AI时代网络安全产业人才发展报告

（2025 年）

编写单位

工业和信息化部教育与考试中心　安恒信息　中国联合网络通信有限公司软件研究院

中国网络空间安全人才教育论坛　中国网络空间新兴技术安全创新论坛　智联招聘

全国数字安全行业产教融合共同体

AI时代网络安全产业人才发展报告

（2025 年）

特别提醒

行业交流分享群

分享：可获取人资行业的报告、方案及其他学习资源，上新群内通知

交流：求职、找人、找资源、找供应商

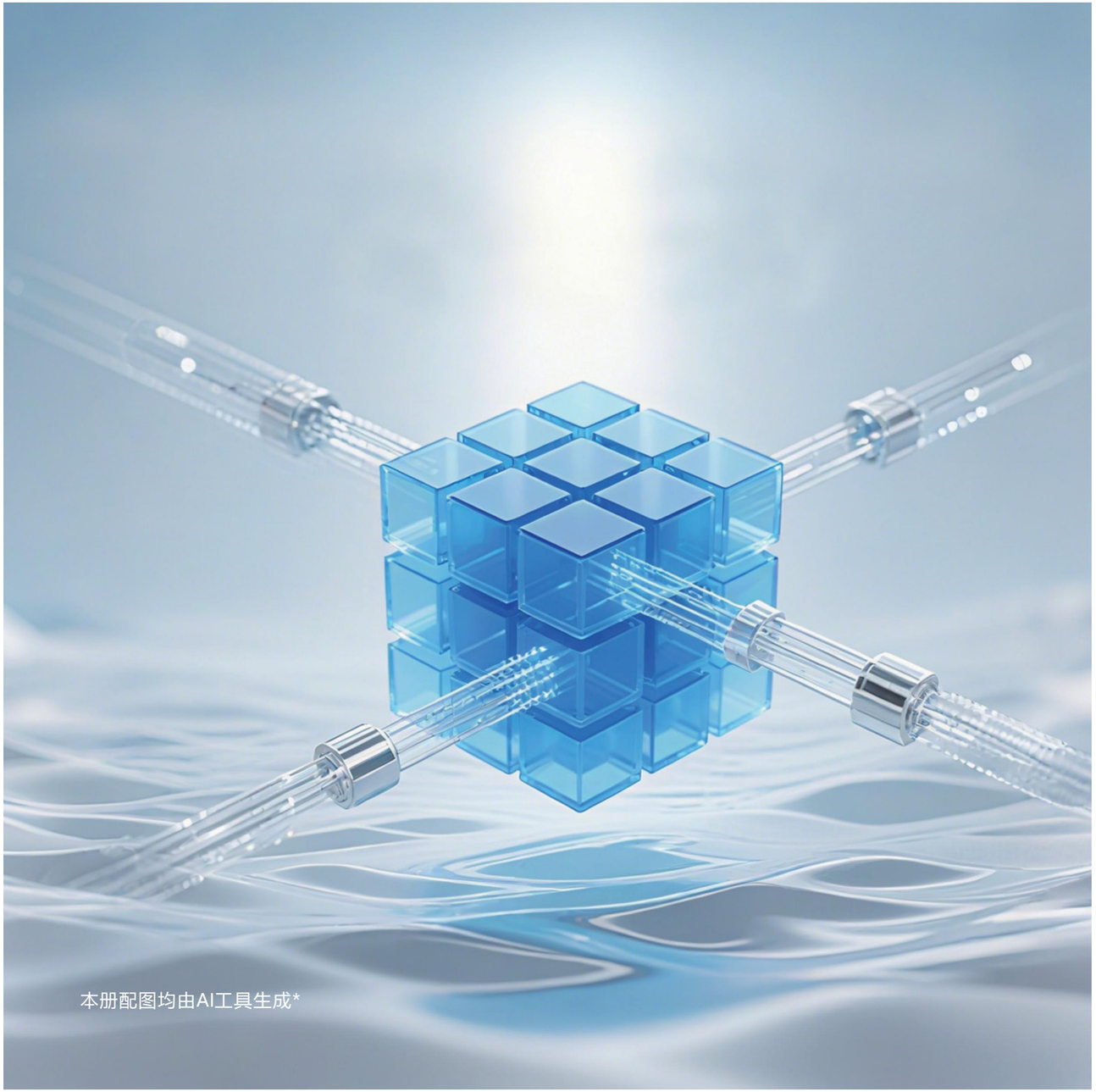
客服

交流群

免责声明

第三方声明：本报告所有内容（数据/观点/结论）整理于网络公开渠道，均不代表我司立场，我司不承担其准确性、完整性担保责任。

侵权处理承诺：如报告内容涉嫌侵权，请立即联系客服微信，我司将在核实后第一时间清理相关内容并配合处理



编写单位

工业和信息化部教育与考试中心　安恒信息　中国联合网络通信有限公司软件研究院

中国网络空间安全人才教育论坛　中国网络空间新兴技术安全创新论坛　智联招聘

全国数字安全行业产教融合共同体

指导组（排名不分先后）

郝志强　鲁　辉　王志军　程德杰　苗春雨　王　乐　段平霞

钟　诚　王一新

编写组（排名不分先后）

谭志彬　咸汝平　张平贺　杜　妍　王淑燕　柏　雪　陈雨欣

方鹏辉　李小丽　倪勤勤　刘　硕　舒　眉　许斯欣　薛晓梦

杨　佳　于天娇　张　浩

前言
PREFACE

在数字经济成为全球增长新引擎的背景下，网络安全产业正经历结构性变革。传统以硬件为核心的“围墙式防御”加速向“数据驱动、智能协同”的新业态演进，产业范畴从网络纵深防御延伸至数据全生命周期安全、AI内生安全、云原生防御等新领域，形成“技术+服务+生态”三位一体模式，生成式AI推动安全运营从“人工响应”转向“智能体协同作战”，90%的告警可自动化处置，人才角色从操作者进化为AI策略指挥官。

人才，作为AI时代网络安全产业的核心驱动力，扮演着至关重要的角色。高素质的网络安全人才是确保网络安全防护体系有效运作的关键。无论是前沿技术研发、安全策略制定，还是大模型安全、威胁情报分析、应急响应处置，都离不开一支高素质、专业化的人才队伍。人才的培养与储备直接关系到AI时代网络安全产业的发展质量和竞争力水平。

鉴于此，《2025年网络安全产业人才发展报告》的编制旨在全面分析AI快速发展以来，网络安全产业人才现状，深入探讨人才需求与供给的矛盾，提出切实可行的人才队伍建设策略。报告广泛收集行业数据，深入访谈众多业内专家与一线从业人员，力求从多个维度呈现网络安全产业人才生态的全貌。

报告主要内容包括:

1.全球网络安全领域依旧面临人才与技能双重缺口扩大的严峻挑战。发达国家呼吁以主动嵌入安全设计、改革招聘机制并强化实战培养渠道改善现状。结合政府立法推动、企业与高校联合培养、学徒制度以及训练平台建设，为整个行业构建更具韧性的人才发展生态。国内网络安全行业正处于高速增长向高质量发展的过渡阶段，市场规模也较2023年实现了稳步增长。

2.从业人员方面，30岁以下的网络安全从业人员所占比例逐年升高，成为网络安全产业的主力军；本科学历人员仍然是网络安全相关职位的主要组成部分；薪资方面，中高收入者小幅上升；2024年网络安全相关岗位的主要来源仍是IT类企业为主，安全运营类岗位占比最高；在校人才培养方面，竞赛成为学生技能提升的重要手段。

3.AI时代的网络安全，正从“传统攻防”转向“AI驱动的新型攻防”，需要围绕“AI工具运用-AI攻防对抗-AI决策优化”构建新的能力体系。近五成从业者认为最需要掌握的技能是AI工具的使用与调优以及对抗性AI攻防技术， AI相关技能正从“补充项”转变为岗位的“标配能力”。AI技术正深刻重塑网络安全领域，催生出大量新型工作场景。核心岗位目前集中于模型与系统安全，如AI/ML安全工程师，他们负责算法与数据完整性保障、对抗性攻击测试及漏洞加固。 AI正成为重塑网络安全人才发展路径的重要变量。从能力结构重构到岗位职责转型，再到认知方式的更新，网络安全从业人员正处于“人机融合”趋势加速演进的关键阶段。

注：以下信息可以帮助读者更好地理解报告的研究主体和方法论，供读者参考与指正。

【调研对象】本报告旨在探讨网络安全行业人才培养现状，调研覆盖142家具有一定代表性的网络安全类公司共7294名从业人员，252所本科和高职院校共8285名网络与信息安全及相关专业（包含计算机科学与技术网络安全特色方向、网络工程等）在校生，35名专家学者、政府有关部门人员及网络安全产业利益相关者。

【数据来源】报告工作组通过在线问卷和线上线下访谈的形式，共收集了15515份有效样本。并查阅了大量公开资料，包括官方文件、国内外行业报告、学术论文等， 以获取全面的数据支持，同时与智联招聘开展合作，智联平台为报告提供部分数据支持。

【调研范围】涵盖国内外行业及人员相关情况、国内行业市场需求分析、产业人才供给分析、AI技术对行业及从业人员影响等方面。

目录
CONTENTS

前　言 01

第一章 国内外网络安全产业及人才概况 05

第一节 欧美等发达国家网络安全产业及人才概况 07

第二节 我国网络安全产业概况及人才概况 10

第三节 国内外AI技术发展对网络安全产业及就业影响 13

第二章 网络安全人才从业现状 15

第一节 我国网络安全从业人才画像 16

第二节 网络安全产业人才的从业现状 20

第三节 AI的发展对网络安全从业人员的影响 22

第三章 网络安全产业人才供需分析 29

第一节 网络安全产业人才需求 31

第二节 网络安全产业人才供给 37

第四章 在岗人才成长 71

第五章 AI时代：网络安全人才的挑战与转型路径 85

第一章

国内外网络安全产业及人才概况

尽管受经济周期影响，多数行业都呈现出发展速度放缓的态势，但伴随数字经济和技术的迅速发展，网络安全产业规模仍呈现持续扩张的趋势，彰显出行业强大的增长潜力。然而，机遇与挑战并存，网络安全产业的快速发展也暴露了人才供需的结构性矛盾，人才问题已成为制约行业进一步发展的瓶颈之一。为了深入理解国际网络安全产业人才的现状与未来趋势，本报告国际产业及人才情况主要参考了ISC2（International Information System Security Certification Consortium，即国际信息系统安全认证联盟）发布的《2023年全球网络安全人才发展报告》。 ISC2作为全球领先的网络安全专业人员认证与教育机构，其报告基于广泛的调研数据，全面剖析了全球网络安全劳动力的现状、面临的挑战以及未来的发展方向，为业界提供了宝贵的数据支撑与洞察。

第一节 | 欧美等发达国家网络安全产业及人才概况

一、欧美发达国家网络安全产业正保持稳步增长

根据CyberSeek数据显示，美国仍是全球最大的网络安全市场。2024-2025财年美国线上发布的网络安全职位超过514,000个，同比增长约12%，显示出持续上升的招聘需求[1,2]。然而，在被发布的岗位中，实际填补的比例仍不到三分之二，导致约74个岗位仅能吸引到55位合格候选人[3]。与此同时，Cybersecurity Ventures表示全球空缺岗位将达到350万，其中美国约占75万，网络安全人才缺口成为全球行业面临的核心挑战[4]。

欧洲网络安全产业也保持快速发展。英国科技部发布的《2025年网络安全行业分析》（Cyber security sectoral analysis 2025）报告指出，2024-2025财年期间，英国网络安全行业实现营收为132亿英镑，同比增长12%；同时行业总产值（GVA）约为78亿英镑，同比增长21%；在职员工数达到67,300人，同比增长11%，新增岗位约6,600个；市场共有2,165家相关企业，同比增加3.5%[1]。此外，据InfoSecurity Magazine报道，投资方面亦颇为活跃，2024年共有206百万英镑资金投入网络安全初创公司，涉及59笔融资交易[5]。

[1]信息来源：Research and analysis Cyber security sectoral analysis 2025
https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2025/cyber-security-sectoral-analysis-2025

[2]信息来源：Cybersecurity jobs on the rise as US industries navigate economic uncertainty
https://www.weforum.org/stories/2025/06/cybersecurity-jobs-rise-us-industries-navigate-economic-uncertainty

[3]信息来源：Axios Future of Cybersecurity
https://www.axios.com/newsletters/axios-future-of-cybersecurity-cbbd9cb0-3caf-11f0-882c-a323f60db9d9

[4]信息来源：Cybersecurity Jobs Report:3.5 Million Unfilled Positions In 2025
https://cybersecurityventures.com/jobs

