作系统安全，数据库安全方向网络安全能力需求有较高需求；渗透测试方向岗位对代码审计方向网络安全能力有较高需求。

3.3.3能力提升需求

根据调查数据分析，仅8%的企业认为集团内部网络安全人员队伍整体较为完善，人员能力也比较综合、全面，暂无需要提升的地方。而大部分用人单位普遍欠缺的业务能力中，逆向分析能力占比35%，其次是渗透测试能力，漏洞挖掘、分析和利用能力，病毒与木马分析能力，分别占比33%、27%、26%，如图3-24所示。

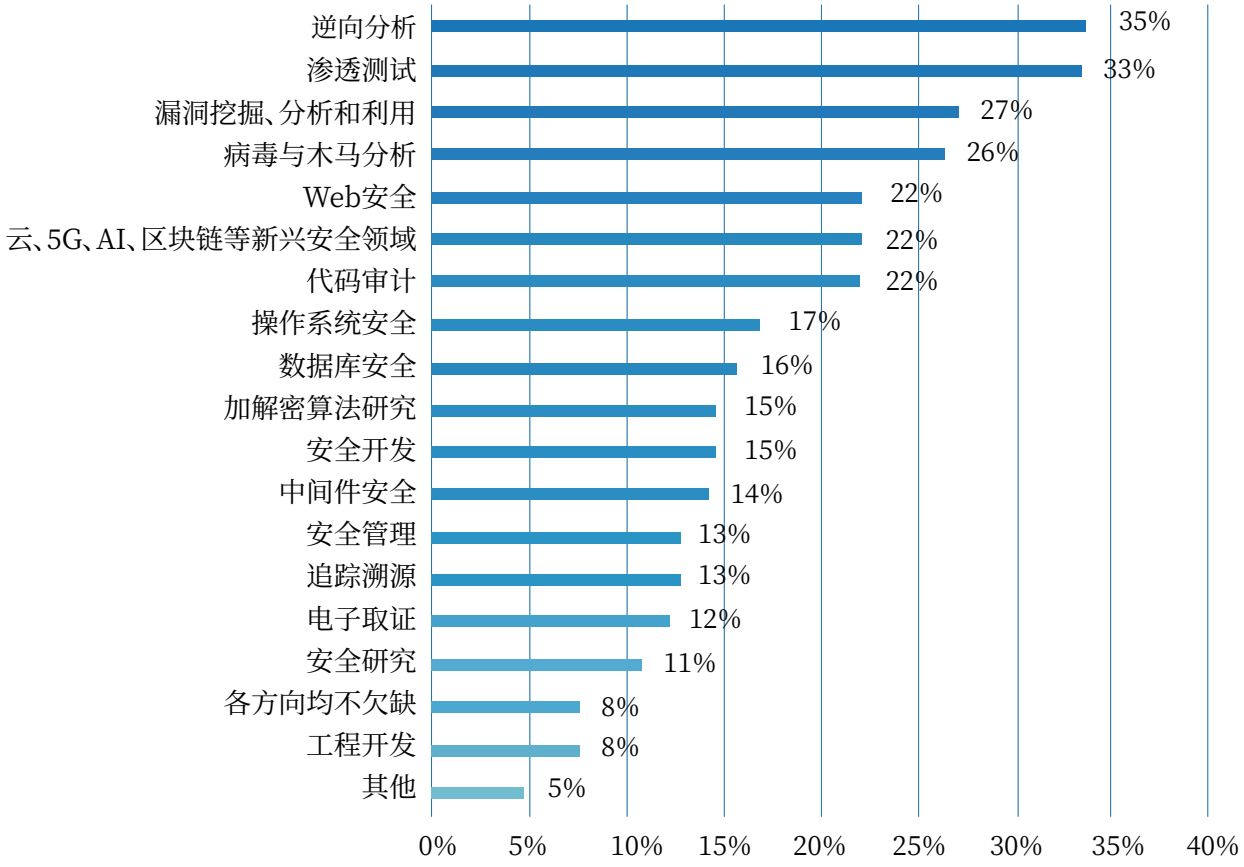


图3-24用人单位普遍欠缺的业务能力

同时，各行业网络安全人才显然也意识到了自己在工作中存在的能力短板，以下仍以金融、通信、医疗卫生、教育、互联网等五个行业为例，分别对其人才能力提升需求进行分析。

（1）金融行业人才能力提升需求

根据调查数据分析，金融行业人才认为目前亟需提升的网络安全专业能力中，渗透测试能力占比60%，Web安全能力占比40%，逆向分析能力占比35%，如图3-25所示。

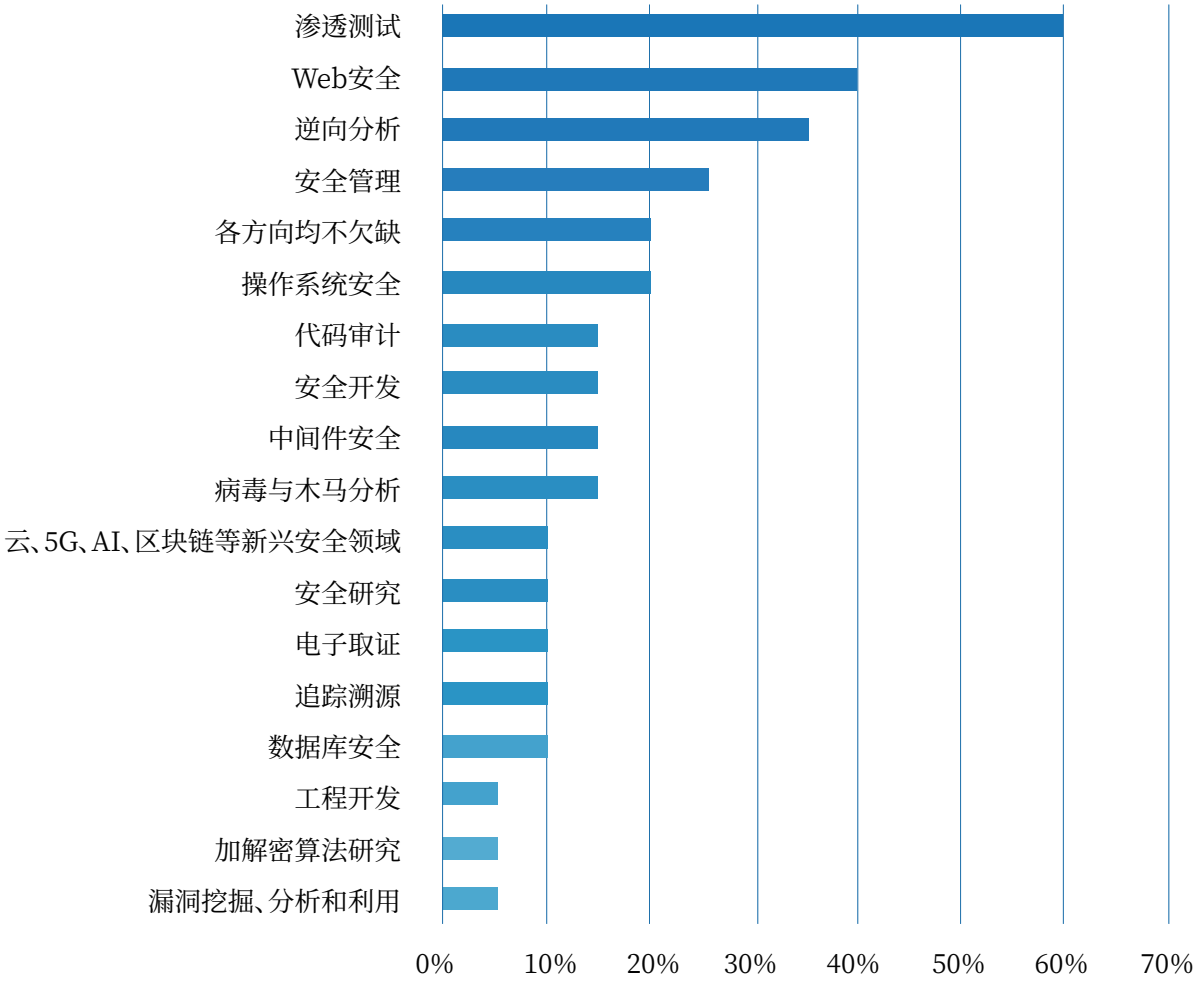


图3-25金融行业人才能力提升需求情况

（2）通信行业人才能力提升需求

根据调查数据分析，通信行业人才认为目前亟需提升的网络安全专业能力中，漏洞挖掘、分析和利用能力占比68%，逆向分析、病毒与木马分析能力均占比59%，云、5G、AI、区块链等新兴安全领域方向、渗透测试能力均占比55%，如图3-26所示。

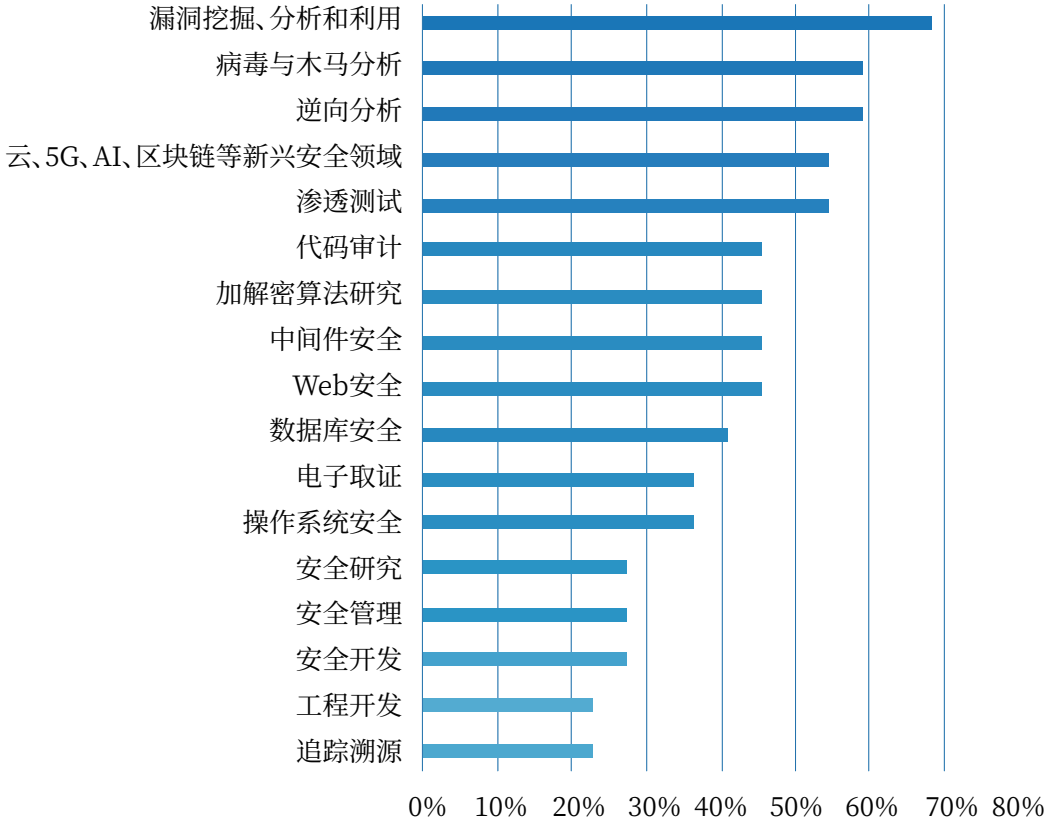


图3-26通信行业人才能力提升需求占比情况

(3)医疗卫生行业人才能力提升需求

根据调查数据分析,医疗卫生行业人才认为目前亟需提升的网络安全专业能力中,渗透测试能力占比50%,逆向分析、数据库安全能力均占比43%,如图3-27所示。

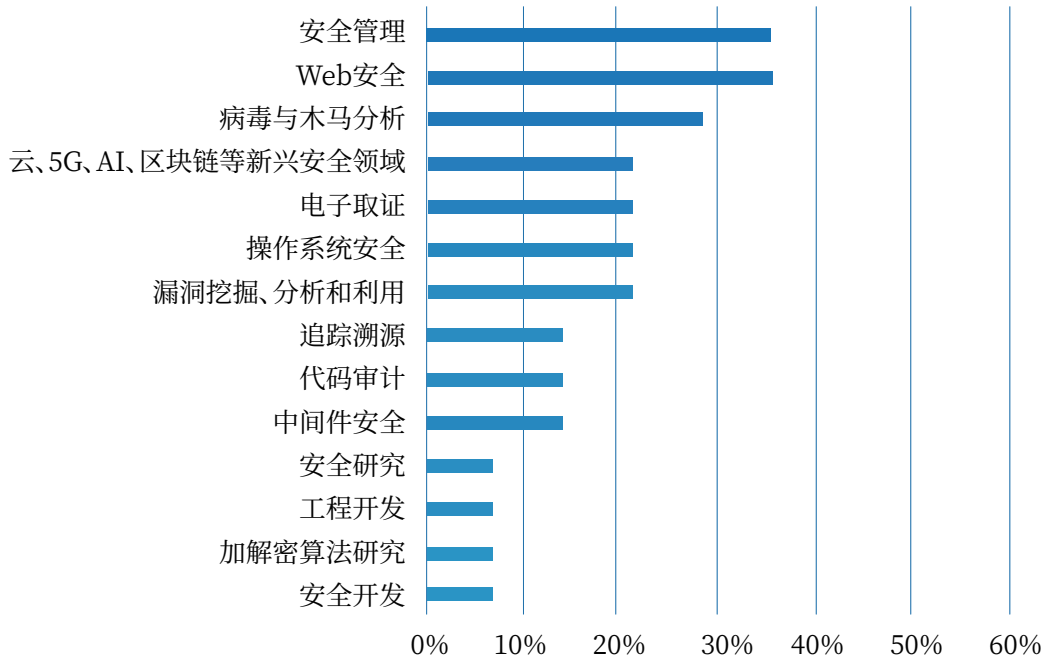


图3-27医疗卫生行业人才能力提升需求情况

(4)教育行业人才能力提升需求

根据调查数据分析，教育行业人才认为目前亟需提升的网络安全专业能力中，渗透测试能力占比38%，Web安全和操作系统安全能力均占比34%，如图3-28所示。

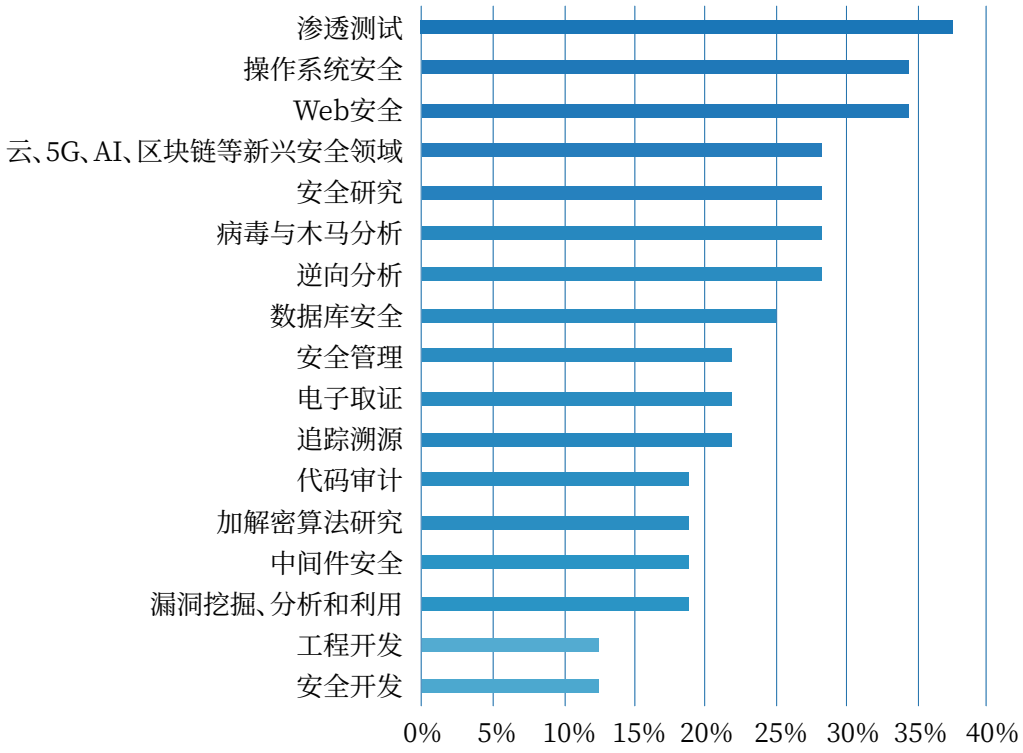


图3-28教育行业人才能力提升需求情况

(5)互联网行业人才能力提升需求

根据调查数据分析，互联网行业人才认为目前亟需提升的网络安全专业能力中，渗透测试能力占比67%，Web安全能力占比50%，逆向分析能力占比42%，如图3-29所示。

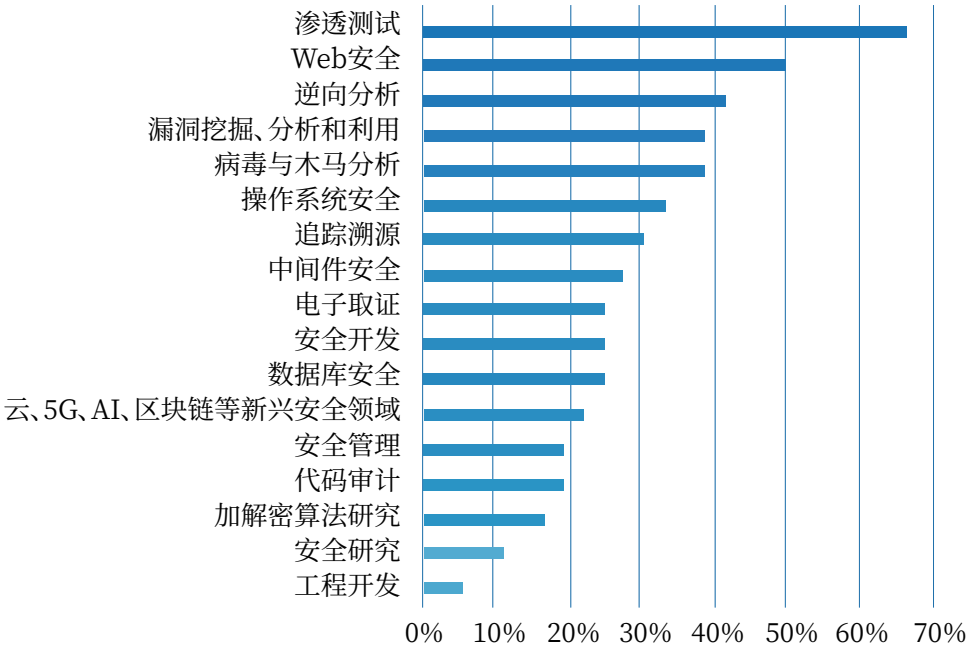


图3-29互联网行业人才能力提升需求情况

网络安全工作是一个系统性工程，根据数据统计分析，如下图3-30所示，用人单位在提升整体安全防护水平方面最为看重且最为有效的方式是构建完善的网络安全人才队伍，其次是充足的网络安全设备和覆盖全员的网络安全意识，接下来是体系化的网络安全人才培训，各个方面统筹布局才能更好的达到安全防御效果。

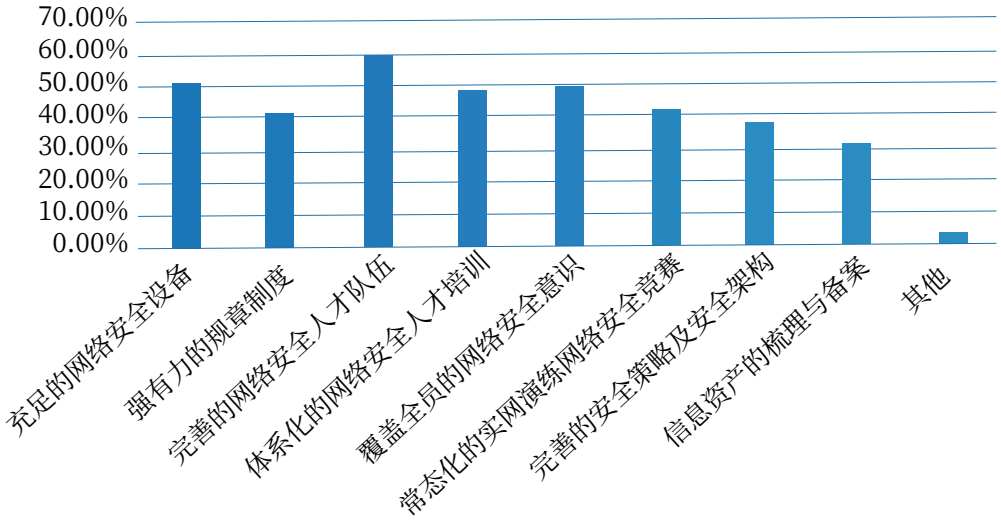


图3-30用人单位提升整体防护水平的措施情况

3.4人员来源分析

超过60%的用人单位在招聘网络安全人员时比较看重网络安全实战能力，超过40%的单位重视网络安全从业经验与网络安全专业知识，其次是学历和教育背景、网络安全资质证书、团队协作能力和工作抗压能力等，如图3-31所示。

