网络安全产业人才发展报告

（2023 年版）

工业和信息化部人才交流中心

2023 年 9 月

编写单位

工业和信息化部人才交流中心

工业和信息化部网络安全产业发展中心

工业和信息化部电子第五研究所

华为技术有限公司

深信服科技股份有限公司

360 数字安全集团

南京邮电大学

四川邮电职业技术学院

北京智谱华章科技有限公司

北京拉勾网络技术有限公司

广东职教桥数据科技有限公司

指导委员会（按姓氏笔画排序）

编委会（按姓氏笔画排序）

目　录

序　言

党的二十大报告提出，“教育、科技、人才是全面建设社会主义现代化国家的基础性、战略性支撑”，并系统阐述了推进教育、科技、人才工作的战略部署。近年来，《网络安全法》《数据安全法》《个人信息保护法》《网络安全审查办法》等颁布实施，信息技术与网络安全标准化、学科建设、网络安全人才培养等取得积极进展，网络安全保障能力显著增强。习近平总书记明确指出，建设网络强国需要高素质的网络安全和信息化人才队伍。目前，我国网络安全人才还存在缺口数量较大的问题，网络安全产业人才队伍建设一直是网络安全产业高质量发展的痛点。

当前，百年未有之大变局加速演进，“后疫情时代”全球产业链供应链深刻变化，全球网络治理体系深刻变革，国内外发展形势发生深刻复杂变化，大国网络空间角力的日益激烈，更进一步加剧了变局中的不稳定性和不确定性。进入数字化浪潮时代，大数据、人工智能、云计算、物联网、工业互联网等技术全面渗透到各领域阶段，深刻影响着生产生活的各个环节。数字时代高质量网络安全人才培养将成为“十四五”时期育先机开新局的重要突破口，我们必须敏锐抓住这一机遇，进一步加强网络安全人才培养，这是顺应建设数字中国、网络强国新发展阶段形势变化必由之路，也是抢抓信息革命机遇、构筑国家竞争新优势、加快建成社会主义现代化强国的内在要求。

2017 年，《中华人民共和国网络安全法》正式实施，其中第二十条指出，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。在经过建章建制、打好网络安全人才培养的基础后，未来，将进一步明确人才培养和行业发展的关系，以更前瞻的方式探索未来网络安全人才发展路径。

“十四五”时期，网络安全人才培养进入快车道新阶段。一方面，网络安全从业者面对的挑战和工作压力不断提升，需要与时俱进地吸收网络安全创新理念、技术和管理方法。另一方面，网络安全新生力量的培养需要进一步加强。为此，在工业和信息化部网络安全管理局的指导下，工业和信息化部人才交流中心、工业和信息化部网络安全产业发展中心（工业和信息化部信息中心）、工业和信息化部电子第五研究所等单位集合各自优势资源，汇集在网络安全人才培养方面的研究成果，结合人才培养实践，进行高校走访、企业调研、专家咨询、策略分析，共同牵头编写了《网络安全产业人才发展报告（2023 年版）》，对我国网络安全人才发展进行了一次系统性的调研分析。

本报告通过梳理国内外网络安全产业发展概况，总结当前网络安全产业人才现状，梳理人才供需端情况，提出了一系列对策建议，意在为今后我国网络安全工作建设、人才能力提升提供重要参考。报告中存在不当之处，还请指正！

摘　要

本报告以探究网络安全产业人才现状为目标，通过对人才供给侧和人才需求侧的现状进行分析，为产学研用多界提供人才发展参考，并提出人才发展工作建议，为产业人才队伍建设提供指导。

本报告数据主要来自工业和信息化部人才交流中心、拉勾数据研究院，以及各参编高校和企业提供的人才调研情况。报告共分为 6 个篇章，从国内外产业发展规模出发，对产业人才现状、产业人才需求、产业人才供给情况等方面开展分析，并提炼出产业人才岗位序列和任职资格，最后给予产业人才发展对策建议。纵观报告全文，可以得出以下主要结论:

（1）2022 年我国网络安全市场规模约为 633 亿元，同比增长率为 3.1%，近三年行业总体保持增长态势。AI 安全技术成为网络安全产业的研究热点。

（2）网络安全人才学历以大专和本科为主，合计占比高达 89%。处于 25-40 岁年龄段的青年从业者占比达到 8 成，其中 30-40 岁的人才最多，占比达到一半。从业者的区域以北上广深等城市为主，合计占比高达 66%。约 32%的网络安全行业从业者来自于计算机科学与技术、信息安全、网络工程专业。

（3）北京、上海、深圳、广州、成都和杭州，占据网络安全产业人才市场总需求的 75%左右。网络安全企业主要需求岗位

为网络安全工程师、安全运维工程师、网络安全研究员、应用安全工程师、网络安全顾问、渗透测试工程师、数据安全工程师等。

（4）2022 年度拟新增的 483 个本科专业中，有 51 个是网络与信息安全相关专业。预估 2023 年网络安全相关专业的毕业生总规模约为 3.2 万人。

（5）我国网络安全产业人才整体呈现供需失衡状态，尤其是实战型人才短缺。在供给端，院校人才培养数量有待提升，需创新产教融合培养模式。在产业端，在职人员能力提升体系欠缺，需重点加强从业人员能力建设。

总体上，我国网络安全产业与人才培养处于一个良好的发展态势，产业人才能力标准不断完善，同时教育供给侧专业对口设置也不断完善，培育人数逐年递增，为产业发展贡献了新鲜力量。随着合规性要求及单位系统性安全能力提升需求增强，企事业单位愈加重视网络与信息安全人才培养，将逐步构建并完善人才成长体系。

一、网络安全产业现状和发展趋势

（一）全球网络安全产业产值规模

随着全球数字化产业蓬勃发展，云计算、人工智能、大数据、5G 等技术的应用范围不断扩大，企业在运用新技术提高自身效率的同时，也面临着更多由新技术诱发的网络威胁，全球网络安全形势越发严峻，这也促使企业不断加大在网络安全上的投入。

目前，全球网络安全市场规模呈现持续增长态势。根据 IDC 数据显示，2021 年全球网络安全市场规模为 1687.7 亿美元。截至 2023 年 3 月 31 日，IDC 披露了 2022 年全球网络安全规模为 1955.1 亿美元，同比增速达到 15.8%。

（二）我国网络安全产业产值规模

1.总体情况

我国网络安全相关政策的顶层设计逐渐完善，网络安全市场规模不断扩大。随着数字化转型的加速，网络安全需求不断增加，市场需求日益强劲。根据中国网络安全产业联盟数据显示，2022 年我国网络安全市场规模约为 633 亿元，同比增长率为 3.1%，近三年行业总体保持增长态势。与此同时，数字经济的发展成为网络安全发展的新引擎、新动力，催生出数据安全、云安全、个人隐私保护等更多支撑网络安全市场规模扩容并高速增长的新板块，这些新板块将促进我国网络安全产值规模持续增长。

2.分类别情况

根据《中国网络安全产业研究报告（2022 年）》数据显示，

我国网络安全下游客户以政府、电信和金融行业为主，三者合计占市场总营收的 58.4%。最大客户为政府和公共事业单位，市场营收占比为 24.1%；其次是金融行业，市场营收占比为 17.4%。

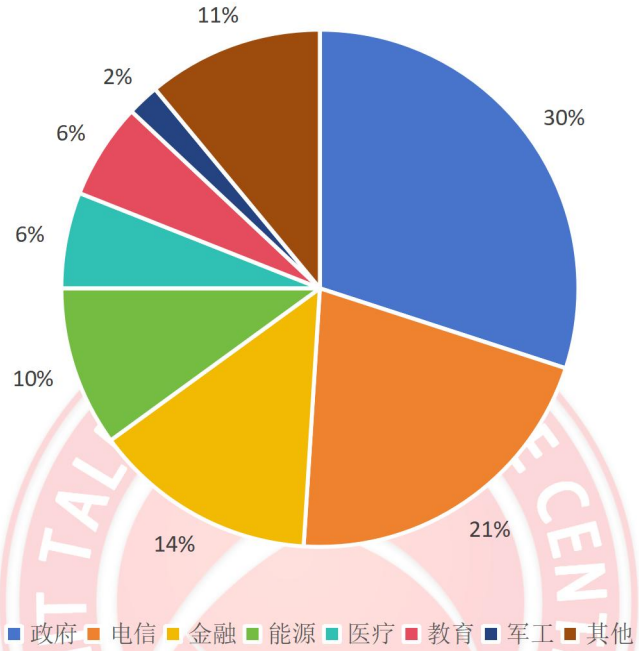

图 1.2022 年网络安全下游客户分布

根据中国网络安全产业联盟数据显示，奇安信、启明星辰、深信服和天融信四家企业的市场占有率均超过了 5%。大部分头部企业收入增速高于行业平均增速，头部企业规模和资源的优势凸显。