[5]信息来源：UK Cybersecurity Sector Revenue Grows 12%to Top£ 13bn
https://www.infosecurity-magazine.com/news/uk-cybersecurity-sector-revenuerity-skills-shortage-cto-guide

二、人才供需失衡问题日益突出

ISC2报告指出，截至2024年，全球网络安全人才缺口已从上一年度的约400万增长至480万，同比增长19%，其中亚太地区缺口最大，而全球网络安全从业人员总数仅约550万，增速几近停滞。这意味着行业缺口占比高达87%，许多组织难以找到足够合格人员[6,7]。

技能差距也十分明显，根据SANS/GIAC调研结果，52%的安全领导者认为问题不在于岗位空缺本身，而是缺乏具备合适技能组合的人员[8,9]。Fortinet调查报告指出56%的组织难以招到合格安全人才，54%的组织也面临人才流失问题，反映招聘与留人双重压力这种供需失衡导致了多重负面后果：岗位填补周期延长[10]。CyberSeek数据显示，网络安全岗位的招聘周期比一般IT岗位平均延迟21%。技能短缺也加剧了安全事件发生率[1]。据ISC2数据，有缺口的组织发生重大安全事件的可能性是无空缺组织的近两倍[7]。

此外，从职业发展角度来看，人才结构性偏高资深岗位，而初中级人才稀缺。 ISC2报告显示，31%的组织没有任何入门级新人，15%的组织没有初级（1-3年）人员[7]。虽然大企业倾向于创建更多中初级岗位，但中小机构缺乏持续培养新人机制，进一步加剧“断代式”成长路径。

[6]信息来源：Navigating the Cybersecurity Skills Shortage:A Guide for Tech Leaders
https://ssojet.com/ciam-101/cybersecurity-skills-shortage-cto-guide

[7]信息来源：Growth of Cybersecurity Workforce Slows in 2024 as Economic Uncertainty Persists
https://www.isc2.org/Insights/2024/09/ISC2-Publishes-2024-Cybersecurity-Workforce-Study-First-Look

[8]信息来源：New SANS/GIAC study finds cybersecurity skills gap,not talent shortage,at core of workforce crisis
https://industrialcyber.co/news/new-sans-giac-study-finds-cybersecurity-skills-gap-not-talent-shortage-at-core-of-workforce-crisis

[9]信息来源：2025 Cybersecurity Hiring Trends:Why Investing in Entry-and Junior-Level Talent is Key to Building a More Resilient Cybersecurity Workforce
https://www.isc2.org/Insights/2025/06/cybersecurity-hiring-trends-study

[10]信息来源：50+Cyber Security Job Statistics&Trends for 2025
https://www.stationx.net/cyber-security-job-statistics/

三、构建更富韧性的长效人才生态体系

发达国家正逐步意识到“技能错配”与过高经验期望是阻碍网络安全发展的一大因素。白宫网络安全负责人呼吁取消入职硬性学历要求，探索更多以技能为导向的招聘路径，以扩大人才来源池。英国则通过立法《网络安全与韧性法》（Cyber Security and Resilience Bill）推动企业加强实战演练与报告制度，确保关键基础设施安全[11]。World Economic Forum指出，行业需“摒弃幽闭学术偏见，拥抱多样人才”，鼓励游戏、艺术、退伍军人等非科班背景人士入行，并通过加强岗位定义提升招聘成功率。另一方面，职业通道搭建成为趋势：英国已推出Cyber Security Technician Level 3及Technologist Level 4学徒计划，由政府提供培训补贴并绑定入职前景，增强学历与就业对接[12]。

总体上，欧美网络安全行业正朝着三个方向推进结构性改革：主动嵌入安全设计、改革招聘机制并强化实战培养渠道。结合政府立法推动、企业与高校联合培养、学徒制度以及训练平台，这一体系融合策略正在为整个行业构建更具韧性的长期人才生态。

[11]信息来源：Securing the future:why cybersecurity must be secure by design-and by default
https://www.techradar.com/pro/securing-the-future-why-cybersecurity-must-be-secure-by-design-and-by-default

[12]信息来源：AddressingTheCyberSecuritySkillsGap_final_1
https://www.port.ac.uk/sites/default/files/2023-02/AddressingTheCyberSecuritySkillsGap_final_1.pdf

第二节 | 我国网络安全产业概况及人才概况

一、产业格局调整与市场发展趋稳：数字安全进入理性增长期

2024年以来，中国数字安全产业步入由高速增长向高质量发展的过渡阶段。数世咨询报告指出，数字安全产业“进入调整阶段”“去泡沫化已成定局”，这反映出市场从前几年的追风潮转向更为理性的发展轨迹。从市场规模来看，2024年我国数字安全业务（含集成）总收入已达到1800亿元人民币左右，较2023年实现了稳步增长。2020年至2024年间，整体行业保持年均12.3%的复合增长率，虽然不及前期爆发式增速，但在宏观经济承压背景下依然展现出强劲韧性。业务结构上，安全产品占比47.8%，安全服务上升至33.1%，集成类业务占比则下降到19.1%，说明企业在数字化转型过程中更加注重安全服务与专业支撑。此外，区域发展呈现出“东强西进”特征，北京、上海、广州、成都、杭州等城市连续多年稳居前十大数字安全城市之列，而四川、湖北、陕西等中西部省份在2024年也显著提高了产业营收与GDP比重[13]。

[13]信息来源：【数世咨询】中国数字安全产业年度报告2025-公开版v5

二、政策引导与技术演进融合：安全合规与数据要素化成为新核心

国家数据治理体系持续深化，特别是在《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》等法律法规推动下，中国正从“被动补防”走向“主动构建可信安全体系”。而这背后是政策驱动与技术落地的深度融合[14]。

2024年，国家发改委、国家数据局等多部委联合发布指导文件，明确提出“到2027年形成制度完备、产业兴盛、协同高效的数据流通安全治理体系”。这一顶层规划为数据确权、分类分级、跨境合规、全生命周期安全技术提供了制度保障，也为数据安全产业带来巨大的市场空间[15]。

数世咨询报告数据显示，2024年国内数据安全市场实际规模为58.03亿元，剔除非纯数据安全相关产品后，依然呈上升态势。数据安全服务商的主要客户集中在政府、金融、运营商和医疗行业，其中政府系统营收占比达16.06%，金融占15.14%，公安、国防、电力等关键领域也在加速布局数据安全能力。“大模型赋能安全”不再是单向赋能模式，“安全优先的大模型”成为新共识，这意味着在AI模型的训练与部署过程中，隐私保护、攻击防御和对抗样本识别能力已成为核心评估指标。整体上，政策与技术正逐步从“被动补防”转向“主动构建可信安全体系”的新阶段。

[14]信息来源：Internet in China https://en.wikipedia.org/wiki/Internet_in_China

[15]信息来源：China to increase data security market size
https://english.www.gov.cn/policies/policywatch/202501/21/content_WS678f09d0c6d0868f4e8ef062.html

三、人才生态重构与产业竞争加剧：高端安全人才供需失衡加剧

数字安全产业的快速演进，对人才的结构与质量提出了更高的要求，也暴露出行业竞争力与资源配置的深层矛盾。

据数世咨询报告数据显示，截至2024年底，全国数字安全从业人员约32万人，其中A股上市公司平均员工人数为420人，而非上市企业仅为136人。年薪水平差距明显，上市公司员工年均收入约24万元，高出非上市企业近50%（后者约16万元）。这表明头部企业对高端安全人才更具吸引力，也意味着人才向大型机构和核心区域进一步集中[13]。

面对紧张的人才供给与激烈的市场竞争，多个省市与龙头企业已展开人才培养创新，如与高校建立联合实验室、设立安全方向实训基地、参与国家级安全竞赛、推广职业技能认证体系等措施。然而长期来看，人才结构的不平衡仍将严重制约产业升级： 一方面高端需求集中、薪酬门槛上升；另一方面中小机构难以形成核心竞争力，区域安全服务能力差异扩大。因此，构建可持续人才生态，成为下一阶段产业政策与市场重点。

第三节 | 国内外AI技术发展对网络安全产业及就业影响

AI与安全技术的加速融合有效提升了威胁检测与响应效率，95%的安全专家认为AI显著提升了安全运营能力，84%表示AI使团队能够更主动地部署防御措施，但这也暴露出旧系统、工具兼容性差、部署落地难等问题[16]。Ponemon Institute的报告显示， 70%的组织难以将AI技术与遗留系统整合，42%认为团队在AI工具应用上准备不足[17]。此外，48%以上的机构表示AI引发了合规与隐私挑战，这意味着技术带来的便利也伴随着更复杂的治理需求。

就业结构正在经历显著转变。虽然AI替代了许多重复性业务， 使初级岗位需求减少，但相应地催生了大量高阶岗位，如AI提示词工程师、智能体开发等。最新数据显示，在英国，这类AI相关的网络安全职位增长率已达20-30%[18]。ISC2指出， AI不会取代专业人员，反而使安全专家能够将更多精力集中在复杂分析决策上[19]。不过，职业技能需求变得更加多元，软技能与跨领域能力开始成为招聘的重点。

[16]信息来源：The State of AI Cybersecurity 2025
https://www.darktrace.com/the-state-of-ai-cybersecurity-2025

[17]信息来源：Cost of a Data Breach Report 2024-IBM
https://www.ibm.com/cn-zh/reports/data-breach

随着数字安全产业向精细化运营和技术深耕演进，人才供需矛盾愈加突出，尤其是具备数据合规、安全运营、AI安全防护能力的复合型人才成为各大企业争抢的对象。当前形势下，政府、教育机构与企业需紧密合作，借助政策引导与培训体系建立复合型人才培养机制，以应对AI所带来的挑战。同时，合理布局AI落地应用，加强数据治理与合规机制建设，并为人才提供职业稳定与发展支持，从而构建应对未来更复杂网络安全形势的坚实人才生态。

总结来看， 国内外网络安全产业在人才与AI融合方面存在三大共性问题：其一，总量不足， 安全人才数量与产业需求存在巨大缺口；其二，质量不均，复合型、高端人才培养滞后，能力水平难以匹配快速演进的技术与合规环境；其三， AI影响巨大，既推动安全能力跃升，也带来治理难题和职业结构重构。这些问题意味着未来网络安全产业必须在政策、技术和人才生态三方面形成联动，才能真正支撑数字经济的可持续发展。

[18]信息来源：Demand for cybersecurity professionals surges with AI threat, cybersecurity and ethical hackers leading the pack
https://www.techradar.com/pro/some-data-centers-are-deliberately-slowing-possibly-tens-of-thousands-of-ai-gpus-to-avoid-blackouts-this-company-may-have-a-solution-clone-clone

[19]信息来源：2024 ISC2 Cybersecurity Workforce Study
https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

第二章

网络安全人才从业现状

第一节 | 我国网络安全从业人才画像

一、网络安全从业人员性别

多年来针对网络安全从业人员性别结构的调研显示，男性从业者比例始终显著高于女性，近三年数据显示女性占比稳定在20%-30%之间。造成该现象的主要原因在于网络安全依赖理工科背景，而相关专业长期性别失衡，导致女性人才供给不足；同时，行业对高强度技术岗位的要求和隐性性别偏见，也提高了女性从业和发展的门槛。值得关注的是，全球范围内已涌现出一系列致力于提升女性参与度的项目与组织，如CyberShikshaa、Women4Cyber等，通过教育赋能、职业培训与导师机制推动性别包容，逐步改善网络安全领域的结构性不平衡。

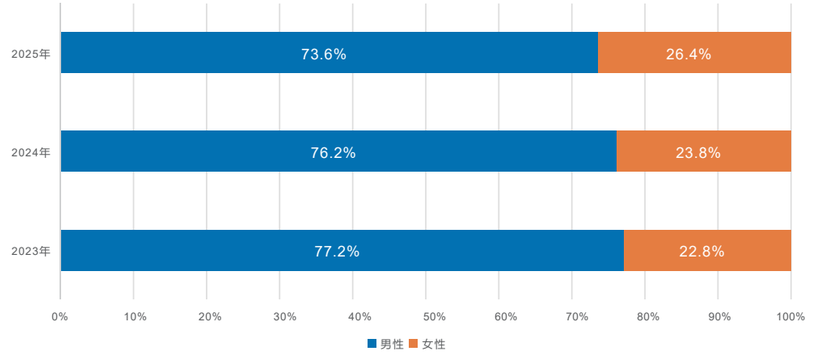


图1 网络安全从业人员男性和女性比例

二、网络安全从业人员年龄结构

近年来的调研数据显示，网络安全从业人员的年龄结构正向年轻化发展。目前，网络安全领域人才主要集中在26-30岁以下和30-40岁这两个年龄段。值得注意的是，30岁以下的网络安全从业人员占比正逐步攀升，并已然成为行业的核心力量。这不仅反映了网络安全行业技术迭代快，场景升级频繁，对新技术应用和创新能力要求较高。同时，这一发展趋势为网络安全领域注入了强大的新活力，有力地推动了技术创新和产业升级。