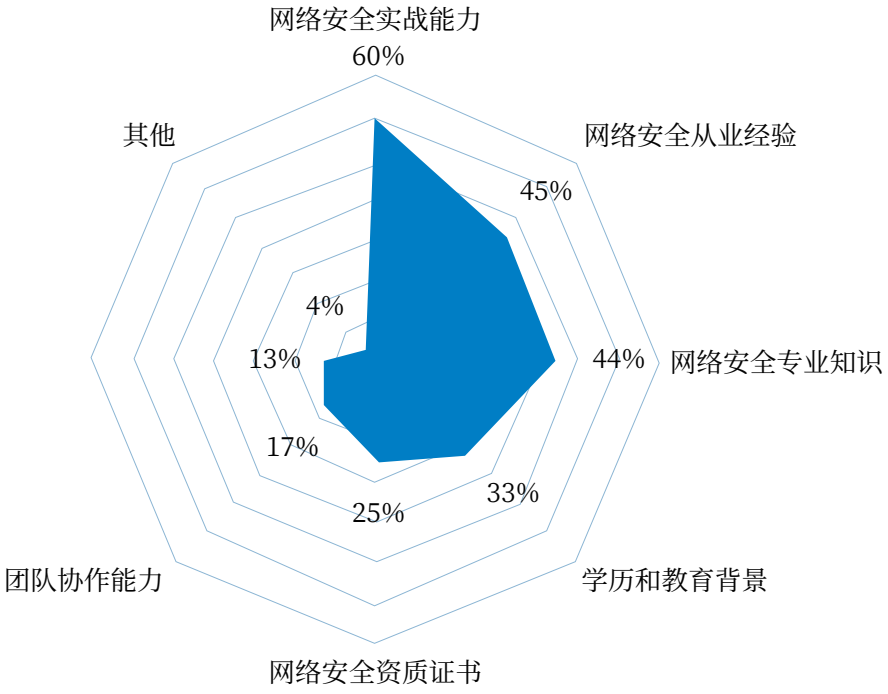


图3-31用人单位招聘网络安全人员时最关注的能力情况

大部分用人单位的人才渠道对招聘网站及校园招聘还是比较依赖，58%的用人单位会通过招聘网站来进行人员招募，45%的用人单位会通过校招来进行人员补充。其次企业内部推荐、业内熟人推荐、猎头推荐等也是常用的人员招募渠道，如图3-32所示。

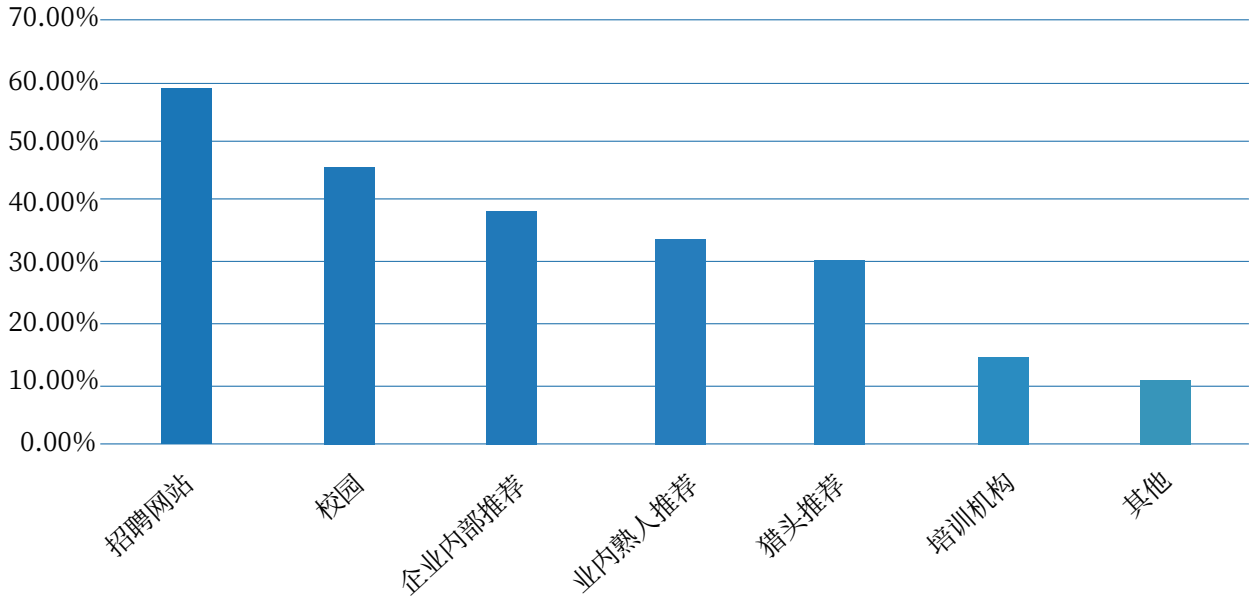


图3-32用人单位招聘渠道情况

用人单位认为最可靠的招聘渠道排名前两名的是，企业内部推荐、业内熟人推荐渠道；其次是校园招聘、招聘网站和猎头机构，如下图3-33所示。其中1000人以上的超大型单位更倾向于企业内部推荐、业内熟人推荐；500-1000人的大型单位、300-500人的中型企业则认为招聘网站及企业内部推荐更为有效。

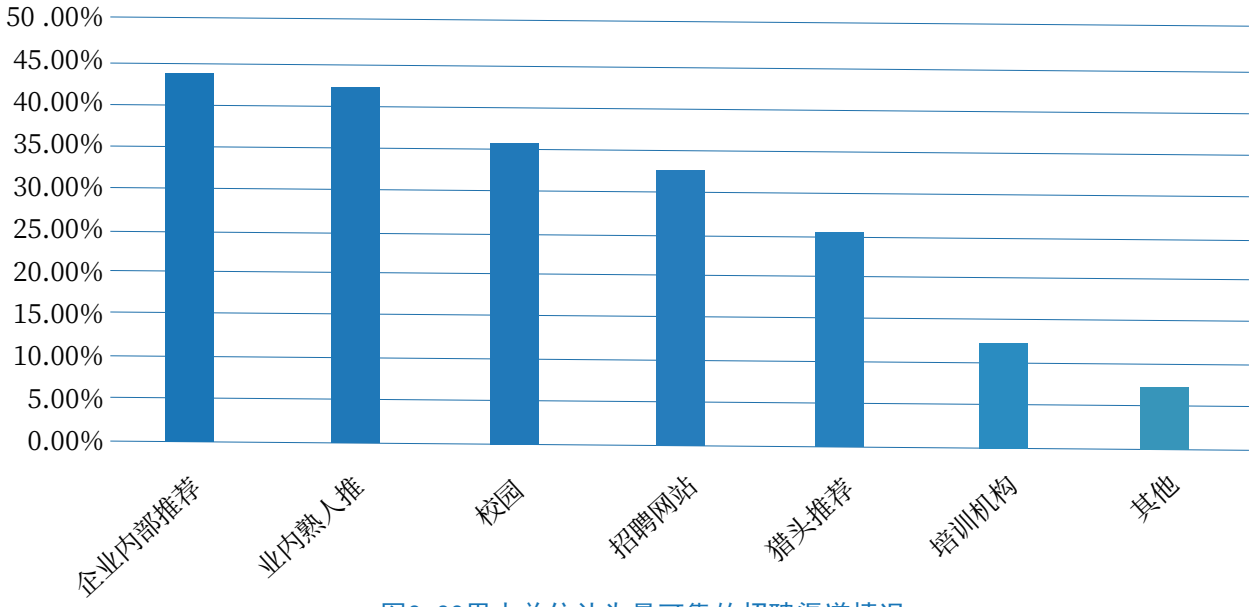


图3-33用人单位认为最可靠的招聘渠道情况

第四章

网络空间安全人才攻防实战能力提升分析

4.1 网络空间安全实战攻防人才培养现状

4.1.1院校网络安全相关专业建设现状

信息化时代到来后，网络应用普及范围日益广泛，随之而来的网络安全问题也越来越多，并呈现出复杂化、多样化、不可预测化的新形态，这对我国的网络安全人才建设提出新的要求。总体而言，我国网络安全人才存在数量缺口较大、能力素质不高、结构不尽合理等问题，有必要完善和优化网络安全课程建设路径，加强网络安全人才建设。

从学科属性看，网络安全作为一门综合性新兴学科，学科交叉性强，导致专业人才培养难度相对较大，周期也长。许多学校除了专门的网络安全相关专业外，还开设了与网络安全相关的一些专业，各专业学科培养侧重点有所不同，可看作网络安全方面的二级专精学科或者交叉学科。针对网络安全领域专业方向特点和发展热度，市场上也越来越有了细分专精的趋势，这也影响了学校的培养方向。经调研，目前我国高校开设的网络安全相关专业主要分为：网络空间安全，信息安全，保密技术，密码科学与技术，区块链工程，网络安全与执法六类，如图4-1所示。

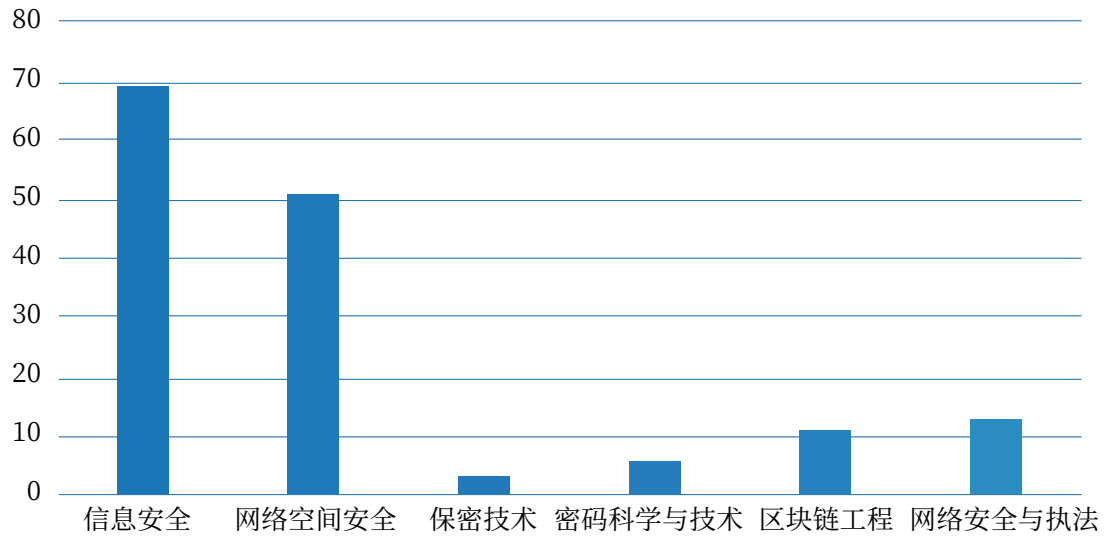


图4-1 网络空间安全相关课程

信息安全是所有网络安全相关课程中开设数量最多的专业，开设的院校包括中国科学技术大学、浙江大学、上海交通大学等69所；其次是网络空间安全专业，共有电子科技大学、华中科技大学、北京邮电大学等51所；开设保密技术的院校数量是所有网络安全相关数最少的，仅包含复旦大学、北京交通大学、湖南大学3所；开设密码科学与技术的高校有6所，全部属于985、211、双一流院校，包括华中科技大学、东南大学、北京邮电大学等；区块链工程仅在太原理工大学、齐鲁工业大学等11所非985、211、双一流的高校所设。网络安全与执法仅在13所公安院校开设，包含中国人民公安大学、浙江警察学院、中国刑事警察学院等。

据统计，在所有开设网络安全相关专业的高校中，双一流院校占比约为57.14%，如图4-2所示。985院校占比约为24.37%，如图4-3所示。

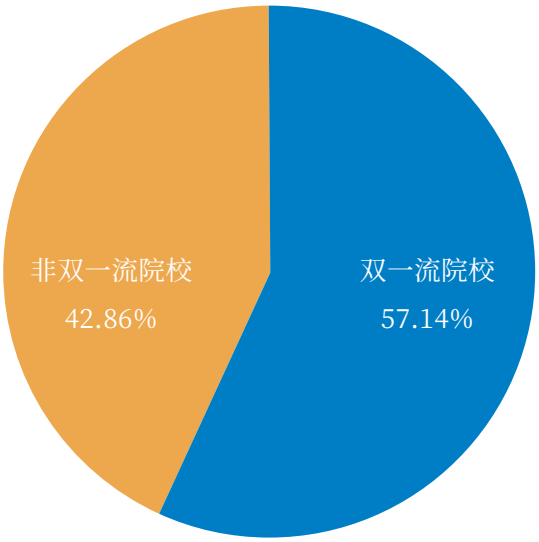


图4-2 双一流院校占比

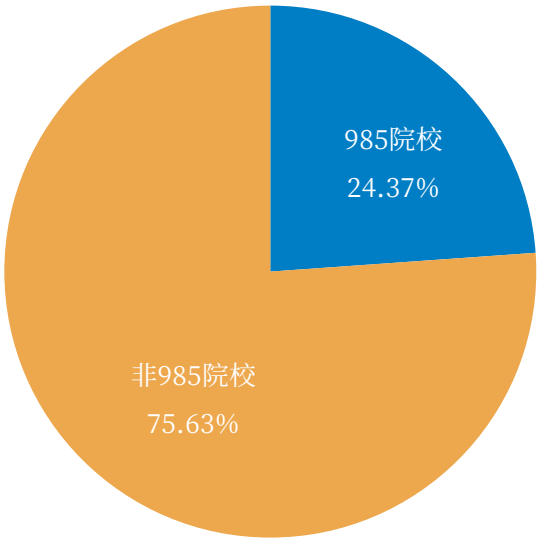


图4-3 985院校占比

在统计结果中，211院校占比超过一半，约为51.25%，如图4-4所示。

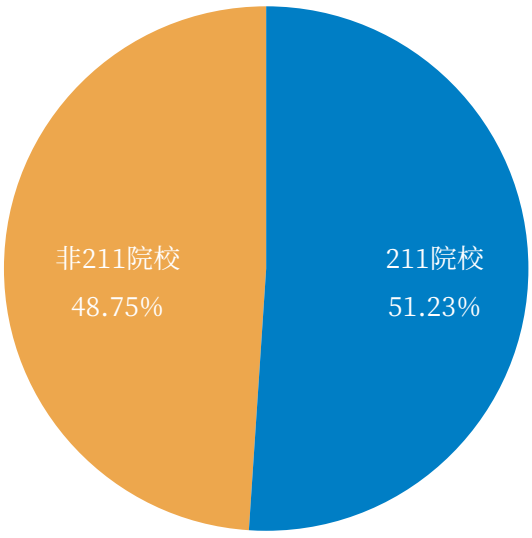


图4-4 211院校占比

其中公安院校的占比情况约为10.01%，如图4-5所示。

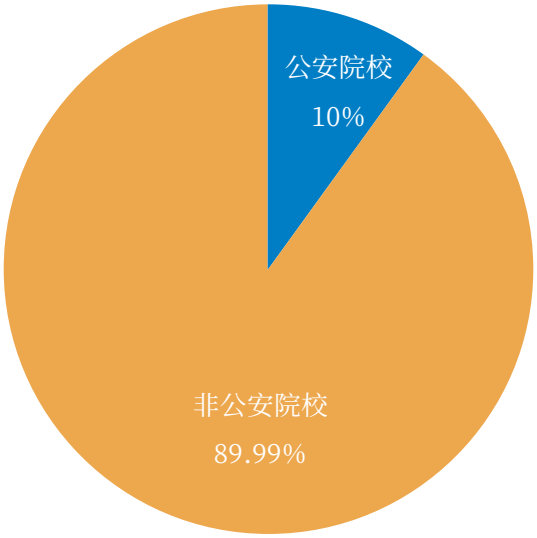


图4-5 公安院校占比

然而从总体上看，我国普通高等学校共2756所（本科1270所、专科1486所），在本科院校中开设网络安全相关专业的院校占比仅为9%，包含专科院校后，占比仅为4%。通过以上数据可以得出结论，目前我国开设网络安全相关课程的高校总数仍然较少，网络安全的教育需要进一步得到重视，如图4-6、4-7、4-8所示。

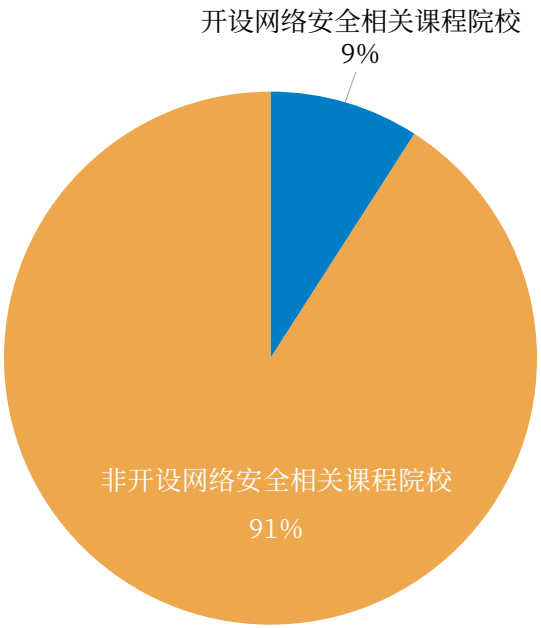


图4-6 全国高校占比（不含专科）

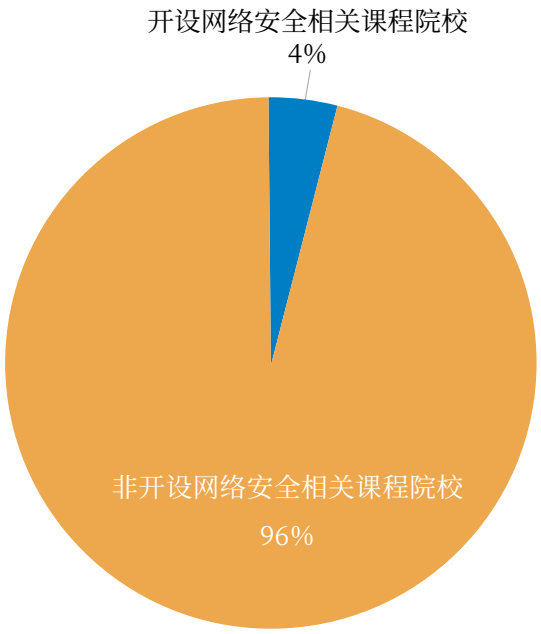


图4-7 全国高校占比（含专科）

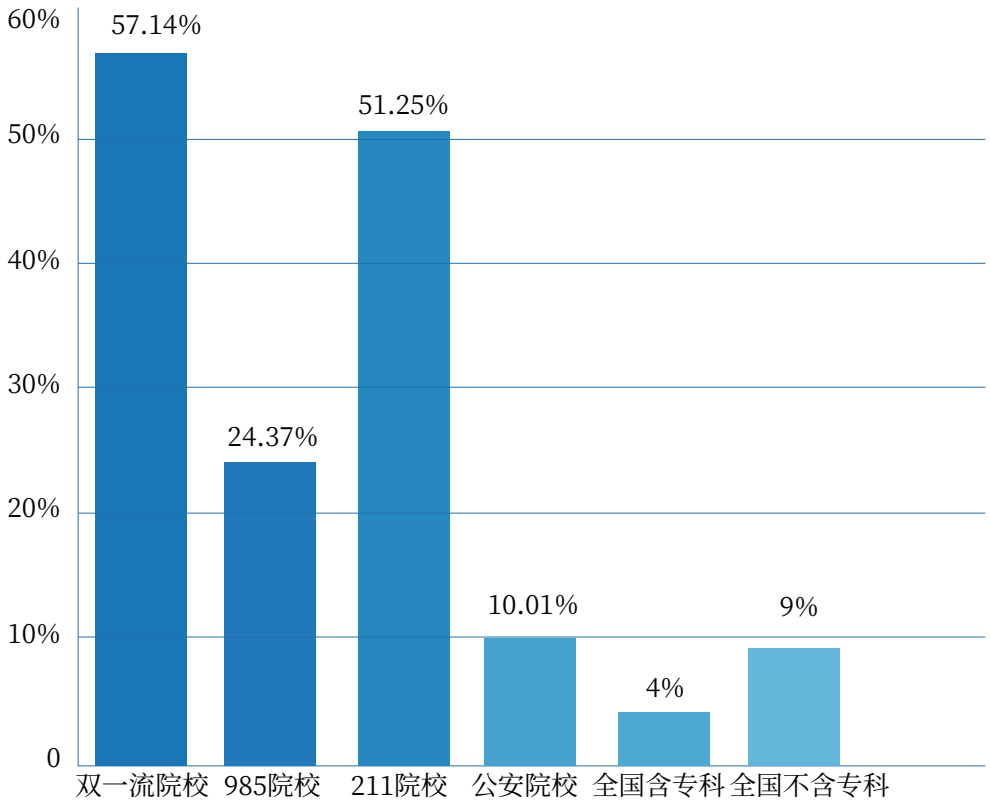


图4-8 各类高校占比

从院校属性看，学校的教育更加侧重打好理论基础，构建知识体系，开阔视野格局，提供资源平台，为国家培养多个层次的网络安全人才。过去学科初建，对于学生攻防实战能力的培养，缺乏足够多的配套资源支持，更多依赖学生自学，算是院校网络安全相关专业能力建设的短板之一。随着培养体系的愈发完善，网络设施更加健全，学习资源的普及，各类比赛增多以及校企结合项目的开展，学生有了越来越多的实战机会。部分学校开设了专门的攻防课程，传授实战经验；部分学校将网络安全实验室升级为网络安全教学靶场，提供模拟实战环境；部分学校开放网络资源，组建CTF战队，提供课外的相关技能培训；部分学校内部举办相关网络安全赛事，并鼓励学生参加各大校外赛事，磨练学生的实战技艺；校企合作举办的各类讲座和项目实践、暑期实习等活动，也给学生的实战技能带来了极大的提升。