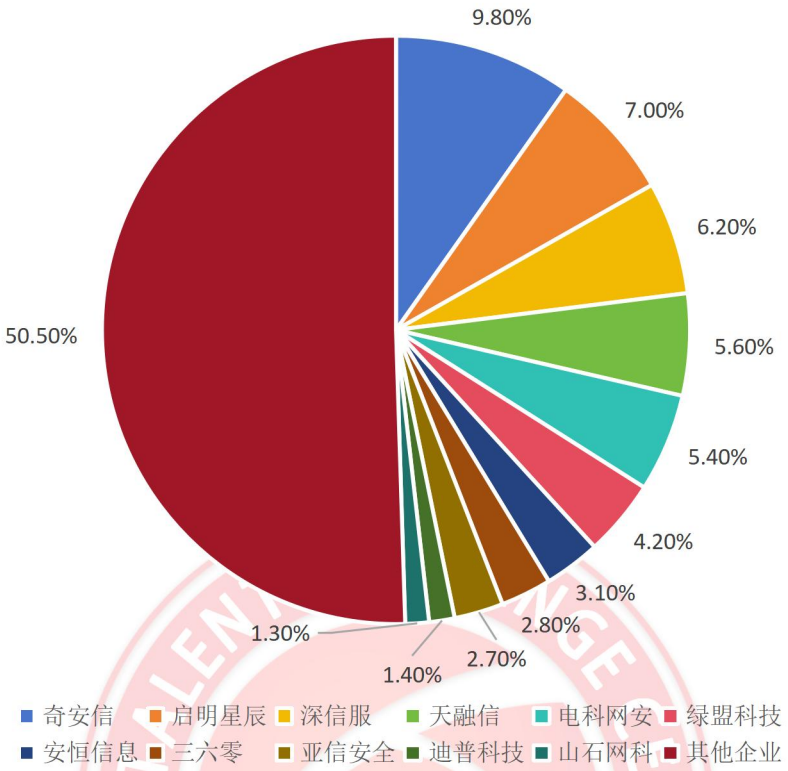

图 2.2022 年中国网络安全主要企业市占率

从区域的角度来看，华北、华东和华南地区占网络安全市场规模的 71%，国内网络安全市场省份分布任呈现不均衡发展态势。

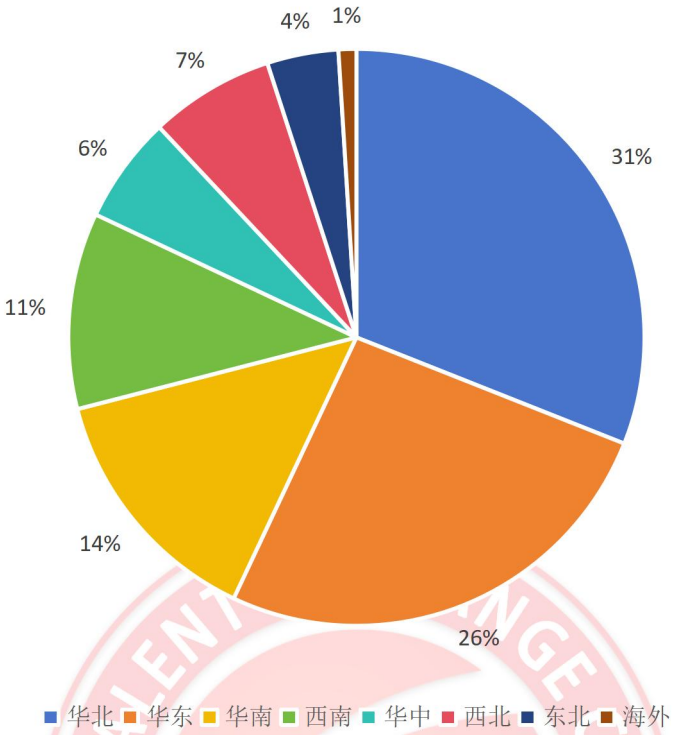

图 3.2022 年中国网络安全产业市场区域占比

（三）网络安全产业产值规模预测

根据 IDC 数据显示，2021-2026 年全球安全支出复合年均增长率为 10.4%，中国安全支出复合年均增长率为 18.8%。根据中国网络安全产业联盟数据，2022 年我国网络安全市场规模约为 633 亿元，同比增长率为 3.1%，预计未来三年将保持增长态势，增速将保持在 15%以上，到 2025 年市场规模预计将超过 800 亿元。

（四）网络安全产业发展趋势

1.技术演进方式

（1）网络安全技术走向成熟。近年来，从人工智能的运用

到云计算的发展，网络安全技术在不断进步。随着我国数字经济不断的发展，防护技术已经达到了一个新的高度，防火墙、入侵检测系统（IDS）、加密技术等都已广泛应用于保护个人和企业的信息安全。其次，随着云计算、5G 和物联网技术的发展，新的安全技术不断涌现，这些技术不断推动着网络安全技术朝着更成熟、更高效的方向发展。

（2）数据安全技术兴起。我国在“十四五”规划和 2035 年远景目标纲要中提出，加快数字化发展，培育壮大网络安全等新型产业。由此，拉开了数字安全的序幕。2021 年 9 月 1 日《中华人民共和国数据安全法》发布实施。2021 年 11 月 1 日《中华人民共和国个人信息保护法》发布实施。这一系列政策与法规的出台，推动企事业单位纷纷部署数据安全技术以保障数据安全与用户隐私。

（3）AI 安全技术成为研究热点。当前，AI 正在日益成为各行各业实现数字化，重塑经济社会发展形态的智能化关键基础设施。随着 AI 被越来越广泛的应用于人脸识别、自动驾驶汽车、AI 领域等关键领域，政府、企业将面临着传统安全攻击、AI 新型攻击与 AI 滥用三方面的安全挑战，因此，AI 日益成为各国监管方、行业客户与业界厂商关注的方向。特别是今年大模型的兴起，让 AI 安全成为监管方、学术界、工业界最关注的方向之一。

2.国内外发展趋势

随着全球政治形势中不稳定因素的增加，以及近年来勒索病

毒等安全威胁的增加，2022 年欧美企业网络安全支出占 IT 支出的比例出现大幅增长，表明欧美企业面临的网络攻击风险正在显著增加。其中，美国、德国、西班牙、荷兰等发达经济体 2022 年网络安全支出已经占到 IT 总支出的 24%。从具体投资部署的安全技术来看，从高到低分别是：零信任网络、基于硬件/固件的安全、安全访问服务边缘等新兴网络安全技术。

我国网络安全市场虽然起步较晚，但增长迅猛，其中安全软件及硬件产品份额占据了绝大部分市场份额，安全服务仅占 29%，未来成长空间巨大。同时，因为我国网络安全市场起步较晚，因此市场竞争非常活跃，TOP8 安全企业仅占 44.91%的市场空间，为广大初创安全企业留下了巨大的市场机会。随着企业对于数据安全的重视，涌现出一大批以隐私计算、机密计算技术为基础的初创企业，推动我国在隐私计算技术领域迈向世界先进行列。未来，随着 AI 技术，特别是大模型技术的普遍应用，针对 AI 的安全威胁也日渐增多。但因为深度学习技术的特殊性，传统安全防护技术在 AI 安全威胁面前束手无策，因此，国内一些企业已经开始探索 AI 安全检测与防护产品。未来几年 AI 安全厂商将成为我国乃至世界安全投资的热点。