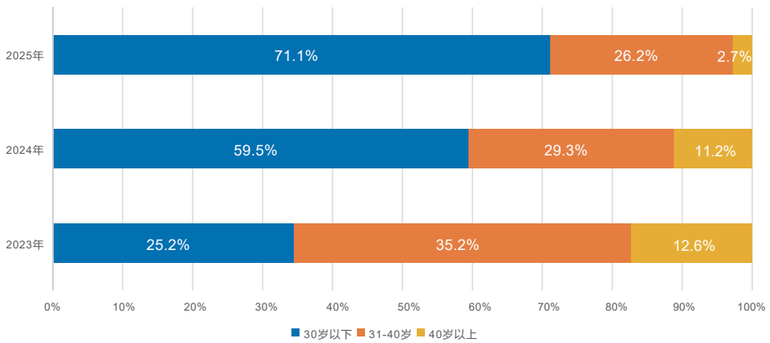


图2 网络安全从业人员年龄结构比例

三、网络安全从业人员教育背景

从受访者的学历来看，网络安全从业人员中本科学历人才占据行业主导地位，比例超过半数。同时，专科及以下学历人才占比30.5%，凸显出应用型人才在行业中的重要地位。硕士以上学历人才占比13.2%，呈现逐年上升态势，与用人单位的学历需求呈正相关。

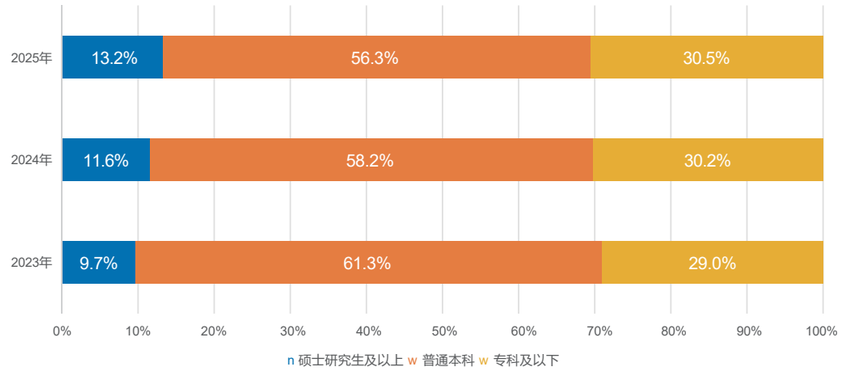


图3 网络安全从业人员最高学历比例

从受访者的专业分布来看，计算机与网络相关专业仍占主导，比例为64.3%；网络信息安全及相关专业占比达到30.8%，呈持续上升态势。随着网络安全作为独立学科体系的逐步成熟，科班出身的人才正在加速进入行业，推动从业结构向专业化方向演进。同时，网络安全作为高度交叉融合的领域，依旧吸引了大量计算机相关专业的跨界人才，体现出该行业强劲的技术包容性与职业吸引力。

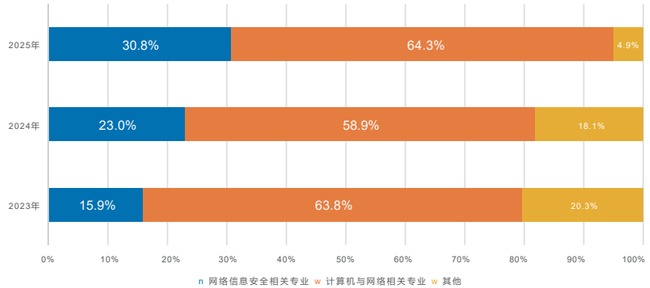


图4 网络安全从业人员专业比例

四、网络安全工作年限分布

从工作年限来看，网络安全从业者中，具有6-10年和2-5年工作经验者占比最多，分别为46.4%和39.4%，构成行业的主要力量。相比2023年以2年以下从业者为主的结构，当前行业人才经验层逐渐扩展，中坚力量不断壮大，结构更成熟。这一变化反映出随着行业发展逐步深入，专业积累与实践能力已成为企业选才的重要标准，也标志着网络安全人才生态正由初期扩张阶段迈向稳步提升与高质量发展阶段。

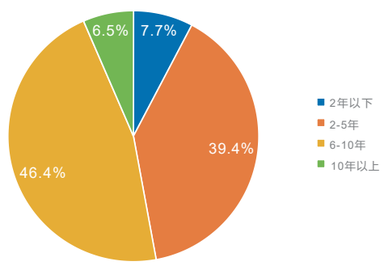


图5 网络安全从业人员工作年限

第二节 | 网络安全产业人才的从业现状

一、城市分布更趋多元，省会城市吸纳能力持续增强

从城市分布来看，网络安全从业人员中，有45.9%集中于新一线城市，39.7%分布在其他省会城市，超一线城市占比则下降至9.3%。相较2023年和2024年以新一线为主要聚集地的趋势，最显著的变化是其他省会城市吸纳网安人才的能力持续增强，接近新一线水平。这一改变不仅与各省加快推进本地网络安全产业园区建设、高校专业布局及人才引育政策密切相关，还反映出网络安全从业者在择业时，正从传统“北上广深情结”转向对职业发展空间、生活成本与产业成长性的综合判断。省会城市凭借日益完善的产业配套和相对友好的发展环境，正在成为人才就业和长期发展的现实选择。

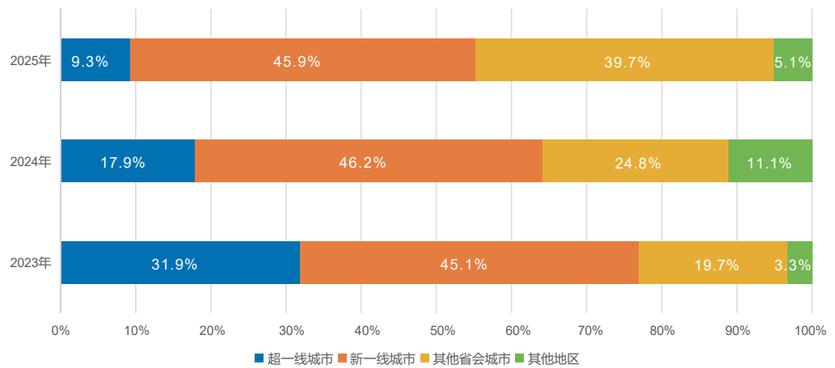


图6 网络安全从业人员城市分布

二、兴趣与前景并重，驱动网络安全人才多元流入

问卷调研数据显示，薪酬待遇是行业人才选择的主要原因， 占比达40.6%；其次是行业前景，和个人兴趣。与之前相比，现实因素成为多数从业者的重要考量，但个人兴趣依然是不可忽视的驱动力，反映出网络安全行业在保障发展机会的同时，也具备持续吸引专业兴趣人才的能力。

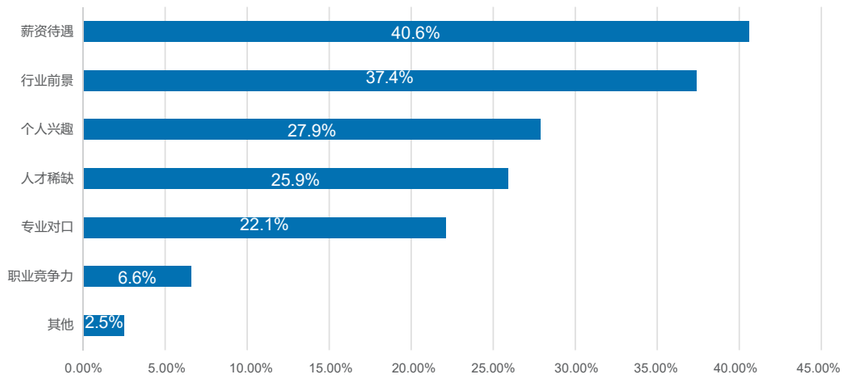


图7 网络安全从业人员择业原因比例

三、薪酬结构趋于集中，中坚人才成为薪资主力

针对于薪酬水平调研显示，有46.2%的受访者税前年薪在20-30万元之间，占比最高；31.9%的受访者税前年薪在10-20万元之间，10.8%的受访者税前年薪在10万元及以下；税前年薪在30-50万元和50万元以上的占比分别为9.9%和1.2%。从薪酬分布整体来看，薪酬结构呈现出中段集中的特征，低薪与高薪群体占比双双缩减，反映出行业在经历初期扩张后，薪资体系正趋于理性与稳定。 一方面，中等收入区间的扩大说明企业更加青睐具备一定经验和实操能力的中坚力量；另一方面，高收入比例的下降也提示行业对高端人才的薪酬投放趋于谨慎。

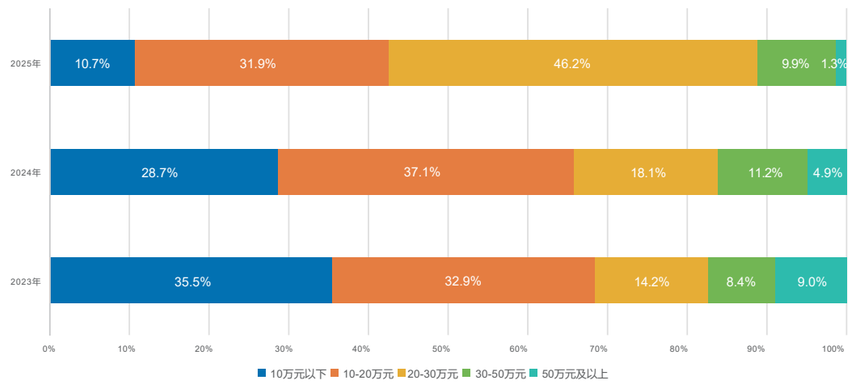


图8 网络安全从业人员税前年薪分布比例

第三节 ｜AI的发展对网络安全从业人员的影响

一、AI嵌入安全场景，工具使用与对抗并重

生成式人工智能与大语言模型的快速发展，正深刻影响网络安全行业生态。一方面，AI在漏洞挖掘、威胁检测、攻击溯源等领域的应用不断深化，显著提升了效率和自动化水平；另一方面，AI生成内容滥用、模型安全性等新型风险也持续显现，要求安全技术人员在机遇与挑战中重新定位自身角色与能力边界。在此背景下，AI技术正以前所未有的速度重塑网络安全从业人员的技能结构与工作方式。

根据对网络安全从业人员必要掌握的技能研究显示，近五成从业者认为最需要掌握的技能是AI工具的使用与调优以及对抗性AI攻防技术，并有超过四成从业人员认为数据分析与算法理解也是必要的。 AI相关技能正从“补充项”转变为岗位的“标配能力”。

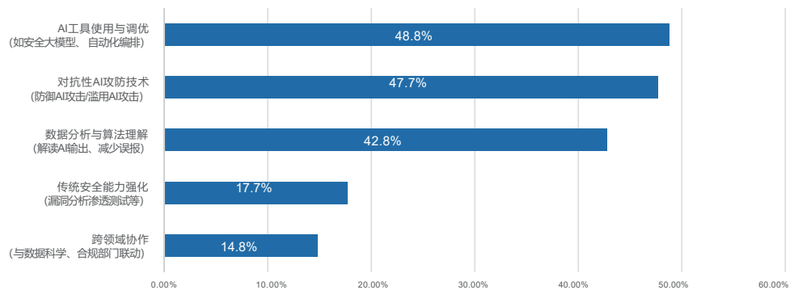


图9 网络安全从业人员认为最需要掌握的前三项AI技能

在实际工作中，AI也在重塑工作重心。56.5%的从业者表示AI技术的发展使其投入更多重心在分析复杂威胁，33.0%从业者表示正从执行层转向策略制定，显示出AI技术不仅提升效率，更推动职责重构与人机协同走向更深层次的融合。

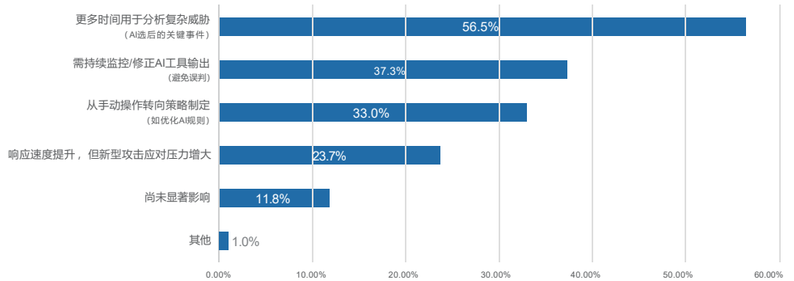


图10 网络安全从业人员工作重心的改变

这一趋势不仅改变了技能需求的排序，也推动了网络安全人才技能方向的革新。随着生成式人工智能和大语言模型的深入应用，从业者在掌握漏洞挖掘、渗透测试等传统技能的基础上，还需具备算法原理、数据治理、模型安全等AI相关能力，以适应更加智能化、复杂化的攻防环境。这种革新不仅是技能组合的拓展，更是职业定位的转变。越来越多的安全人员正从执行层面走向威胁研判与策略制定，承担更高层次的安全设计与风险预判工作。 AI素养、跨领域理解与前瞻性思维，正成为未来网络安全人才的核心竞争力。