4.1.2社会培训机构发展现状

2019年5月，国家市场监督管理总局颁布《信息安全技术网络安全等级保护基本要求》、《信息安全技术网络安全等级保护测评要求》和《信息安全技术网络安全等级保护安全设计技术要求》三大标准。此后，网络安全对于很多政企单位来说，从以前的可有可无变成了必选项甚至是强制项。这进一步刺激了国内网络安全领域的飞速发展。各政企单位纷纷成立单独的网络安全部门，为自己的数据和服务保驾护航。

根据中国网络安全产业联盟（CCIA）发布的《2022年中国网络安全市场与企业竞争力分析》报告显示，2021年我国网络安全市场规模约为614亿元，同比增长率为15.4%。预计未来三年将保持15%+增速，到2024年市场规模预计将超过1000亿元。

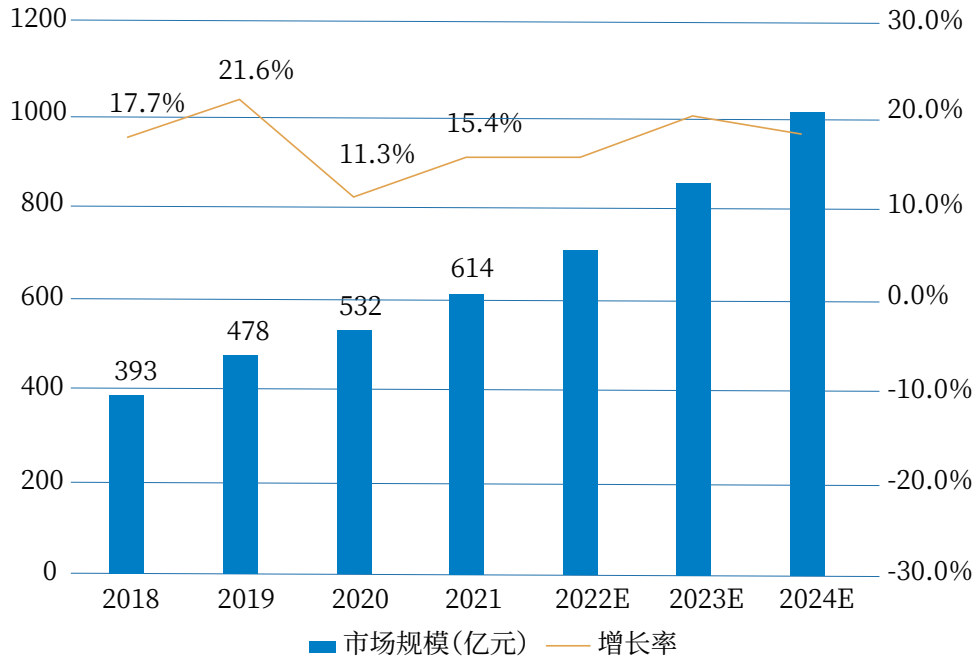


图4-9 2021年我国网络安全市场规模及增速

随着后疫情时代的复工复产，国内经济高速回温，企业对网络安全人才的需求也持续提升。加上《网络安全法》、《数据安全法》、《个人信息保护法》、《关键信息基础设施安全保护条例》等法律法规的颁布导致用人单位的人才需求激增，国内网络安全相关专业人才缺口越来越大。而另一方面，院校培养的学生少有能直接满足用人单位的实际需求，加上连续多年持续上升的就业压力，很多人员会选择专业社会培训机构进行能力提升，以实现就业或者晋升的目的。

根据调查问卷结果，参加社会培训的群体多数是基于岗位就业、系统学习专业知识、增强实战技能的目标，占比分别为22%、21%、21%，以考取证书为主要目的人员占比达13%，同时也有出于兴趣爱好、升职加薪、参加安全竞赛等其他目标。总体来看，基本都是从事网络安全领域的人员，希望通过培训，夯实自身理论基础，增强实践操作能力，获得更好就业机会。

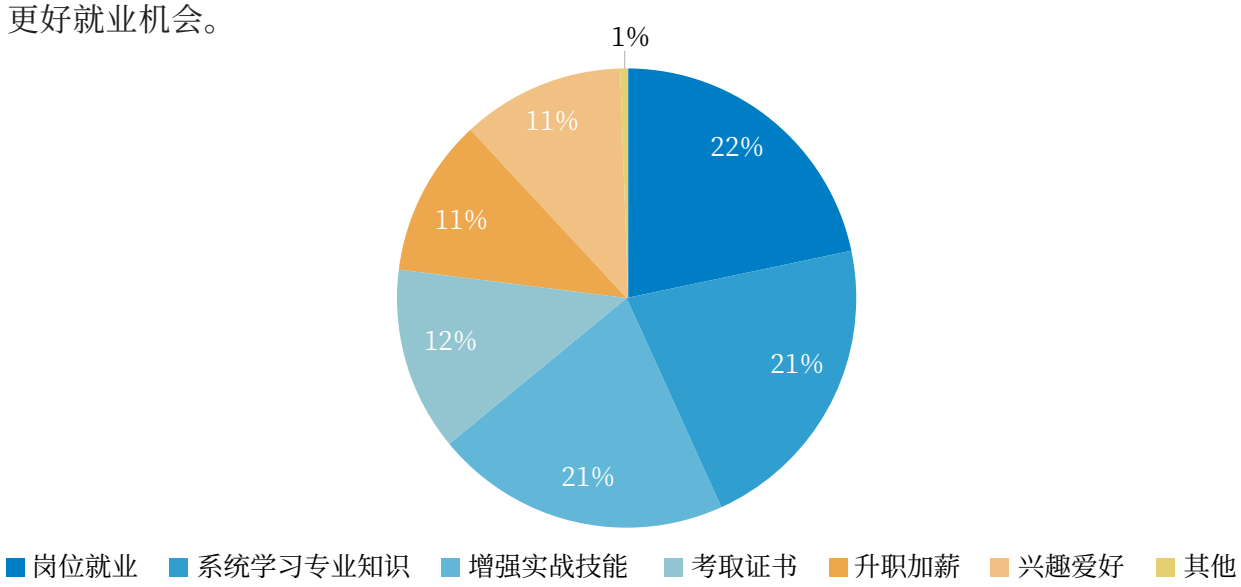


图4-10 参加培训希望实现的目标

在多方面因素作用下，网络安全行业的社会培训机构得到了迅速发展，出现了一批专业的培训机构，有专注就业方向的定向培训班，有专注考证方向的专职培训班，也有结合就业、考证、能力提升等多个维度的综合型机构，许多人经过中短期的培训后，即投身进入网络安全领域。

相较于院校教育，社会培训机构更加注重培养学员的实战能力，不仅设置了大量基于真实场景的实践教学课时，还提供模拟实验室，针对各种漏洞提供真实的模拟环境，并结合网络安全竞赛、SRC众测服务、渗透测试、攻防演习等实践活动带领学员进行实战训练，让学员能够快速完成理论到实践的高度转化。当然，机构培训的质量也决定了能达到的目标与实现的效果。

社会培训机构根据人员参加培训的目标及预算设置了不同时长的班型，以保证能够在有限的时间内达成既定目标。调查问卷数据显示，网络安全人员在选择参加培训班的时候，4个月时长的线下培训班更受青睐，有55%的人群选择参加；16%的人员选择了培训时长达到半年的培训班，25%的人员培训选择了时长时间只有一个月及以下，在职人员考虑工作原因更多的也会选择不限期的线上培训。

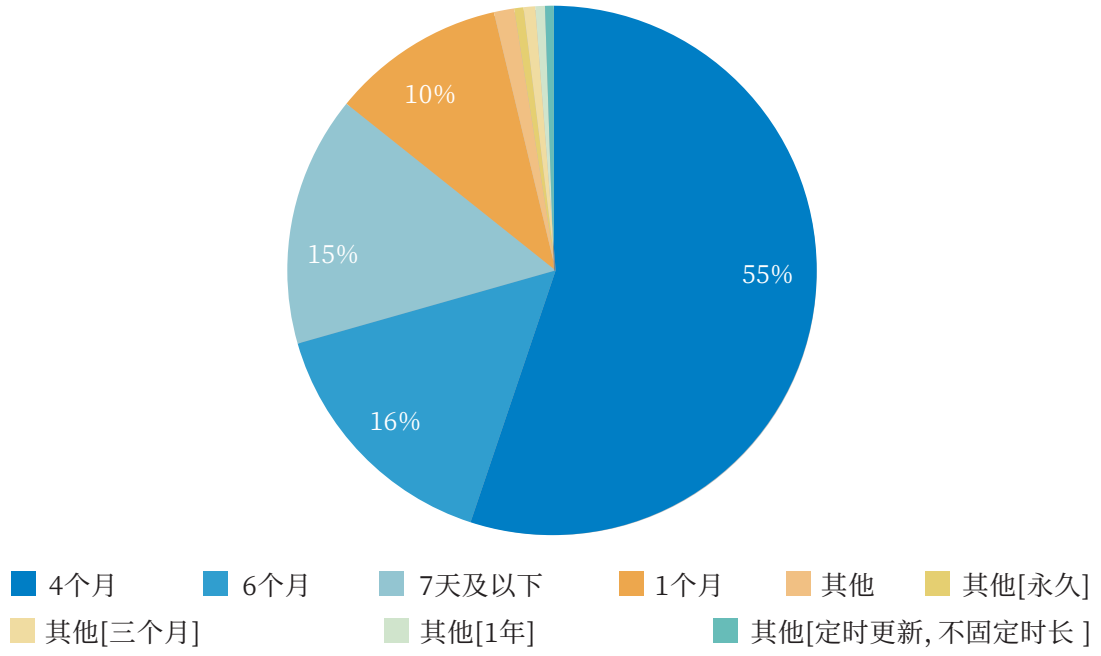


图4-11 网络安全从业人员参与培训班时长

从市场需求情况来看，目前社会培训机构开设的课程中，Web安全类、渗透测试类以及安全运维类等的需求更为旺盛。一方面现实的网络安全人才缺口较大，这类型课程对应的岗位属于企业急缺的，学员就业会更容易；另一方面这类型的课程体系化设计较为完善，利于系统掌握对应知识，学员综合能力提升会更明显。

图4-12 网络安全课程项目词云图

与此同时，随着网络安全领域的快速发展，信息安全专业认证已经逐步成为各行业对信息安全人才认定的方式，网络安全领域从业者持证上岗已经成为大势所趋。根据IDC《2021年中国IT安全服务市场跟踪报告》显示，在国内安全教育与培训市场里，安全教育认证培训（包括认证培训、认证考试等）的市场份额占据了半壁江山，达到了54.2%。

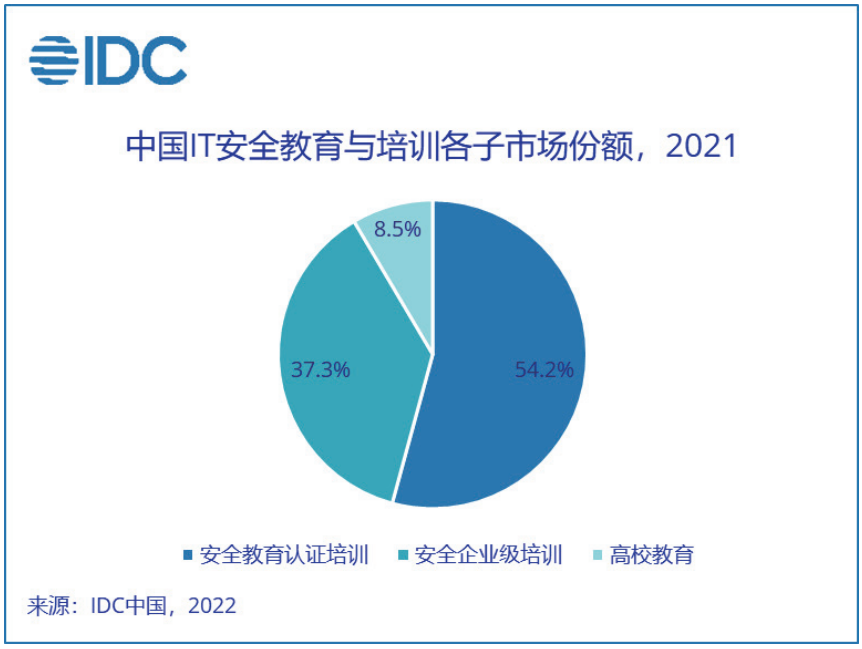


图4-13 2021年中国IT安全教育与培训各子市场份额

大量网安从业者认为考取信息安全资质证书有助于提高就业率和专业能力，这主要是因为考取证书的过程同样是全面学习掌握特定安全领域前沿知识和技术的过程，有助于提升个人在特定安全领域的竞争能力，使个人职业生涯稳步提升。据中国信息安全测评中心发布的《中国信息安全从业人员现状调研报告》显示，从网安从业者已考取的信息安全资质证书类型来看，持有注册信息安全专业人员（CISP）资质证书的占比最高，达71.8%，其次是注册信息系统安全专家（CISSP）和国际注册信息系统审计师（CISA），占

比均超过5%。相较而言，其他几类证书考取人数较少，这主要是受资质证书的权威性、认可程度及受众范围等因素的影响。

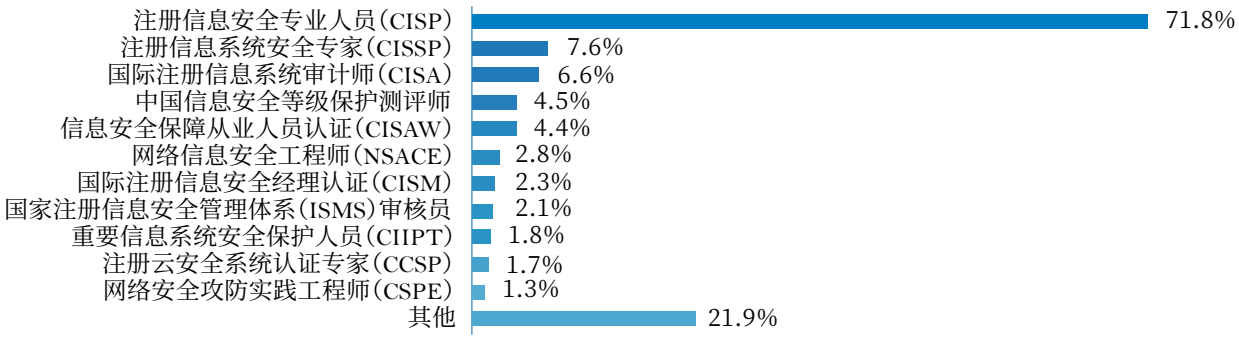


图4-14网络安全从业人员资质持证类型

4.1.3企业内部从业人员培训现状

随着信息技术的飞速发展和网络边界的逐渐模糊，关键信息基础设施、重要数据和个人隐私都面临新的威胁和风险。网络安全问题的日益凸显，也让企业对多元化、多样性、高质量的网络安全人才需求急剧上升，尤其是掌握核心技术的实战型、实用型人才。不少企业已经在内部采取措施，设置相应的网络安全岗位，对安全从业人员进行培训。

经过对网络安全、互联网、金融、交通、化工、电力、政法以及医疗卫生等数十个行业的企业进行调研，可以发现，随着网络在各行业的“渗透”，各企业也越来越重视网络安全问题，并设置了诸多的安全岗位、聘请专业人员以提供保障。目前，企业内部的安全岗位主要有Web安全工程师、安全服务工程师、安全攻防研究员、安全管理岗、安全建设与开发岗和安全运营岗等，如表4-1所示。

表4-1 企业安全从业人员岗位列表

序号	岗位
1	Web安全工程师
2	安全服务工程师
3	安全管理方向岗位
4	安全建设与开发方向岗位
5	安全运维工程师
6	安全运营工程师
7	代码审计工程师
8	监管执法方向岗位
9	科研教育方向岗位
10	渗透测试工程师
11	运维工程师

针对网络空间软硬件的生命周期，不同岗位的安全从业人员需要负责不同阶段的安全职责。从安全实战方向看，主要的安全岗位职责包括资产梳理、安全研究、工程开发、防御加固、渗透测试、安全管理、安全运维、情报收集、漏洞发现与利用、风险评估与发现、应急响应、追踪溯源、逆向分析等，如图4-15所示。其中，渗透测试、漏洞发现与利用、安全运维、应急响应、风险评估与发现以及安全管理尤其受到企业的重视，大部分企业在这些方向设置的岗位较多。

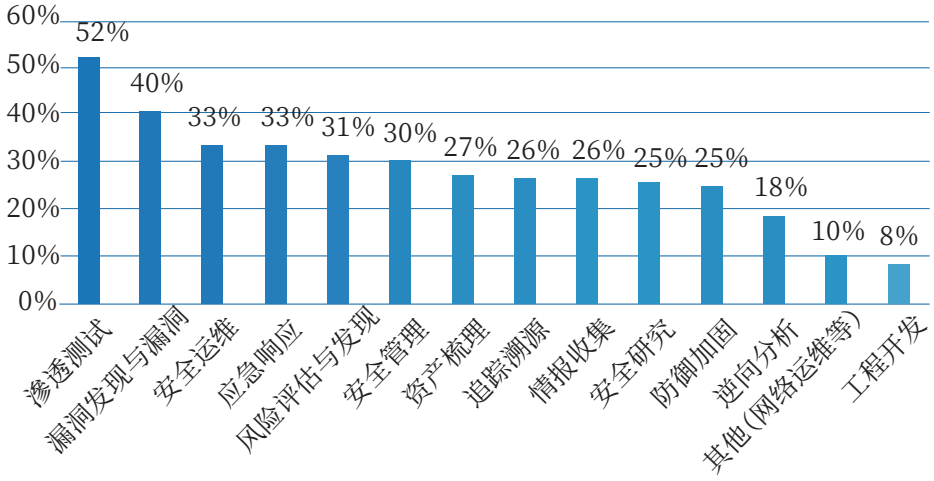


图4-15从业人员就职岗位负责的安全实战方向

然而，伴随着网络攻防的对抗与互相促进，面对越来越复杂多样的网络攻击，能够熟练掌握并运用渗透测试、逆向分析、Web安全以及漏洞挖掘等专业能力的从业人员却十分匮乏，从业人员亟需提升这些能力。同时，由于专业从业人员不足以及部分企业缺乏系统的安全管理经验等问题，有相当比例的企业存在岗位编制不合理导致员工身兼数职或岗位编制合理但人员招募困难的情况，甚至存在专职人员严重缺口多达50人以上的。可以发现，以上种种均使得多数企业存在较为严重的网络安全隐患。如图4-16 、4-17、4-18所示。

