2022

网络安全人才实战能力白皮书

攻防实战能力篇

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

目录

CONTENTS

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。

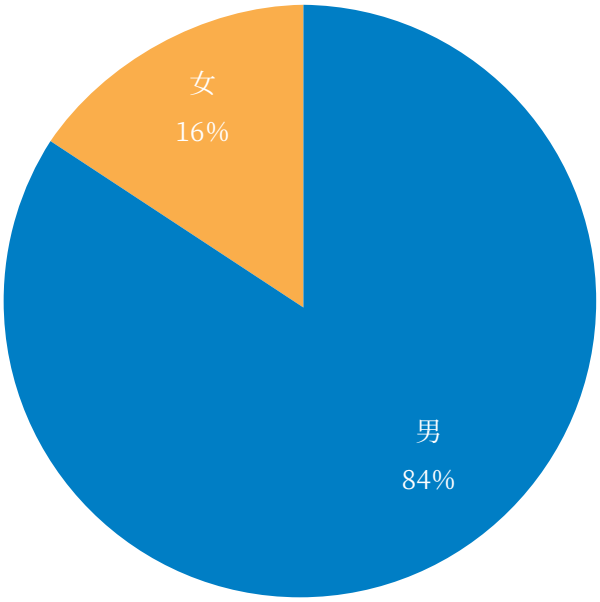


图2-1 网络安全攻防实战人才性别分布

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。

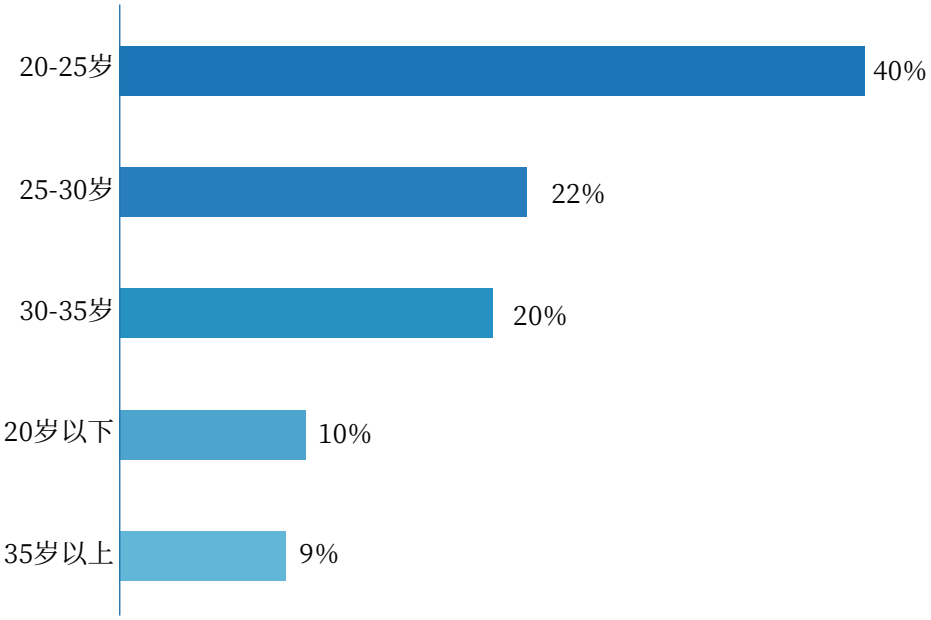


图2-2 网络安全攻防实战人才年龄分布

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。

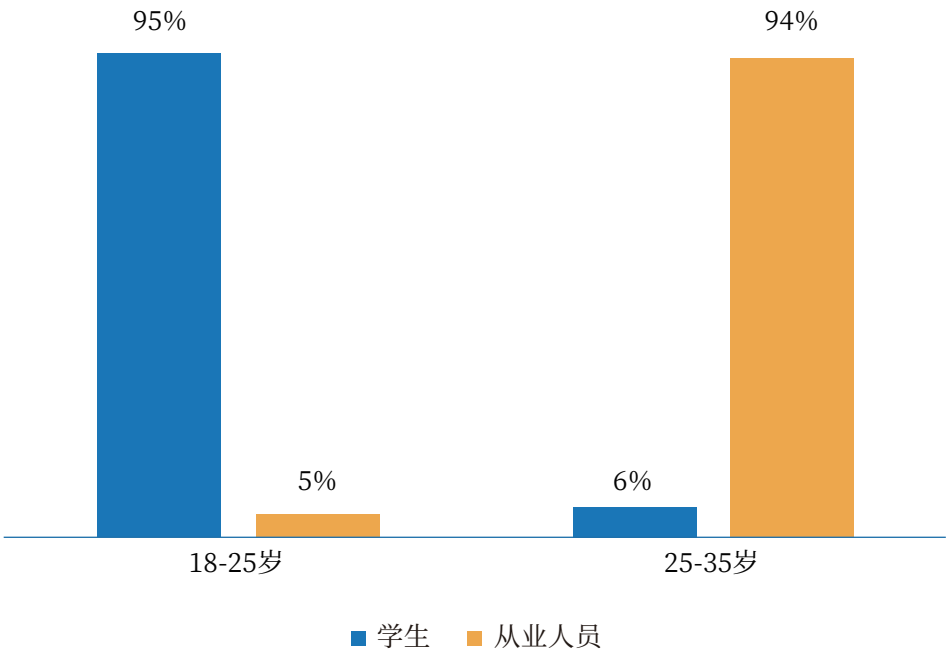


图2-3 不同年龄群体属性分布

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。

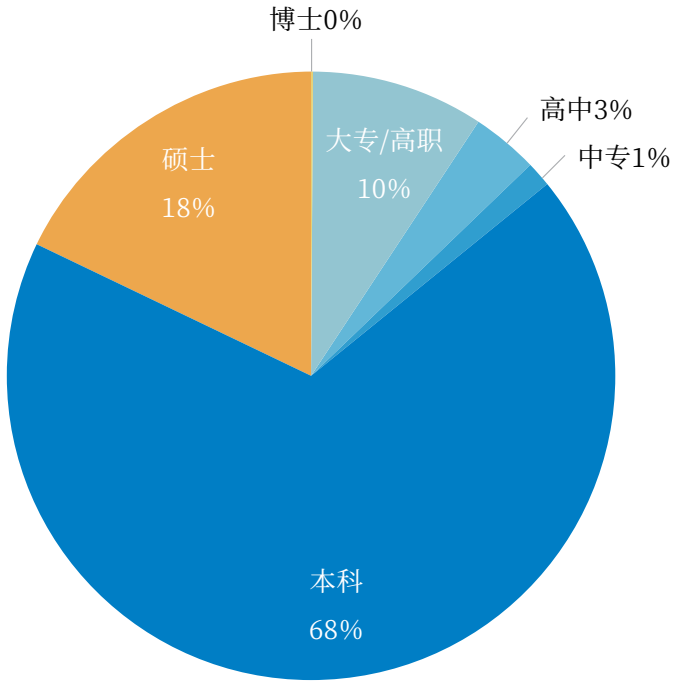
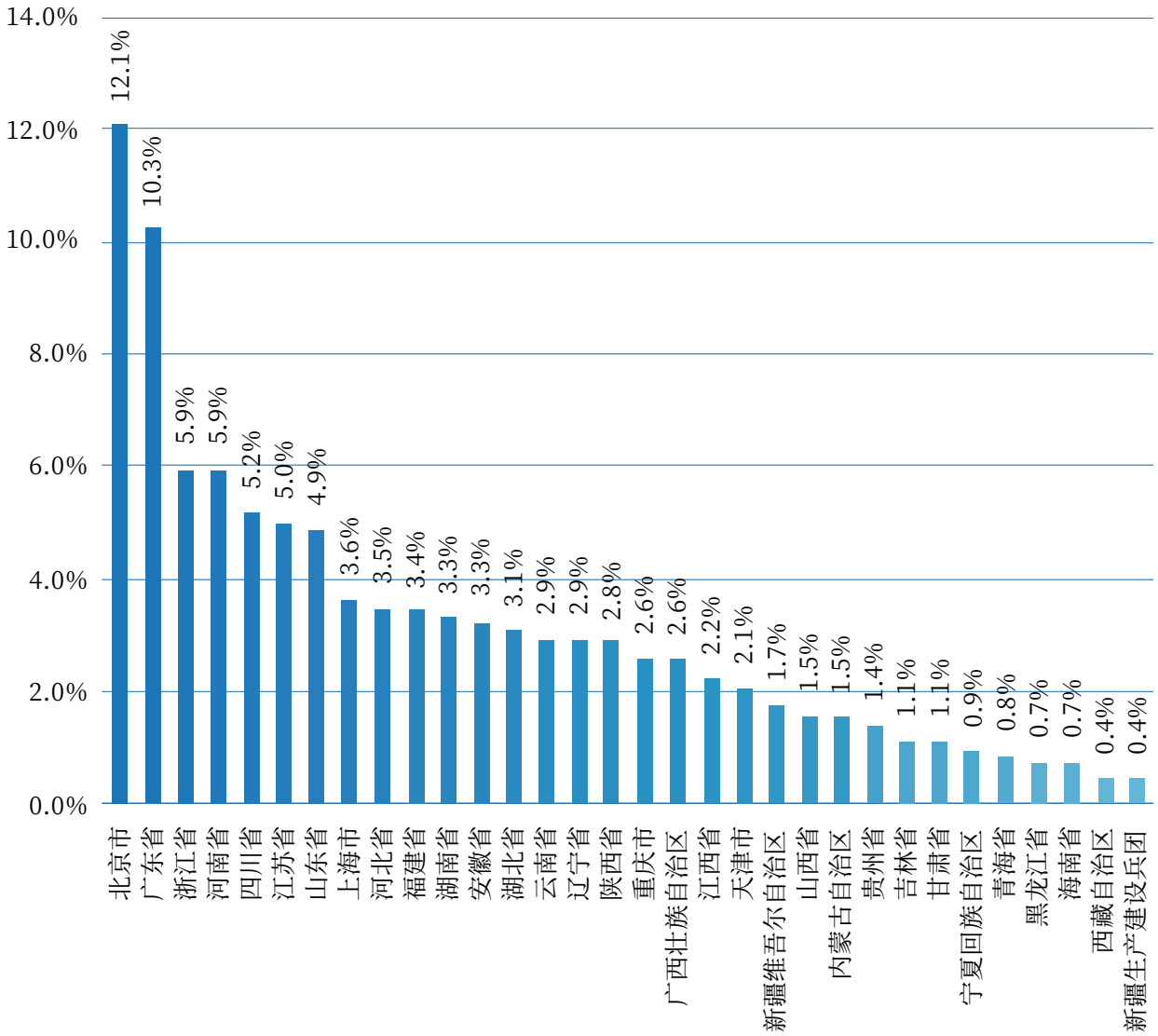