二、挑战与焦虑交织，协同意识渐成型

AI技术的快速发展不仅显著提升了网络安全工作的效率，也带来了一系列新的安全挑战与结构性压力。根据调研数据，有37.9%的受访者指出AI在处理大量数据时对系统算力和响应能力提出了更高要求，37.0%的受访者担忧AI可能被用于恶意目的，另有8.6%的受访者认为当前行业在AI复合型人才储备方面存在明显短板。这些反馈表明，网络安全行业在AI深度嵌入的背景下，正经历从能力体系到资源配置的全方位调整，面临适应性重构与风险治理的双重压力。

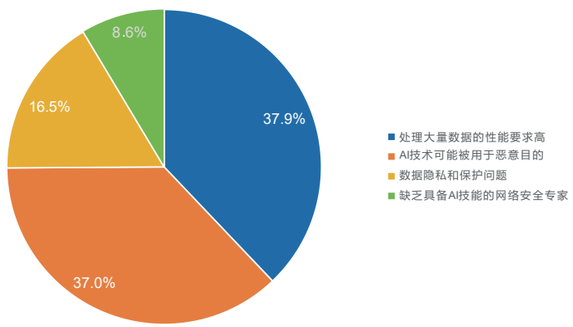


图11 AI技术在网络安全领域中存在的挑战

尽管面临诸多挑战，AI在网络安全领域的探索与应用仍在稳步推进。从调查结果看，42.1%的受访者认为其仍处于局部试验阶段，36.5%认为仅在关键行业有广泛应用；而预测AI将迅速普及并成为行业标准的受访者仅占14.4%，另有7.0%指出其发展受阻于技术和伦理挑战。这说明AI安全要实现全面落地仍需时间与突破，但其未来发展潜力依然广阔。

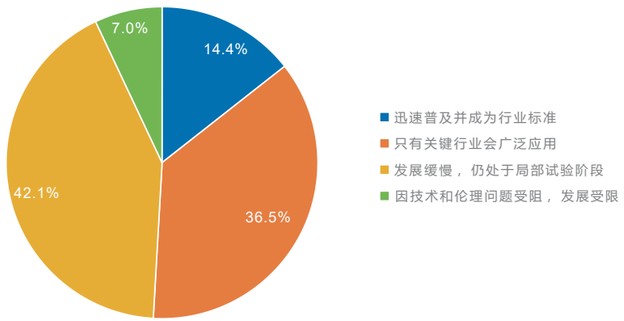


图12 网络安全从业人员预测未来五年AI网络安全领域的应用发展

但在此过程中，AI正在重塑网络安全从业者的技能结构与工作重心。行业实践正从传统的手动操作转向依托大模型与数据智能的高效模式，促使从业者将更多精力投向AI工具使用与调优、对抗性攻防技术及算法结果解读等新技能领域。在人与AI的关系方面，行业普遍认同“人机协作”而非“技术替代”的发展逻辑：39.4%的受访者认为AI应是具备动态协同能力的伙伴，与人类优势互补；27.2%的受访者则倾向将其视为辅助工具，由人类保留核心决策权。

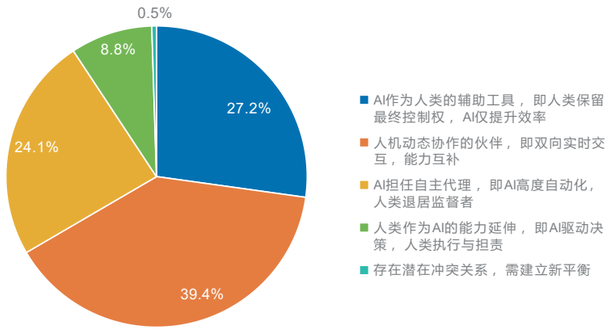


图13 网络安全从业人员认为的人与AI理想关系

总体来看，AI正成为重塑网络安全人才发展路径的重要变量。从能力结构重构到岗位职责转型，再到认知方式的更新，网络安全从业人员正处于“人机融合”趋势加速演进的关键阶段。未来，随着AI伦理治理体系、算法可信机制与安全技术实训体系的不断完善，复合型、协同型人才将在智能化安全体系中发挥更加核心的作用。

三、机遇与变革并行，AI造就新场景

在AI驱动的网络安全体系中，新型岗位正重构防御架构，推动安全由被动响应向主动预警转变。智能体架构师设计的AI Agent可自主执行威胁情报收集、漏洞扫描等任务；数据合成专家利用生成模型构造多样化攻击样本，弥补真实数据稀缺短板，夯实防御基础。

在安全运营层面，AI产品集成工程师将大模型与现有安全设备深度融合，实现跨系统的智能联动响应；模型性能优化师针对实时检测需求持续调优算法，确保在海量流量中高效、精准识别威胁，形成快速闭环的防御机制，显著提升防护效率与稳定性。

在治理环节，模型安全红队专家通过模拟攻击发现潜在漏洞，模型对齐工程师确保决策逻辑符合技术规范与法律标准，AI风险顾问制定全生命周期风险管控方案，使AI安全应用既具高防御能力，又稳固合规与伦理底线，为可持续安全发展奠定保障。

图14 AI驱动的网络安全岗位结构

第三章

网络安全产业人才供需分析

网络安全产业的发展推动了人才招聘需求的增长，也激活了相关领域的就业，带动了人才供给。本章节将以智联招聘平台数据以及问卷调研数据为依据，从网络安全产业人才的供需两个维度出发，盘点人才供需情况。

第一节 | 网络安全产业人才需求

一、计算机软件行业招聘网络安全职位数最多

调研数据显示，2025年，计算机软件行业招聘职位数占比达到了10.0%，紧随其后的仍是IT服务和互联网，招聘职位数占比分别为9.5%和7.6%，值得一提的是，这三个行业自2023年以来，招聘网络安全职位数已连续三年排名前三。计算机软件、IT服务和互联网行业作为数字化经济的核心载体，对网络安全有着最直接和迫切的需求。此外， 网络/信息安全、通信/网络设备、咨询服务、企业服务等行业对网络安全人才有较大需求。

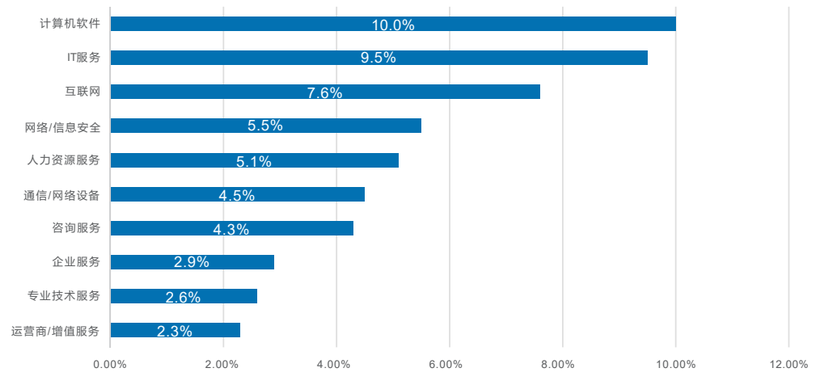


图15 2025年招聘网络安全岗位数占比TOP10行业

二、一线及新一线城市需求占主导，北京连续三年居于首位

据智联招聘平台数据显示，今年网络安全岗位招聘职位数前十的城市均为一线和新一线城市，这些城市因其核心的经济地位、密集的关键基础设施及高度发达的数字化产业，成为网络安全产业人才需求的“风暴眼”。其中，北京市招聘网络安全岗位数量占比为14.4%，排在全国之首，自2023年以来，北京市已连续三年居于首位，北京作为国家政治中心、核心机构总部聚集地，集中了全国最密集的关键信息基础设施与最高级别的网络安全防护需求。紧随其后的是深圳和上海，各占6.2%和5.3%，凸显了经济与技术中心对安全人才的高度吸纳能力。

值得关注的是，根据智联招聘的数据显示，2025年郑州市招聘网络安全岗位数开始上升，跻身新的TOP10行列，源于郑州市近年来不断出台相关政策，加大金融支持，推动网安产业发展。

排名	2025年	占比	2024年	占比	2023年	占比
1	北京	14.4%	北京	16.6%	北京	18.0%
2	深圳	6.2%	上海	5.6%	上海	7.7%
3	上海	5.3%	深圳	5.2%	深圳	6.2%
4	成都	5.0%	成都	4.6%	成都	5.2%
5	广州	4.9%	广州	4.0%	广州	4.3%
6	西安	3.2%	武汉	3.1%	杭州	3.3%
7	武汉	3.1%	西安	3.0%	南京	3.0%
8	南京	2.8%	南京	3.0%	武汉	2.8%
9	郑州	2.8%	杭州	2.7%	济南	2.8%
10	杭州	2.7%	济南	2.7%	西安	2.7%

表1 近三年招聘网络安全岗位数占比TOP10城市

三、学历需求以本科为主，硕博学历需求占比逐年上升

从调研学历要求来看，企业招聘网络安全人才主要以本科学历为主，需求占比过半，达到了55.5%，可见企业普遍将本科学历作为网络安全人才的基础门槛，这与技术复杂度高、需系统化知识储备的岗位特性高度契合。

此外，尤其值得关注的是，硕博学历需求占比呈逐年上升趋势，今年硕博学历占比达到了10.3%，这是行业对抗性升级和技术裂变的必然结果。这些能力深度依赖系统化的科研训练和跨学科知识融合，硕博教育提供的系统性思维及技术预见性，正成为破解高级威胁、抢占技术制高点的核心筹码，推动学历门槛持续上移。

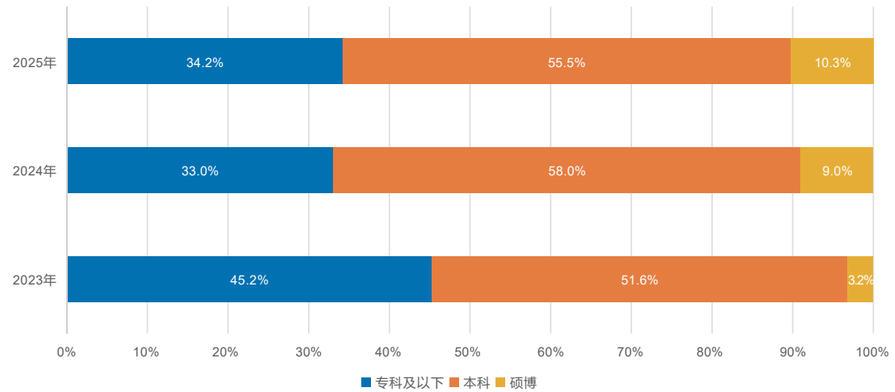


图16 2023—2025年网络安全岗位学历需求分布

四、要求3-5年工作经验的招聘职位数占比最高

网络安全岗位的工作年限要求往往与岗位的性质、工作技能紧密相关，招聘单位对网络安全人才的工作经验也越来越看重。很多企业在招聘时会优先考虑那些具有实际项目经验、能够迅速适应工作环境并解决问题的应聘者。据智联招聘平台数据显示，2025年网络安全岗位要求3-5年工作经验的职位数占比最高，达到了28.2%，凸显了行业对实战能力的重视。3-5年经验者是网络安全攻防战力的“黄金期”——既能独立迎战中高危威胁，又是企业人力成本与效能的最优平衡点，构成防御体系的中坚力量。

值得关注的是，企业招聘网络安全人才呈现越来越年轻化的趋势，2025年，网络安全岗位要求1-3年工作经验的职位数占比达到27.4%，远远高于5-10年及10年以上工作经验占比数，这与网络安全岗位需要更快的响应速度及更持久的“盯梢”能力有关。