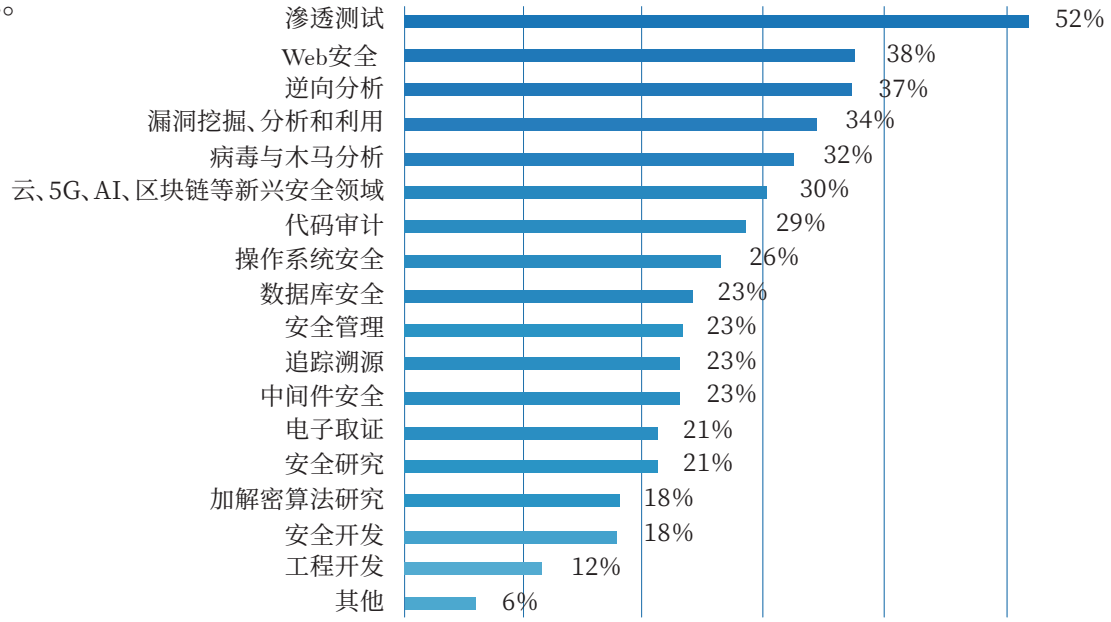


图4-16 从业人员亟需提升的网络安全专业能力

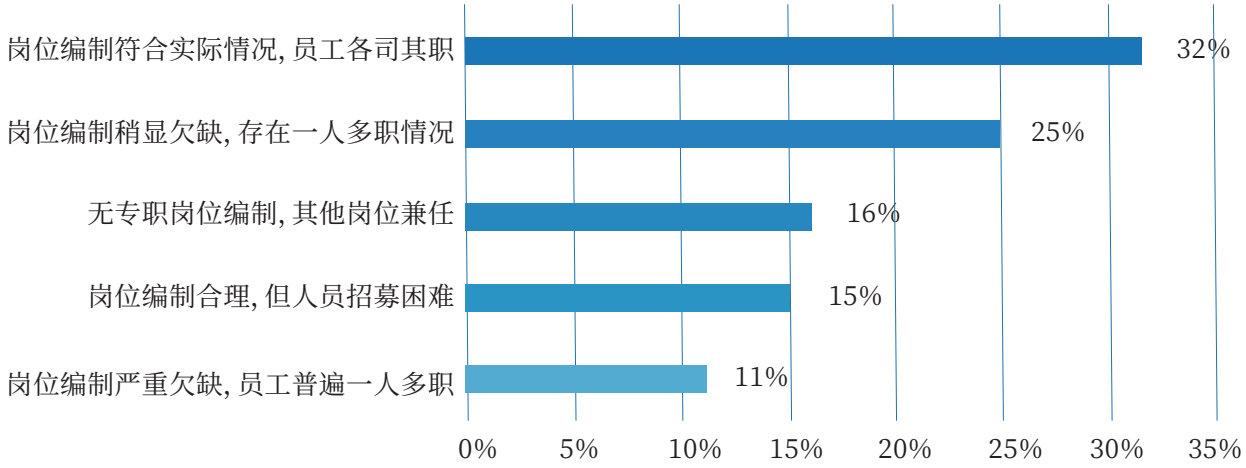


图4-17 各单位的网络安全专职人员数量能否满足业务需要

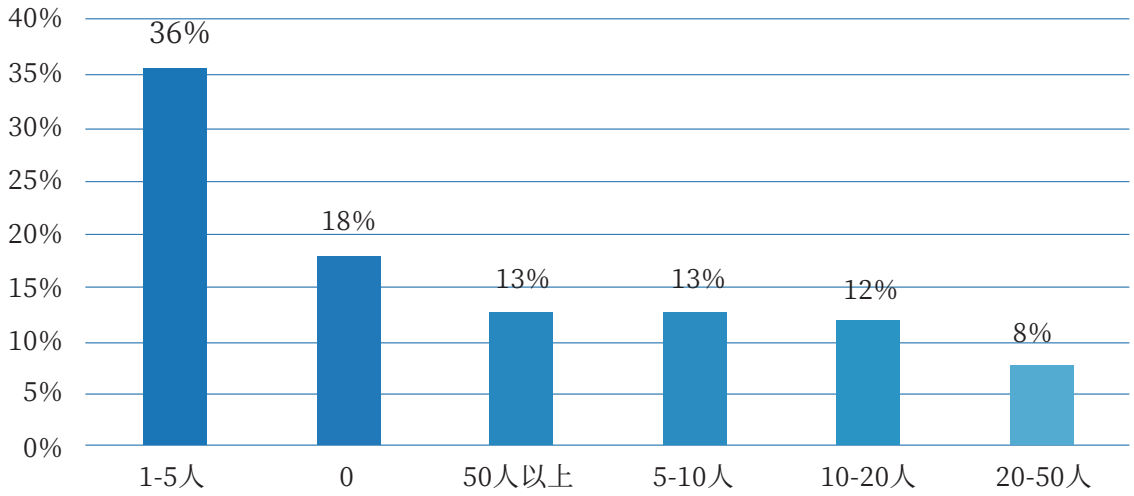


图4-18 各单位的网络安全专职人员缺口

4.2 人才培养方式分析

4.2.1院校培养方式分析

据统计数据显示，开设网络空间安全课程的51所院校中有战队或实验班的院校达37所，其中竞赛获奖情况最具有代表性的是西安电子科技大学和东南大学。西安电子科技大学获全国密码技术竞赛特等奖、全国大学生信息安全竞赛一等奖等各类奖项共计290 余项；东南大学学生各类网安竞赛获奖超过30项。

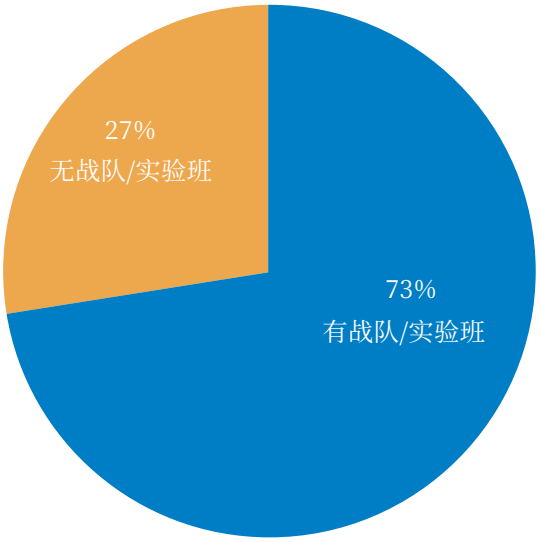


图4-19 战队/实验班比重

在所有开设网络安全相关实践类课程的院校中，根据各院校培养方案统计，实践类课程主要分布在第3至7学期，如图4-20所示。

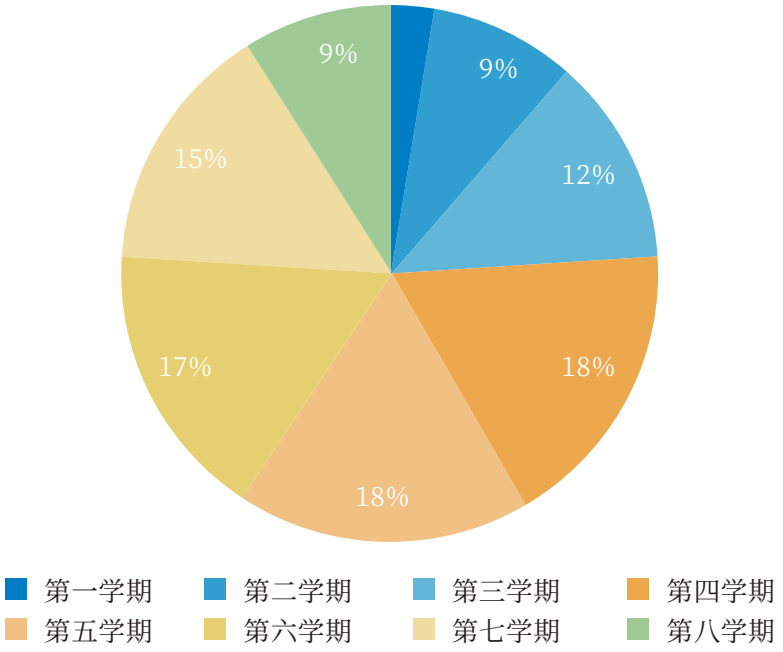


图4-20 实践课时间分布

在校企合作课程方面，能查阅到的信息较少，仅有黑龙江大学开设5门，桂林电子科技大学2门，吉林大学1门。在校企合作方面，有16所院校与企业进行合作，有7所院校与企业无合作，有28所合作信息无法获得。各院校与企业合作的数量也不一样，其中南昌大学与企业合作数量远超其他院校，多达38家企业，如图4-21所示。

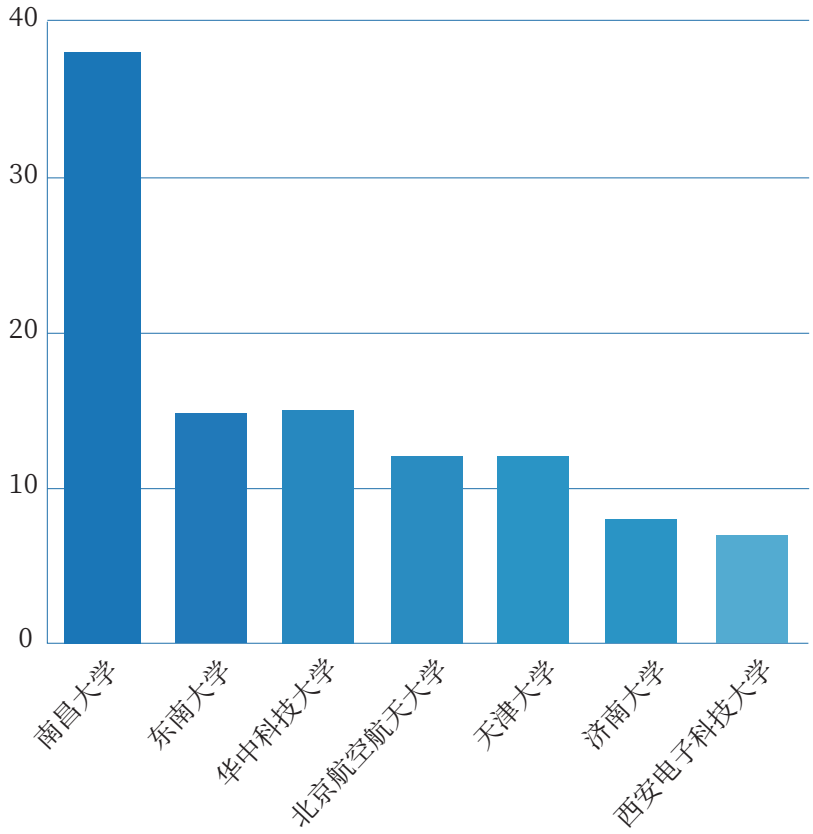


图4-21 与企业合作数

对开设网络空间安全课程的51所院校进行相关课程统计，可以发现，计算机网络、离散数学、数据结构、操作系统是开设数量最多的四门课程。其课程词云如图4-22所示。

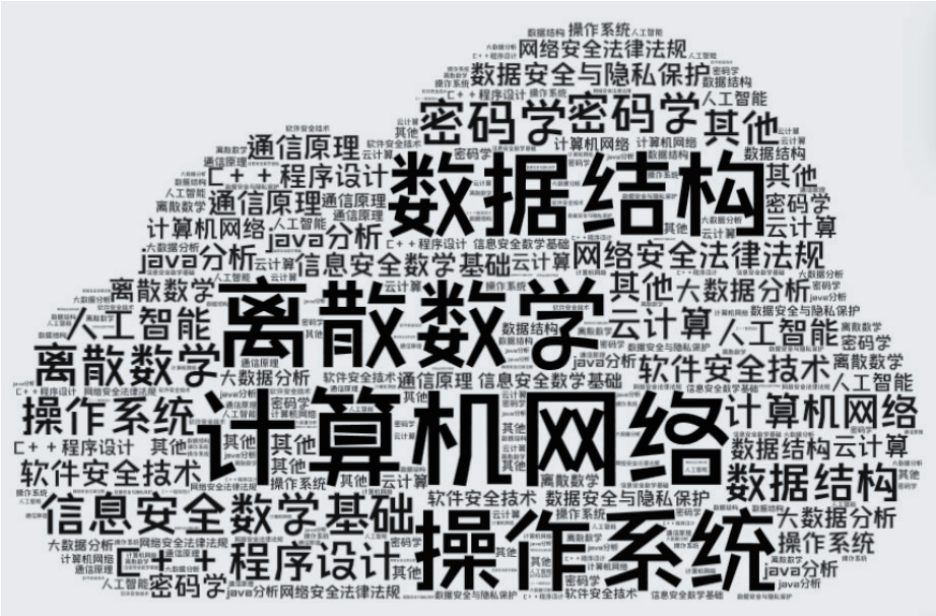


图4-22 课程词云

根据以上数据可以看出，拥有战队或实验班、竞赛奖项多的院校多数为双一流、985、211院校；各学校都颇为注重实践课程的设置，且开设的专业课都符合人才培养的需求；但是开设校企合作课程的院校很少。将来或可多开设此类课程，让社会上的知识技术走入学生课堂，更好的培养学生个人能力。

整体而言，学校秉承课内课外结合、线上线下融合、校内校外混合的实践能力养成体系，通过理论授课、案例研讨、实验操作、模拟对抗、比赛竞技、项目课题实习等多个方面对学生的能力进行培养。除去上文提及课程设置、比赛奖项、校企合作方面外，学校还广泛采取讲座培训、夏令营、社团俱乐部以及社会活动等方式，来丰富学生的培养途径，采取建设攻防靶场、提供学习资料与实现工具、参加攻防演练行动以及参与实际项目等方式，增加学生的实践渠道。这些活动普遍设置丰厚的奖品奖金，并与学分、各项荣誉甚至工作推荐等方面结合，激励更多的学生积极参与，锻炼个人和团队的实践能力。

4.2.2社会培训机构培养方式分析

社会培训机构的培训方式主要分为线上网课、线下面授，线上线下结合三种形式。受疫情影响，近年来有不少线下课程转为线上形式。从数据统计来看，56%的人员会选择通过线下面授的方式进行学习，仅14%的参训人员倾向于选择线上网课。大多数人员如果不考虑疫情影响，都倾向于选择线下面授的培训方式，可能是因为线下培训教学能构建良好的学习环境，面对面的交流也使得沟通更为顺畅，方便及时解决学习中的各种问题。线上网课则更受学业、工作繁忙的群体的欢迎，使得他们能够利用碎片时间参与培训，也是提高自己理论知识与实践操作水平的一种选择，如图4-23所示。

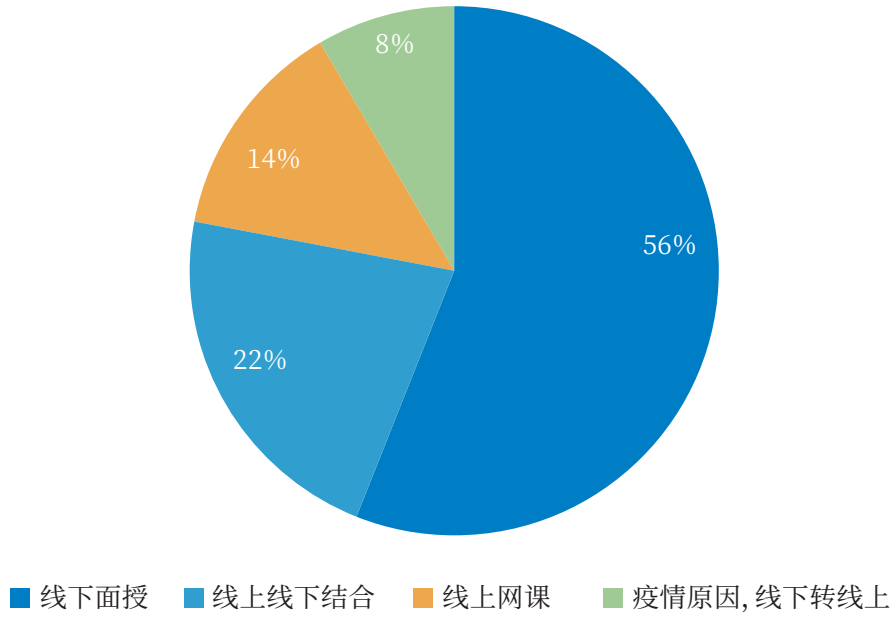


图4-23 参与网络安全培训人员参加培训的形式

如何有效提升人员攻防实战水平，培养出能够应对真实网络安全威胁、解决实际安全问题的安全人才至关重要。为提高网络安全人才建设，国内网络安全培训机构积极制定各自人才选拔与培养方案，结合理论学习与实战训练多个维度，构建高质量水平的实战攻防训练靶场和配套的整体培训体系，建立、健全网络安全人才的选拔与培养体系。

在课程设置方面，服务比较完善的社会培训机构会包括“理论课程、实操练习、考核评价、社会实践、面试辅导”五个模块，实现了人员从培训到实践到就业管理的闭环，占比30%。具备四个模块能力的机构占比19%，只具备其中三个模块的机构占比达到了32%，还有一些机构只专注理论课程+实操练习的培训上。有50%的机构会提供面试辅导，以帮助学员更好的完成就业面试，找到心仪工作。同时35%以上机构在社会实践方面的资源比较有优势，能够提供专项实践模块为学员提供从理论到实践的立体化提升服务，如图4-24所示。