二、网络安全产业从业人员现状分析

为更好了解网络安全企业及从业人员现状，本报告从拉勾数据平台提取了我国 18 万网络安全相关企业样本和 64 万网络安全人才样本进行分析，数据显示如下。

（一）企业情况

1.人员规模

从网络安全企业规模来看，小微型企业的数量占比超过半数，达到 51%，而 500 人规模以上企业占比总计 19%。

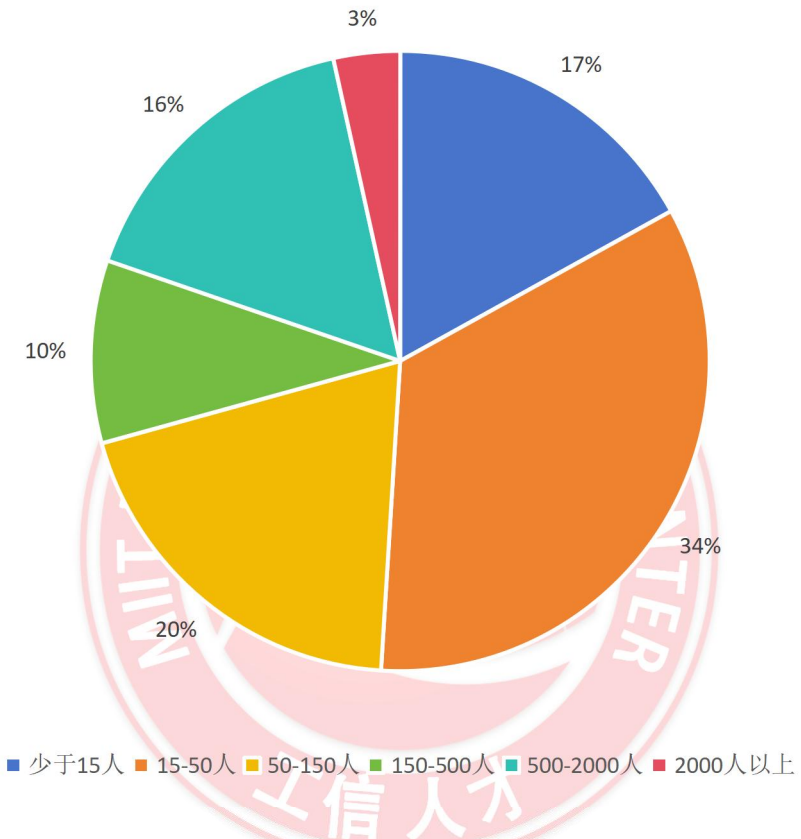

图 4.网络安全企业人员规模占比

2.区域占比

网络安全企业在北上广深等城市合计占比达 41%。此外成都、杭州等互联网企业聚集城市占比分别为 6%、5%。值得注意的是在其他区域的占比为 48%，说明网络安全企业在全国分布较为分散，这与网络安全产业链分工关系密切。

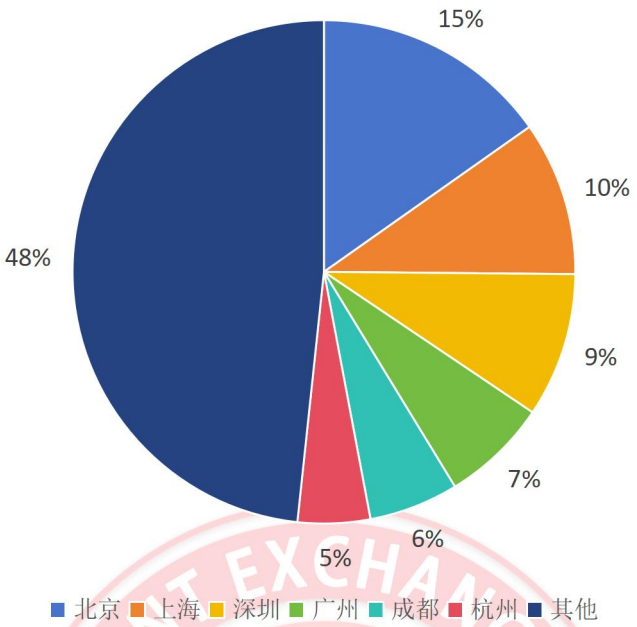

图 5.网络安全企业地区分布占比

3.融资阶段

网络安全企业中未融资企业占比高达 83%，天使轮占比 6%，A 轮占比 4%，B 轮占比 1%，C 轮占比 1%，D 轮及以上占比 1%，上市企业占比 5%。这从侧面反映了我国拥有一大批网络安全的初创企业，提升网络安全企业竞争力任重道远。

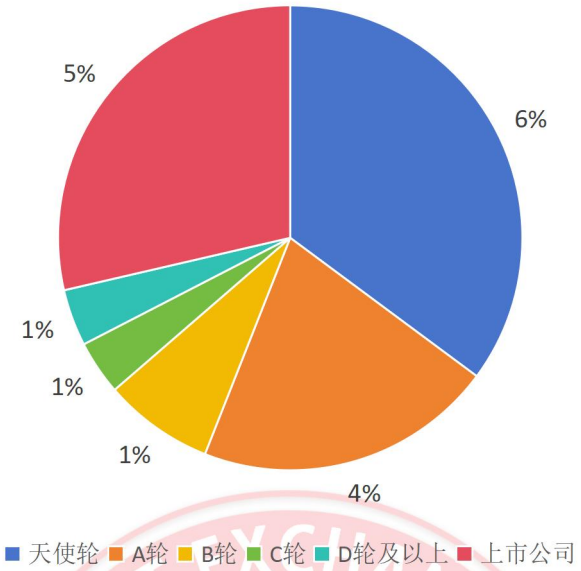

图 6.网络安全企业融资企业占比

（二）从业人员特征分析

1.学历分布

网络安全人才学历以大专和本科为主，合计占比高达 89%，硕士及以上学历占比 11%，这与从事基础安全保障工作的技术人员占大多数有关，用人单位对基础安全保障工作人员往往更看重技术实践能力和经验而非学历。

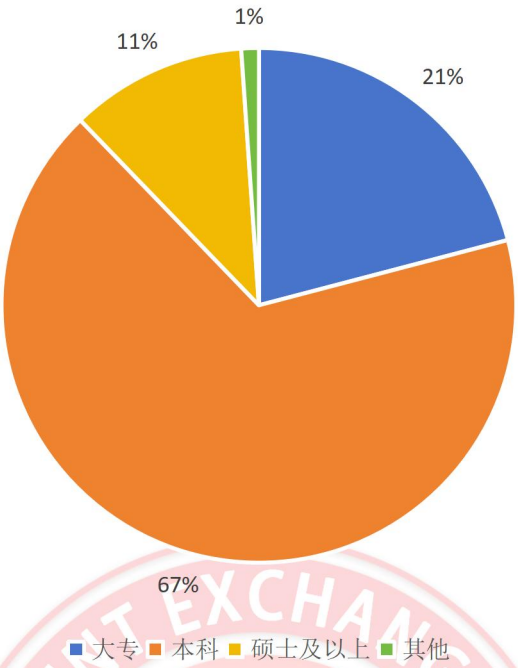

图 7.网络安全人才学历占比

2.年龄分布

从年龄来看，网络安全产业人才呈现年轻化态势。处于 25-40 岁年龄段的青年从业者占比达到 8 成，其中 30-40 岁的人才最多，占比达到一半。随着近年来我国网络安全宣传教育工作深入开展，年轻一代对网络安全及相关职业的认识程度加深，加之网络安全产业发展势头迅猛，就业形势良好，未来将有越来越多的年轻人涌入网络安全行业。

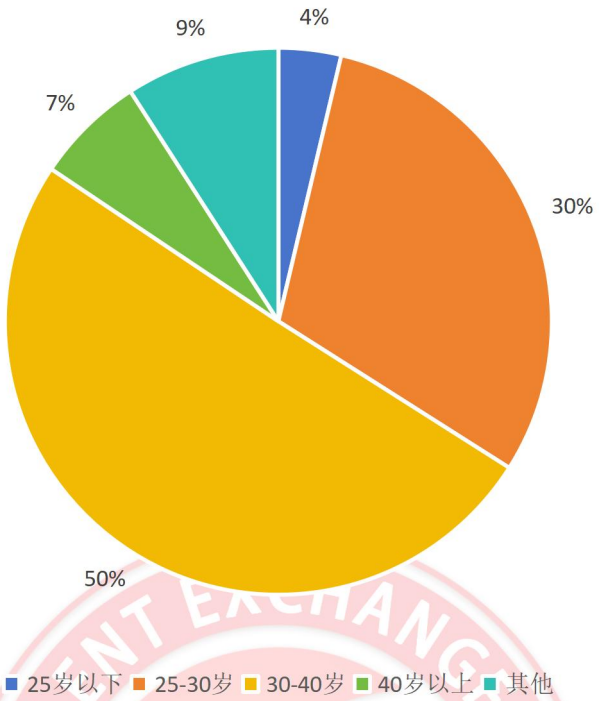

图 8.网络安全人才年龄占比

3.区域分布

网络安全人才从业的区域以北上广深等城市为主，合计占比高达 66%。另外，杭州占比 7%、成都占比 6%，说明在互联网龙头企业分布地区，网络安全产业人才相应占比较高，符合产业地区分布与人才需求的匹配度。