图2-4 网络安全攻防实战人才学历情况

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。

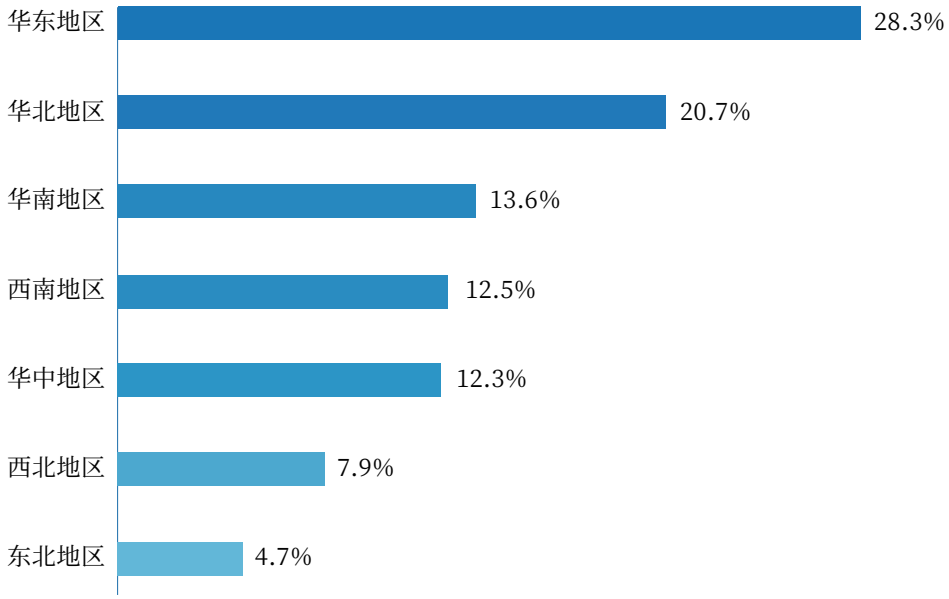


图2-6 网络安全攻防实战人才区域分布情况

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。

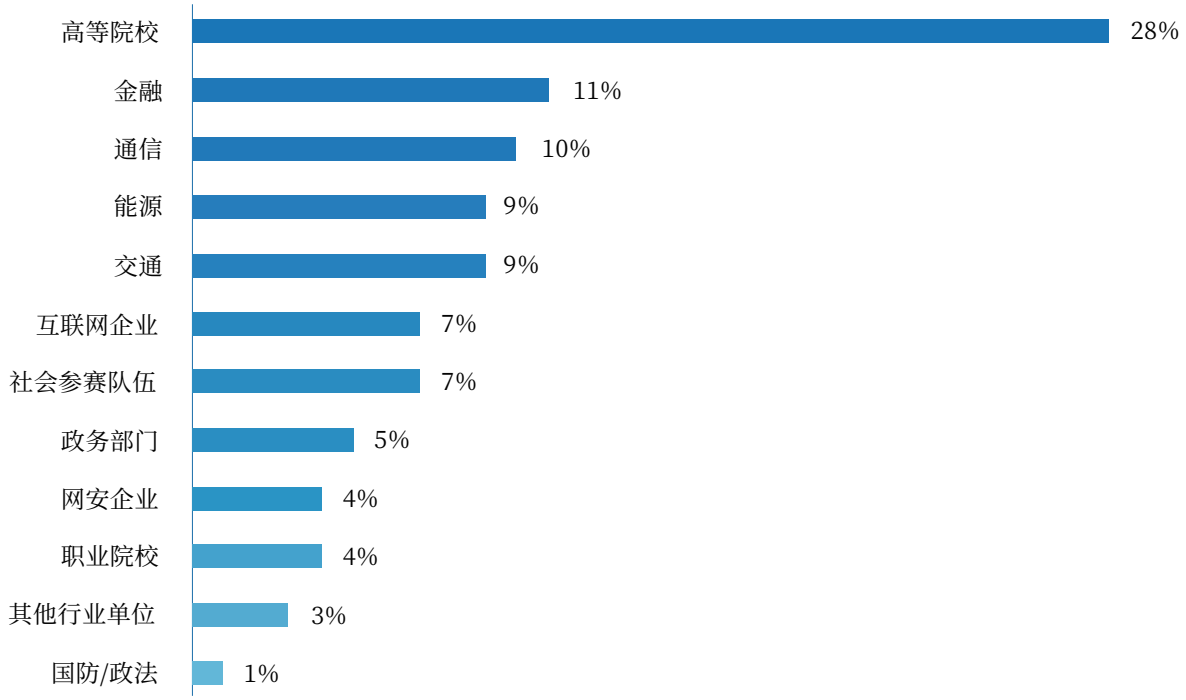


图2-7 网络安全攻防实战人才行业分布情况

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。

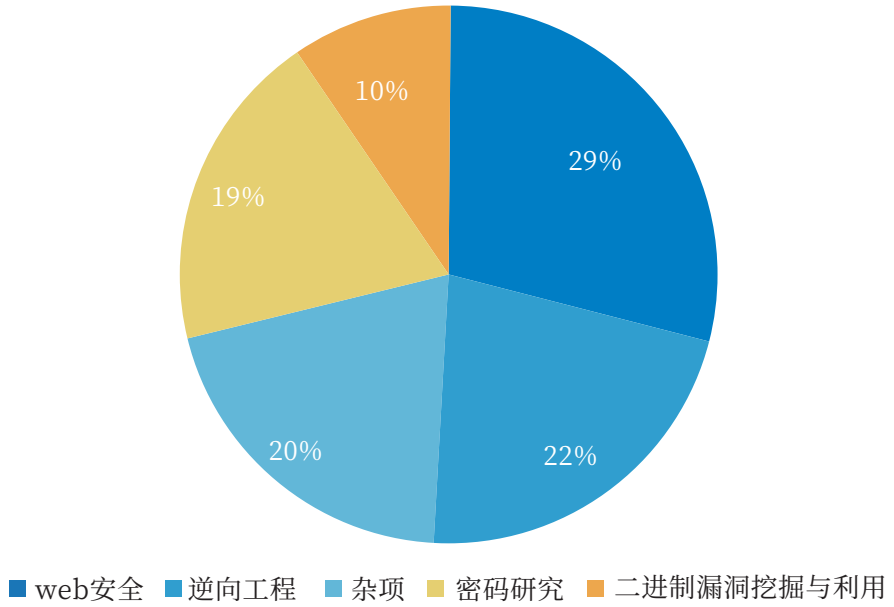


图2-8 专业人才能力分布

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。

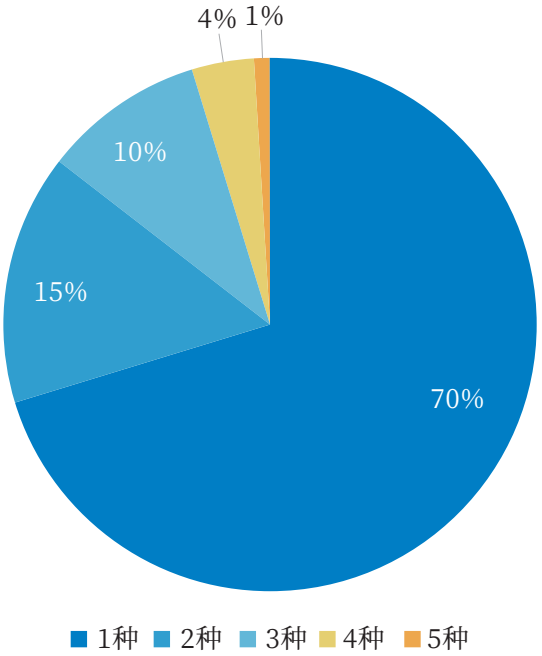


图2-9实战攻防人才能力种类覆盖

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。

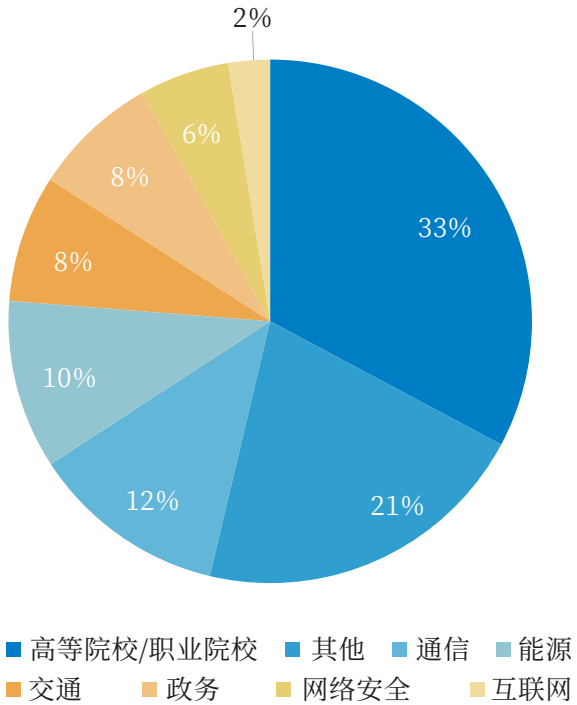


图2-10 Web安全人才行业分布

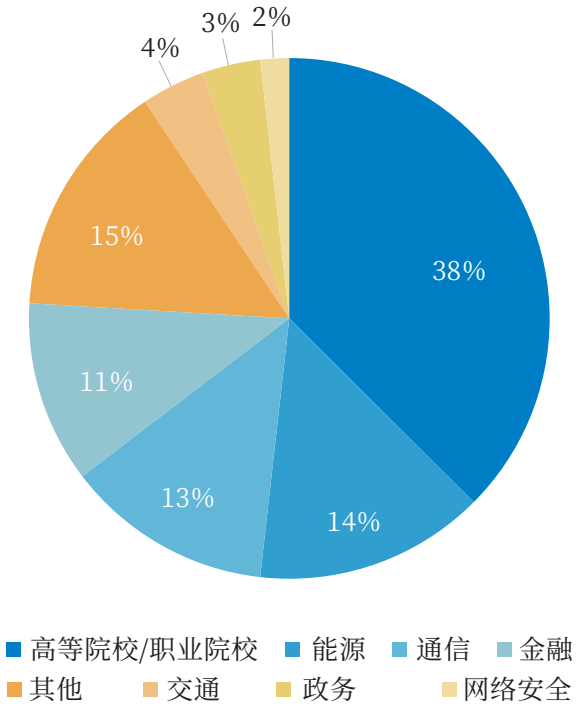


图2-11 密码研究人才行业分布

(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。

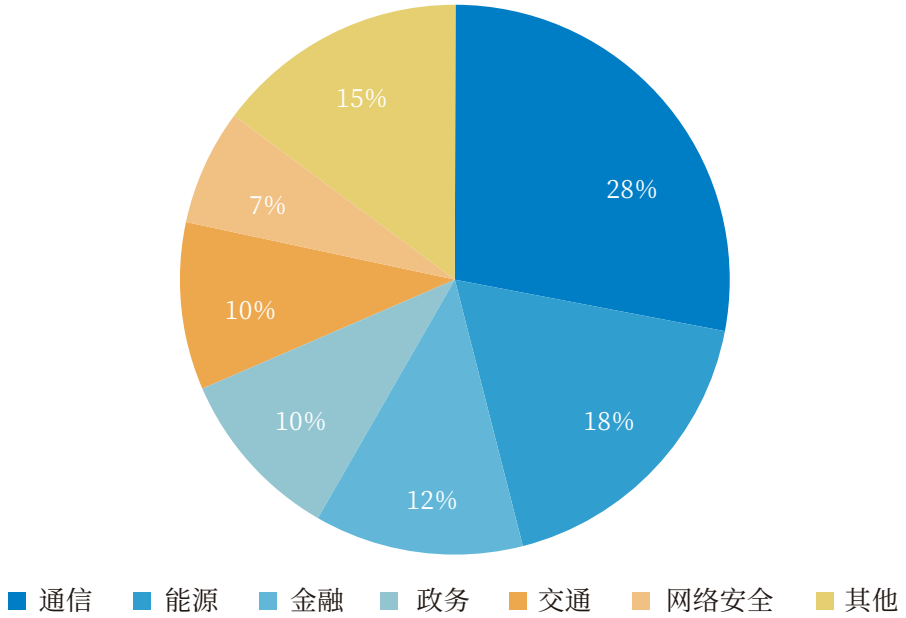


图2-12 杂项人才行业分布

(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。