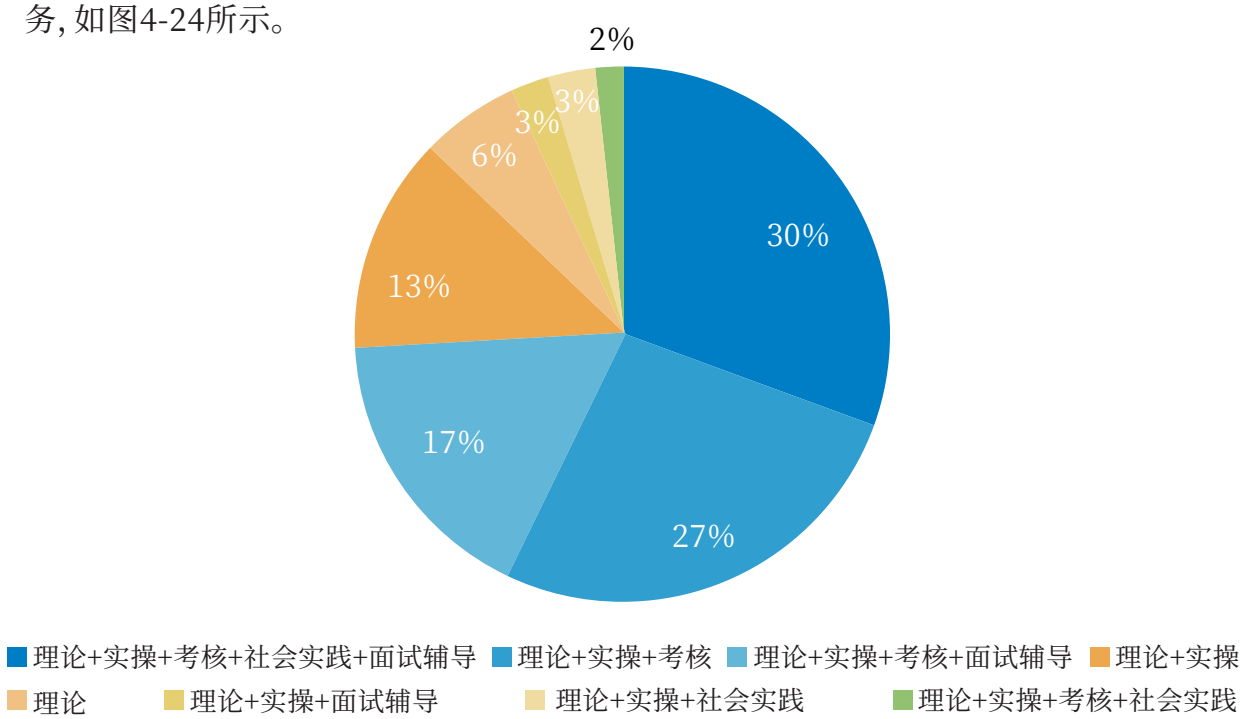


图4-24社会培训机构模块设置情况占比

根据问卷调查结果，培训机构的课程方向通常涵盖安全领域多个具体方向，例如安全软件、安全运维、安全集成、工控网络安全、应急服务、渗透测试、电子数据取证、网络舆情分析与处理和风险管理等。其中Web安全、渗透测试最为常见，几乎是每位参训学员的必修课程，其次是应急服务、安全运维与安全集成，其余方向培训机构会参照参训人员的具体需求进行安排，如图4-25所示。

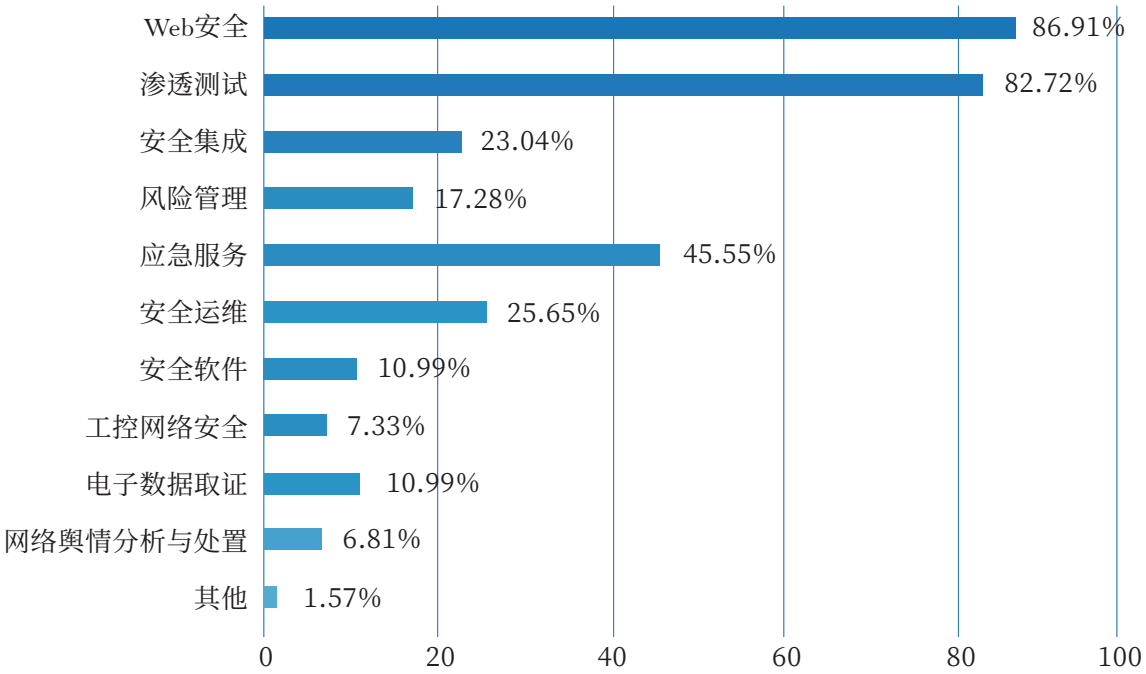


图4-25 网络安全培训课程设计方向

依据i春秋、赛宁网安、合天智汇、谷安天下、易霖博及湖南网安基地多个业内知名网络安全培养机构人才培养方案来看，培训机构通常采用学、赛、演、评、攻、防等多维度结合的培养方式对安全人才进行选拔培养。例如以邀请领域专家线下授课或线上公开课的形式进行专业理论知识教学；搭建高质量水平的实战攻防训练靶场，提供线下实习实训场所；组织参与各类网络安全竞赛，培养实操实战能力；委派专门导师进行每日学习任务的安排与辅导，讲解行业发展形势，给予就业规划指导；针对特定需求，如标准化就业、校企合作或认证考核培训，定制化培训方案等，如图4-26所示。

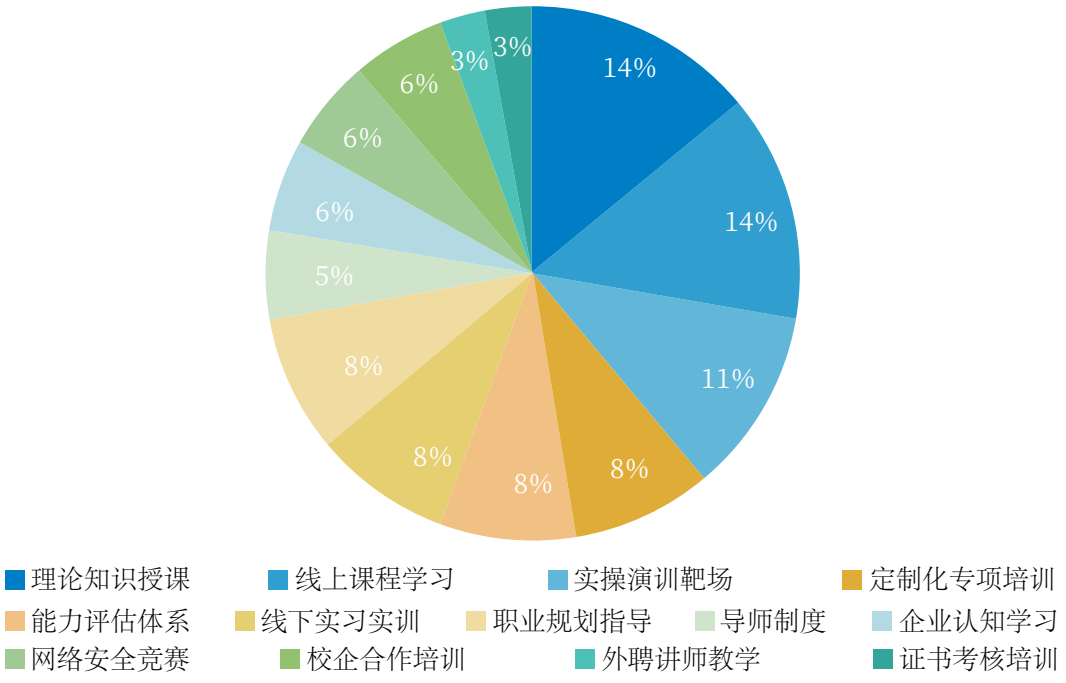


图4-26 主流培训机构常见培训方式

各大培训机构结合理论教学、动手实践、导师引导、定制培训多个维度，秉承“人是安全的核心”主导思想，积极研发全面、专业、完善的网络安全人才培训方式，致力于提升网安人才专业技能，选拔培养更多网络空间安全人才。

4.2.3企业内部培养方式分析

为了缓解有效解决网络安全人才不足，网络安全业务能力不够的问题，越来越多的企业意识到对员工进行安全人才培养十分有必要。

据统计，在各企业单位中，渗透测试方向、漏洞发现与利用方向以及逆向分析方向的网络实战人员最为紧缺，其次是安全运维方向、情报收集方向与追踪溯源方向。下图4-27显示了各单位最紧缺的网络安全实战人员方向的情况。

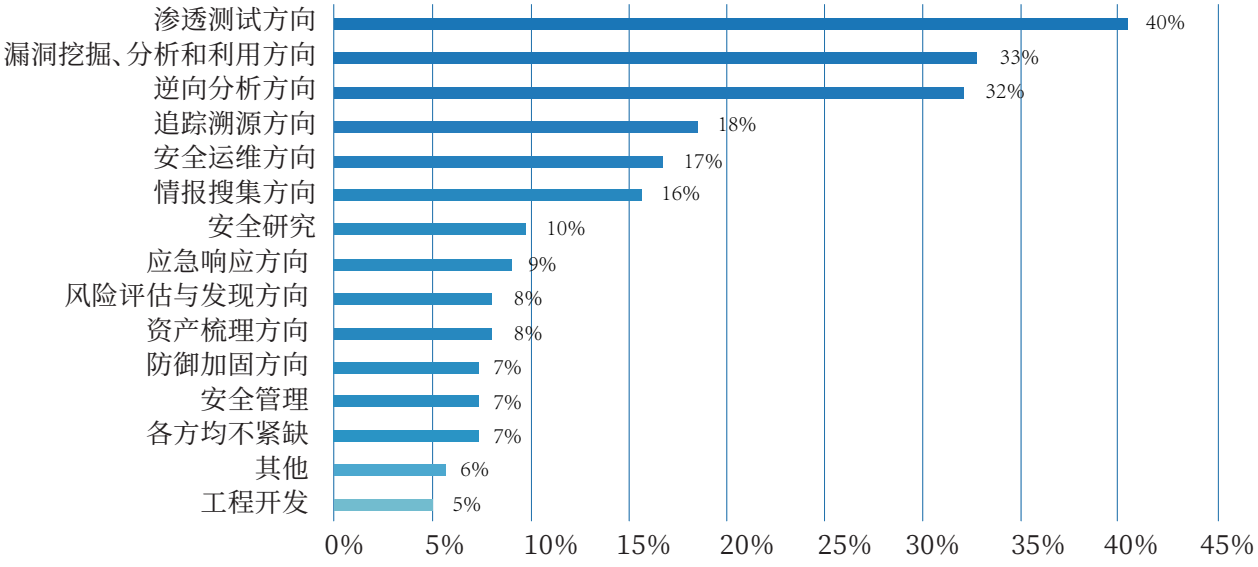


图4-27 各单位最紧缺的网络安全实战人员方向

具体到网络安全业务能力中，由于掌握安全核心技术的人员供不应求，导致企业也普遍欠缺相应的逆向分析、渗透测试、漏洞挖掘，木马与病毒分析等业务能力。与此同时，随着新兴技术的创新发展和新基建产业的加速布局，云、5G、AI、区块链等新兴领域的安全业务能力也存在较大的缺口。图4-28显示了各单位普遍欠缺的网络安全业务能力的情况。

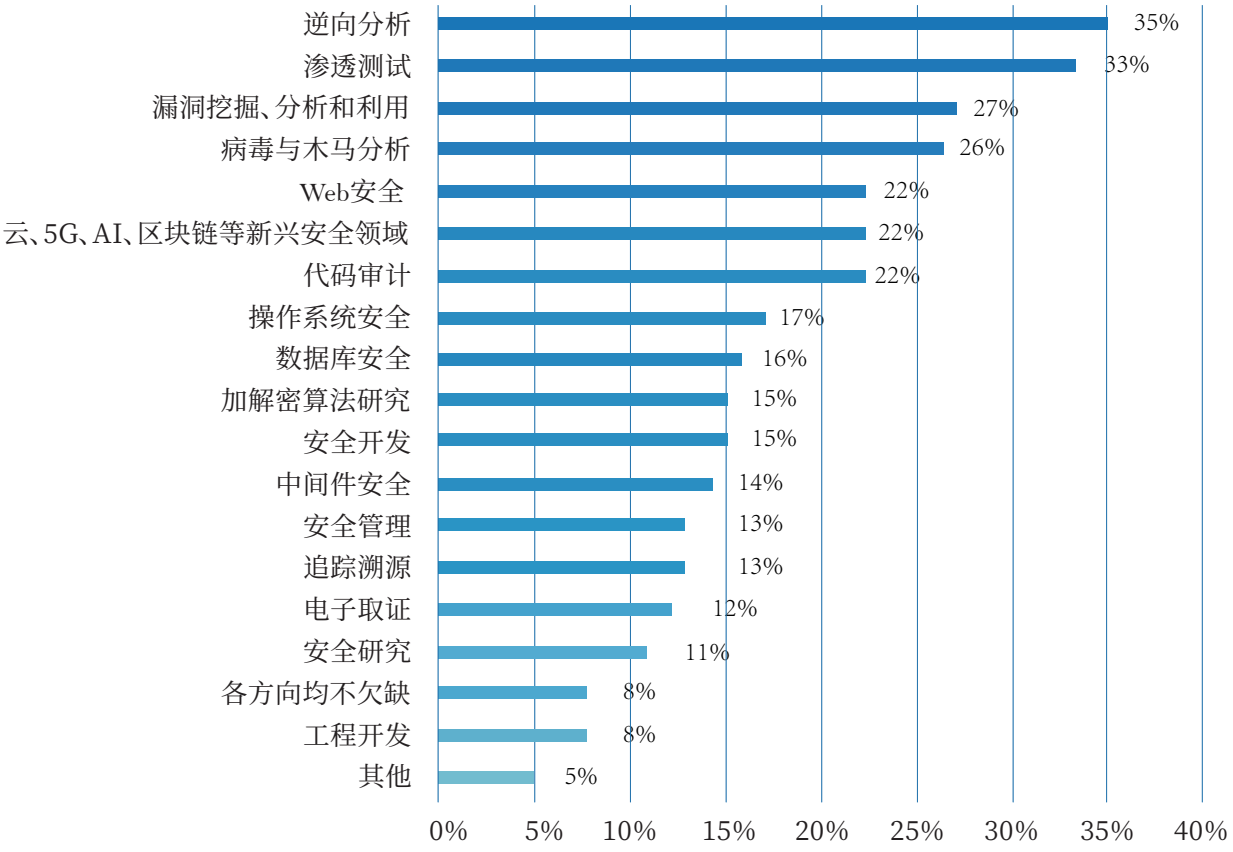


图4-28 各单位普遍欠缺的网络安全业务能力

企业内部通常采用多种方法培养安全从业人员，例如，建立以老带新的导师制、邀请专家进行授课、定制攻防实战平台、定期组织攻防演练活动、举办企业内部网络安全竞赛、鼓励员工参加外界举办的网络安全竞赛等。大部分集团型企业网络和安全顶级企业都组建网络安全实验室或战队，并组织其参与一些国家级别的网安竞赛，一方面以赛代练，磨炼技艺；另一方面宣传自身实力，收获荣誉。如腾讯的eee战队在2018年首届“网鼎杯”网络安全大赛上获得冠军，在2021年“强网杯”网络安全挑战赛上获得特等奖，奇安信集团的虎符战队在2020年第二届“网鼎杯”网络安全大赛上获得冠军，中国移动的守望者衡山队、上海观安无相实验室、国家电网的护网先锋队和赤霄队获得二等奖。在2021年首届以防为主的网络安全大赛“陇剑杯”中，南网电网、中国移动等集团旗下的多个战队表现不错，取得多个奖项。长亭科技组建的战队也曾获得2019年“强网杯” 网络安全挑战赛一等奖、2018年“网鼎杯”网络安全大赛二等奖和2016年中国网络安全技术对抗赛一等奖等。由此可见，在国家重要关键行业及大型互联网企业中，组建一支顶尖的，具有实战经验的战队已是常态，同时也反应出大型企业对于整体网络安全专业人员攻防实战能力的重视度越来越高。

除比赛外，由于数据泄露、病毒勒索等网络攻击对企业造成重大损失的事件频有发生，组织网络攻防演习也成为许多企业培养员工网络安全意识与攻防能力的重要方式。通过这类活动，企业能查出自身短板漏洞，提高网络、系统以及设备等的安全能力，并培养员工的攻防实践能力。

总体而言，对于员工能力的培养，其中以老带新的导师制最为普遍。但也依旧存在

部分单位没有采取任何的措施来培养从业人员。各单位采取的提升措施如图4-29所示。

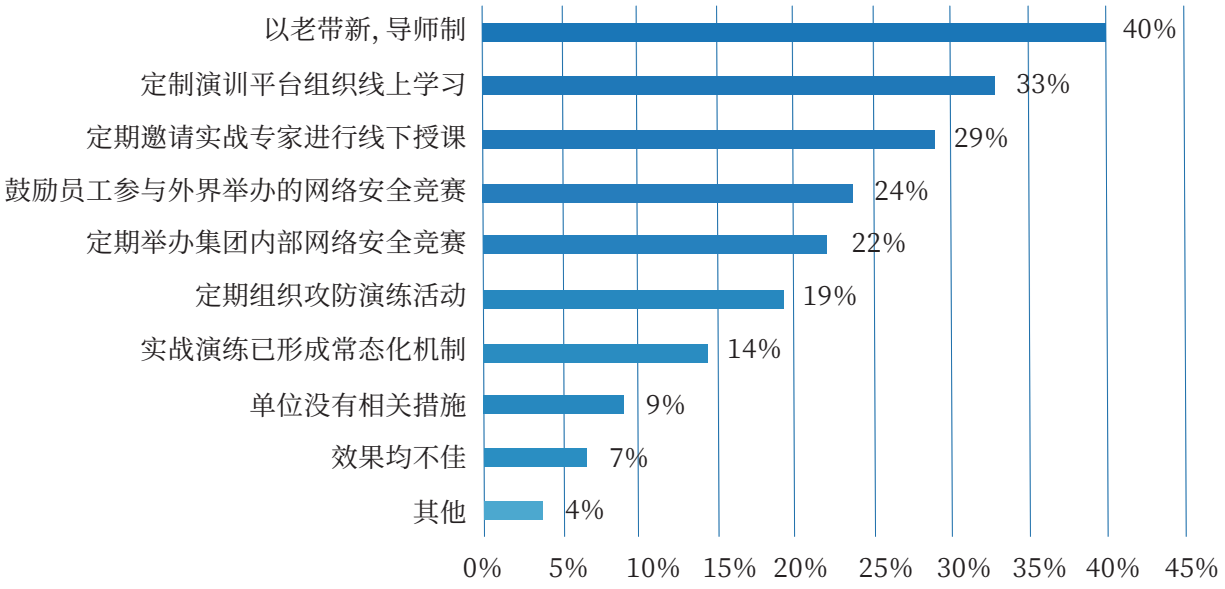


图4-29 各单位采取哪些措施提升员工的实战能力

4.3 人才培养效果分析

4.3.1院校培养效果分析

在开设网络空间安全专业的院校中，据能查阅到的官方数据显示，就业率都超过90%。其中有的院校培养成果突出，例如西北工业大学，每年培养数量54人，21年毕业生就业率高达100%；北京邮电大学2021届本科毕业生123人就业率高达96.75%，硕士190人就业率高达100%。