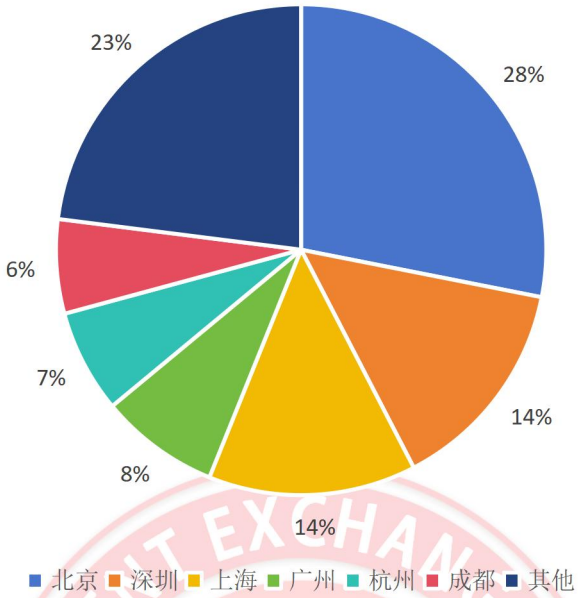

图 9.网络安全人才地区占比

4.专业分布

约 32%的网络安全行业从业者来自于计算机科学与技术、信息安全、网络工程专业。此外，还有信息安全与管理、网络空间安全等网络安全相关专业进入前十。值得注意的是，前十名专业中，计算机网络技术、计算机应用技术、信息安全与管理属于高职院校培养专业，反映出高职院校对人才供给的重要作用。此外，仍有大部分从业者是电子信息工程、通信等相关专业毕业，这是由于网络安全的学科交叉特性，以及多元化兴趣驱动的人才发展特点决定的。

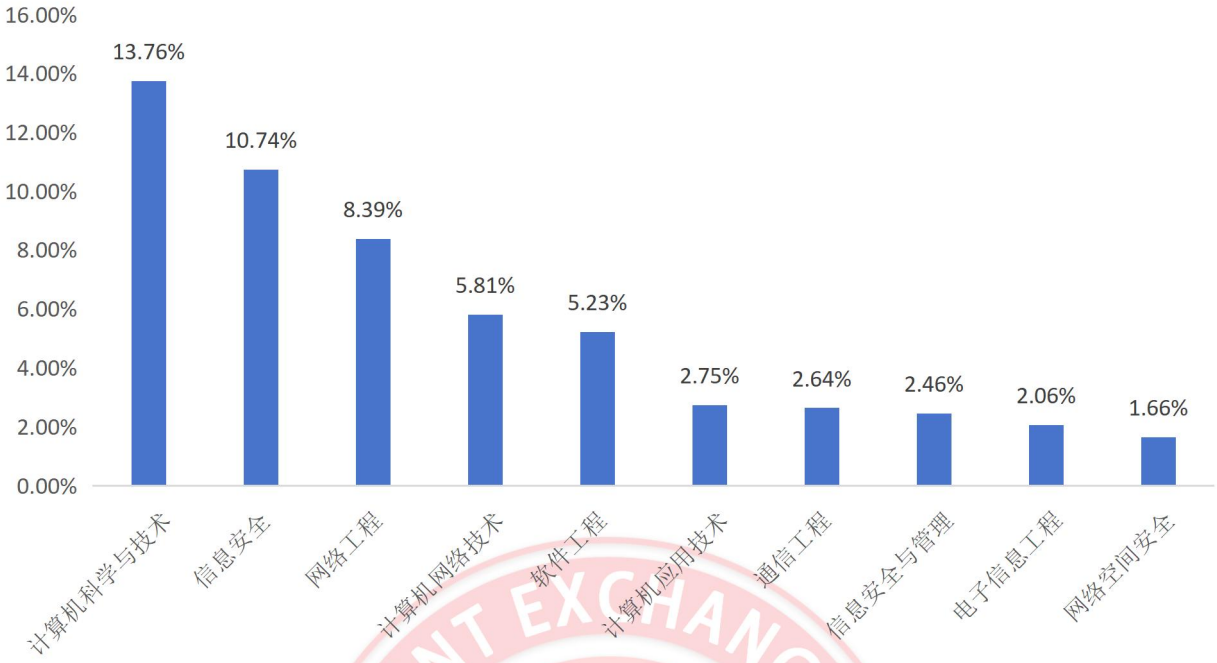

图 10.网络安全人才专业占比

5.毕业院校分布

根据拉勾数据研究院提供的数据看，成都信息工程大学、北京邮电大学、西安电子科技大学、哈尔滨工业大学、广东工业大学为网络安全行业输送了较多的人才。下表所示为拉勾招聘平台上，投递网络安全岗位的求职者毕业的前 20 所国内学校，其中，前 20 所大学所属城市前三名分别是成都（6 所）、广州（3 所）、西安（2 所）。

表 1.网络安全人才毕业学校占比 TOP20

序号	毕业院校	简历占比
1	成都信息工程大学	1.11%
2	北京邮电大学	0.85%

3	西安电子科技大学	0.71%
4	哈尔滨工业大学	0.70%
5	广东工业大学	0.69%
6	电子科技大学	0.67%
7	天津理工大学	0.58%
8	西南科技大学	0.54%
9	中北大学	0.54%
10	四川大学	0.50%
11	广州大学	0.46%
12	桂林电子科技大学	0.46%
13	广州大学华软软件学院	0.45%
14	南阳理工学院	0.44%
15	郑州大学	0.41%
16	电子科技大学成都学院	0.41%
17	南京邮电大学	0.41%
18	西安邮电大学	0.40%
19	成都东软学院	0.40%
20	西华大学	0.40%

三、网络安全产业人才供需分析

（一）产业人才需求分析

为更好了解网络安全产业人才需求现状，我们提取了拉勾数据平台近期网络安全相关岗位 1.8 万条职位发布信息和 6.4 万个用户投递信息，数据显示如下。

1.人才供需比

按照供需比=投递用户量/发布职位量，计算得到总体供需比

为 3.5，数据表明平均每个网络安全相关岗位投递简历数量为 3.5 个。其中，北京、深圳、广州、成都的供需比超过 5，数值分别为 5.1、5.0、5.5、5.8，表明这些城市网络安全产业对人才的吸引力是较高的。值得关注的是，成都作为我国西南区域主要经济承载地，人才供需比具首位，这与区域经济发展以及城市生活文化氛围密不可分。

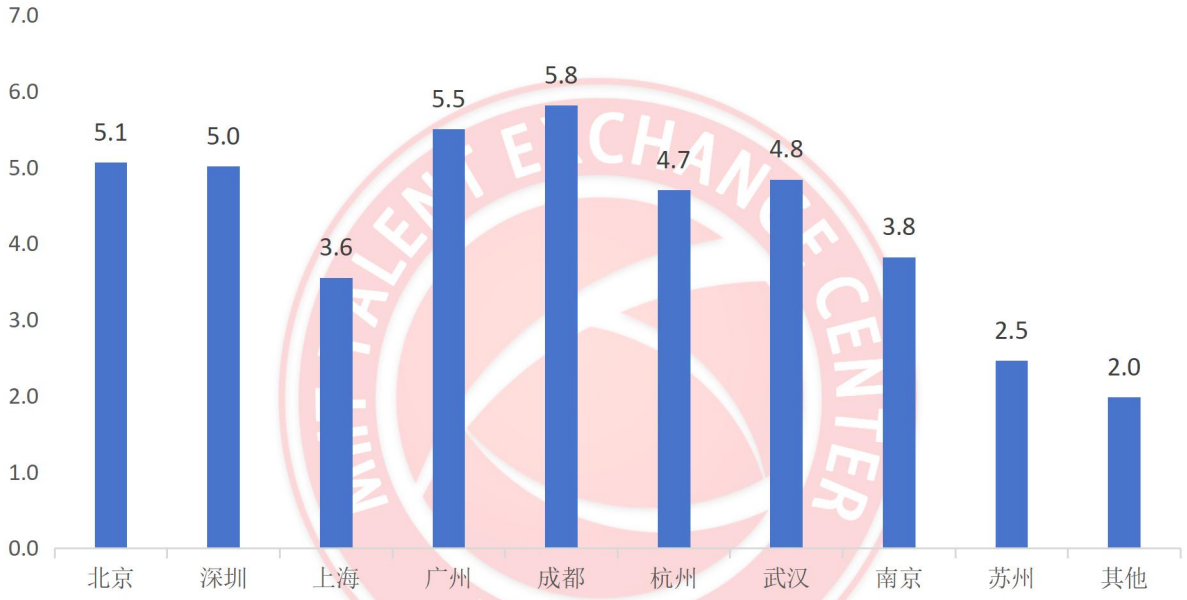

图 11.网络安全人才供需比

2.地区分布

根据拉勾数据显示，最新网络安全人才需求排名前六的城市分别是北京、上海、深圳、广州、成都和杭州，占据市场总需求的 75%左右。数据表明，北上广深等超大城市是网络安全产业人才需求的城市主力军，这与北上广深产业集群密不可分。