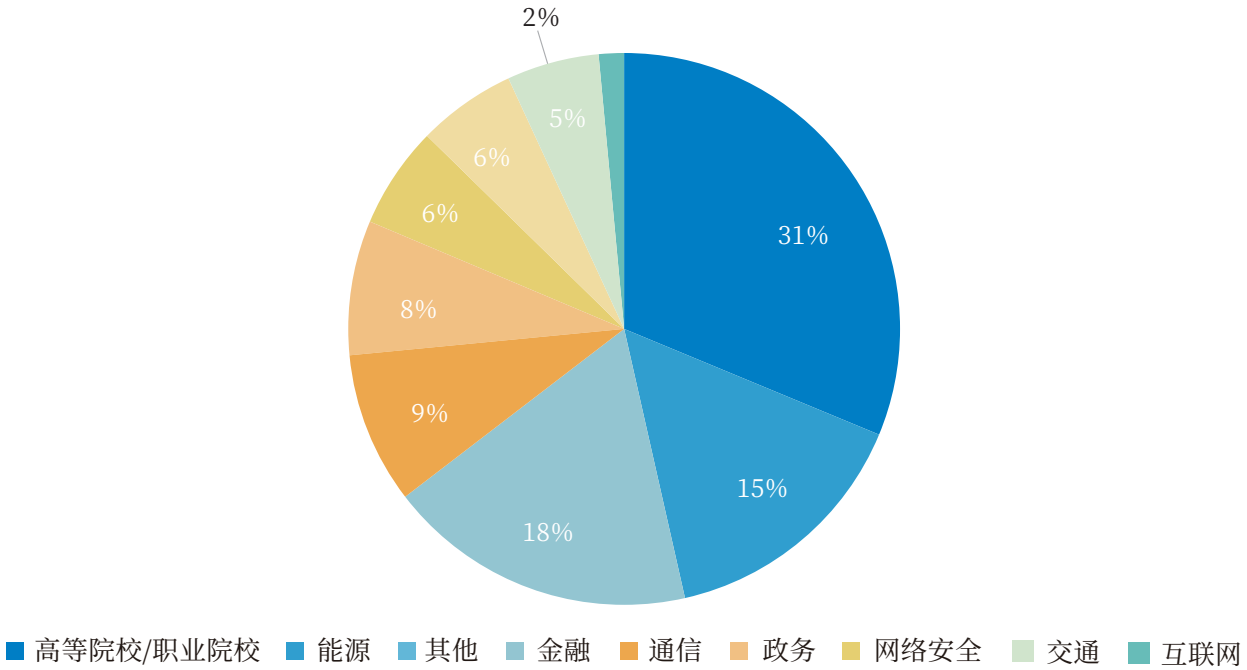


图2-13 二进制漏洞挖掘与利用人才行业分布

(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。

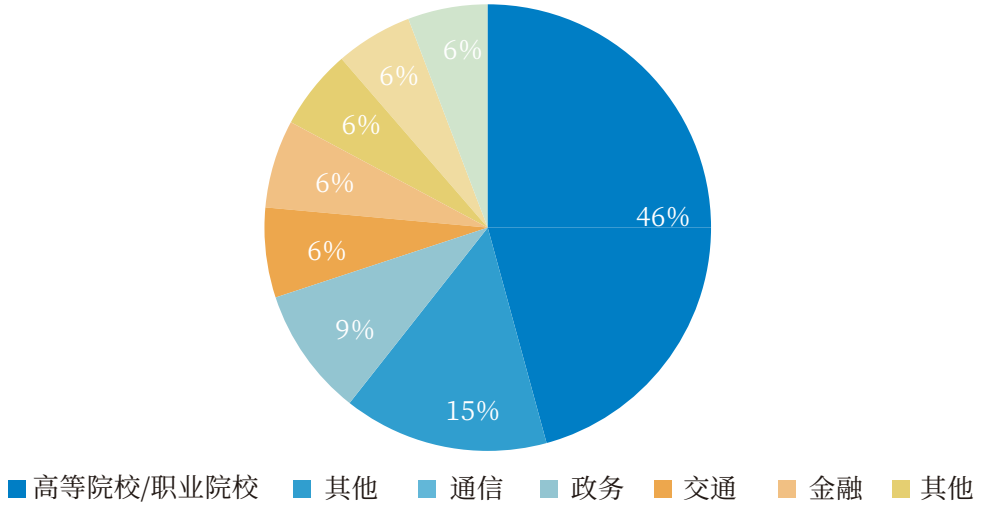


图2-14 逆向工程人才行业分布

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。

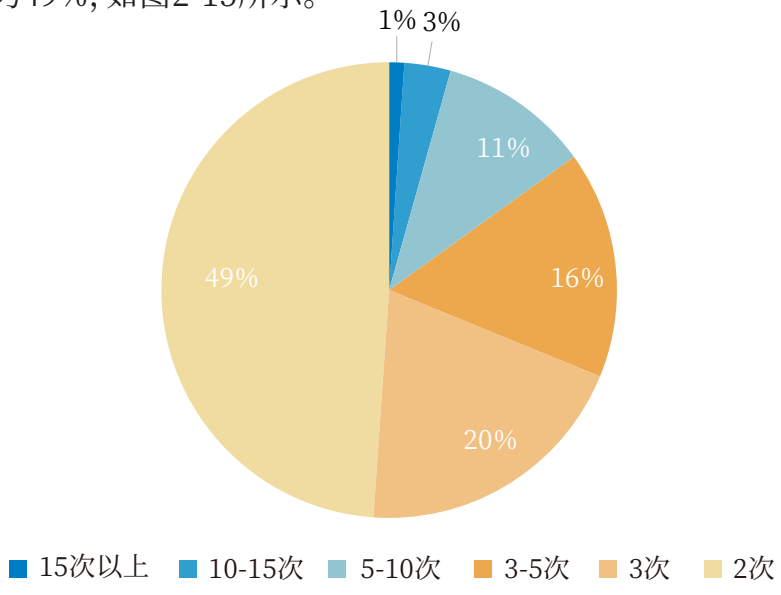


图2-15 选手参赛次数

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。

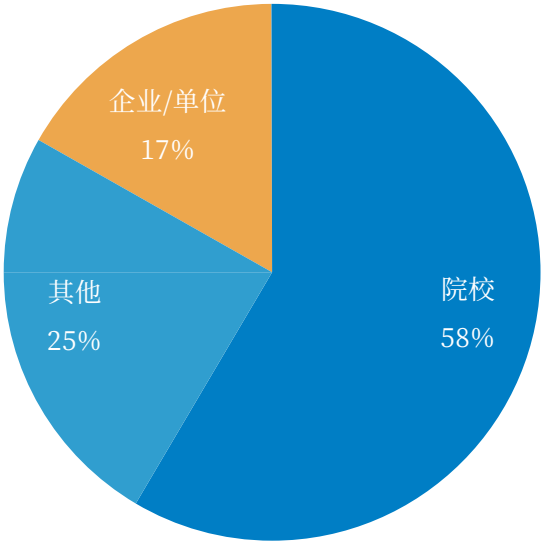


图2-16 参赛选手所在单位（2次及以上）

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。

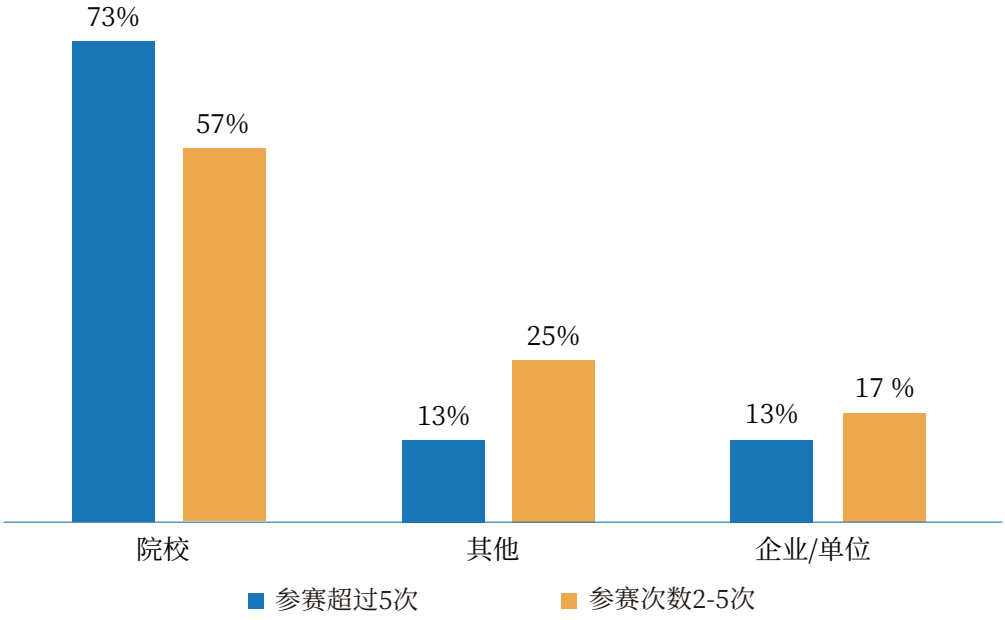


图2-17 参赛选手所在单位（2-5次、5次以上））

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

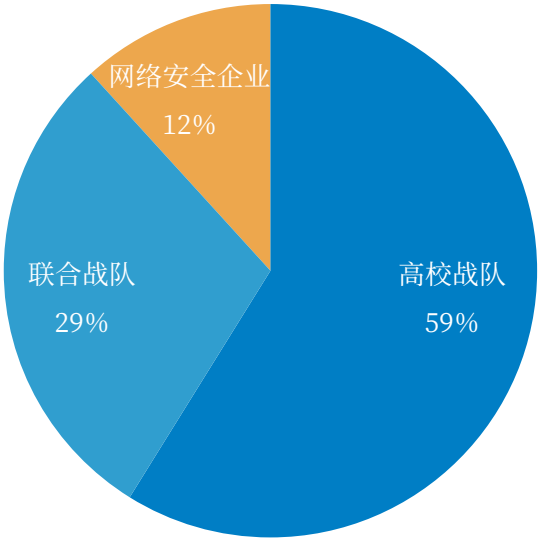
内最大规模工业互联网网络安全大练兵的“护网杯”、国家卫健委主办聚焦医疗行业的“卫生健康行业网络安全技能大赛”、聚焦数据安全领域的国家级赛事“全国数据安全大赛”、面向全国高等院校的高规格赛事“大学生信息安全竞赛创新能力实践赛”、面向全国警院学生的高水平网络安全赛事“蓝帽杯”等行业品牌赛；全国首个“以防为主”国家级网络安全赛事“陇剑杯”、全国首个城市级靶场演习的“巅峰极客”、聚焦华南地区的“红帽杯”、东北地区的“祥云杯”、京津冀地区的“长城杯”等区域品牌赛。