经调研，院校培养的相关专业学生大部分认为能完全掌握课程内容，学习游刃有余，相对轻松，如图4-30所示。

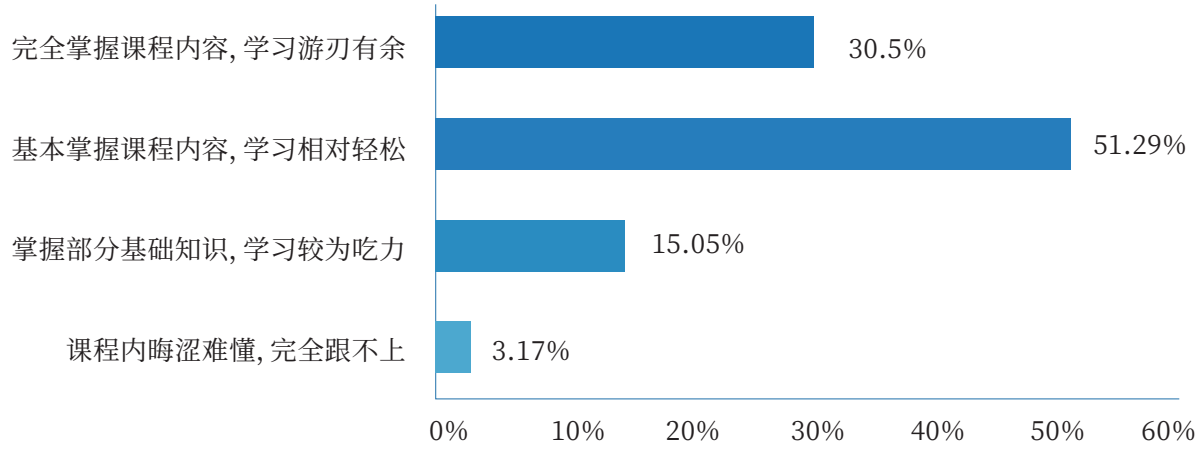


图4-30 学生对知识掌握情况

虽然目前院校就业率、学生掌握情况良好，但在培养过程中仍存在一些问题。部分在校学生认为老师教学方法单一、重理论轻实践，学校培养方案与社会需求脱节、培养目标定位不准确等。这些问题需引起重视，学校要在今后的教育教学中逐步克服，完善教学方法，以培养更能满足社会需要、理论和实际相结合的网络安全新人才。

4.3.2培训机构培养效果分析

根据调研数据统计显示，在培训课程难度控制和学员的接受程度上，大部分的学员能够良好理解和掌握课程中的知识，但仍有部分学员表示，当前的课程设置是对他们而言是有较大难度的。从图4-31可以看到，目前学员对课程总体的接受度是比较好的，难度设置合理适中。

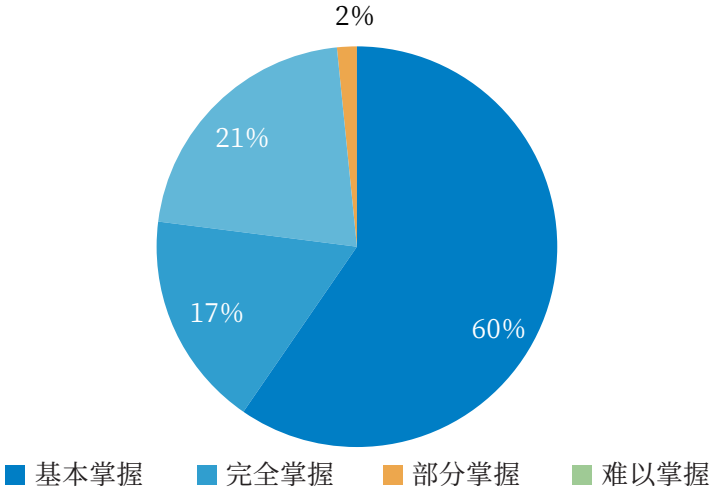


图4-31 网络安全培训机构学员对课程的掌握情况

在培训机构的课程实用性评价方面，约三分之二的受调查人员表示培训课程体系完善，注重实际操作实践，具有较强的实用性。有四分之一的被调查人员表示课程的体系较为完善但并不注重实际操作。从图4-32可以看到，总体上大部分的培训机构的课程都具有不错的实用性，但仍有部分培训课程体系设计不合理，缺乏对学员在动手实操能力方面的培养。

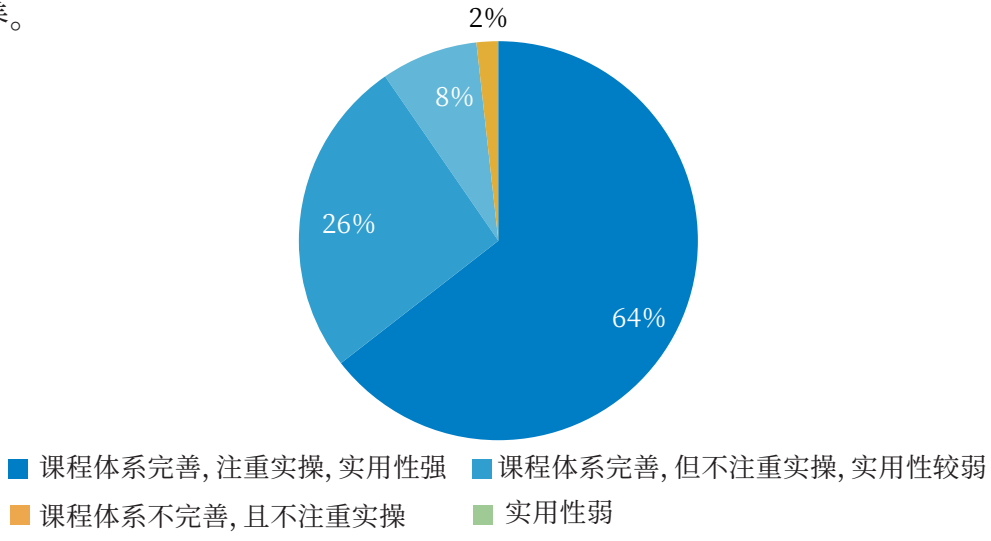


图4-32 网络安全培训机构学员对课程的实用性评价

在毕业学员的就业情况上，不同培训机构的学员表现出不同的结果。有少部分培训机构在培养学员的信誉上得到一些企业的高度认可，刚开班时就有企业前去预定学员；大部分培训机构的学员会在培训结束前就有一部分已经有签约单位，在培训结束后，学员们基本都能找到就业单位。但仍有少部分受调查人员表示，在培训结束后，多数学员迟迟没有意向单位。总体来看，受培训学员的就业前景良好。

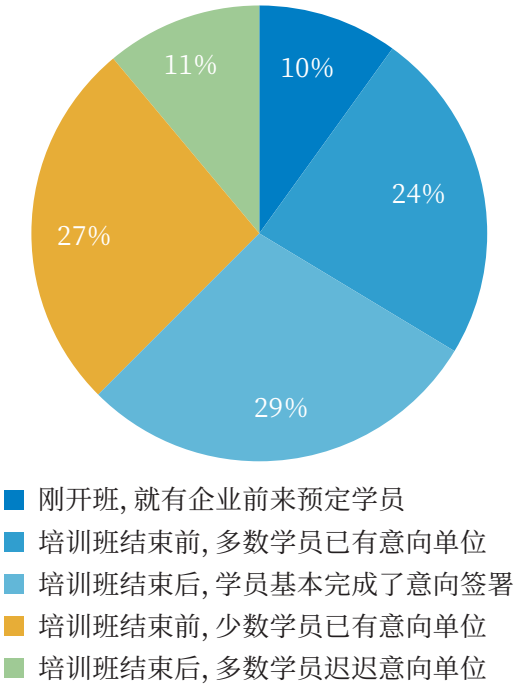


图4-33 网络安全培训机构学员的就业状况

在未来期望提升的能力方面，主流意见为期望在渗透测试、漏洞挖掘、分析和利用、逆向分析、Web安全、病毒与木马分析等方向做进一步的提升学习。此外，在一些近年兴起的网络安全新方向，例如云、5G、AI、区块链等安全领域，也成为了培训学员未来计划提升的方向。

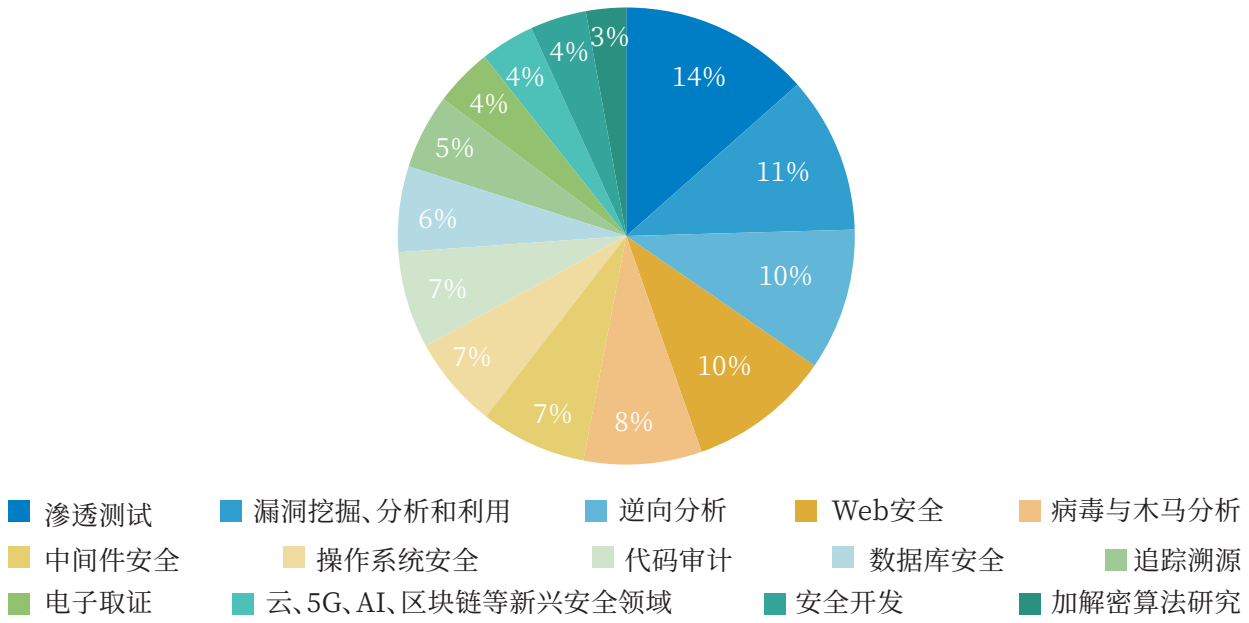


图4-34 网络安全培训机构学员未来期望提升的能力

4.3.3企业培养效果分析

对于不同的培养措施，其培养效果也会存在相应差异。其中，以老带新的导师制，由于具有工作经验丰富的导师指导学习与教授知识，往往培养效果最好；此外，通过定制演训平台组织线上学习、定期邀请实战专家线下授课、参与安全竞赛等手段也具有较好的效果。从业人员认为对于提升实战能力最有效的培养措施，如图4-35所示。

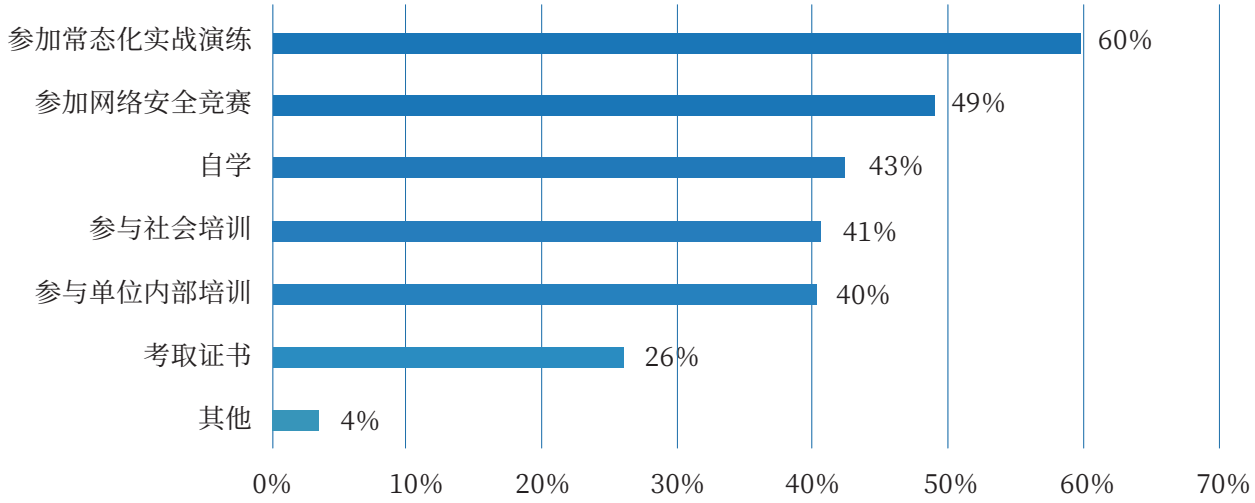


图4-35 各单位哪些措施对于提升实战能力最实用有效

第五章

第五章网络安全人才攻防实战能力评价分析

5.1 网络安全人才攻防实战能力评价现状

网络空间安全攻防实战能力评价的目的是评判从业人员是否达到网络空间安全专业技术人员独立从事某种网络空间安全专业技术工作知识、技术和能力的要求。

5.1.1主流评价方式

目前，国内外主要评价方式包括岗位/职业认证、等级认证、(企业)产品培训认证、等级积分等。主要网络安全相关技能认证由政府、大学(研究机构)、行业协会和各大公司等提出。

1.岗位/职业认证

如国际信息系统安全认证联盟(ISC)²的CISSP(注册信息系统安全师)认证、CCSP(注册云安全师)认证，信息系统审计与管控协会ISACA(Information System Audit and Control Association)的CISA(注册信息系统审计师)认证，中国信息安全测评中心的CISP(注册信息安全专业人员)认证，各地网信办和人社部组织的网络信息安全工程技术人员职称评审等。

2.等级认证

如公安部的网络安全等级测评师认证，国际电子商务顾问局EC-Council的CEH(道德骇客)认证、CPENT(认证渗透测试专家)。

3.(企业)产品培训认证

比较典型的是Cisco公司的Cisco Certified Network系列安全认证，中国信息安全认证中心ISCCC的CISAW(信息安全保障人员认证)，华为的HCIE-Security认证，华三的H3CSE-Security认证等。

4.等级评价

常见于各类安全竞赛、企业安全响应中心(Security Response Center, SRC)的白帽认证。

在各类安全竞赛中，往往按赛队进行排名评价，一般分为一、二、三等奖或一、二、三名。如教育部高等学校网络空间安全专业教学指导委员会举办的全国大学生信息安全竞

赛创新实践能力赛，根据参赛队伍的线下赛得分，评选出一、二、三等奖。中央网信办指导的“强网杯”全国网络安全挑战赛，线上赛和线下赛的前32名分别获一、二、三等奖。公安部指导举办的网鼎杯网络安全大赛，依据参赛队伍成绩评出一、二、三等奖，根据队伍积分，面向单位颁发金鼎、银鼎、铜鼎，面向个人会颁发“网络安全优秀人才”、“网络安全高端人才”等证书。

企业SRC一般对个人能力进行等级评价。阿里安全响应中心根据一段时间（720天）内“白帽”提交有效漏洞的贡献值将SRC平台的白帽等级分为江湖少侠、武林高手、一代宗师三个级别。 i春秋、漏洞盒子等平台则将白帽的等级从低到高依次分为：青铜、白银、黄金、铂金、钻石等段位。奇安信在2021年6月发布的《中国实战化白帽人才能力白皮书》中表示，经调研，55.8%的白帽子处于“无证上岗”的状态。

5.1.2 有效评价方式

网络攻防实战能力评价分为攻和防两方面。一般而言，攻击能力往往呈现实践性，防御人才往往首先呈现学术性。因而有效的评价方式应该要体现学术性和实践性两者的结合。目前我国几个全国级攻防实战类的竞赛或典型的攻防能力认证中，都对学术、实践两方面能力有所考虑。

如在全国大学生信息安全竞赛创新实践能力赛中，初赛采用在线答题形式，包括知识问答环节和场景实操环节两个环节，题目覆盖多种创新实践能力基础技能，复赛采用AWD或AWD+攻防赛模式，决赛采用半开放命题的攻防竞赛形式，由Build（创新安全应用开发）、Break&Fix（攻击、防御综合对抗）两个环节组成，各占权重比例分别为15%：85%，考察较为全面。强网杯的线上赛采用在线解题（Jeopardy）模式，线下赛采用采取攻防对抗（KOH）+实战解题（Realworld）模式。网鼎杯则采用夺旗赛（CTF）、攻防赛（AWD PLUS）、靶场赛（ISW）、实景防御赛（RDG）、人工智能漏洞挖掘赛（RHG）等多种模式相结合的方式。

在由全国网络空间安全教指委举办的全国大学生信息安全竞赛实践赛中，根据参赛队伍的线下赛得分，评选出一、二、三等奖。在公安部指导举办的网鼎杯网络安全大赛中，依据网鼎个人积分对参赛人员进行网鼎杯网络安全人员能力评定，分为初级、中级、高级三个级别。

典型的攻防能力认证，如国际电子商务顾问局EC-Council的CEH（道德黑客）认证，针对个人能力进行评价，分为两个级别：CEH认证和CEH大师认证。CEH认证为知识评价，需要参加为时4小时的考试，完成共125个选择题；CEH大师认证要在通过CEH认证的基础上，参加时长6小时的实践挑战，在iLabs网络靶场中解决20个类似于真实场景的实践挑战。

5.1.3 存在问题

但上述的攻防类竞赛或攻防类认证用于网络安全人才攻防实战能力评价方面还存在一些问题。

一方面两者都没有形成标准化的可推广的评价体系。另一方面在分级评价方面各有

短板。

各类攻防类安全竞赛进行攻防能力评价存在的普遍问题在于：竞赛得到的是相对评价，采取被评价人/团队之间互为参照的方式进行评价，即参赛人员水平决定了竞赛结果的含金量；大多只进行团队评价，较少进行个人评价。

我们发现，近几年有关部门对个人评价也重视了起来，例如“网鼎杯”大赛有专门面向个人的奖项设置。

攻防类认证项目，CEH（道德骇客）认证将理论和实践技能完全独立进行考核，无法实现对攻防实战能力的评价区分度；而其他公司类认证会将理论和实践结合来考核，但一般考察点基本围绕公司产品及其功能展开，有产品依赖性。

5.2 网络安全人才攻防实战能力评价分级

基于对网络安全人才攻防实战能力的理解和分析，考虑到网络安全攻防人才长远发展的需要，我们提出了知识评价与技能评价相结合的网络安全人才攻防实战能力分组评价体系。

5.2.1能力分级说明

网络安全人才攻防实战能力的评价，可分为初级、中级、高级三个层次，形成由低至高的阶梯成长路径。

初级人员：熟悉网络攻防实战的基本概念和流程，并能在他人指导下得以应用，有一定独立工作能力和实践经验，能够对常规化、结构化的情况进行安全评估和防护。

中级人员：对网络攻防实战的基本概念和流程有充分的了解，能独立完成较为复杂的网络攻防实战任务，具备指导他人工作的能力，具有一定实践经验，能够对非常规、较为复杂的情况进行安全评估并给出结论和处置建议。

高级人员：对攻防实战相关的先进概念和流程有深入的了解，并能够独立加以应用，精通关键的网络攻防专业技能，能够对非结构化的复杂情况进行安全评估、成功处置，具有丰富的实践经验，可以为他人提供指导和建议。

5.2.2 能力评价内容

对网络安全人才攻防实战能力的评价包括知识和技能两方面内容，两方面评价内容的具体组成与下图所示。

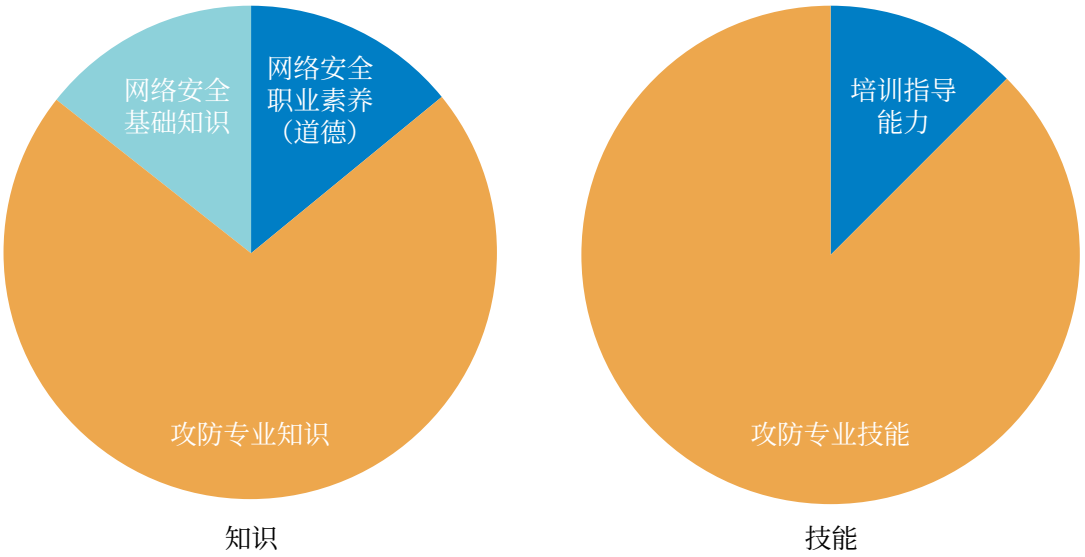


图5-1攻防实战能力评价内容组成示意

知识评价涉及网络安全职业素质（道德）、网络安全基础知识和攻防专业知识三方面。在评价人才攻防实战能力时必须注重考察其职业素质。因为网络安全人才职责本身是为了保护和营造良好的网络生态环境，推动互联网行业的健康发展。而攻防实战人才拥有一定破坏性技能，更应该自觉规范职业行为、加强职业道德、强化法律意识。对知识的评价主要通过笔试或答辩等方式进行。