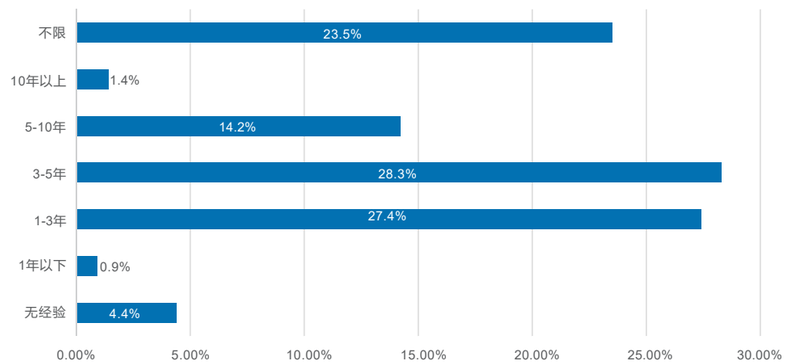


图17 2025年网络安全岗位工作经验要求分布

五、网络安全运营岗位招聘数连续三年占比最高，达26.8%

从工作类别来看，网络安全运营的招聘职位数占比最高，达到了26.8%，这已是自2023年以来连续三年招聘数占比第一，网络安全运营岗位是将安全策略、技术投入转化为实际防护效果的核心枢纽，是应对当前动态威胁环境、满足合规要求、保障业务连续性的不可或缺且持续运转的关键环节。其次是网络安全建设、网络安全管理、数据安全类职业，分别占比18.8%、16.0%和11.0%。从典型职位上来看，安全运维工程师和网络安全开发师的招聘职位数占比最高，分别达到了13.2%和10.6%，凸显企业首要目标是建立稳定的安全防御体系，技术落地仍是当前重心。

一级职能	二级职能	典型职位	招聘职位数占比
网络安全运营 (26.8%)	网络安全运维	安全运维工程师	13.2%
	网络安全集成	集成方案解决师	5.3%
	网络安全应急响应	网络安全应急响应工程师	8.3%
网络安全建设 (18.8%)	网络安全开发	网络安全开发师	10.6%
	网络安全架构	安全系统架构师	7.2%
	个人信息保护	/（无典型职位）	0.8%
	供应链安全	供应链安全管理	0.2%
网络安全管理 (16.0%)	网络安全测试	安全测试工程师	6.7%
	网络安全合规	安全合规工程师	5.1%
	网络安全咨询	安全咨询工程师	2.3%
	网络安全规划	安全规划师	1.2%
	网络安全防护	安全等级保护测评师	0.8%
数据安全 (11.0%)	数据安全体系	数据安全体系工程师	3.0%
	数据安全管理	数据管理师	3.3%
	数据安全评估	数据安全评估师	2.5%
	数据安全保护	数据安全保护工程师	2.0%
	电子数据取证	电子数据取证师	0.2%
网络安全审计和评估 (9.7%)	网络安全分析	渗透测试/漏洞挖掘工程师	7.4%
	网络安全评估	网络安全评估师	2.0%
	网络安全认证	安全认证工程师	0.3%

表2 网络安全岗位分类及招聘占比统计表

六、实战型网络安全人才更受招聘单位青睐

根据调研数据显示，2025年用人单位对网络安全求职者的工作经验和实战能力更加看重，分别占比为76.2%和72.2%。面对日益严峻的网络安全威胁和不断攀升的安全事件成本，企业招聘偏好已破除传统的“唯学历论”。具备真实攻防对抗经验、熟练安全工具操作、能快速响应处置安全事件的“实战型”网络安全人才，正成为招聘市场上的稀缺资源。这一趋势深刻影响着教育培养模式和个人职业发展路径，推动着网络安全人才生态向“能力实战化”加速演进。

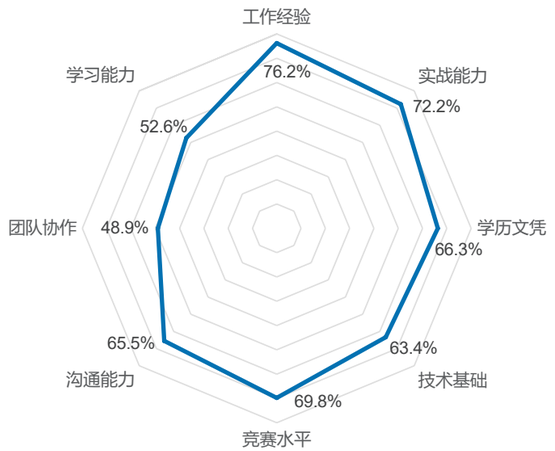


图18 2025年用人单位对网络安全人才能力要求

第二节 ｜ 网络安全产业人才供给

一、高校网络安全专业开设情况

按照教育部最新发布的《全国高等学校名单》[20]显示，截至2025年6月20日，全国高等学校共计3167所，其中：普通高等学校共计2919所，含本科学校1365所，高职（专科）学校1554所，其中有87所职业本科。根据相关数据显示，全国共有792所普通高等学校开设网络安全相关专业[21]，其中本科院校305所，职业本科院校31所，高职院校456所，占全国普通高等学校总数的27.1%，较去年增长5.3%，可见，网络安全专业教育在我国高等教育体系中逐渐占据重要位置。从省份分布来看，开设网络安全相关专业院校最多的TOP3省份分别是河南、山东、四川，这与这些省份本身就是教育大省、人口大省，高校数量众多有关。

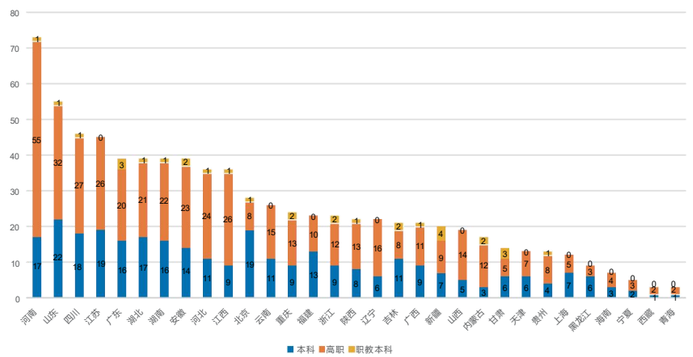


图19 各省开设网络安全相关专业院校统计

从各省份不同办学层次院校开设网络安全相关专业情况看，山东、四川、江苏、北京、河南五省市的本科院校开设网络安全相关专业较多；河南、山东、江西、四川、江苏五省的高职院校开设网络安全相关专业较多。这些信息对企业开展校园招聘大有裨益，能助力人力资源部门更精准地锁定不同能力水平的网络安全人才储备区域，进而让招聘策略得到优化。

网络安全是一门融合性极强的新兴学科，知识更新快、技术迭代快，具有明显的后伴生特征和跨学科属性，导致人才培养周期长、路径复杂、难度高。其战略意义日益凸显，国家层面高度重视，近期正式成立中国人民解放军网络空间部队亦是国家强化网络空间防御能力的重大战略举措。也正因如此，网络安全专业在本科院校中开设较早，奠定了重要的学科基础。与此同时，伴随国家深化现代职业教育体系改革、大力倡导“增强职业技术教育适应性”，高等职业教育领域对网络安全人才培养的重视程度和扶持力度持续加强。在此政策导向和产业发展双重驱动下，开设网络安全专业的高职高专院校数量更是增长快速，目前总数已经明显超越本科类院校。职业教育凭借其紧密对接产业需求、培养应用型技能人才的独特优势，在国家网络安全战略布局和人才梯队建设中扮演着愈发关键的角色，正日渐成为支撑国家网络安全事业的重要力量。

[20]本名单未包含港澳台地区高等学校。

[21]网络安全相关专业统计口径为：

本科：信息安全专业、网络空间安全专业、网络安全与执法专业

职业本科及高职：信息安全技术应用专业、网络安全与执法专业、司法信息安全专业

二、在校生基本特征

1．性别比例：男女比例仍保持约7:3

最新调研显示，网络安全专业在校生男女性别比例约为72:28。相较于前几年，整体格局保持稳定，男性学生在报考该专业群体中的占比呈现持续主导态势。

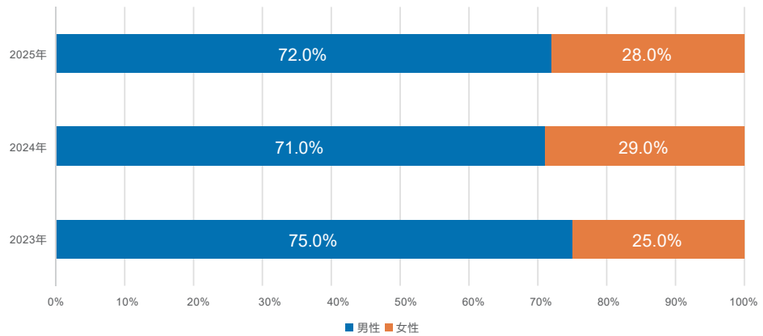


图20 近3年在校生性别比例分布

2．学历分布：本科仍占主导，高职持续增长

从在校生的学历结构来看，当前网络安全专业在校生以本科学历为主，占比达53.5%；高职高专学历占比为36.1%，位列第二，且较去年显著增长了8%，这一显著增长主要得益于近年来众多高职院校积极增设网络安全专业以满足市场需求；而中职/技师学历和研究生及以上学历占比较小，分别为4.3%和6.2%。

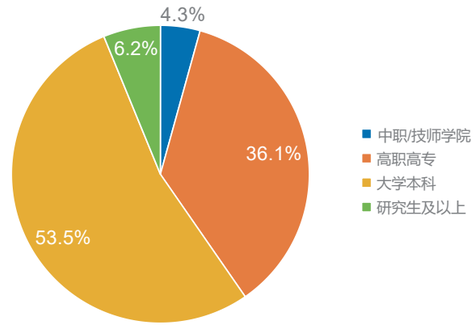


图21 网络安全专业在校生学历分布

结合近3年的学历分布数据可以发现，网络安全专业学生在学历分布结构上较为相似，按人数比例从大到小依次为本科 > 高职高专 > 研究生 > 中职/技师（部分本科院校设置了网络安全相关的研究生培养方向，并不纳入统计）。可以看到高等职业教育近年来越发注重网络安全人才的培养，与本科院校一同成为培育网络安全人才的主力军。

3．专业报考原因：就业前景仍是网络安全专业报考的首选理由

在选择网络安全专业的主要理由中，就业前景以40%的占比成为首要因素，直接指向未来工作机会的保障；同时，薪资待遇（19.4%）的重要性进一步提升，成为学生选择的第二大原因，关乎就业后的经济回报水平；而亲友建议（18.6%）往往基于对就业稳定性和发展潜力的判断提供决策支持，其占比也呈上升趋势。可见，在当前整体就业形势严峻的背景下，“能否找到一份好工作”已成为学生及家长的核心关切，这促使就业前景、薪资待遇及亲友建议共同构成了主要的择业考量。因此，院校应着力凸显专业方向与个人职业成长路径、市场人才需求之间的紧密结合，作为专业设置和招生宣传的核心关注点。

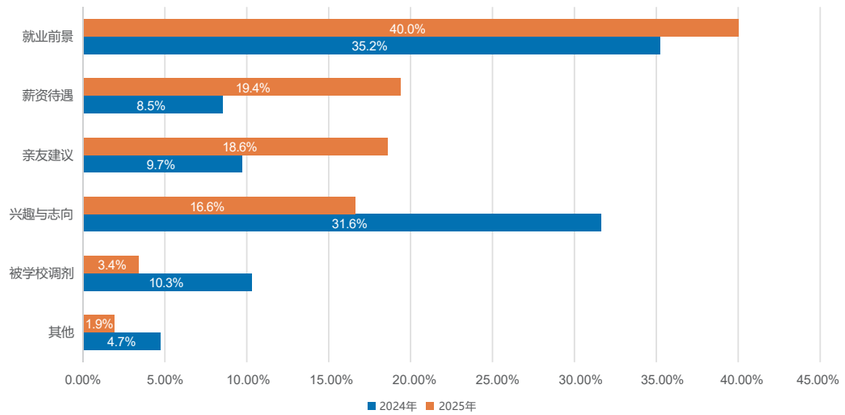


图22 近两年在校生选择报考网络安全专业的主要理由

三、实践教学情况

1．学生拥有多重学习途径选择

调研显示，在校生学习网络安全知识的主要途径中，校内课堂学习以65.3%的占比位居首位，在线课程学习普及率也较高；此外，专业书籍、技术论坛、安全竞赛、校内协会、校外培训、企业兼职及实践项目等多种方式也被广泛采用。由此可见，网络安全专业在校生正通过多种途径主动学习，不仅限于传统课堂，更拓展至利用在线资源、投身实践项目以及参与社区互动等多样化形式。

