网络安全人才攻防实战能力评价

2022

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。

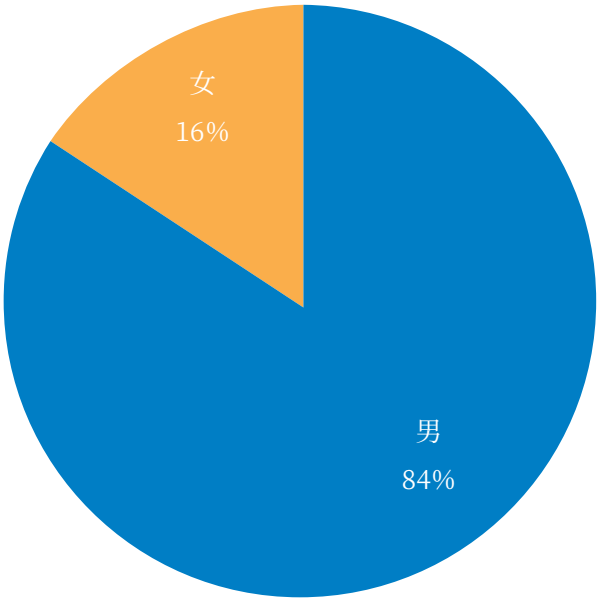

图2-1 网络安全攻防实战人才性别分布

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。

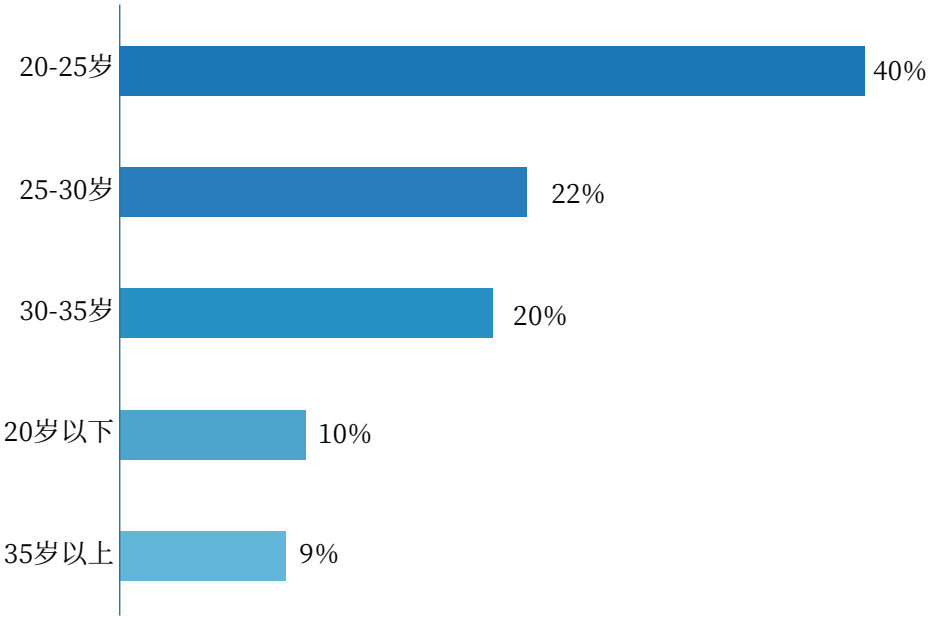

图2-2 网络安全攻防实战人才年龄分布

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。