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。

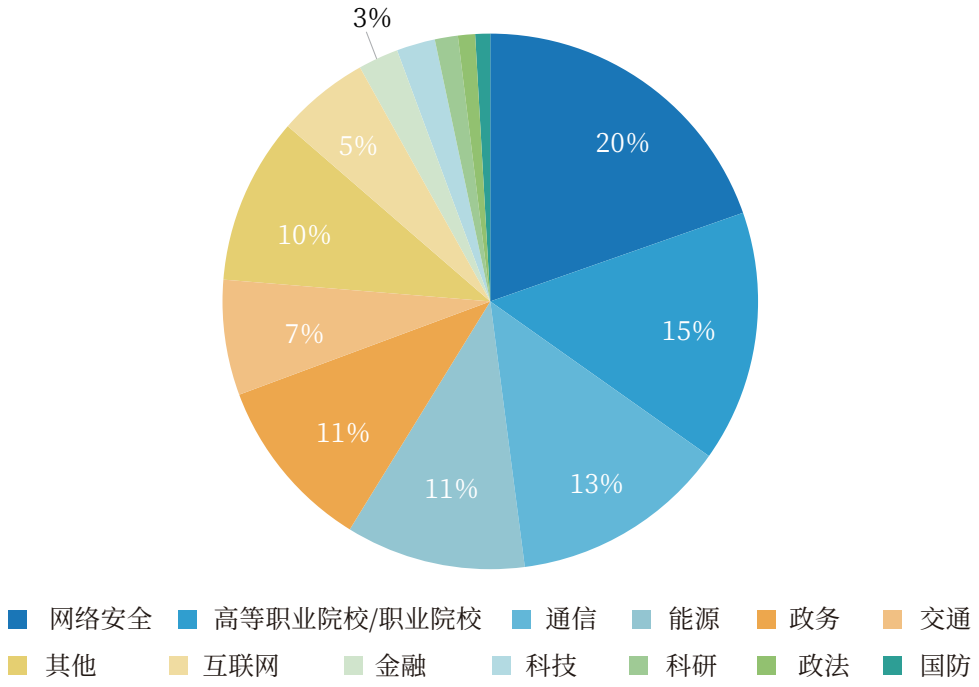


图2-19 TOP100人才行业分布

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。

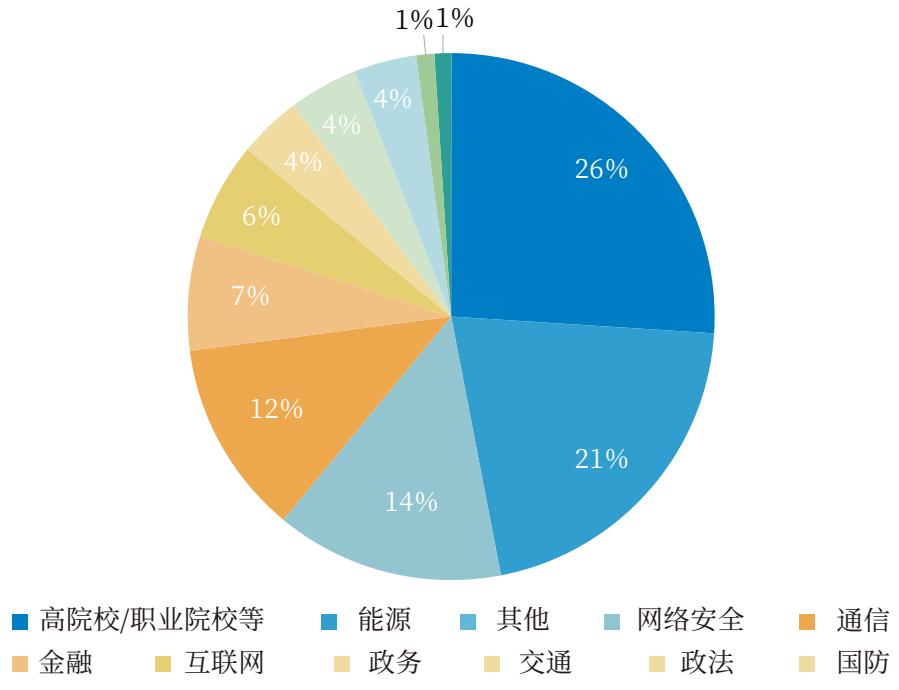


图2-20 Web安全TOP100人才行业分布

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。

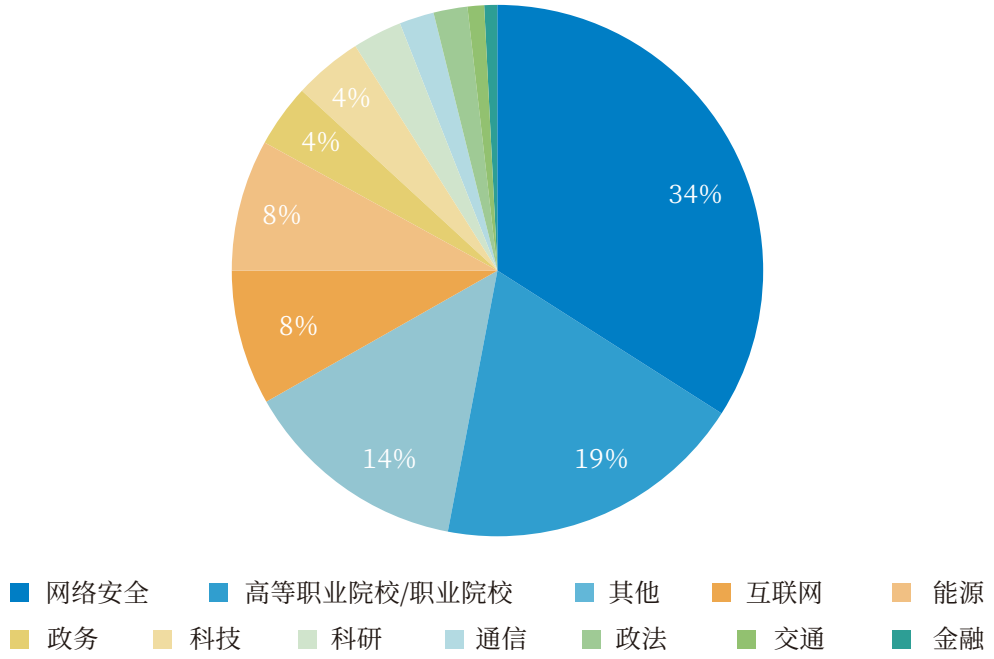


图2-21 杂项TOP100人才行业分布

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。

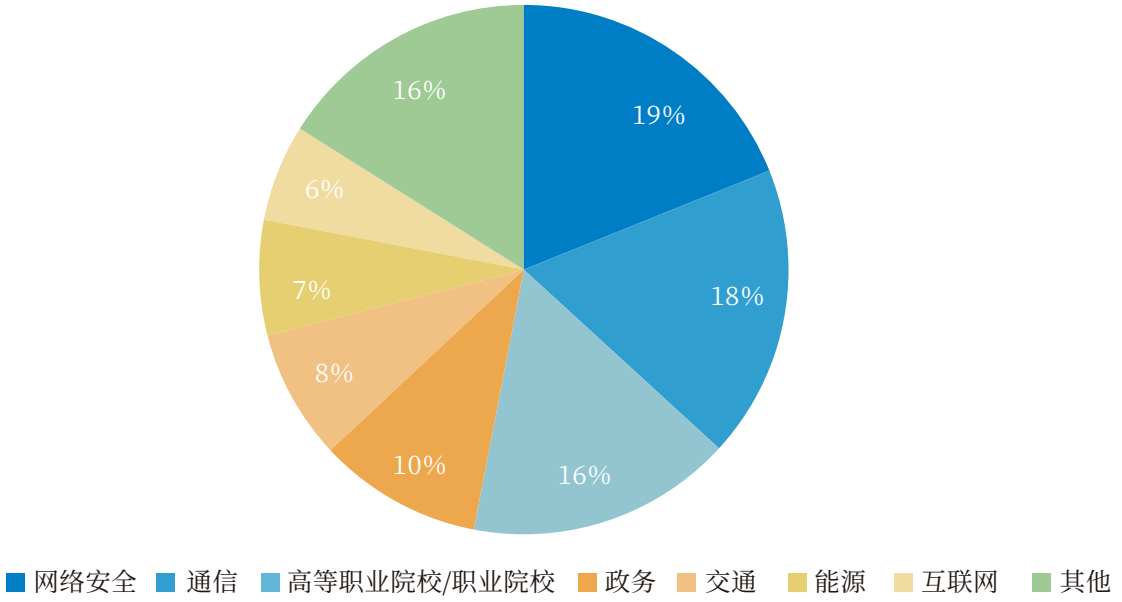


图2-22 密码研究TOP100人才行业分布

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。

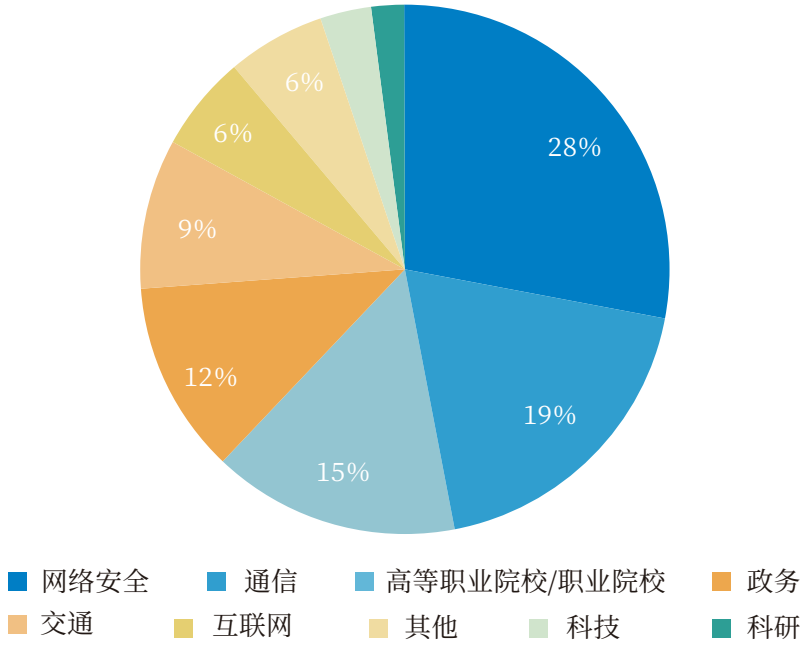


图2-23 二进制漏洞挖掘与利用TOP100人才行业分布

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。

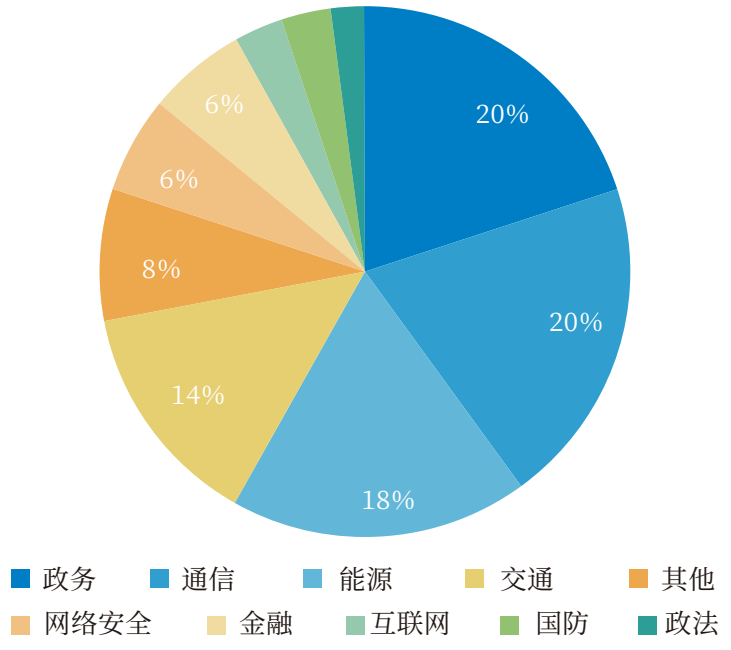