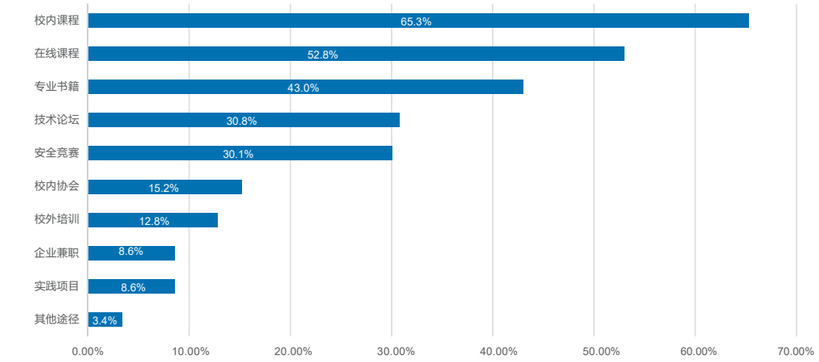


图23 在校生学习或了解网络安全知识的主要途径

2．超八成在校生对网络安全专业教学表示满意

为了更好地了解网络安全专业的教育质量和教学效果，重点考察了课程设置、师资力量和实训资源三个方面，从调研结果来看，学生对上述三者的满意度从高到低分别为：师资水平满意度＞课程及教材设置满意度＞实训资源满意度，这一结果也与教材和实训资源的建设具有一定滞后性有关。

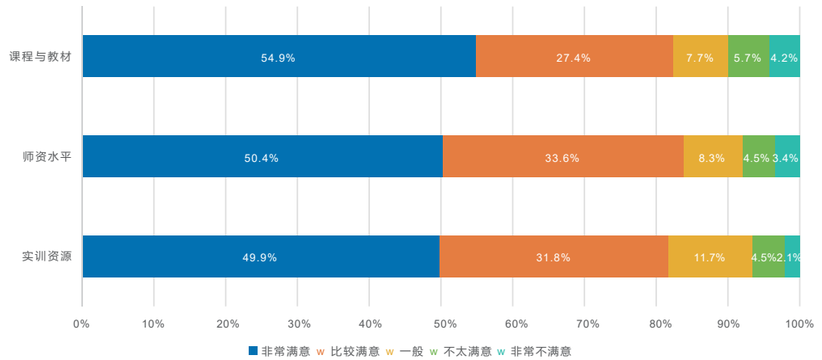


图24 在校生对专业教学满意度

细分来看，84%的受访网络安全专业在校生对当前师资水平表示满意（含50.4%非常满意和33.6%比较满意），尽管占比仍高，但相较前两年（2023年满意占比86.8%，2024年满意占比87%）已出现小幅下降。这一变化主要源于学生对师资实战经验的要求不断提高，而当前教学体系在对接快速发展的行业需求和满足就业导向的学习预期方面存在一定滞后性。

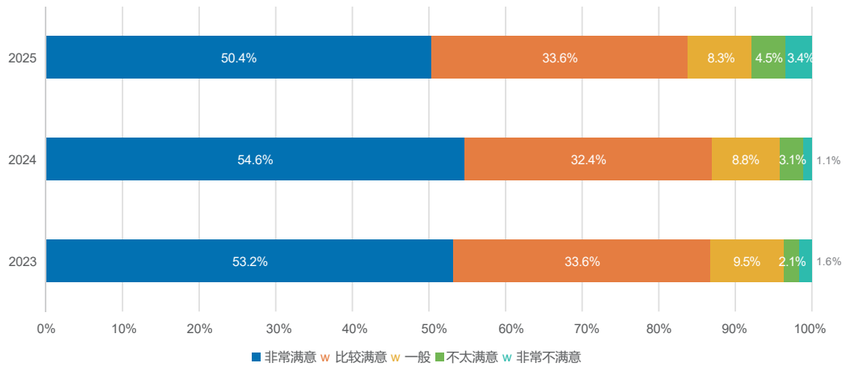


图25 近三年在校生对师资水平的满意程度

在课程及教材设置方面，82.3%的网络安全专业在校生表示满意（含54.9%非常满意和27.4%比较满意），虽然满意度基数较高，但较前两年（2023年满意占比89%，2024年满意占比85.7%）略有回落。这种变化反映出学生对课程内容的前沿性、实践应用性以及与就业市场技能需求的契合度提出了更高要求，而当前课程体系的更新速度在面对网络安全领域的快速迭代和严峻就业形势时，存在一定的滞后与不足。

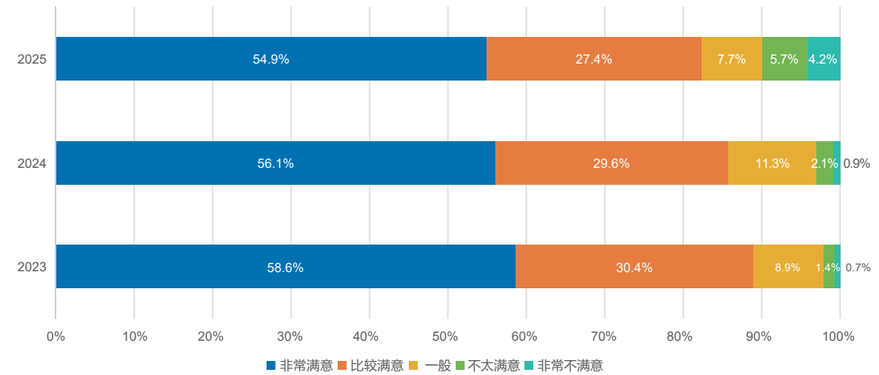


图26 近三年在校生对课程及教材的满意程度

从实训资源来看，在校生对网络安全专业实训资源的总体满意度为81.7%（含49.9%非常满意和31.8%比较满意），尽管整体认可度较高，但较前两年（2023年满意占比83.7%，2024年满意占比86%）略有下滑，且存在近7%的学生明确表示不满意。这一变化反映出，随着网络安全技术快速演进，学生对实训环境的要求正从“有资源可用”向“资源优质、实用”升级。

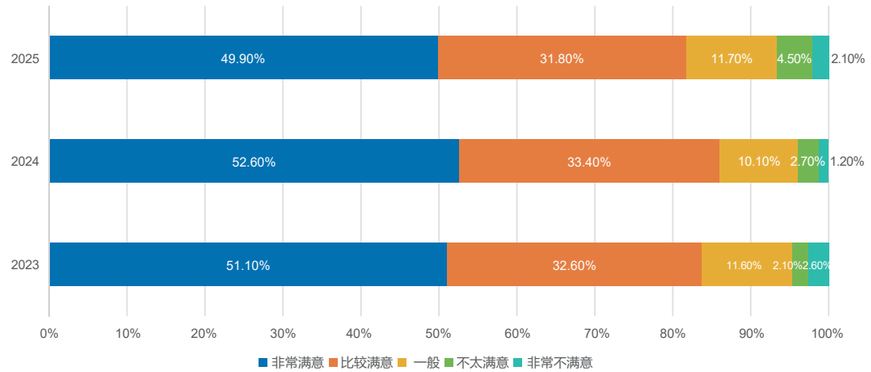


图27 近三年在校生对实训资源的满意程度

虽然受访学生对课程设置、师资力量和实训资源的整体满意度依旧较高，但相比往年有所回落。这一变化反映了学生对实践技能提升的迫切需求，而这种需求的上升，或可归因于近年来就业环境的变化：企业对具备较强实践能力和项目经验的毕业生青睐有加。

3．超九成学校已建设网络安全实训室或实训平台，与去年持平

据受访学生反馈，学生调研显示：91.3%的院校已建成网络安全实训室（或实训平台），其中52.4%提供充足实训项目，38.9%实训项目覆盖有限；另有6%的院校虽未建设专用实训室，但通过其他形式提供实践项目；仅2.8%的院校尚未建立任何实训条件。这表明设立网络安全专业的院校中，超九成搭建了实践教学平台，实训项目整体覆盖率高达97.2%，较去年持平。

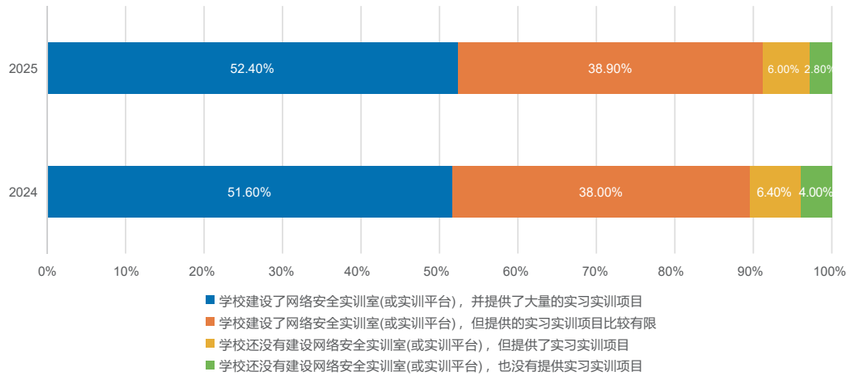


图28 院校网络安全实训室（或实训平台）建设情况

4．网络安全专业实践实操课程占比较为合理

调研发现，网络安全专业实践实操课程占专业课（专业课特指专业平台课、专业核心与选修课）比重在1/3至1/2之间的院校占比最大，表明多数院校实践教学比例设置相对合理；然而，实践课程比重少于1/3的院校仍占28.7%，高于1/2的仅占11.5%。为更有效地培育产业急需的实战型、应用型网络安全人才，院校有必要适度增加实践实操课程的设置比重。

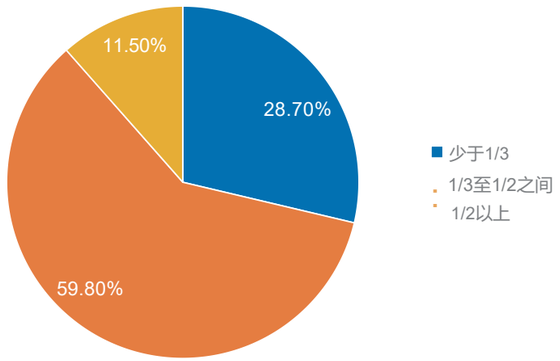


图29 实践或实操课程占专业课程比重

5．超六成网络安全课程依托企业讲师强化产业连接

据受访学生反馈，67.8%的网络安全专业课程教学有企业讲师参与，而32.2%则无企业讲师介入，与去年持平。这表明，引入具有行业实践经验的企业讲师参与授课，已成为大部分院校提升教学与产业对接度的关键举措。

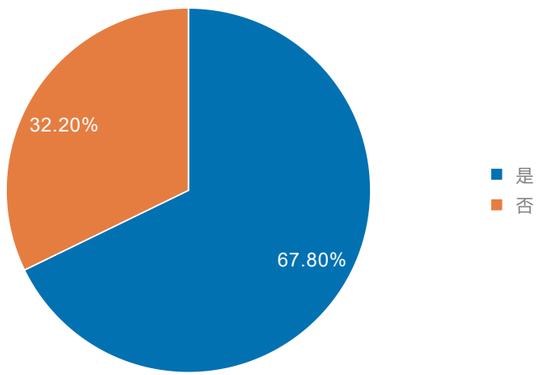


图30 企业讲师参与教学授课比重

6．在校生愈发注重网安竞赛，提升实战能力占主导因素

调研数据显示，当前61.2%的受访学生在校期间已参与网络安全相关竞赛，32.9%的学生虽有意向但尚未行动，参与比例较去年显著提升，表明了竞赛在学生群体中的普及度与参与热情持续攀升。这一趋势的深层动因在于：用人单位普遍将竞赛经历作为评估求职者实战能力和问题解决潜力的关键指标，成为毕业生提升就业竞争力的重要抓手；竞赛为学生提供了超越课堂理论的实战平台，弥合了理论学习与岗位需求的实践差距。竞赛参与度的快速提升，既体现了学生对行业用人导向的精准响应，也凸显了其作为连接高校人才培养与企业实战需求的关键纽带所展现出的强劲发展动能。

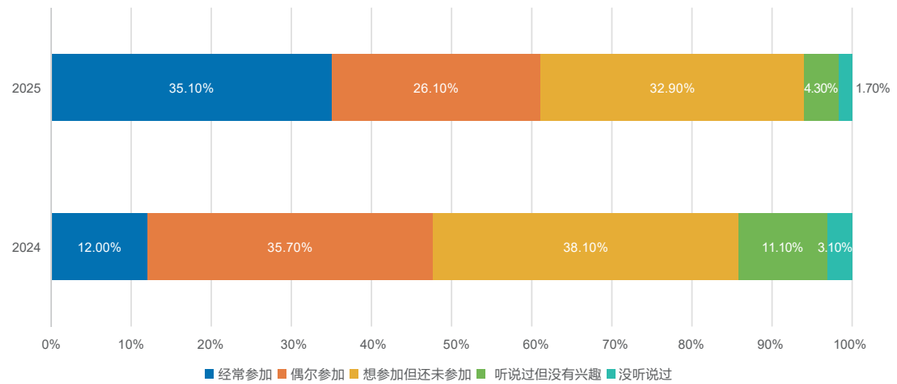


图31 在校期间是否有参与过网络安全相关的竞赛

网络安全竞赛的参与动机呈现多元化特征，从在校生参赛原因来看，出于学习、提升实战和竞赛荣誉占比较大，分别为45.6%和43.6%。其次是由于个人兴趣，占比38.1%。此外，也有部分学生因学校/老师要求、结交朋友、奖金等原因而参与。总体而言，提升自身实战水平是学生参与网络安全竞赛的核心驱动力，学生通过竞赛强化实战能力，本质上是应对就业市场要求、增强职业发展潜力的前瞻性策略。