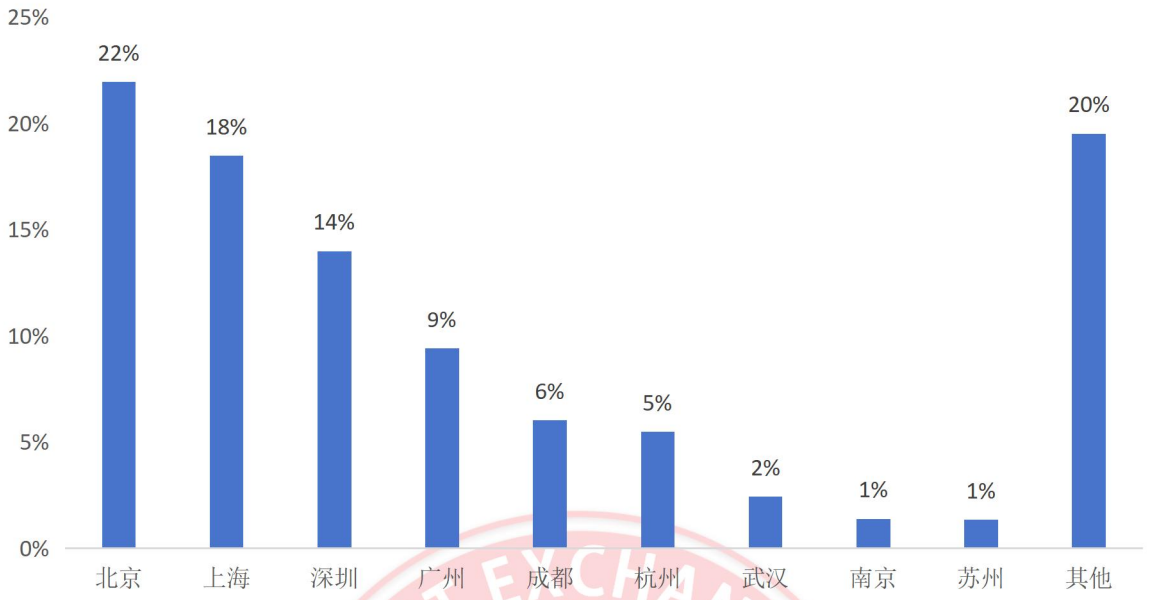

图 12.网络安全人才城市需求占比

3.行业分布

从各行业对网络安全人才的需求分布来看，人才招聘需求量最大的是信息安全行业，占据总需求的 30.45%。目前我国网络安全企业覆盖网络安全设备、安全服务、安全软件、安全集成等网络安全各个环节。随着 5G、人工智能等新一代信息技术与实体经济深度融合，安全风险加速传导、渗透、叠加和放大，网络安全已成为各领域各行业“刚需”，产业发展进入快车道，网络安全龙头企业加速壮大，新成立企业纷纷跑步入场。

互联网和 IT 信息技术行业的人才招聘需求占比之和超 35%，对于网安人才的渴求显著高于其他行业。互联网、IT 信息技术企业往往是高科技大数据企业，掌握着海量用户数据，一旦发生数据泄露损失将无法估量，这让以基于数据应用提供产品和服务的

企业必须在产品原生安全性方面加大考虑和投入。在产品安全覆盖式和风险合规性双轮驱动下，未来，相关单位、企业对网络安全人员的需求将持续增加。

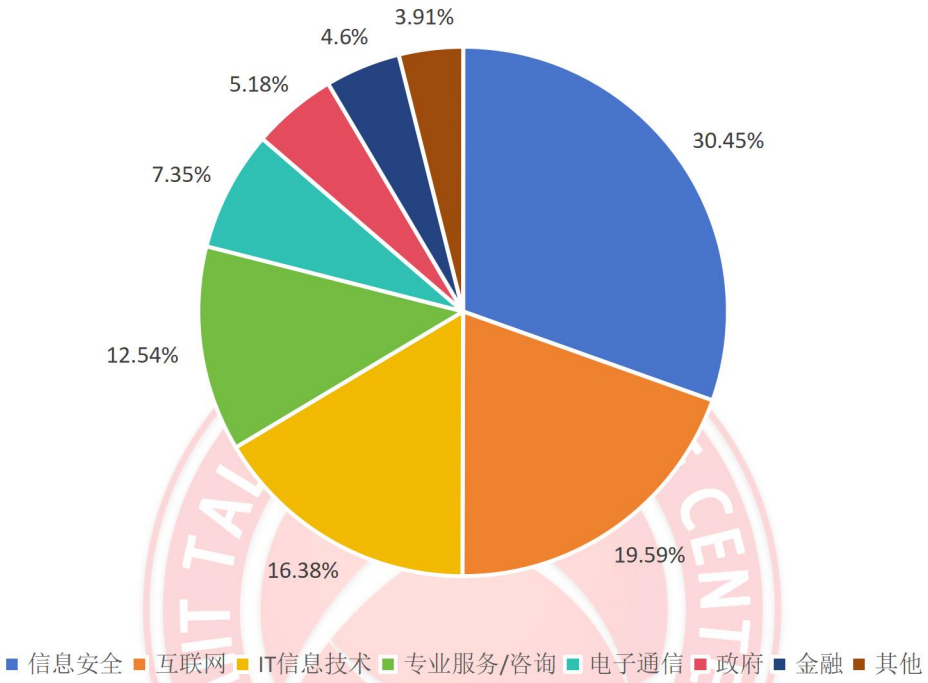

图 13.网络安全产业按行业人才需求占比

4.岗位分布

通过走访调研行业头部企业，以及分析拉勾招聘平台岗位数据及任职文本数据，我们遴选出企业具有代表性的 7 种网络安全岗位，并梳理出相关工作内容。

表 2.网络安全产业主要岗位及工作内容

岗位	工作内容

网络安全工程师	风险评估/渗透测试/安全加固/漏洞扫描/基线检查/应急响应/等级保护合规/编写安全服务方案/项目协作/项目管理/技术支持
安全运维工程师	安全产品运维/安全态势监控/安全运营保障/安全事件响应与处置
网络安全研究员	网络空间学科理论和方法论/新兴技术与应用/产业发展趋势/法律/法规/政策/标准
应用安全工程师	应用安全评审和评估/安全开发规范流程的开发与完善/安全开发规范培训/威胁建模/优化 DevOpSec 流程/SDL 安全开发项目管理
网络安全顾问	安全规划/设计/实施/运维/管理/合规咨询/技术咨询
渗透测试工程师	应用上线安全测试/例行检查/渗透测试/风险评估/漏洞跟踪与修复/安全研发流程的制定与实施/安全意识和安全开发培训
数据安全工程师	企业数据安全规划与设计/安全建设方案/数据安全体系设计建设运营/数据安全策略与执行/安全事件响应溯源审计/前沿技术研究

（二）院校人才供给分析

1.专业设置情况

2015 年 6 月，“工学”门类下增设“网络空间安全”一级学科，这一决策的实施对于我国网络安全领域的发展和人才培养产生了积极的影响。一方面，它促进了网络安全学科的建设和发展，为培养更多的高素质网络安全人才提供了更加专业的学科基础；另一方面，它也提高了全社会对网络安全问题的关注度和重视程度，为保障国家安全和社会稳定做出了贡献。

事实上，网络安全类专业在不同学历层次都有涉及。在研究生阶段，专业重点包括网络与信息安全、网络空间安全、计算机科学与技术、计算机软件与理论、计算机应用技术等，这些专业的研究方向主要侧重于理论研究和高端技术研发。在普通本科阶段，专业设置主要涉及信息安全、网络空间安全、网络安全与执法、保密技术、信息工程等，这些专业侧重于基础理论和技术应用。在高职阶段，专业设置主要包括信息安全技术、软件技术、网络安全与执法、计算机应用技术、计算机网络技术等，这些专业侧重于实践操作和基础技术应用。总体来说，这样的设置旨在培养不同层次、不同类型的网络安全人才，以满足不同领域的需求。

表 3.网络安全相关学科专业梳理

学历层次	相关学科专业
研究生	网络与信息安全、网络空间安全、计算机科学与技术、计算机软件与理论、计算机应用技术、软件工程、计算机系统结构、信息与通信工程
普通本科	信息安全、网络空间安全、网络安全与执法、保密技术、信息工程、计算机科学与技术、软件工程、网络工程
高职本科	数字安防技术、网络安全与执法、信息安全与管理、计算机应用工程、软件工程技术、现代通信工程
高职	信息安全技术、网络安全与执法、软件技术、计算机应用技术、计算机网络技术、网络工程技术