图2-24 逆向工程TOP100人才行业分布

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。

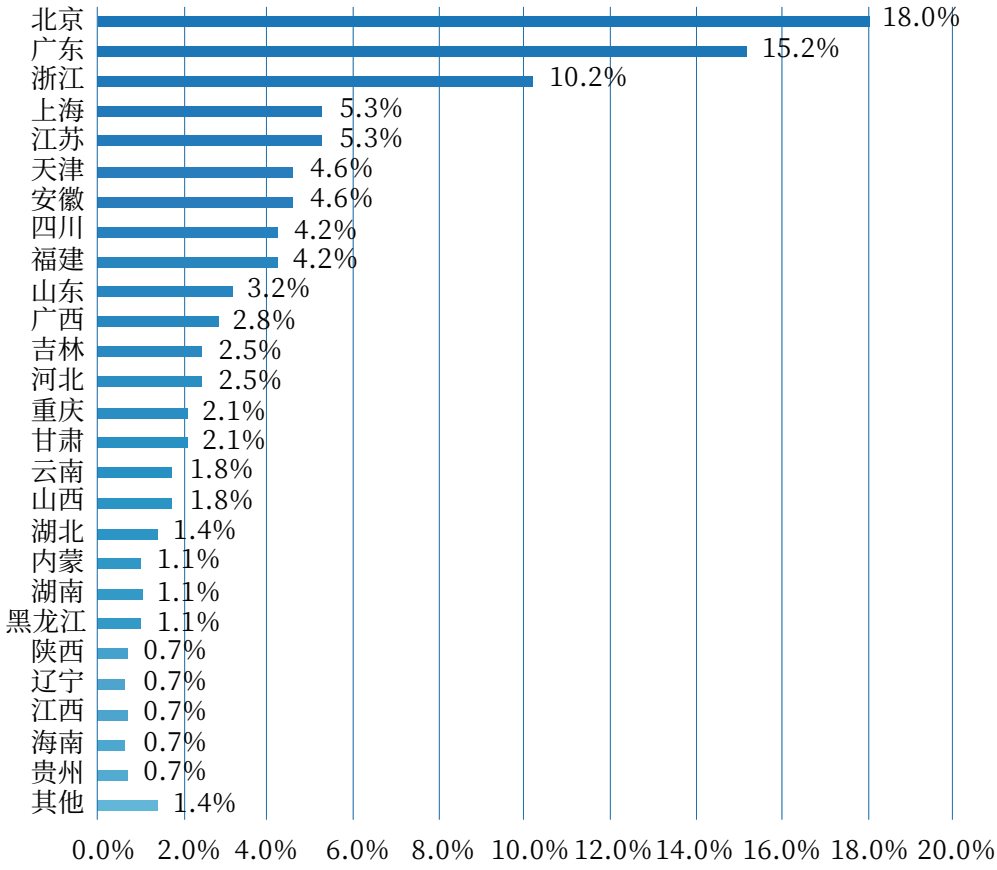


图3-1用人单位区域分布统计

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。

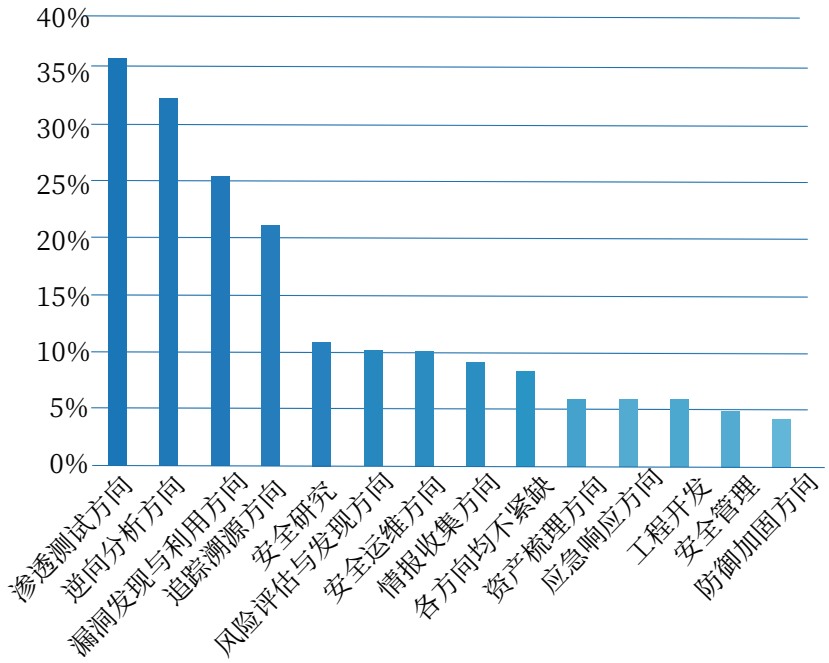


图3-2北上广浙人才需求方向占比情况

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。

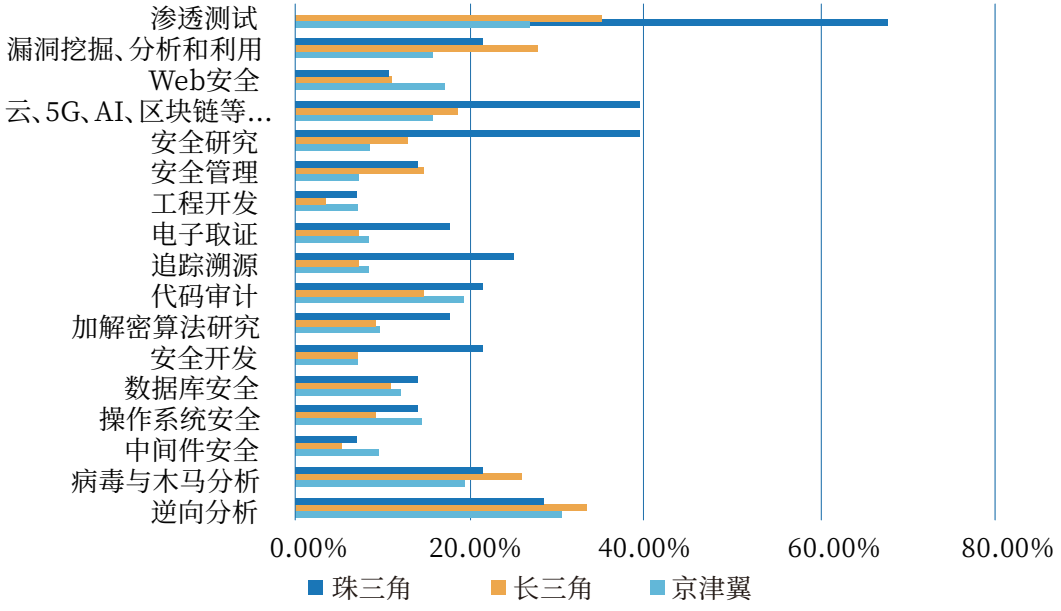


图3-3 三大区域人才能力需求占比情况

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。

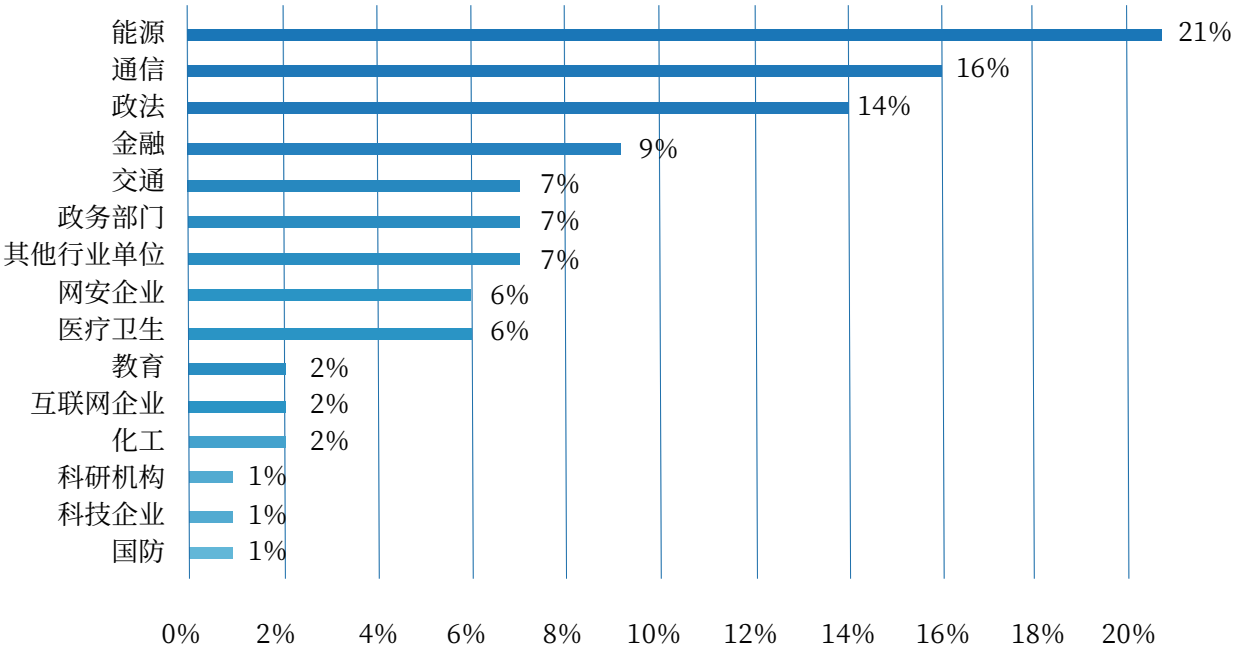


图3-4行业需求分布

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。

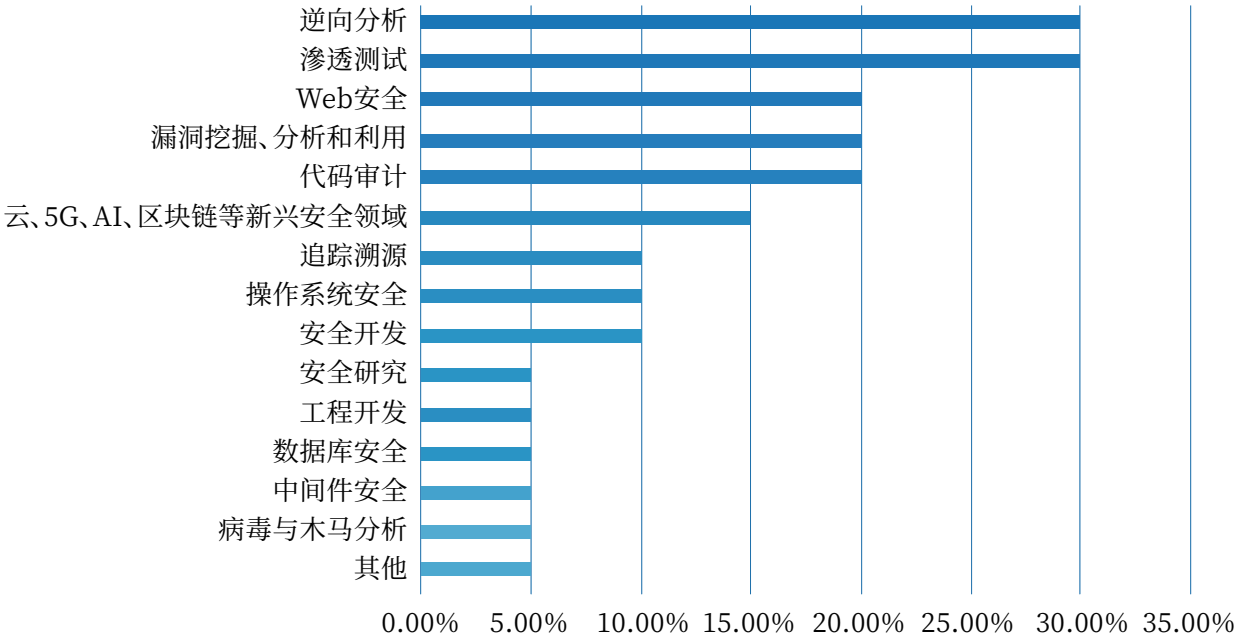


图3-5金融行业人才能力需求占比情况

(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。