技能评价涉及攻防专业技能和培训指导技能两个方面。对技能的评价主要通过实战、演练或取得相应证书等方式进行。

攻防实战能力评价的核心内容，攻防专业知识和攻防专业技能，包括六方面内容的考察，其中，网络安全监测与分析、应急响应考察应急响应能力，漏洞发现与分析、渗透测试考察网络攻击能力，攻击事件研判、攻击样本及情报分析考察网络防御能力。

1.网络安全监测与分析

对设备日志、网络流量等安全数据以及安全态势进行监测和分析，发现威胁并进行报警、响应。

2.应急响应

针对信息、信息系统、信息基础设施和网络进行分析，制定安全事件应急响应预案，对突发安全事件进行分析、处理，完成快速应急响应。

3.漏洞发现与分析

对信息、信息系统、信息基础设施和网络进行分析，发掘未知漏洞，对现有漏洞和安全威胁进行评估，评估风险水平，制定或推荐适当的加固措施。

4.渗透测试

对目标信息、信息系统、信息基础设施和网络进行模拟渗透攻击，以检验和测试其安全性。

5.攻击事件研判

在日常运行和攻防演练中，对各类系统应用的安全事件进行研判分析，快速准确地进行事件确认、定级、问题定位、溯源分析，提供可靠的遏制和恢复方案。

6.攻击样本及情报分析

对攻击样本进行逆向分析，通过分析程序代码、进程反编译，发现恶意攻击程序与行为；收集网络安全威胁情报，对获取的情报数据归类分析，及时发现网络威胁。

5.2.3 评价标准

不同层次的网络安全人才在知识和技能方面的要求是不同的。初级更侧重于知识的理解，高级更侧重于技能的应用。各级评价中两者的权重表，如表5-1所示。

表5-1 评价权重表

级别	知识	技能
初级	60%	40%
中级	50%	50%
高级	30%	70%

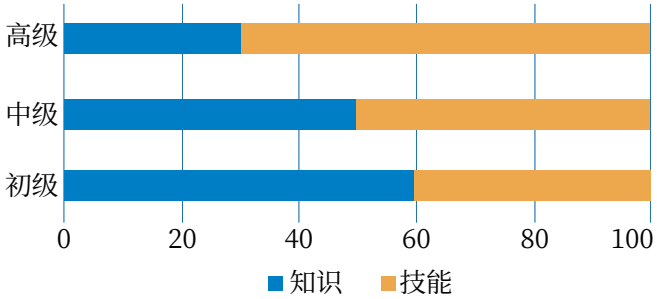


图5-2 网络安全人才攻防实战能力评价权重占比

不同层次的人才在其知识和技能的掌握要求、掌握重点也是不同的。

在知识评价方面，随着由低到高的级别提升，对职业素质（道德）的要求是一致的，对专业知识的要求占比会有所提高，其中对操作性的知识掌握会降低，对攻击研判、样本分析等分析性的知识掌握要求逐步提高，如表5-2所示。

表5-2知识要求占比权重表

项目		初级	中级	高级
网络安全职业素质（道德）		5	5	5
网络安全基础知识		20	10	5
攻防专业知识	网络安全监测与分析	30	20	5
	应急响应	15	15	20
	漏洞发现与分析		10	15
	渗透测试	20	15	10
	攻击事件研判	10	15	20
	攻击样本与情报分析		10	20
合计		100	100	100

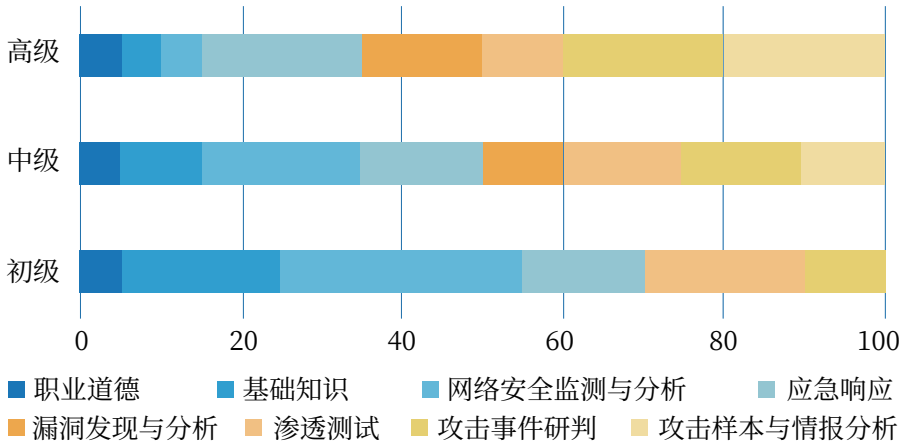


图5-3知识要求占比权重示意

在技能评价方面，随着由低到高的级别提升，除了在漏洞分析、攻击研判、样本与情报分析等高阶攻防实战技能的要求逐步提升外，对中级和高级人员还应该相应地具备培训、指导他人开展攻防实战的能力，如表5-3所示。

表5-3技能要求占比权重表

项目		初级	中级	高级
攻防专业技能	网络安全监测与分析	40	20	10
	应急响应	20	20	20
	漏洞发现与分析		10	16
	渗透测试	25	20	8
	攻击研判	15	15	20
	样本与情报分析		10	16
培训指导能力			5	10
合计		100	100	100

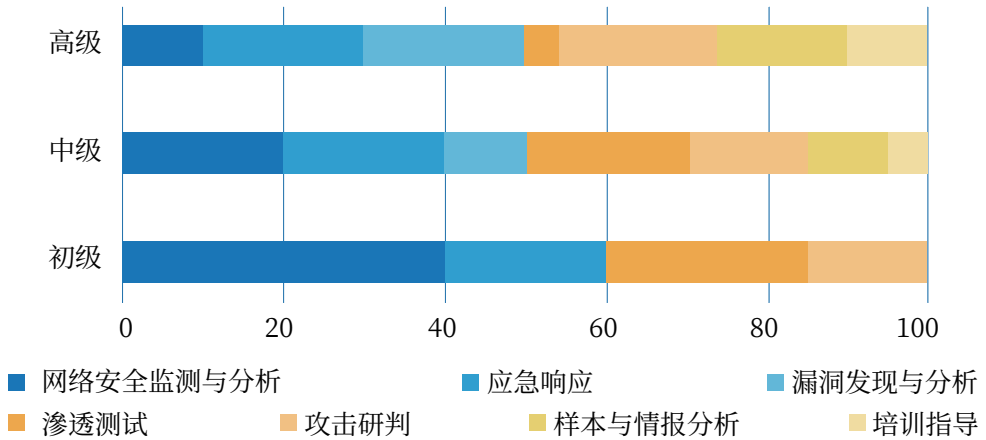


图5-4技能要求占比权重示意

5.3 网络安全人才攻防实战能力提升与评价方式

网络安全人才攻防实战能力提升的有效方式包括：安全竞赛、专业培训/认证、安全会议、众测项目、攻防演练等。

5.3.1 安全竞赛

安全竞赛，是检测和提升人员实战能力的重要方式。“以赛促教、以赛促学、以赛促练”，在贴近真实的对抗环境中发现自身不足，切磋彼此技艺，提升人才攻防技术水平和团队协作能力，是网络安全竞赛举办的初衷。

网络安全竞赛最早起源于DEF CON创始人Jeff Moss于1993年发起的一次BBS黑客竞赛。此后，在各界的广泛参与下，各类网络安全竞赛蓬勃发展。当前，网络安全竞赛类别主要包括：夺旗赛（CTF）、攻防赛、靶场赛、漏洞挖掘赛、运维赛、取证赛以及政策赛等。目前国内安全比赛数量众多，适合于全方位安全知识的入门提升。

经过20年左右的发展，如今每年的高水平国际安全竞赛有近百个，以美国、德国、俄罗斯、韩国、日本为代表的国家组织的安全竞赛由于其高水平的赛题，受到了全球对计算机和网络安全感兴趣的学生和安全行业从业者的热烈参与和推崇，一批批安全人才在激烈的比赛中成长起来。作为发现人才、培养人才的有效途径，近几年国内各类网络安全赛事也蓬勃发展。每年的高水平国家级竞赛也有几十场，各大部委均有发起官方赛事，仅2022年在全国各地已经举办或即将举办的国家级赛事中，就有由中央网信办指导的第六届强网杯全国网络安全挑战赛、公安部直接指导的第三届“网鼎杯”网络安全大赛以及教育部高等学校网络空间安全专业教学指导委员会举办的全国大学生信息安全竞赛实践等知名赛事品牌，均受到了各行各业爱好或从事网络安全相关工作的群体关注与参与。其中许多在校大学生通过大量赛事训练，在网站安全渗透测试、二进制漏洞挖掘与利用、密码学等许多网络信息安全相关的实践技能方面获得了很大的提高。

网络安全竞赛的特点在于：一是模拟真实场景，能够有效提升参赛人员的技术、沟通、领导、协调等各方面能力；二是环境安全可控，不会造成实际破坏和损失。

网络安全竞赛对参与各方均有积极作用：

----对于政府来说，网络安全竞赛是提升保卫国家、行业及公民能力的手段；

----对于行业资质认定机构来说，网络安全竞赛越来越多地被视为资质维持所需的相关工作经验；

----对于专业人员来说，网络安全竞赛能够锻炼和展示专业技能、评估人员能力、提升意识和士气，进而提高生产效率；

----对于学生来说，中学和大学开展各种级别的竞赛，在教学中补充动手实训课程，能够丰富学习形式；

----对于整个网络安全领域来说，开展网络安全竞赛有利于在技术和战术层面，以及在攻防两个方面促进创新，推动知识、技术、技能和实践的共享。

网络安全竞赛也能够给不能层次的人在技术上带来提高：没有网络信息安全基础的学生通过竞赛，建立了安全攻防的概念；有初步基础的学生，通过高质量赛题的实践练

习，提升了实战能力；已经学有所成的学生，通过国际竞赛和国际强队比拼，开阔了视野。

长远来看，网络安全专业竞赛，不仅对于网络安全人才攻防能力的提升大有助益，也能为前沿研究储备人才，更能够推动安全行业的发展。

5.3.2 安全会议

积极参与各类安全会议也是网络安全人才提升攻防实战能力的一种有效方法。在网络安全会议举行的同时，不仅会有最新研究成果的发布，还可以与同行进行技术交流，有的会议还会组织与最新技术相关的技术培训。

每年夏季在美国拉斯维加斯举行的BlackHat黑帽大会和DEF CON大会是网络安全相关专业研究人员心中的盛会。能作为Speaker（演讲者）登上黑帽大会或DEF CON大会，展示在网络攻防领域的最新研究成果是许多安全研究团队的梦想。近年来，上海交大、360、腾讯、盘古等多个中国安全研究团队的议题登上黑帽大会的讲台。大会期间，除了邀请研究人员发布安全漏洞破解和安全技术研究成果外，还会交流和讨论攻防技术、策略，为参会人员提供专业安全训练，是网络安全人才了解攻防技术趋势，提升攻防能力的绝好机会。

5.3.3 培训认证

政府、大学和研究机构，专业组织和商业机构等针对网络安全人才攻防能力的培训和认证活动包括：提供培训课程、会议、产品技术的专业认证等。

目前，具有较高的权威性和认可度的网络空间安全攻防能力相关的国际培训和认证包括：

1.美国国家网络安全学术卓越中心计划（NCAE-C）

美国国家网络安全学术卓越中心计划（NCAE-C, National Centers of Academic Excellence in Cybersecurity）由美国国安局联合美国网络安全和基础设施安全局（CISA）推出，旨在指导美国社区学院、学院和大学等学术机构，建立网络安全课程和学术卓越标准，组织网络安全实践，提升全国网络安全教育，培养下一代网络安全专家。

该计划是一种对教育机构从事网络安全人才培养能力的认证，分为三类认证：

- CAE-CD，国家网络防御学术卓越中心（National Centers of Academic Excellence in Cyber Defense）
- CAE-R，国家网络研究学术卓越中心（National Centers of Academic Excellence in Cyber Research）
- CAE-CO，国家网络运营学术卓越中心（National Centers of Academic Excellence in Cyber Operations）

目前美国已经有300多所院校通过CAE-CD认证，79所院校通过CAE-R认证，22所院校通过CAE-CO认证。

2.国际信息系统安全认证联盟(ISC)²（International Information Systems Security Certification Consortium）

● CISSP(注册信息系统安全师)

● CCSP(注册云安全师)

3.信息系统审计与管控协会ISACA(Information System Audit and Control Association)

● CISA(注册信息系统审计师)

4.国际电子商务顾问局 EC-Council(International Council of E-Commerce Consultants)

●道德黑客 CEH(Certificated Ethical Hacker)

● CPENT(认证渗透测试专家)

5.美国计算机行业协会 CompTIA(Computing Technology Industry Association)

● CompTIA Security+

6.思科Cisco公司

● CCIE(Cisco Certified Internetwork Expert)-Security

国内认可度较高的网络安全攻防能力相关培训认证有:

1.中国信息安全测评中心认证

● CISP(注册信息安全专业人员)

● CISE(注册信息安全工程师)

2.公安部的网络安全等级测评师认证

3.华为公司安全工程师职业技术认证

● HCIA-Security(工程师)

● HCIP-Security(高级工程师)

● HCIE-Security(专家)

4.杭州华三通信技术有限公司H3CSE-Security(安全技术高级工程师)认证

5.3.4 安全众测

安全众测是一种新兴的网络安全测试方法,它依靠网络上的工作者帮助完成测试任务,具有成本低、效果好、速度快的特点。网络安全众测是通过互联网平台聚集安全人才对特定目标系统开展安全测试的新型安全服务模式,是一种指向性明确的、开放的、经授权的渗透测试。网络安全众测作为蓬勃发展的网络安全产业应用,在许多重要行业领域如金融、通信、工业等均有强烈的应用需求。

在网络安全众测任务中,厂商或平台将测试目标资产及相应的规则(比如禁止DDoS攻击,禁止修改数据,禁止高强度扫描行为等)在特定的人员和时间范围内进行公示并设立相应的奖项和酬金,公开招募安全人员对其进行安全测试并反馈安全漏洞信息,按照实际的测试效果对安全人员进行激励。这种开放式安全测试模式能够有效突破原先在封闭式环境下由有限的测试人员和工具进行安全测试的局限性,大幅提高了测试人员的数量和效率,从而能够在有限的资金和时间投入下,实现安全测试效果的最佳化。网络安全众测遵循开放、公平、公正的原则,主要适用于面向公网开放的信息系统的

安全测试工作，采用预先设定测试目标和奖励办法，先提交者先得奖励，漏洞等级越高奖励越高，安全测试查找漏洞过程的同时也是各个接受测试任务的安全人员比速度、比能力的竞赛过程。

2016年3月美国国防部（DoD）宣布，邀请1400名白帽子参与“黑进五角大楼”的漏洞赏金计划，体现了美国最高国防机关对网络安全众测的开放态度。从2016年4月18日至5月12日，在短短的一个月内，共有约250位安全人员报告了五角大楼存在的漏洞隐患，最终有138人被确认符合奖励资格，并获取了100到15,000美金不等的奖金。据统计，该计划共为此支付了多达75,000美元的奖金。在这次漏洞赏金计划中，最年轻的获奖者年仅14岁。可见众测项目对于年轻的网络安全爱好者来说，是个极好的锻炼和崭露头角的机会。

在我国，i春秋、补天、漏洞盒子等众测平台以及企业的SRC等平台通过等级贡献表、排行榜、积分奖励以及各类挑战活动、技术分享会等线上和线下活动等方式，也吸引了不少年轻的白帽，是网络安全人才成才成长的平台。在i春秋的白帽成长体系中，把白帽由低到高分为青铜、白银、黄金、铂金、钻石、星耀等等级。

5.3.5 攻防演练

网络安全攻防演练是以获取指定目标系统的管理权限为目标的攻防演练，由攻防领域经验丰富的红队专家组成攻击队，在保障业务系统稳定运行的前提下，采用不限攻击路径，不限制攻击手段的贴合实战方式，而形成的有组织的网络攻击行动。攻防演练通常是真实网络环境下对参演单位目标系统进行全程可控、可审计的实战攻击，拟通过演练检验参演单位的安全防护和应急处置能力，提高网络安全的综合防控能力。

“网络风暴”（Cyber Storm）是美国网络安全和基础设施安全局（CISA）举行的国家级网络活动，是全美范围最广的网络安全对抗演习，始于2006年，每两年在美国本土举行一次。“网络风暴”演习将政府(联邦、州政府)、行业机构、国际合作伙伴以及私营企业（如关键基础设施类企业以及高科技企业）聚集在一起，一般以先前发生的真实事件为基础，模拟对影响国家关键基础设施的网络危机的响应，通过演练最新的应急响应政策、流程和程序，加强美国在应对影响范围波及多个行业的网络攻击的网络安全战备和应急处置能力。

“网络欧洲”(Cyber Europe)是由欧盟网络与信息安全局（ENISA）主办的由欧盟国家、欧洲自由贸易区（EFTA）以及欧盟各机构与部门参与的全欧范围的网络安全攻防演习，每两年举办一次，用于测试并培养成员国携手并解决跨境网络事件的能力。刚刚结束的CyberEurope2022涉及对欧洲医疗基础设施的模拟攻击，来自欧盟29个国家和欧洲自由贸易区(EFTA)以及欧盟机构和机构的800多名网络安全专家参与了演习。

2016年开始，我国对网络攻防演练的重视和实战提上日程，并且在近几年不断常态化，民间机构、各大企业也尝试开展日常化的攻防演练，而网络靶场产品的涌现和应用则进一步推动了攻击演练的发展。

护网行动是由公安部组织的国家级网络安全攻防演练，每年举办一次，针对机关和企事业单位的网络安全领域的真刀实枪式的攻防演练，用以评估企事业单位的网络安全

活动。攻防演练主要目标涵盖国家重要行业的关键信息基础设施，每年覆盖行业、单位、系统都在逐渐扩大。公安部组织进攻方在一段时间内（一般半个月）内对防守方发动网络攻击，检测出防守方（演练目标）存在的安全漏洞。

通过真实网络中的攻防演练，可以全面评估目标所在网络的整体安全防护能力，检验防守方安全监测、防护和应急响应机制及措施的有效性，锻炼应急响应队伍提升安全事件处置的能力，更能够锻炼和快速提升网络安全人才的攻防能力，有助于形成一支训练有素、经验丰富的应急响应团队。

5.4 网络安全人才攻防实战能力提升路径

人才培养的途径包括院校培养、企业培养、机构培训、个人自学等方式。如何将这几种方式合理结合或打通，形成有效的网络安全人才攻防实战能力提升路径，促进人才的不断涌现？

建议首先建立统一的网络安全攻防实战能力框架，形成对人才培养的指导，进一步对网络安全攻防实战能力相关课程/培训进行认证认可，同时通过“竞赛选拔、分类提高、职业引导”的方式，将竞赛、众测、攻防演练、技术分享等方式相结合，形成常态化攻防人才成长通道。

5.4.1 统一的网络安全攻防实战能力框架

建议参照美国的“国家网络空间安全教育计划”（National Initiative of Cybersecurity Education，NICE），首先由国家有关机构主导，建立统一、公开的“网络安全人才队伍框架”或“网络安全攻防实践能力框架”（以下简称为“能力框架”），明确网络安全人才攻防实战能力的具体要求。在该能力框架的指导下，各院校、企业、个人学习者都可以找到适合自身的内容加以建设，或找到合适的定位和发展方向。