根据教育部数据，截止 2022 年底，我国超过 200 所高校设

置了网络安全相关专业点。根据国家智慧教育公共服务平台数据，我们梳理本科开设了网络安全专业（信息安全、网络空间安全、网络安全与执法）的院校信息，按区域统计分布如下。

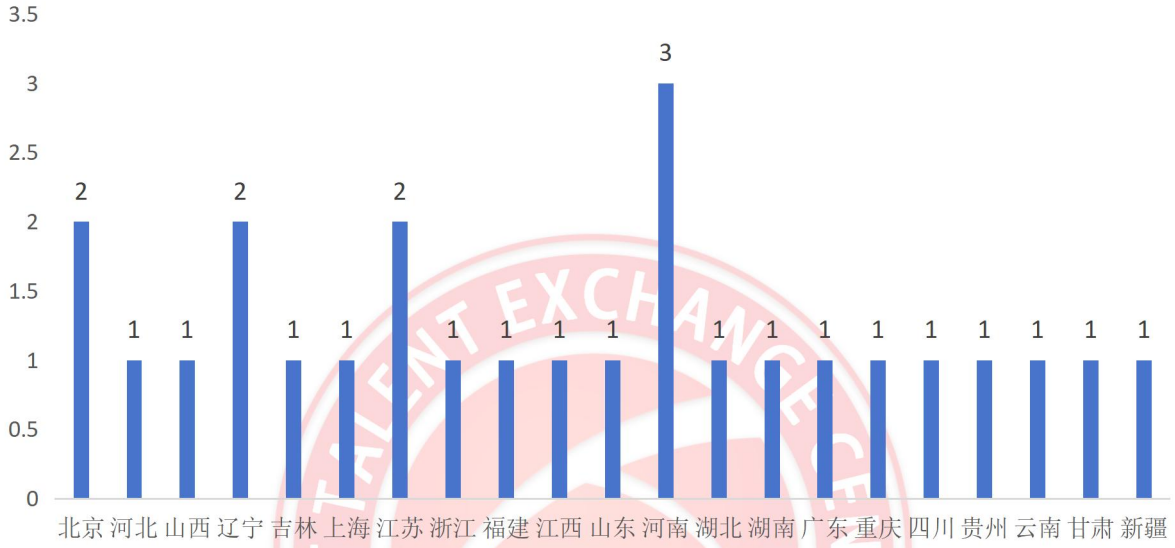

图 14.本科网络安全与执法专业点院校数量按区域统计

图 15.本科网络空间安全专业点院校数量按区域统计

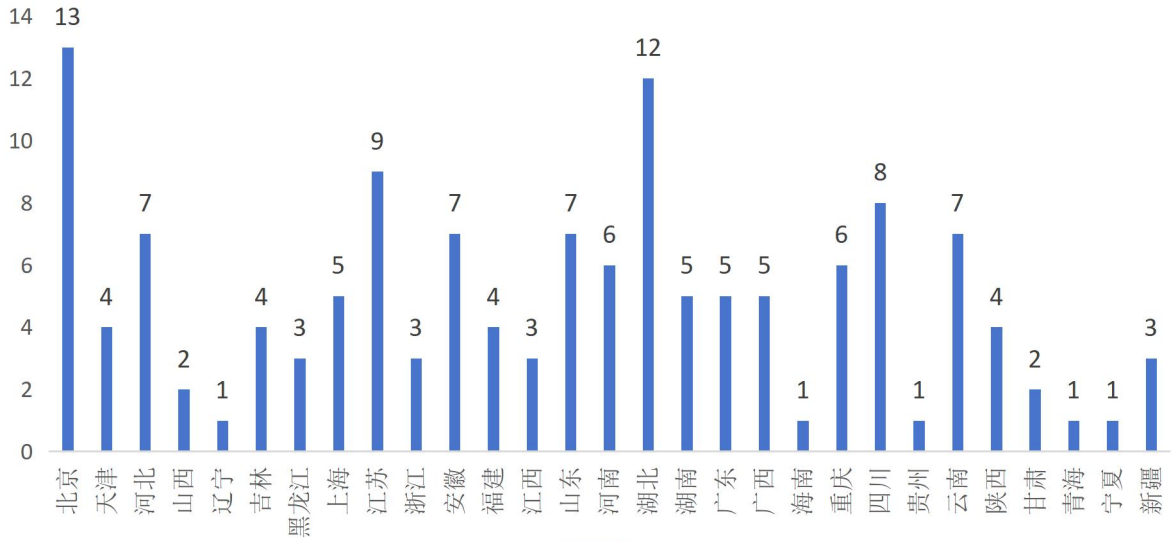

图 16.本科信息安全专业点院校数量按区域统计

本科设有信息安全专业点的院校全国共计 139 所，其中北京（13 所）、湖北（12 所）、江苏（9 所）位居前三。本科设有网络空间安全专业点的院校全国共计 98 所，其中山东（10 所）、广东（8 所）、四川（8 所）位居前三。本科设有网络安全与执法专业点的院校全国共计 26 所，其中河南（3 所）、北京（2 所）、辽宁（2 所）、江苏（2 所）位居前列。

此外，根据教育部《2022 年度普通高等学校本科专业申报材料公示》，2022 年度拟新增的 483 个本科专业中，有 51 个是网络与信息安全相关专业。

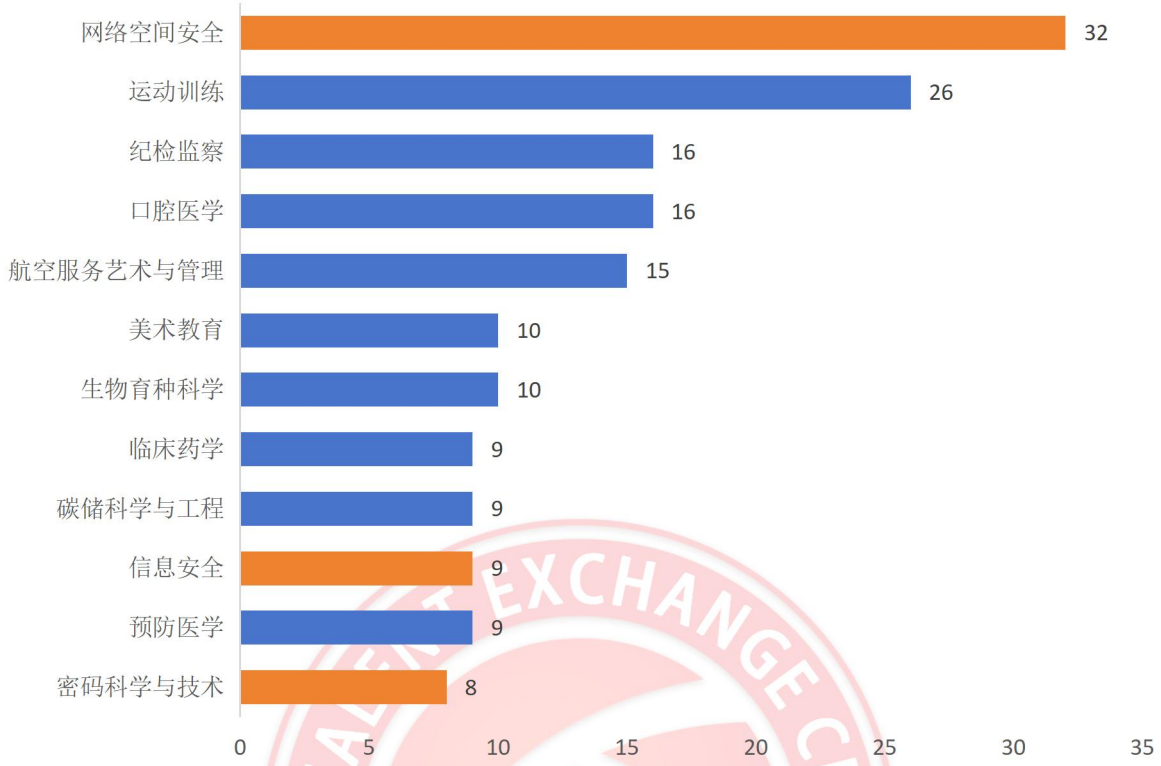

图 17.2022 年度拟新增本科专业中排名前 12 的专业

2.毕业生规模

根据国家智慧教育公共服务平台数据，2023 年网络安全相关本科专业（信息安全、网络空间安全、网络安全与执法）毕业生规模约为 1.45 万人。根据教育部统计数据，2022 年我国本科毕业生规模约占总毕业人数的 45%。按照该占比数值预估，我国 2023 年网络安全相关专业毕业生约为 3.2 万人。总体上，网络安全产业人才供需关系为供不应求。