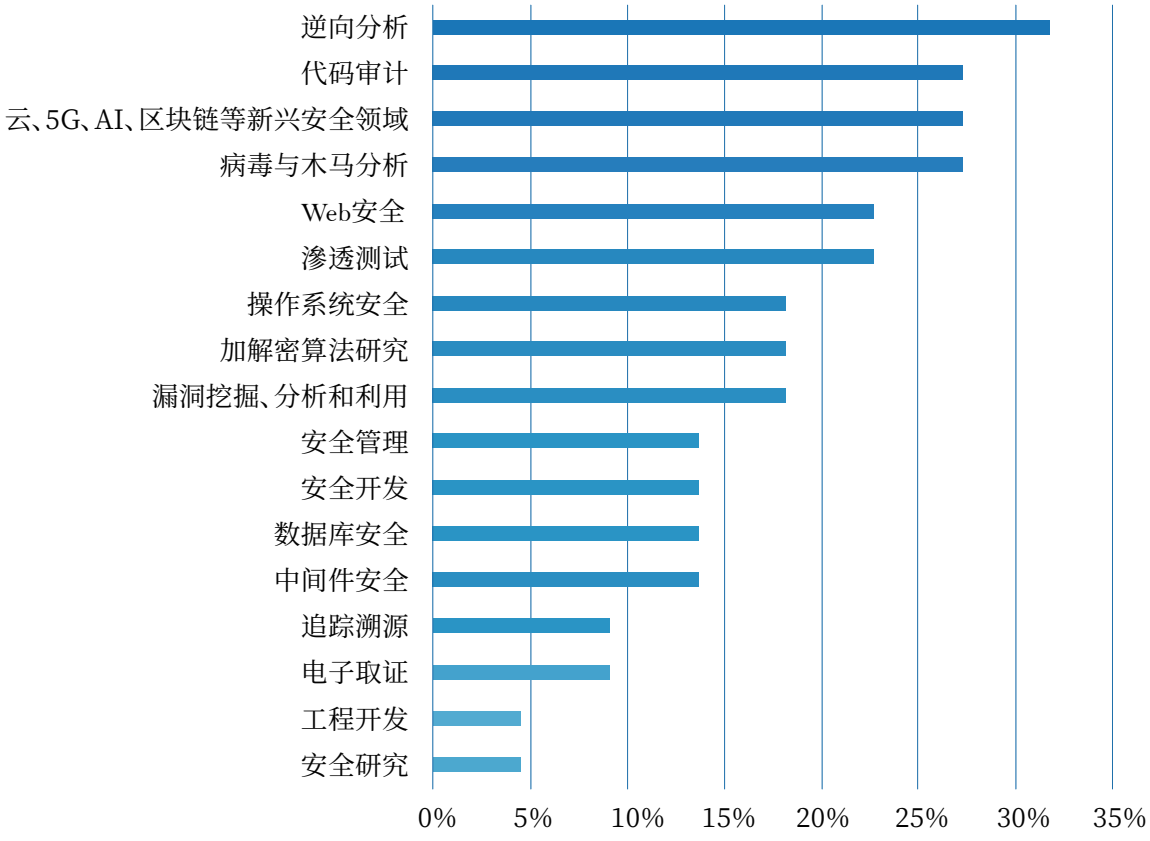


图3-6通信行业人才能力需求占比情况

(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。

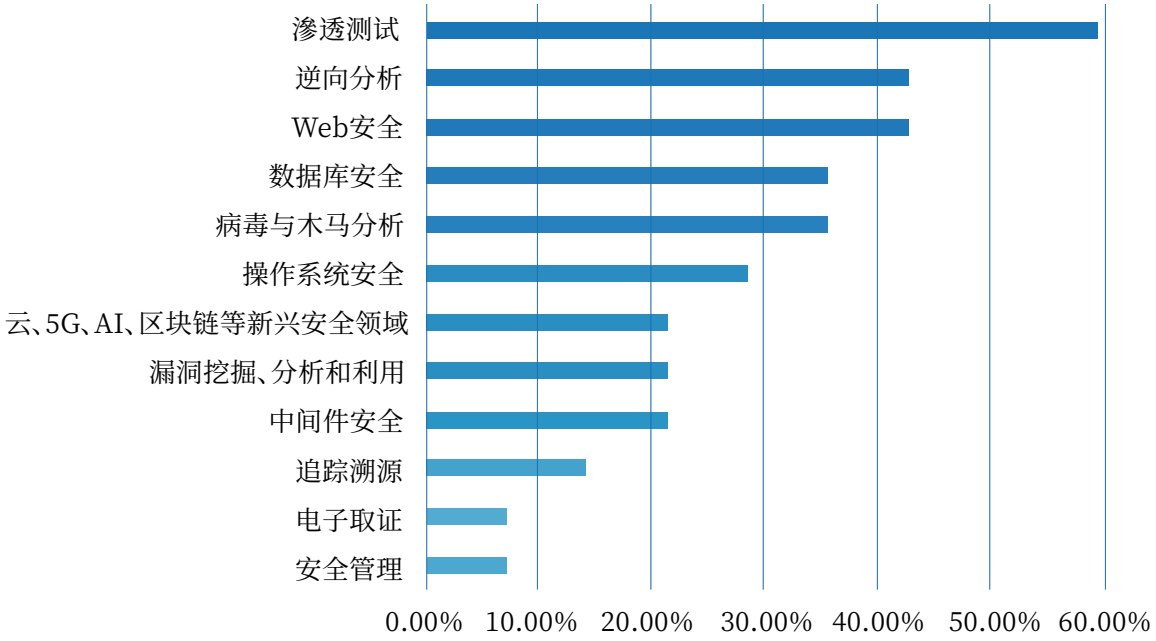


图3-7医疗卫生行业人才能力需求占比情况

(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。

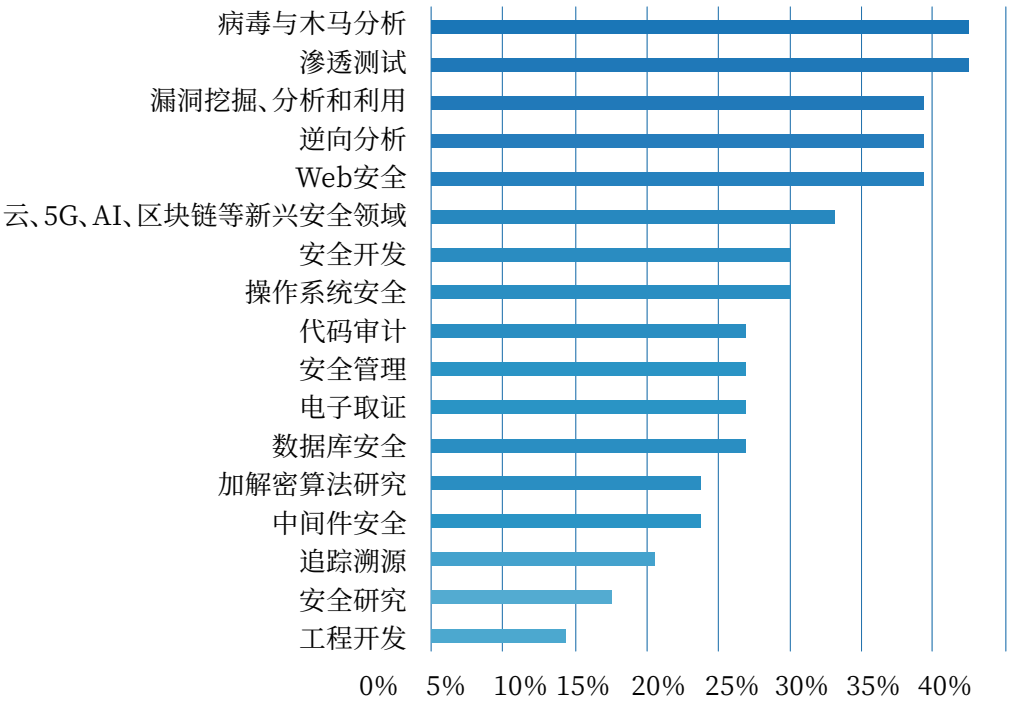


图3-8 教育行业人才能力需求占比情况

(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。

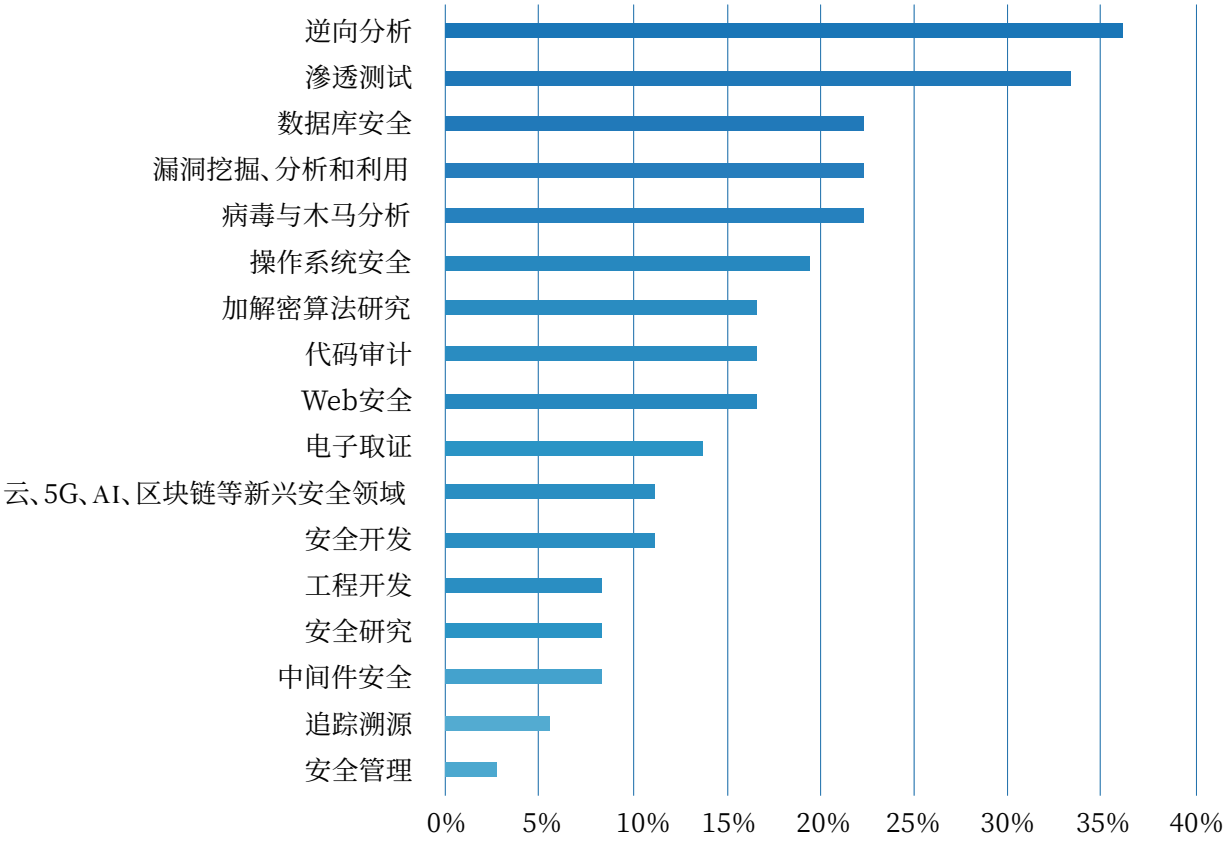


图3-9互联网行业人才能力需求占比情况

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。

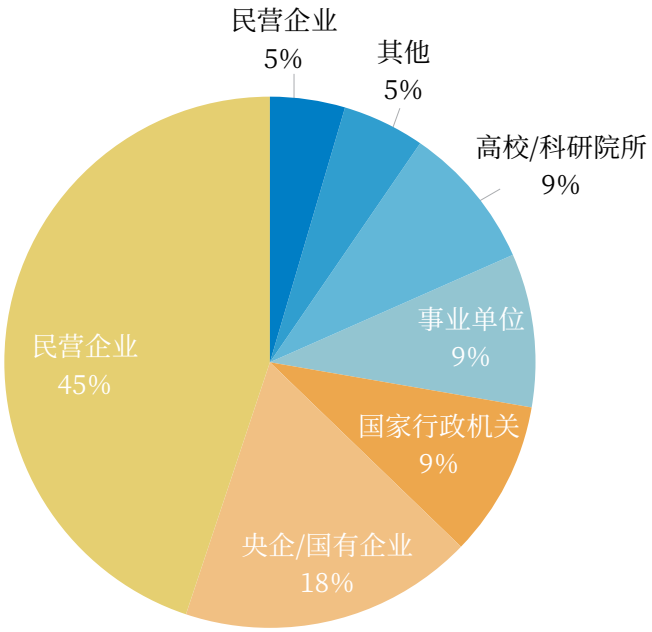


图3-10企业性质统计情况

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。

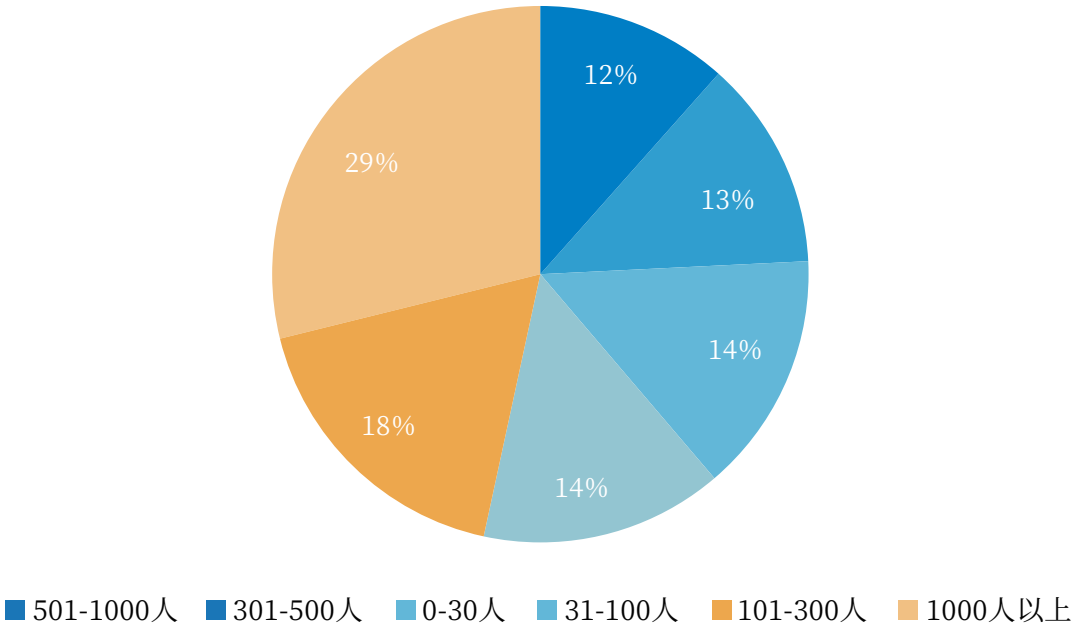


图3-11企业规模统计情况

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。