美国国家网络安全教育计划（NICE）由美国国家标准技术研究院NIST 牵头，国土安全局（DHS）、国防部（DoD）、教育部（ED）、美国国家科学基金会（NSF）、国家情报总监办公室（ODNI）、美国联邦人事管理局（OPM）等共同领导。该计划于2010年计划启动，2017年正式发布《NICE网络安全人才队伍框架》（NICE Cybersecurity Workforce Framework，NIST SP 800-181）（以下简称“NCWF框架”）。该文件提出了网络安全人才角色分类、知识能力框架，可用于评估工作人员的专业化水平，为预测未来网络安全需求推荐最佳的实践活动，为招募和挽留人才制定国家策略。

NCWF框架通过对行业内分析各类组织的职位描述的分析（包括公开渠道、DoD 和联邦政府内部数据），并通过广泛、充分的行业内讨论对安全行业内的工作类型、专业领域、工作角色、知识、技能、能力和任务进行了体系化的梳理。该框架用类别（Category）、专业领域（Specialty Area）和工作角色（Work Role）来描述网络空间安全工作，每个工作角色由大量独立的工作任务（Task）和与之对应的 KSA（知识、技能、能力的统称） 组成，见5-4。

图5-4 NCWF框架

不可否认的是，网络安全作为一门实践性极强的学科，对人员攻防实战能力的评价离不开基础知识、基本技能以及能力水平等维度的考核。而面对日益复杂的网络环境，如何更有效地规避各类网络安全风险，除了知识与技能的必要保证，最根本的人员安全意识恰恰是最容易被忽略、也是最可能以低成本减少安全风险的版块。

NCWF框架的工作角色（Work Role）中对“能力”的检验需要通过具体实践（Practice）来衡量，同时实践也是提升与检验知识和技能最好的方式，更能直接衡量培养效果。而学习知识（Knowledge）、具备技能（Skill）的前提是意识（Awareness），所谓意识决定行为，有了良好的意识才能主动学习知识，积极提升技能，有参与实践的能力和意愿，才会有更高的积极性去了解行业规范及所需能力等。这里将网络安全人才培养模型分为意识、技能、知识、实践四个维度，每个维度对应的子模块示意如图5-5所示。

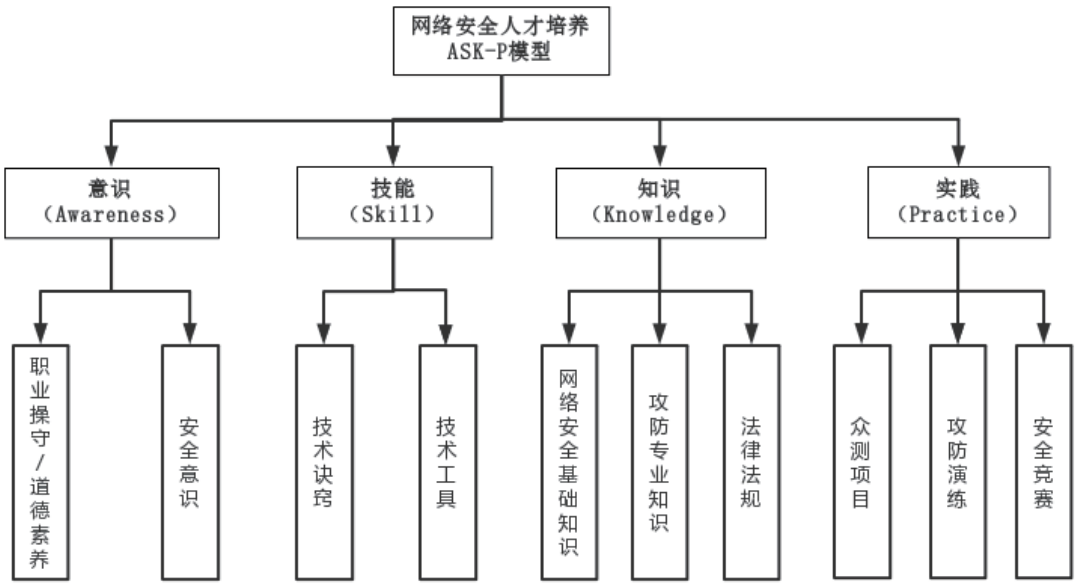


图5-5 ASK-P框架

从模型来看，K（知识）是最容易获得的，S（技能）需要持续训练，在实际工作的工程实践中才能获得综合P（实践），而A（意识）是贯穿始终的。

安全意识体系-提升安全意识（A）

首先，要让网络安全从业人员建立一个良好的职业素养，从意识上先认可并重视网络安全相关岗位。安全意识获取是主观认知，用来判断价值、影响行为，个人在网络设备使用和网络系统使用过程中的操作或活动对网络安全风险的感知意识、防范意识和行为意识，这些都涉及人的态度和情绪。安全意识的形成至少要经过价值判断和情绪反应两个阶段，除了直接影响安全的行为因素，也包含品德、职业精神，对工作的负责程度等间接影响因素。所以安全意识培训是要让大家认识到“为什么学安全”，了解本岗位知识及技能需求，从价值判断上知道安全意识培训的价值和自我成长的价值，从而建立良好的职业素养。

安全技能体系-提升应用技能（S）

其次，在安全岗位中需要人员具备实际操作能力，不管处于什么岗位，都要能承担起岗位职责，要具备处理岗位工作的技能。在具备高度安全意识前提下，加强技能的训练，以满足项目与工作的需求。安全技能的获取是实操训练，通过网络安全技能提升实验、仿真环境专业实训、实操演练等培训方式，提升技术能力、实操技巧、协作沟通能力等，以做到能够将技能学以致用。

安全知识体系-掌握专业知识（K）

再次，根据网络安全岗位的人才等级需要具备的知识体系开发系列课程，知识域可分为安全知识、专业知识、拓展知识、设备与工具知识等内容，确保具备岗位的专业知识，并为后续的综合实践打下理论基础。安全知识的获取是客观记忆，而网络安全又是一个交叉学科，除了涉及数学、通信、计算机等自然科学知识外，还涉及法律、心理学等社会科学知识，对于网络安全知识的学习是要建立一个多领域的复杂知识系统。知识可以体系化主动学习，也可以从经验中直接获得，也可以通过他人传授间接获得，认知心理学对大脑的研究发现，知识在人的大脑中是以分类树状结构存储的。所以想要掌握安全知识靠的是学习和思考。

安全实践体系-进行岗位实践（P）

最后，通过攻防实战演练、攻防竞赛等实践形式，进行业务能力提升的岗位实践。将知识与技能融会贯通，综合利用各种技术和非技术手段，动态提升实战攻防的工程实践能力，挖掘前沿技术，发现安全风险趋势，输出知识沉淀内容，继而形成新一轮培训的良性循环。

网络安全是强调实战能力的实践性学科，尤其面对现在“万物互联”的复杂网络空间环境，我们面对的网络安全威胁可能来自技术的和非技术的攻击手段，比如利用“电脑漏洞”发起的技术攻击和利用“人脑漏洞”发起的社会工程学攻击。不能仅仅孤立的掌握安全意识、安全知识和安全技能，还需要将意识、知识、技能融会贯通，具备综合实践能力。

5.4.2网络安全攻防实战能力课程/培训认可

高等院校培养，包括普通大学、高职高专、民办高校等，是人才批量化培养的主要方式，也是为人才提供基础知识储备、系统性理论支撑教育的重要保证。但院校培养体系在具备系统化、理论化和学术化等特点的同时，在针对性、实用性、灵活性、技能性方面存在不足。

企业培训一般围绕特定岗位或任务展开，针对性、实用性强、灵活度高，强调技能实操，但缺少系统理论上的指导，人才发展后劲不足。

机构社会化培训方面，参与培训人员往往以取得证书或者提升能力实现就业为目标。在网络安全方面，尤其是网络攻防领域，新技术、新方法层出不穷，也较容易形成热点，培训机构蜂拥而上，导致各类培训证书层出不穷，鱼龙混杂，难断高下。

建议在统一的“能力框架”的基础上，形成一批高校、企业、培训机构的认证（认可）课程或认证（认可）证书。

各高校、企业、培训机构在相关课程／培训中，如果内容覆盖有“能力框架”中足够的知识点、技能点，可以向有关机构进行报备获得认可（类似于学历认证）。

根据不同领域、不同专业的要求，覆盖知识点、技能点的情况，获得足够的认可证书或通过足够的认可课程，相当于取得了相应级别的能力认证。相应的课程、证书也可以成为企业人才招聘的依据之一。

5.4.3常态化攻防人才成长通道

建议借鉴美国网络挑战赛（USCC, US Cyber Challenge）的模式，通过建立常态化的“竞赛选拔、分类提高、职业引导”的培养方式来打通院校和企业实际需求之间的网络攻防人才成长通道。

美国网络挑战赛（USCC, US Cyber Challenge）[https://www.uscyberchallenge.org/]是由国土安全部支持的一项国家计划，面向高中、大学和研究生开展竞赛和现场培训，旨在寻找和支持有才华的年轻美国人，发展他们的技能，获得高级培训，并获得奖学金、实习和工作的认可，是美国挑选、吸引、培训、招聘和吸纳新一代网络安全相关专业人员的重要项目。

USCC由两个计划组成：Cyber Quests竞赛以及Cyber Camp计划。

Cyber Quests竞赛一般每年举行1—2次，分别在春季和秋季，是一整套的在线挑战，测试信息安全的基础知识和动手能力，涵盖从安全编码到网络监控任务。根据Cyber Quests的表现，参与者被邀请参加USCC组织的某一个Cyber Camp。

Cyber Camps一般暑期举行，安排在全国各大学或研究机构，是为期一周的线下研讨会（2022年线上举行），内容包括动手实验、黑客竞赛，会由领先的大学和行业顶级的专业人士介绍新概念和安全技术，并在渗透测试、伪数据包制作、网络战，甚至职业发展道路等方面进行指导。

1.竞赛选拔：

竞赛选拔可以采用多种方式，如在线CTF、众测、漏洞挖掘等，或多个赛道，目的是要让更多的自主参赛人员有进一步的上升途径。让他们体会到，竞赛不是少数人的游戏、多数人的围观，而是得以进入到一个更大更广的成长空间的入场券。

可以仿效DEF CON，设立一些授权外卡赛，或国内春秋杯通过春秋积分进行个人能力评定的春秋认证模式，取得相应外卡或积分的人员方可以申请进入下阶段的培训提高。

在选拔过程中，应注意以下几点：

- 要实现竞赛选拔人才与制定的“能力框架”之间的对应；
- 要注意不同竞赛之间，以及参赛个人和团体评价考核的标准化；
- 要针对不同年龄阶段、不同技术水平参与者设置不同的联盟，形成竞赛梯队。

2.分类提高

对通过竞赛选拔出来的不同赛道、不同技术水平、不同年龄阶段的优秀人员分配进入每年夏季举办相应的全国性训练营或研讨会，或进行不同主题的集中培训，着重加强某方面攻防实战能力的提升。

3.职业指导

在培训的同时，选派资深的企业人员对参训人员进行职业发展道路、成长路径等方面的引导，还可以通过推荐实习、项目实践等方式引导网络安全人员提早进入专业/职业轨道，投身于网络安全事业。

通过这样每年相对固定时间、常态化的“竞赛选拔、分类提高、职业引导”的方式，可以吸引更多更广泛的学生或社会人员投身于网络安全事业，专注于攻防能力的提升，对于我国网络安全人才的培养必然会形成良性循环。

于各行业、各领域的从业人员而言，匹配其对应的岗位实践进行能力提升无疑更为重要。与学生群体不同的是，在这一方面，无论是从业人员自发性进行个人能力提升的行为，亦或是其所在企业单位创造或提供的各种能力提升途径，均代表了从业人员这一群体的个人成长通道。概言之，以“实践选拔、梯队建设、价值引领”为核心的培养方式不仅能够促进从业人员整体能力的提升，同时也能达到人才培养与企业发展相辅相成、彼此成就的最终目的。

1.实践选拔

从业人员与学生群体在进行个人能力提升时最大的不同在于所处的岗位与职责，而这些也是实践经验的一部分。企业通过组织一系列攻防演练与竞赛比武等实践活动，进行常态化人员检验与磨砺。既能发现并及时处置安全风险，有效检验整体网络安全防护水平和应急处置能力，又能锻炼队伍，选拔人才。此外，作为企业员工通过积极参与内外部的安全竞赛、攻防演练，甚至众测等实践活动，在提升自身实践能力的同时，取得的成绩也可以作为有效选拔的依据，证明自身的能力价值。

2.梯队建设

通过各种实践方式对不同部门、不同岗位、不同方向的网络安全从业人员进行分级分类，建设多层次专业化的网络安全人员梯队，按照实践经验与擅长技能分别进行人员与工作岗位的专业匹配。员工根据自身的职业发展可以明确成长路径，进行针对性的能力提升。

3.价值引领

一方面企业承认员工在实践过程中取得的荣誉，并通过晋升、调薪等直接有效的方

式给予认可；另一方面，各地方、各单位针对网络安全技术人才陆续出台的福利政策，对从业人员的积极性有极大的促进作用。作为从业人员自身而言，无论是出于企业硬性规定与要求进行自我学习与提升，还是基于未来发展与规划而做的努力，都可看做是个人成长道路上的价值引领。微观层面上，每一个从业人员不同的诉求、不同的价值驱动，体现在宏观层面上，其产生的结果均是在结合知识、技能与在岗经验的协调与平衡后，个人能力提升与企业稳健发展的良性互动。

第六章

总结和建议

6.1 院校人才培养体系建设建议

6.1.1 理论教学体系建设

网络安全学科是一门实践性极强的学科，面向网络安全人才实战能力的培养，院校的人才培养体系应开设针对性的实践性课程，同时开设攻防实战相关课程及培训，这对课程内容的深度和系统性应有更高的要求，培养学生能理论结合实际应用综合分析问题、对前沿技术的探索、攻防博弈思想的理解及综合构建知识体系的能力，以提高学生的网络安全实战能力。

企业讲师进驻理论和实践课堂，为学生带来企业一线的最新内容、实时内容。鼓励企业深度参与院校网络安全人才培养工作，从培养目标、课程设置、教材编制、实验室建设、实践教学、课题研究及联合培养基地等各个环节加强同院校的合作。

企业根据学校制定的教学大纲和计划，与教师进行教材编制、配套实践教学内容设计，让理论教学与实际需求结合的更加紧密。以知识点需求和应用为主线，采用经典+前沿的方式对各个技术领域进行系统性介绍，确保教材内容的完整性和前沿性，同步开展实验资源与教学互动平台建设，提升课程建设质量。

6.1.2 实践教学体系建设

网络安全人才的实战能力与行业企业需求仍然不匹配，解决实际问题能力仍然不足。需要推动校企合作，参与网络安全课程建设，建立校外实习实训基地，将实战需求与课程学习有机结合。通过师生走进企业、企业进入校园等多种方式，共同培养符合企业用人需求的、高水平的网络安全实战人才。

建立联合创新研发机构，加快产业技术转化，共享技术研发成果。广泛开展院校与企业的项目合作，开展建设合作项目。广泛深入开展协同育人项目，设立优质联合创新研发实验室，建立校企协同创新中心，通过协同创新，加快推进科研成果产业化，助力相关产业高质量发展。

院校与网络安全企业合作，进行各种形式校企合作，引导行业企业加入创新创业人

才培养体系，从培养目标、课程设置、教材编制、实验室建设、实践教学、课题研究及联合培养基地等各个环节加强同院校的合作。积极探寻学生与院校科研团队的合作模式，使学生在科研过程中体验实际科研团队的工作，真正真实地参与实际科研活动，丰富学生自己的网络安全技能，在此过程中全面提升网络安全工程及攻防实战能力。

推进科教融合，不仅包括高等院校与科研院所的联合，还包括高校内部科研活动与教学活动的融合。实现科研与教育的有机融合，推动科技创新全过程与人才培养全过程的紧密结合，把科研创新成果转化为教学内容，把科研项目转化为学生工程实践案例，把一流的科研平台与科研设施转化为学生学习平台与实践环境。

推进产教融合，既充分发挥企业的工程实践主体作用，又紧密对接社会对人才的需求。深化产教融合，实施校企合作，改革人才培养模式，创新考核机制，创新合作模式，总结在实施过程中存在的问题和不足，进一步创新提升专业人才培养质量为核心的“产学研一体”任务化教学人才培养模式，以及以企业真实项目为任务的教学模式，将教、学、产、创等教学环节相结合相融通，是提升学生学习效果、实际上手操作能力、学生职业素养的更好方式，更加有利于培养学生的创新实践能力和综合应用能力。

6.2 企业单位人才培养建设建议

企业单位的人才培养建设包括人员培训、竞赛演习、高校深造、高校联合培养等方式。需要将这几种方式持续执行并有机结合，形成企业单位的网络安全人才攻防实战能力提升路径，促进网络安全人才的培养，成长与涌现。

加强人员培训和培养，定期开展网络安全攻防实战，网络安全管理等方面的专题培训讲座，在完成培训后，可以对人员进行网络安全知识的考核，强化企业单位人员的网络安全意识。通过培训、教育、考核等诸多措施，实现企业单位网络安全人员应对网络安全风险的能力。在培训中，选派资深的网络安全人员对参训人员进行职业发展成长等方面的引导，对企业的网络安全人才的培养形成良性循环。

开展网络安全类攻防竞赛演习训练和竞赛活动，组织员工参加国家级网络安全竞赛，在实战中评估企业单位网络安全水平，在实战中挖掘，检验并培养网络安全人才，提升企业单位网络安全实战能力和水平。

支持高等院校引进企业单位的网络安全领域高端人才，支持网络安全领域人才赴高校培训进修。以此结合理论与实践的结合，改善参训的企业单位网络安全人才的知识结构，进一步提升他们的网络安全攻防实战能力。

鼓励企业单位参与高校网络安全人才培养工作，校企共同合作，共同设立人才培养项目，构建“顶尖人才引进+基础人才培育+实用人才培训”的梯度人才体系，打造良性的，可持续发展的网络安全人才梯队建设。鼓励企业单位参与高校人才培养工作，统筹各自优势资源配置，积极完善网络安全学科布局，培训不同岗位的专项人才，培养“学术型+应用型”复合人才，推进形成以产业需求为导向、以岗位能力为基础的人才培育模式，加快培育高层次、跨领域、创新型、实用型的人才和团队。

打造具有丰富行业企业经验与教学经验的双师型团队是提升院校与企业合作水平极为重要的举措。按照企业需要，实施校内+企业联合培养；企业导师，案例加实践分享；建立企业与高校双导师制，突出人才培养的实用性和实效性，培养复合型人才。

6.3 政府扶持政策建议

对于网络安全人才的培养体系，政府配套的扶持政策要扮演重要的角色，各级政府需要积极参与引导，政府作为外部力量逐步将重心转移到对整个校企合作的规范性建设，推动在法律、标准框架以及产学平台和联盟的制定与搭建，作为学校和企业的自身局限性的外部支撑和保障，同时也是整个合作有序运转，促进双方内生性动力所必须的适配性环境。政府应该在政策上制定更加有利的政策和制度。如科学规划、营造氛围、鼓励创业，简化公司注册的程序，举办一些活动促成企业与高校的联合，进行舆论引导等等。

建议政府大力增加职业教育的财政投入，支持院校有序改善条件，适应产业发展和市场用工的需求。引导、鼓励、支持企业参与大学教育，关键是能出台相关的政策、规定，提高企业参与的主动性和积极性。各级政府从地方经济社会发展的高度，规划职业学校和企业的发展，统筹校企合作，将校企合作任务作为推动区域经济发展的重要手段，建立政府主导、职业学校和企业为主体、行业协会为中介的校企合作发展新机制。

校企合作只有在政府统筹和支持下，部门、企业和学校才能在校企合作上建立有效的合作模式与机制，校企合作才能够真正实现，达到双赢的目的。各级政府必须从地方经济社会发展的高度，规划职业学校和企业的发展，统筹校企合作，将校企合作任务作为推动区域经济发展的重要手段，建立政府主导、职业学校和企业为主体、行业协会为中介的校企合作发展新机制。坚持产教融合、教产合作、校企一体和工学结合的改革方向，提升职业教育服务区域经济发展和改善民生的能力。

扫描二维码, 发送关键词“白皮书”, 获取电子版。