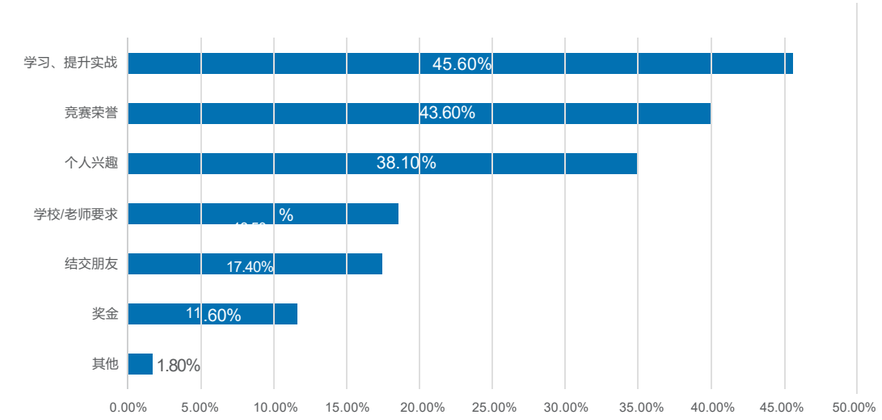


图32 在校学生参赛原因

7．网络安全专业学生对AI在网络安全领域的应用了解持续提升

网络安全专业学生对AI在网络安全领域应用的了解度显著提升，这反映出院校教学与行业对该技术的高度重视，也反映出社会科普程度加深所带动的学生认知意识普遍提高。调查显示，高达71.1%的学生表示非常或比较了解其应用，了解程度一般和较低者占比不足三成。在AI安全成为社会风向与技术焦点的背景下，当前成效值得肯定，但仍需持续深化前沿技术教育与实践，确保学生认知与产业变革同步升级。

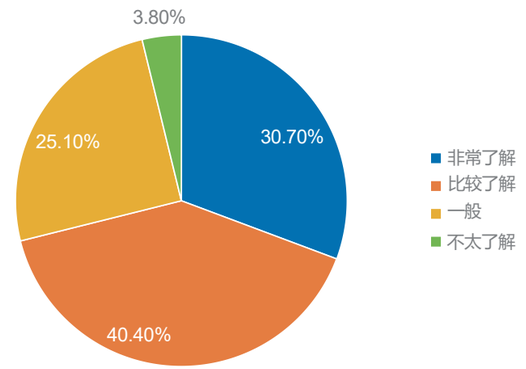


图33 在校生了解AI在网络安全领域的应用的程度

8．网络安全专业AI课程加速渗透，开设率跃升至65.9%

根据调研数据显示，在已开设网络安全专业的高校中，65.9%的院校已将人工智能相关课程纳入教学体系，这一比例较去年实现显著提升。随着人工智能技术的突破性发展，网络安全领域对兼具AI技术与安全防护能力的复合型人才需求急剧增长。基于行业发展需求与人才培养规律，尽管AI相关课程开设逐年增加，但与高校教师访谈过程发现人工智能在网络安全领域的实践应用类占比较低，建议尚未开设相关课程的高校，将人工智能核心课程纳入网络安全专业必修体系，以精准对接数字时代网络安全防护能力升级要求。

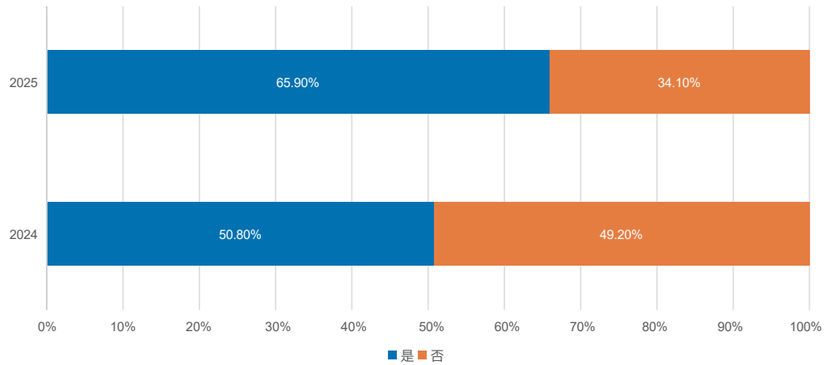


图34 近2年学校开设AI相关课程情况

9．近九成在校生已成AI辅助学习的“常客”

随着人工智能技术加速迭代与AI大模型的全面普及， AI工具正以“学习助手”的身份深度融入教育场景，成为在校生提升效率的重要支撑。最新调研数据显示，87.8%的在校生已主动借助AI技术辅助学习，仅12.2%尚未尝试，且这一使用比例较去年呈现稳步上升态势。这表明，利用AI工具辅助学习在大学生群体中已成为普遍现象。

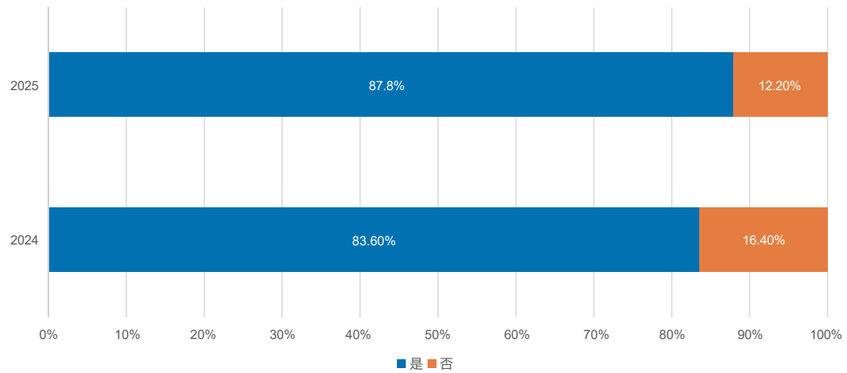


图35 近2年在校生使用过AI技术来提升学习效率情况

四、在校生实习情况

1．超六成学生表示学校有安排实习

63.8%的受访学生表示他们所在的学校安排了实习机会，其中高职高专类院校安排实习的比例最高，达74.3%，其次是本科院校，达到70.1%。由此可以看出当前高校对网络安全类专业学生实习实训的重视程度颇高。实习作为能让学生将理论知识与实际工作相融合的重要途径，已成为众多大学生提升自身竞争力、为未来职业发展筑牢基础的关键环节。

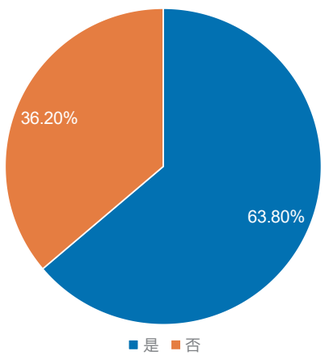


图36 学校安排实习的在校生占比

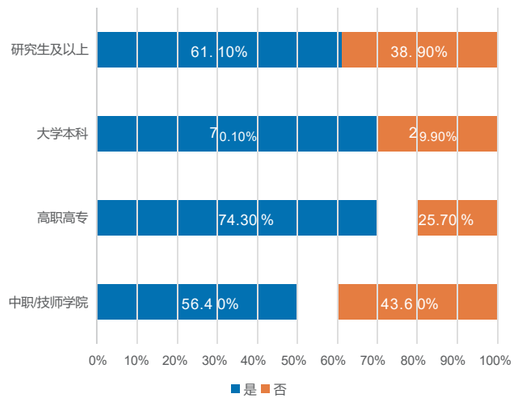


图37 不同学历层次院校实习安排情况

2．实习内容以网络安全服务和运维为主

根据调研数据显示，在参加实习的学生群体中，超过半数的实习机会集中在网络安全服务（包括攻防演练和渗透测试）和网络安全运维（告警监控、现场值守等）。据访谈反馈，因行业内从事产品配置部署的网络安全技术服务和具备实战技能的安全服务的人员较多，属于人员体量较大的部门，学校统一安排实习情况下，从事这两类相关技术岗位也顺理成章。

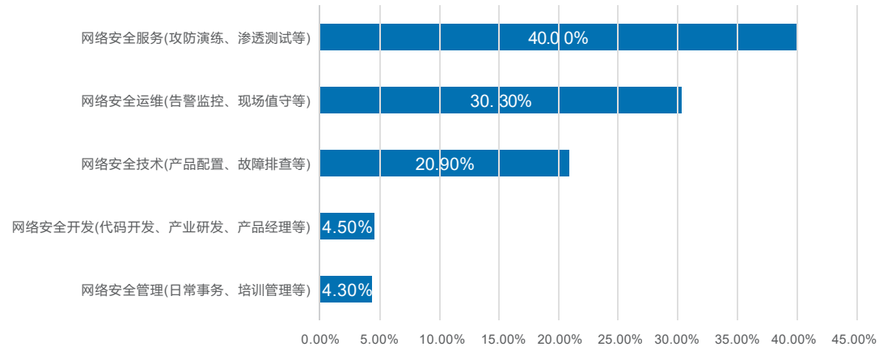


图38 实习主要工作内容

3．实习学生的实习时长主要在3个月

从网络安全类专业在校生企业实习时长分布来看，超半数（54.5%）学生选择3个月左右的实习时长，占比最高；近三成（28.3%）学生倾向半年左右实习；选择1个月左右实习的学生占10.7%；而选择一年左右实习的学生占比最少，为6.5%。整体呈现出短中期实习更受青睐，长期实习选择较少的特点，反映出网络安全专业学生实习安排或受课程进度、求职规划等因素影响，多数倾向在一学期内（3-6个月）完成实习，以平衡学业与实践积累。

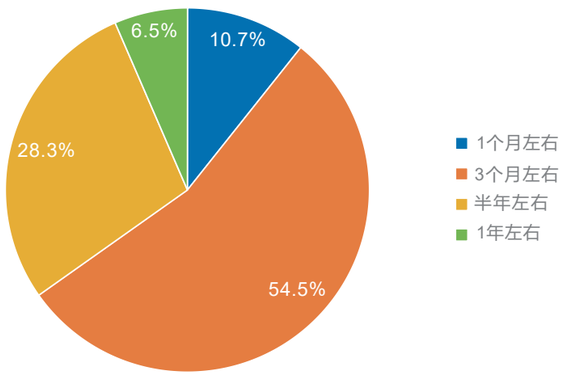


图39 实习时长分布

4．实习薪资主要集中在3000元/月左右

从网络安全类专业在校生实习工资数据来看，实习薪资主要集中在3000元左右，3000-5000元/月的占比最高，为43.2%；3000元/月以下的占42.5%，两者合计超八成，构成实习薪资的主体区间。整体反映出网络安全专业在校生实习工资水平差异较大，多数集中在中低档位，高薪资实习岗位占比较小，也侧面体现出实习薪资与学生技能水平、企业需求及实习岗位性质等因素关联。

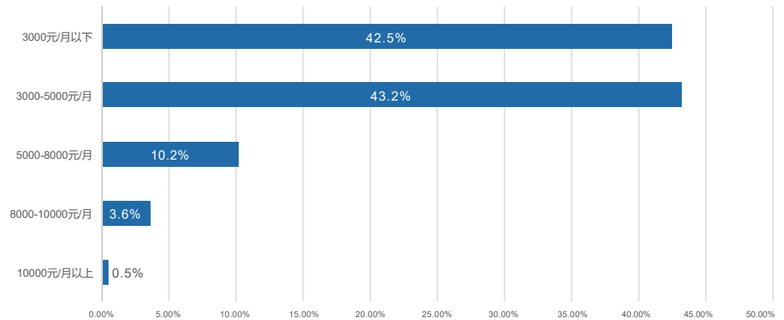


图40 实习工资情况

5．近五成实习学生认为实习对自身技能提升帮助最大

在被问及企业实习的最大收获时，超五成学生认为对自身技能提升帮助最大；其次是对职场发展的提升，第三则是认为对自身技术提升有帮助。与2024年相比，技术提升虽占比最高但略有下降；职场发展、沟通协作、组织管理占比相较2024年略有上升，反映出学生对实习在这些维度价值的认可在提升。沟通协作占比的上升，体现出实习对学生人际交往与团队协作能力的显著促进。实习中，学生需融入工作团队，与同事、上级及客户互动，在分工协作、跨部门协调中，锻炼出倾听、表达与换位思考能力，逐渐掌握精准沟通的技巧，为适应职场团队环境打下基础。通过实习，学生得以零距离体验职场文化，深入认识企业运作机制、团队合作模式及行业前沿动态，这些实践经验将成为他们未来职业生涯的重要基石。