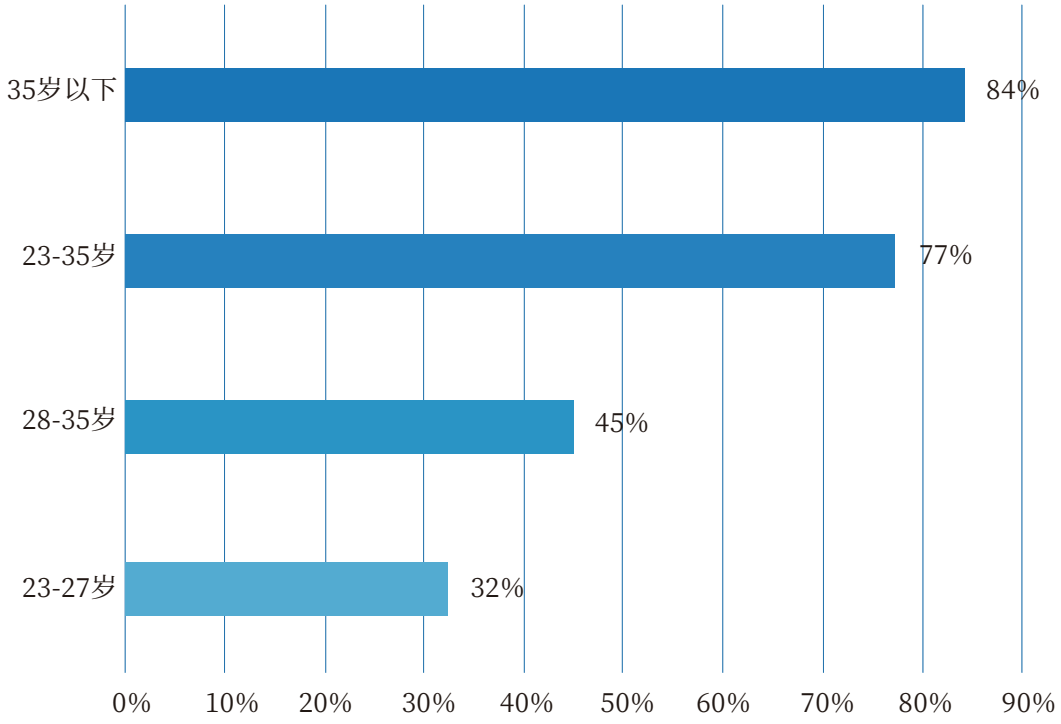


图3-12网络安全人才年龄分布

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。

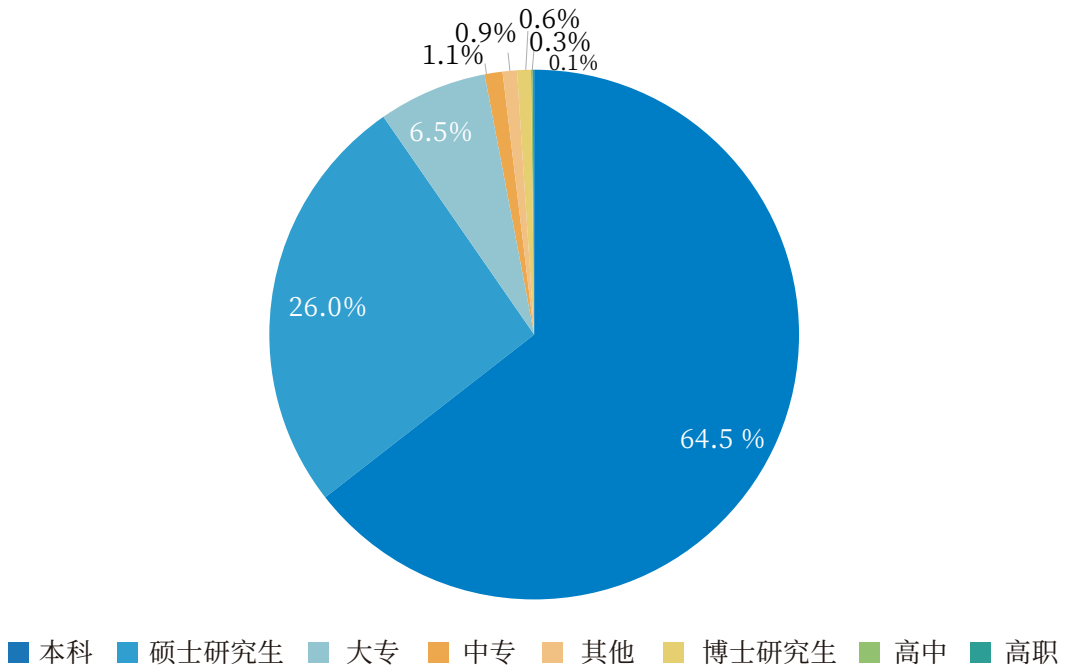


图3-13网络安全人才学历情况

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。

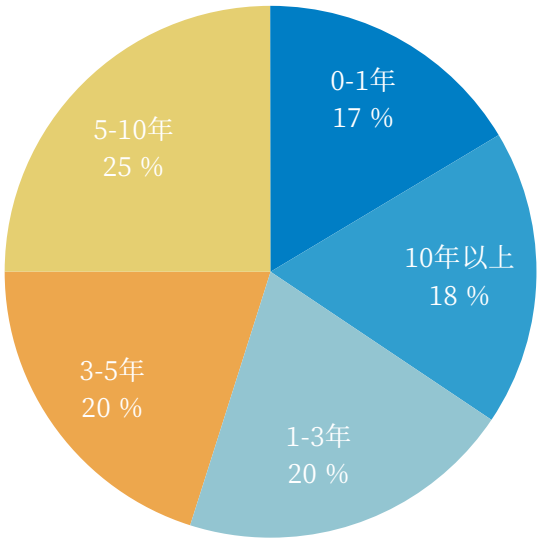


图3-14网络安全人才工作年限情况

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。

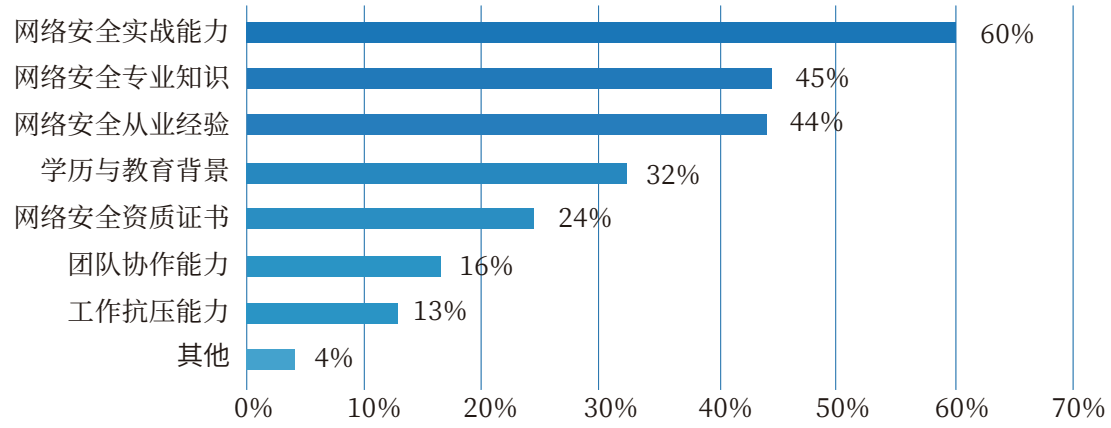


图3-15 用人单位招聘网络安全人员看重的方面

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。

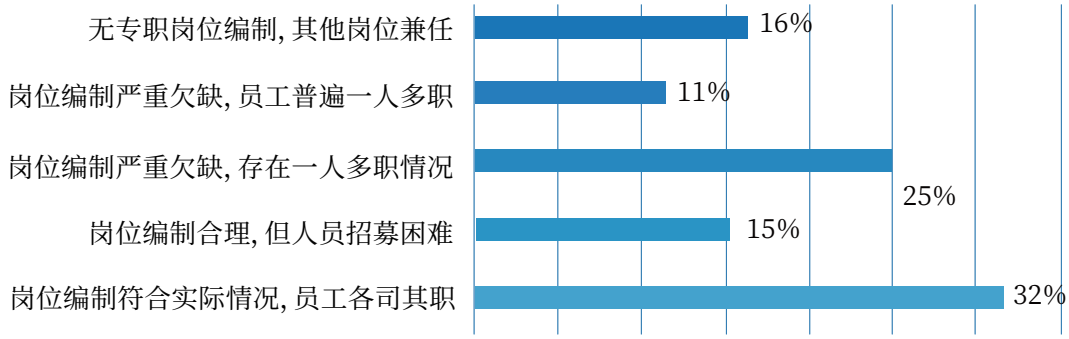


图3-16岗位编制情况

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。

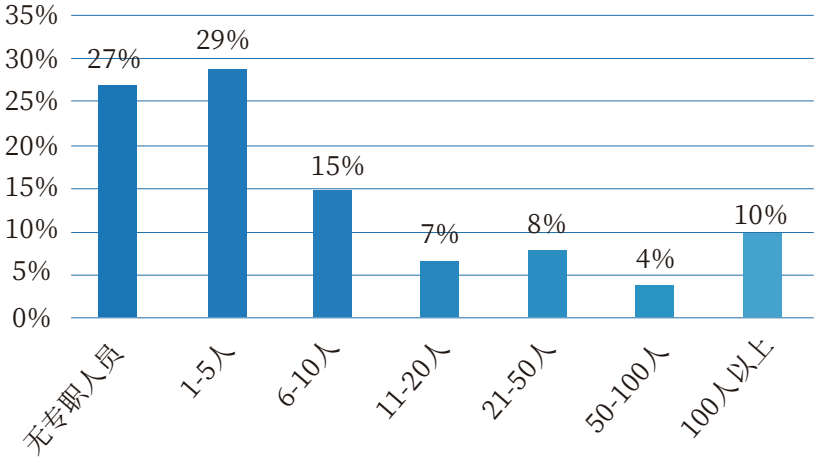


图3-17关键信息基础设施单位安全队伍建设规模占比

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。