四、网络安全产业从业人员岗位序列和任职资格

（一）从业人员岗位序列

依据中华人民共和国职业分类大典（2022 版）、国家职业技

能标准（2020 版）、GB/T 42446-2023《信息安全技术 网络安全从业人员能力基本要求》等文件，通过问卷调研、企业访谈等方式，结合网络安全产业全链条核心企业在主要招聘平台上发布的职位信息，我们将 7 类企业主要从业人员岗位与国家职业分类（小类和细分）进行对应后，详细情况如下表所示。

表 4.网络安全产业从业人员岗位序列

职业类别	职业编码	职业细分	企业岗位名称
信息通信网络运行管理人员（4-04-04）	4-04-04-02	网络与信息安全管理员	网络安全工程师
			安全运维工程师
			网络安全研究员
			应用安全工程师
			网络安全顾问
	4-04-04-04	信息安全测试员	渗透测试工程师
工程技术人员（2-02）	2-02-38-12	数据安全工程技术人员	数据安全工程师

（二）从业人员任职资格

网络安全产业从业人员岗位任职资格可从岗位任职要求和与之匹配的知识、技能、经验等三个方面展开分析。通过走访调研行业头部企业，以及分析《网络安全产业人才岗位能力要求》

文本数据，梳理出网络安全产业 7 种主要从业人员岗位任职资格能力矩阵，如下表所示。

表 5.网络安全产业从业人员岗位任职资格能力矩阵

岗位	知识		技能	经验
	学科专业	理论知识		
网络安全工程师	计算机/网络空间安全/信息安全/网络工程相关专业	安全设备原理/安全协议与安全系统原理/Web 安全原理/TCP/IP 原理	安全攻防技能/数据库风评与加固/网络配置与障	1-3 年网络/信息安全相关工作（学习）经验；安全日志分析经验
安全运维工程师	计算机/网络空间安全/信息安全/网络工程相关专业	网络安全防护体系/操作系统原理/常见漏洞原理/安全产品原理	漏洞识别与修复/编程能力（Python、Java、Php)	1 年以上安全运营、安全运维经验；安全防护产品实践经验
网络安全研究员	计算机/网络空间安全/信息安全/网络工程相关专业（硕士以上）	网络安全发展历程现状趋势/国内外产业发展法律法规政策标准方案/风险、供应链、运营、应急、漏洞管理知识/网络安	沟通协调能力/制度、策略、机制的建立和执行/研究与创新能力/学术交流	网安现状与趋势研究课题经历/项目经验

		全体系知识（网络、通信、计算机组成、操作系统、密码学、PKI/CA、身份鉴别、访问控制等）		
应用安全工程师	计算机/电子/信息安全相关专业	Web 安全原理/常见漏洞原理/Web 应用架构原理/SDL 安全开发流程	代码审计能力（Java、.net、Python)/SDL 实践能力/渗透测试常见工具/DevOps 工具部署及流程	3 年以上工作经验/SDL 项目实践经验
网络安全顾问	计算机/网络空间安全/信息安全/网络工程相关专业	网络安全发展历程现状趋势/国内外产业发展法律法规政策标准方案/风险、供应链、运营、应急、漏洞管理知识/网络安全体系知识（网络、通信、计算机组成、	沟通协调能力/目标识别/制度流程建立和执行/安全需求识别/安全规划与设计/安全体系与人员能力梯队建设	3 年以上工作经验/大型安全项目经验

		操作系统、密码学、PKI/CA、身份鉴别、访问控制等）/行业安全知识		
渗透测试工程师	计算机/网络空间安全/信息安全/网络工程相关专业	常见漏洞原理与修复/编程语言/等级保护/ISO27001/ITIL	渗透测试工具和项目能力/漏扫、反编译跟踪测试工具/编程语言能力（Java、Python、Ruby、Perl、C、go)/漏洞测试 POC 编写能力	漏洞挖掘经验/CTF 获奖经历/网络攻防与应急响应经验/事件调查溯源经验
数据安全工程师	计算机/网络空间安全/信息安全/网络工程/应用统计相关专业	安全相关法律内容/隐私保护技术原理/安全标准知识（等级保护、ISO27001、GDPR）/安全产品与方案	数据分析与挖掘能力/数据分析工具（SQL、Python、正则表达式等）/数据安全权威认证	3-5 年数据安全运营工作经验/数据安全审计存储访问交易实战经验/合规测评风控经验

从宏观视角可见，随着网络安全在各行业受到重视程度不断

提升，人员岗位的设定呈现出分工细化、专业化趋势。从任职要求匹配度方面来看，从业人员除了需掌握安全攻防基础理论之外，还需要着重实战（践）能力培养。

通过分析表格，结合调研结果，可以发现。

（1）网络安全工程师和安全运维工程师属于较广泛类岗位，主要体现在 2 个方面，一是需自行负责安全防护的企业往往不太区分两者的工作内容；二是该类岗位对知识、技能要求的专业面优先于专业深度，所以从业年限要求一般为 1-3 年不等。

（2）网络安全研究员和网络安全顾问岗位均需深入理解产业和技术的发展历程和趋势，以资深的能力视角识别需求，并提出解决方案，不同点在于前者关注对象为技术难点，后者关注对象是客户的安全“难题”。

（3）应用安全工程师和渗透测试工程师岗位对知识、技能的专业度要求较高，在各自的岗位分工中均需具备全局流程视角，前者对于漏洞原理、安全开发技术等要求有较深入的理解和实战能力，后者对基于风险的攻防能力要求有深入的实战研究，包括日常的渗透测试评估、安全事件的应急响应处置等。

（4）数据安全工程师属于新型岗位，在大数据背景下，数据继土地、劳动力、资本、技术之后，成为推动数字化社会快速演进的第五项重要生产要素，数据安全也进一步受到国家和社会的重视，该类岗位通常要求兼具合规、运营、攻防一体知识和技能，且要求程度较其它岗位更细“粒”。

（三）在职人员能力提升体系建设

为更好了解在职人员的能力提升体系情况，我们深入相关网络安全企业进行了问卷调研及现场访谈，数据显示如下。

1.人才队伍建设

7.57%的受访从业人员认为其所在单位对于网络安全人才队伍建设不重视，27.53%的人员认为用人单位给予较少重视，29.26%的人员认为重视程度一般，，20.44%的人员认为重视程度较好，以及 15.21%的人员认为用人单位非常重视。尽管大部分企业建立了职业任职资格标准和人才机制，但对应的职业发展培养体系仍不完善，能力提升培训和成长机会供给不充足，导致多数从业人员感到发展空间有限。

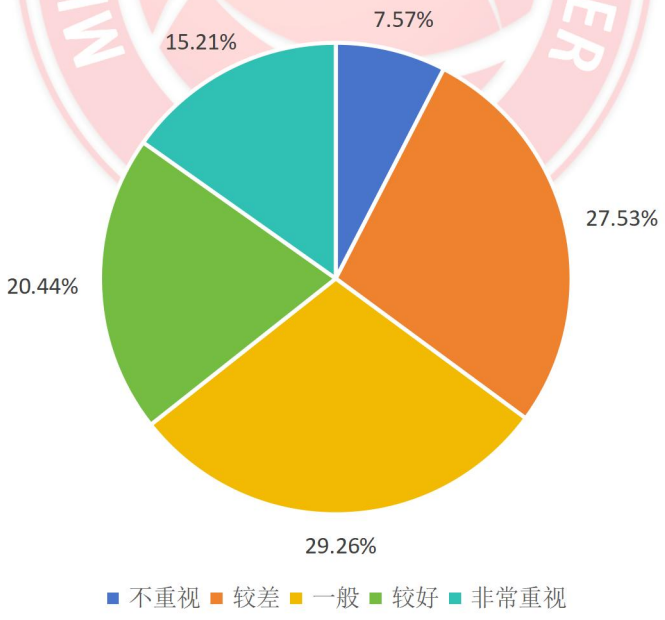

图 18.人才队伍建设的重视程度

2.人才培养项目

在体系化人才培养项目（即有明确的培训路径和清晰的受训人员规划）组织方面，仅有 42.28%的用人单位开展过类似项目，剩下 57.72%的用人单位未曾开展过，这表明整体上在职人员体系化的人才培养项目较为缺乏。