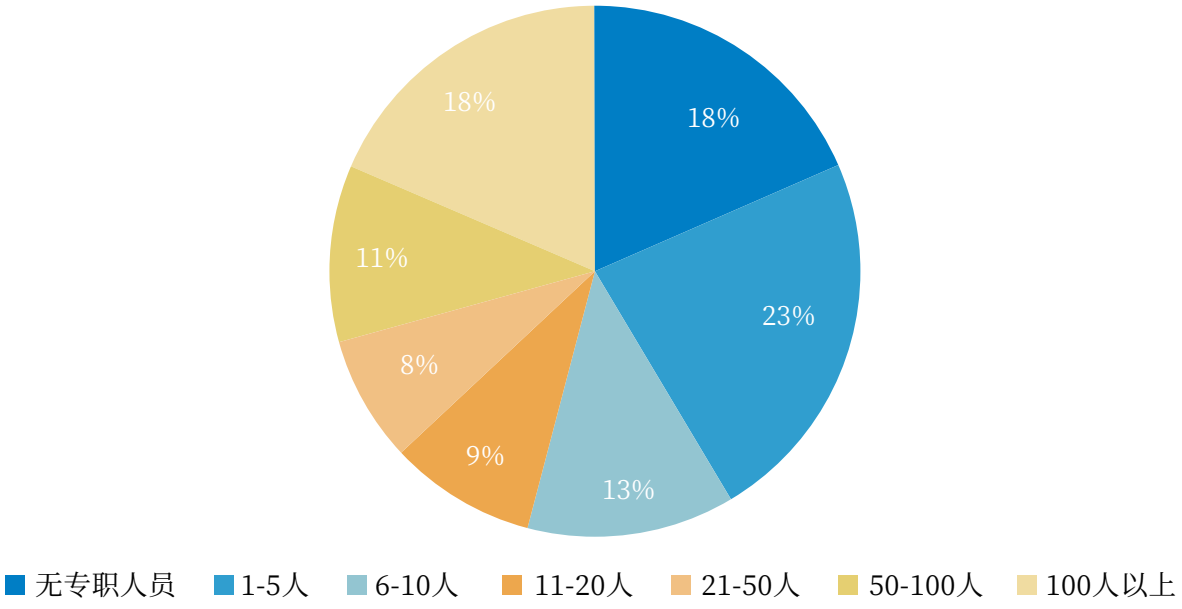


图3-18网络安全专职队伍规模

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。

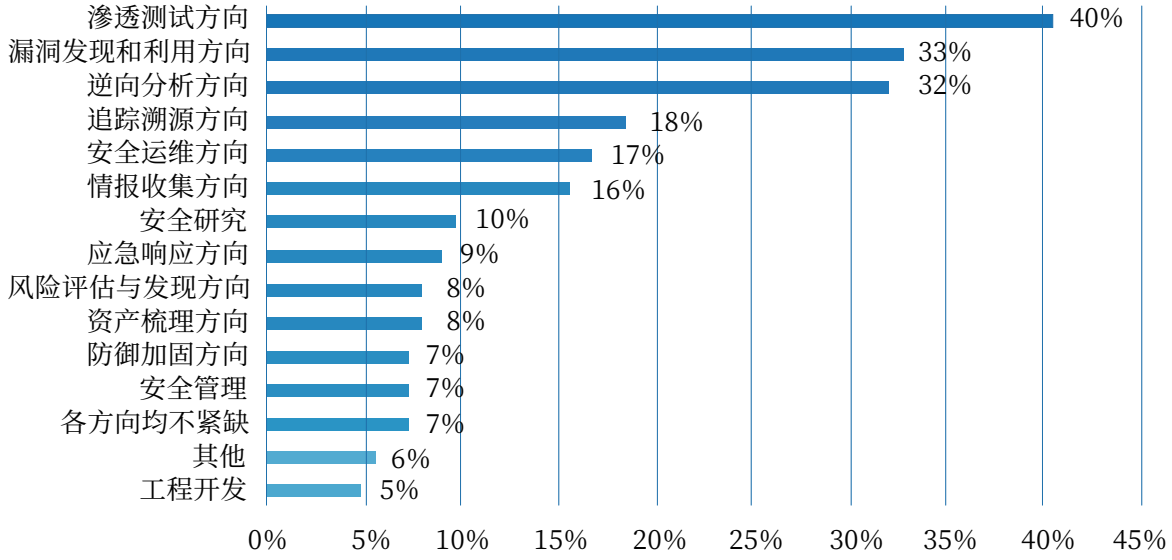


图3-19用人单位紧缺的实战人员技能方向

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。

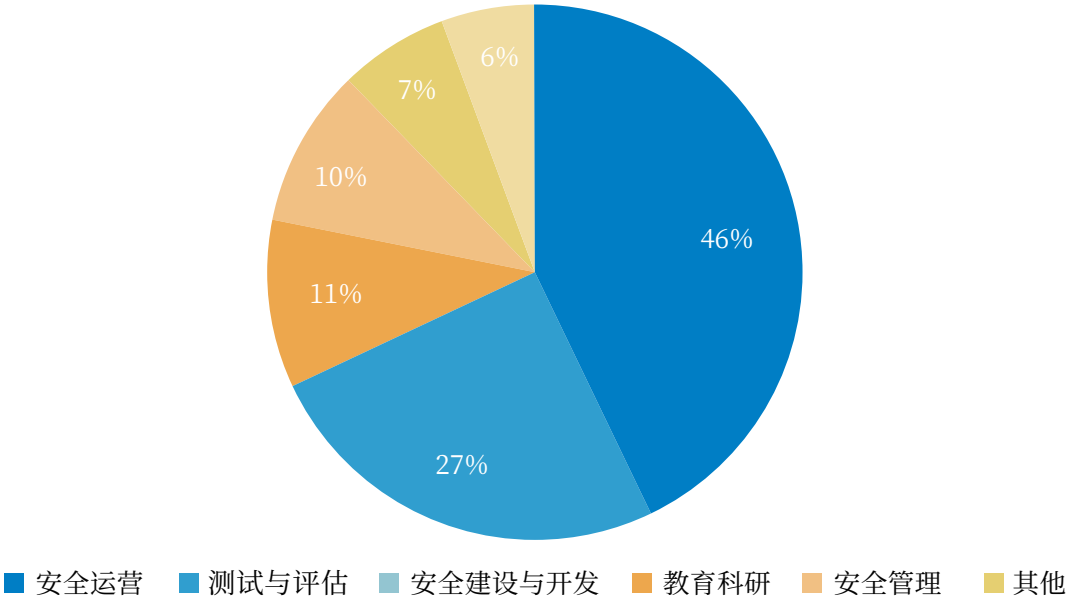


图3-20岗位类型分布

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。

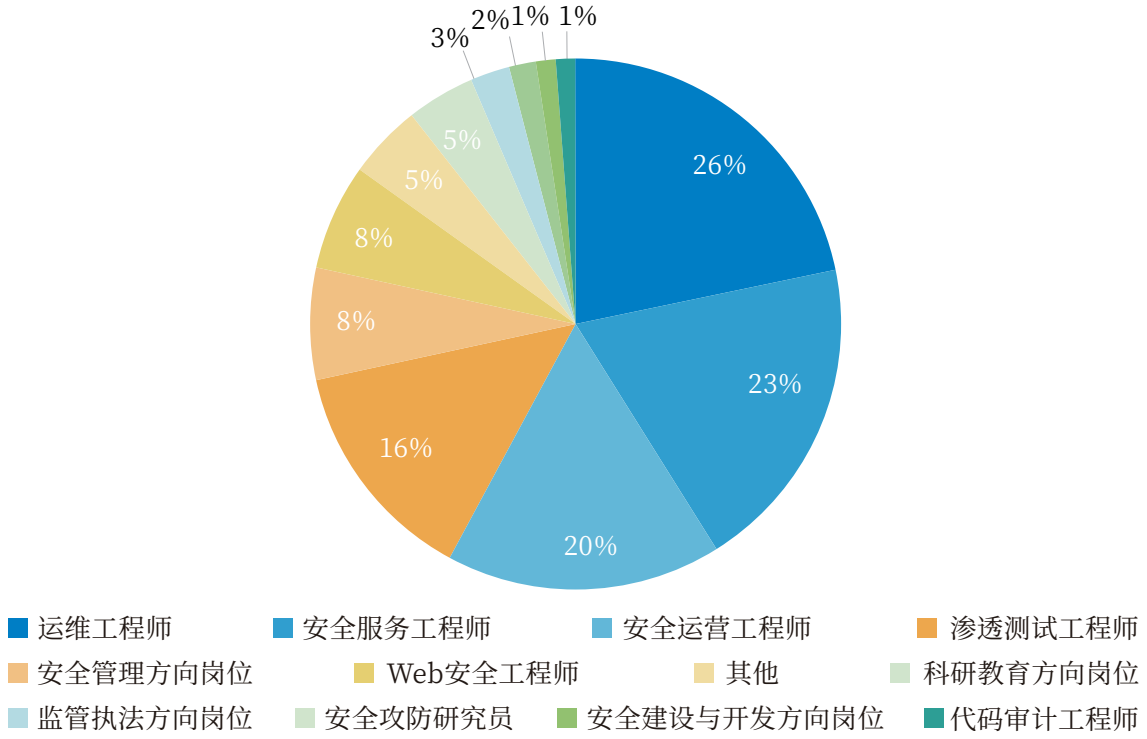


图3-21岗位分布

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。

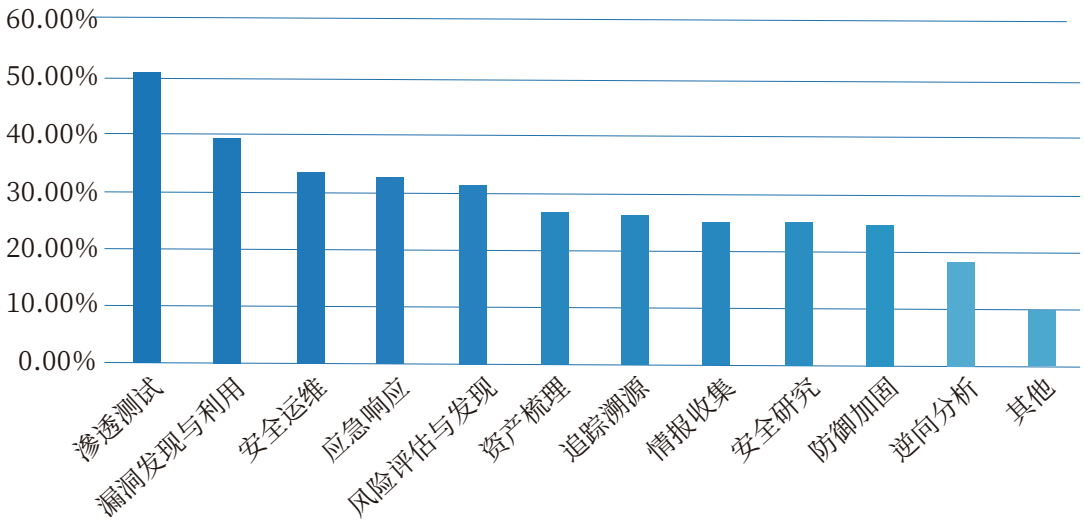


图3-22主要实战方向

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。

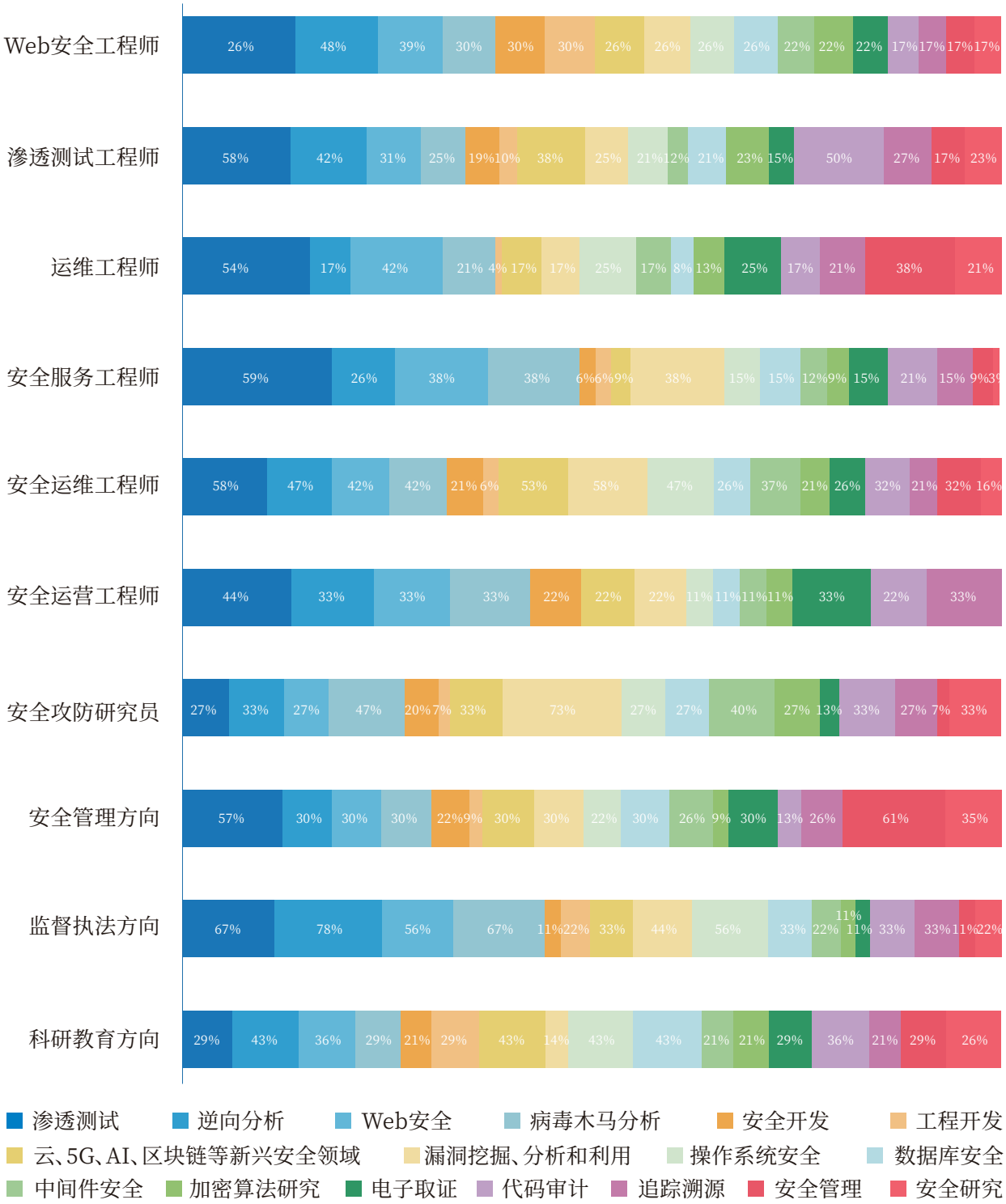


图3-23各岗位专业能力需求情况

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。