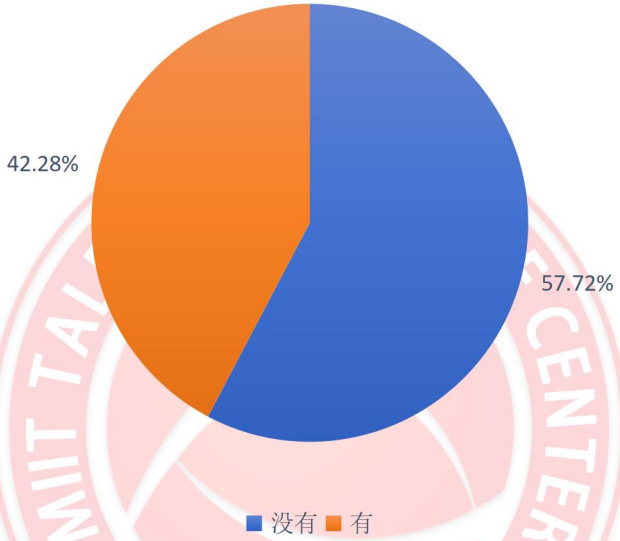

图 19.用人单位人才培养项目开展情况

3.能力提升方式

对于从业人员在实际工作中应用的知识与技能，38.27%来源于工作项目的经验积累，32.44%是从业人员工作之余自学而成，13.7%来源于有效的用人单位内部培训，12.64%受益于在校时的专业学习，因受工作时间限制，仅有 2.95%的从业人员通过自主参与社会培训获取工作知识与技能。

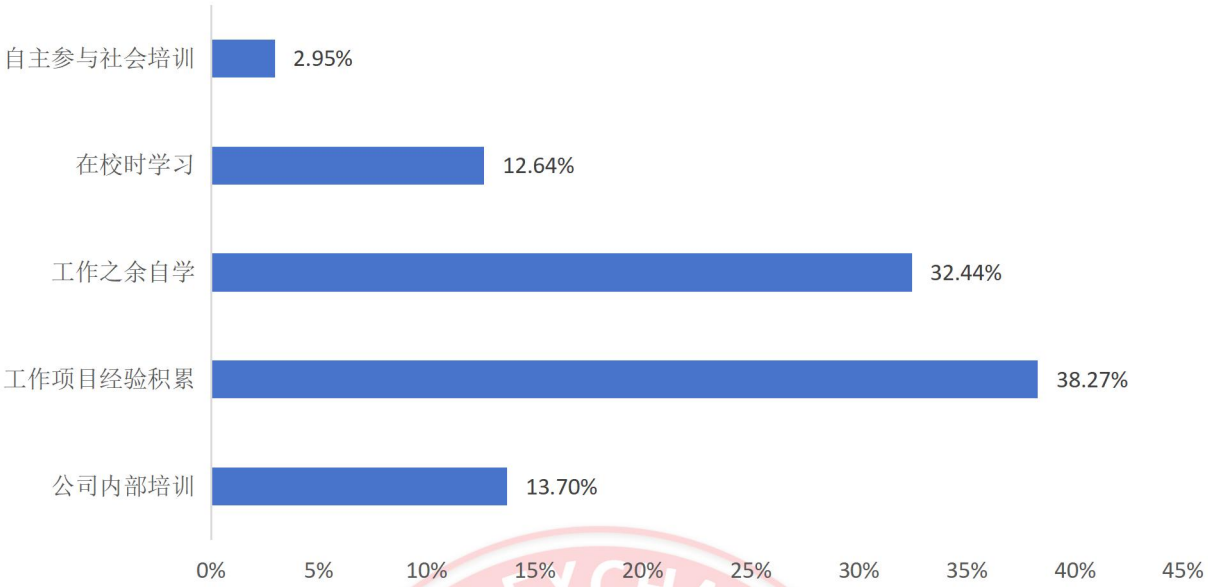

图 20.从业人员能力提升方式

五、网络安全产业人才发展存在的主要问题

（一）网络安全产业人才整体供需失衡

根据中国网络安全产业联盟数据，2022 年我国网络安全市场规模约为 633 亿元，同比增长率为 3.1%，预计未来三年将保持增长态势，增速将保持在 15%以上，到 2025 年市场规模预计将超过 800 亿元。未来，我国网络安全人才需求数量持续增长。然而，与网络安全人才需求不匹配的是院校人才供给的滞后性，按照相关数据推测，2023 年网络安全相关专业的毕业人数规模在 3.2 万左右，院校供给端难以满足我国网络安全产业发展对人才的需要。

（二）网络安全实战人才严重短缺

数据显示，网络安全工程师、安全运维工程师、网络安全研究员、应用安全工程师、网络安全顾问、渗透测试工程师、数据

安全工程师是当前公司主要需求岗位。其中，数据安全工程师是紧缺度最高的岗位，这与《数据安全法》《个人信息保护法》相继颁布实施、企业迫切需要开展数据安全及隐私保护、合规治理等方面工作有着密切关系。其次，可以看到，网络安全工程师、安全运维工程师、网络安全研究员、应用安全工程师、网络安全顾问、渗透测试工程师等企业需要的主要岗位都与网络安全实战应用相关，这也在一定程度上反映了目前我国网络安全产业重“硬件盒子”、轻“软件服务”的发展现状。

（三）院校专业开设和培养方案严重滞后

网络安全专业在本科类院校中开设较早，但近几年高职高专类院校的人才培养数量呈现赶超态势，这主要是因为高职高专类院校在专业设置具有一定自主性，可根据产业发展需求进行专业备案或专业方向的灵活调整。网络安全人才培养具有多学科交叉、涉及面广等特点，现有培养方案并不完全适用于网络安全本身的发展需求。调研发现，院校在网络安全人才培养方面存在以下三方面问题：一是专业建设方面。课程设置不够合理、与产业实际脱节，课程教材实用性不强。二是师资水平方面。教师专业与授课水平一般、实践经验较少、工程实践能力有待提升。三是实习实践方面。学生去相关企业实习和实践机会较少，院校实践体系方面的建设仍有加强空间。

（四）在职人员能力提升体系欠缺

调研显示，多数用人单位的人才培养体系尚不完善，具体表

现在以下几个方面：一是网络安全人才队伍建设受重视程度不高。29.26%的从业人员认为所在单位对网络安全人才队伍建设的重视程度一般，27.53%的从业人员认为用人单位给予较少重视，7.57%的从业人员认为不重视。二是体系化人才培养项目缺乏。57.72%的用人单位未开展过体系化人才培养项目。三是从业人员能力提升方式有限。多数从业人员仍靠经验积累或自学来获取知识技能，38.27%来源于工作项目的经验积累，32.44%是从业人员工作之余自学而成，12.64%受益于在校时的专业学习。

六、网络安全产业人才发展对策建议

（一）完善产业人才激励机制

国家层面，建议开展网络安全急需紧缺人才专项行动，对技术研发等做出突出贡献的人才给予物质奖励，支持网络安全龙头企业与海外人才服务机构或团体联合设立海外人才联络处，把人才“引进来”。企业层面，在本地区人才政策框架下，配套并优化企业自身的人力资源制度，强化企业主体投入作用，加大人才创新中心、人才培养基地等建设力度，提升其对人才的吸引力。院校层面，根据自身办学基础和办学条件，设立网络安全一级学科或在相关一级学科下设网络安全专业方向，并根据产业发展需求进行灵活调整，扩大招生培养规模。

（二）搭建实战人才成长平台

建立健全高校的网络安全学科专业与人才培养的评价机制，向实战人才的需求靠拢，为培育网络安全实战人才提供丰沃土壤。

在全国范围开展网络安全实战人才高级人才洽谈会等招聘服务，搭建网络安全产业中高层次岗位与实战人才匹配的平台，为网络安全产业链上下游企事业单位提供招聘中高端网络安全实战人才的服务，促进实战人才合理流动。国家出台有关政策，促进我国网络安全产业升级，完成从“产品导向”到“服务导向”的转变，扩大网络安全市场份额，为网络安全优秀实战人才搭建舞台和平台。

（三）创新产教融合培养模式

强化院校网络安全人才培养的产业需求导向，推动院校进一步了解网络安全行业对人才知识结构、专业技能等方面的岗位要求，科学规划网络安全核心课程、必修课程、选修课程、实习课程等教学内容。推进校企合作，鼓励企业与院校共同制定培养方案、设计课程、开发教材，共建教学团队、实践实训平台、建立校外实习实训基地等。鼓励教师到网络安全企业挂职锻炼，打造双师型团队。构建政府、企业、培育机构、高校等共同参与的共享型人才培养实践平台，构建培育产学研项目合作实验室、协同创新中心等。

（四）加强从业人员能力建设

加强网络安全产业人才现状研究，建立急需紧缺岗位人才需求预警机制。针对急需紧缺岗位，鼓励行业龙头企业、社会培训机构推出有针对性、可解决问题的培训课程体系。对从业人员定期开展网络安全实战管理、网络安全实训等方面的专题培训讲座，

开展网络安全类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。企业可针对特定岗位设立人才培养项目，选派网络安全人才赴高校培训进修，根据企业需要培养专项人才。