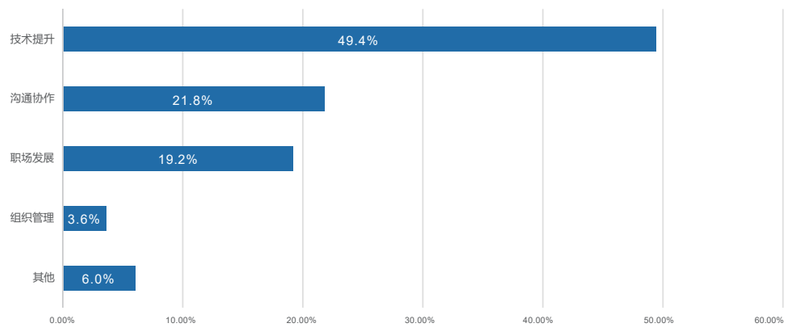


图41 实习收获情况

6．近六成学生反馈实习岗位的知识技能要求与在校专业学习内容相匹配

有过实习经历的学生反馈显示，认为实习岗位知识技能要求与在校期间专业学习内容相匹配的学生占比为59.6%（包括十分匹配22.3%，较匹配37.3%），这相较于2024年的56.8%，有小幅提升。这表明院校的专业课程设置与行业企业的岗位要求衔接得越来越紧密，专业建设取得了显著成效。

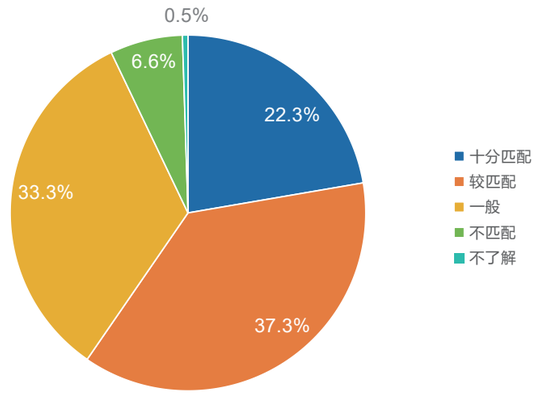


图42 实习知识技能需求匹配情况

五、在校生就业规划

1．超六成在校生对就业持乐观态度，但与往年相比有所下降

在未来就业趋势的展望中，网络安全专业在校生展现出了较为积极的整体态势，超过六成的学生对行业就业前景抱有乐观态度，包括20.5%的学生表示“非常乐观”，39.8%的学生认为“比较乐观”。这一数据分布直观地反映出，大部分在校生对网络安全领域的就业潜力仍充满信心，这种信心源于数字时代对网络安全的刚性需求，毕竟从政府机构到企业组织，网络安全已成为数字社会运转的“刚需防线”，行业人才缺口长期存在。

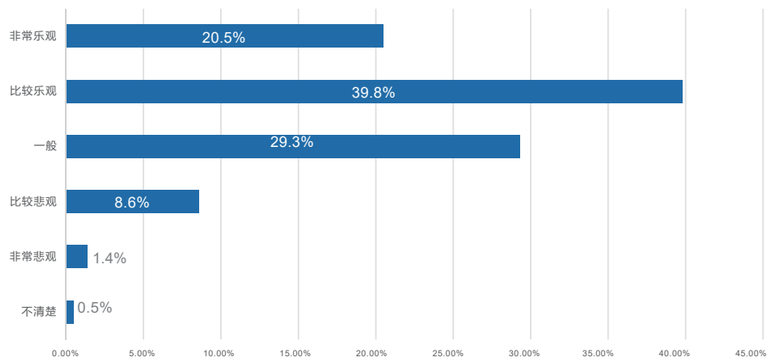


图43 在校生对未来就业趋势的态度

然而，与过去两年相比，乐观态度的比例整体下滑，悲观情绪持续抬头，持悲观态度的学生占10%（包括8.6%的比较悲观与1.4%的非常悲观），较去年上涨2.3%。这与就业市场的挑战相关。 一方面，行业门槛快速提升，企业对人才的要求从单一技术能力转向复合素养，让在校生有能力匹配焦虑；另一方面，经济环境不确定性使得部分企业收缩招聘，头部企业竞争加剧，这直接削弱了学生的乐观预期。

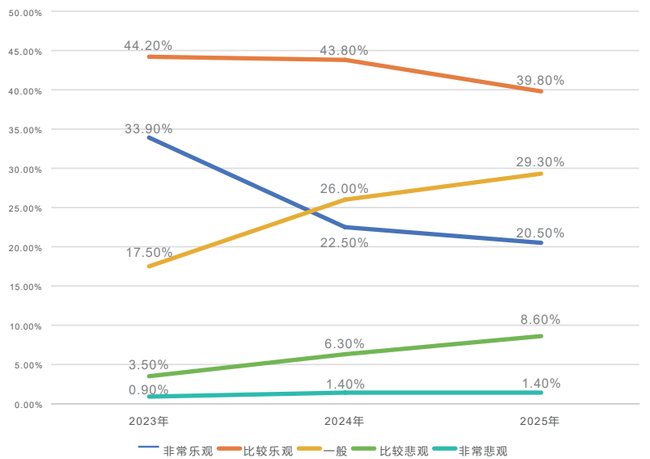


图44 近3年在校生对就业态度变化趋势

2．新一线城市蝉联三年成为网安毕业生首选

在就业城市的选择方面，51.1%的受访学生倾向于将杭州、成都、武汉等新兴一线城市作为首选；其次是北上广深等产业基础雄厚的超一线城市。自2022年以来，新一线城市已连续四年成为网络安全专业毕业生首选就业地点，且呈现逐年递增的趋势，这与这些城市近年来网络安全产业布局成效显现、产业发展势头良好、就业机会增多有关。

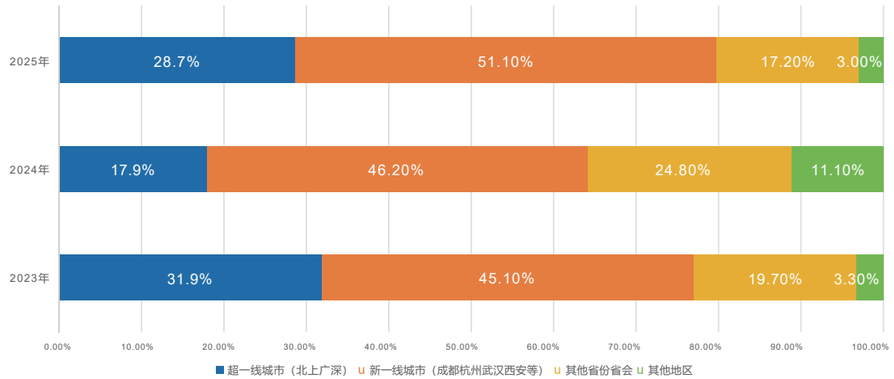


图45 近3年在校生毕业后优先选择的城市情况

3．网安毕业生就业意向明确，央国企事业单位持续走热

在就业行业或企业选择上，调研结果表明，超四成（43.1%）网络安全专业在校生倾向入职央国企事业单位等网络安全部门，央国企事业单位持续走热，是因其工作稳定性高，且在数字安全建设中责任重、需求大，能提供规范职业环境与发展路径。

选择直接进入网络安全企业的学生占比为19.7%，与2024年相比有所下降；而选择互联网及IT企业网络安全部门的学生占比上升至31.6%，这可能是因为互联网及IT企业业务迭代快，对网络安全依赖强，岗位多、薪资与发展空间有吸引力。不同选择反映出学生对职业稳定性、行业活力、专业深耕的多元诉求。整体来看，当前网络安全专业的学生在就业选择上，更加考虑职业稳定性以及与自己所学内容的匹配度。

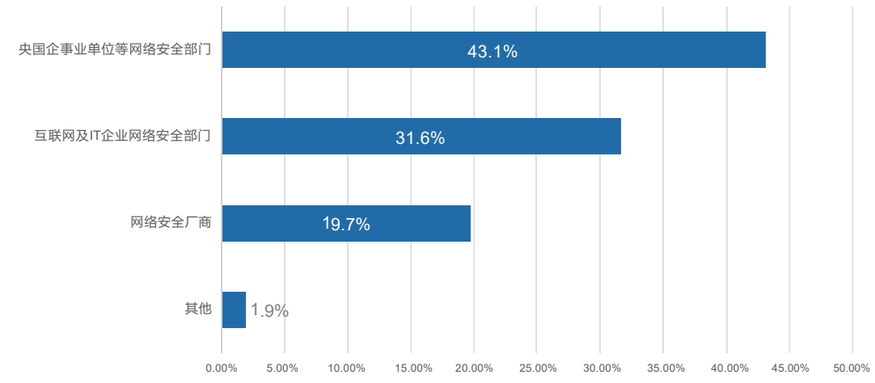


图46 在校生意向就业行业/企业

4．超7成网安学生意向未来从事岗位为核心安全技术岗位

从网络安全类专业在校生职业意向数据来看，超七成（71.8%）学生期望进入核心安全技术岗位，像渗透测试、安全运维、漏洞研究工程师等，反映出网络安全技术赛道对学生吸引力强劲，专业教育培养出的技术钻研倾向，让学生聚焦核心技术攻坚，契合行业对深度技术人才的需求。近两成（17.6%）学生考虑企业非技术岗，说明部分学生结合自身综合能力与职业规划，选择在网络安全企业生态里，从行政、人力、市场等维度助力，体现职业选择的多元适配。整体而言，学生职业意向与行业技术刚需高度契合，但在复合岗、体制内及创业方向的探索度有待拓展，院校可通过跨领域实践、职业规划引导，助力学生拓宽职业视野，适配多元行业需求。

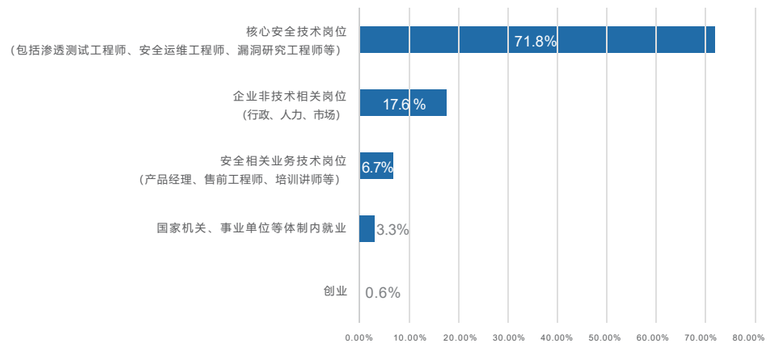


图48 学生未来职业意向

5．薪酬待遇是在校择业时最看重的因素

调查数据显示，薪酬待遇以45.5%的占比成为在校生就业规划的首要考量因素。其次是岗位内容（15.2%），反映出学生对专业对口和职业发展的重视。其他影响因素依次为：行业领域（13.9%）、个人兴趣（12.1%）、就业地区（8.5%），而企业规模和人生规划等因素占比较小。从这一结果可以看出，虽然薪资水平是学生择业的关键指标，但职业发展空间、个人兴趣匹配度等内在因素同样受到关注，体现了网安专业大学生在就业选择上既重视物质回报，又兼顾职业认同感和长远发展的双重考量。

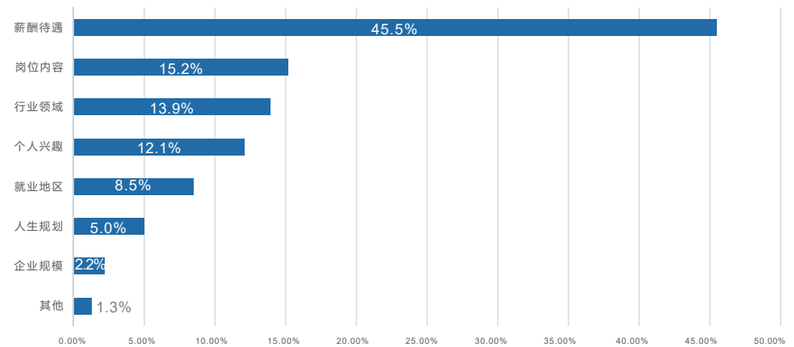


图49 在校生就业规划中优先考虑因素

6．在校生对比赛指导与就业相关活动有强烈兴趣和需求

调研数据结果显示，49.0%的在校生将“相关竞赛赛前指导”列为最急需学校提供的服务。这与前面调查数据中在校生愈发注重网安竞赛，参赛和想要参赛的同学比例大幅上涨是契合的。在就业竞争加剧的当下，学生希望借参赛积累实践经历、打磨简历亮点，为求职增添筹码，却受困于专业赛前培训的缺失。此外，对“就业指导与服务”“专场招聘会”“专业实习实训机会”“网络安全专业培训认证”的需求占比，依次为45.1%、35.1%、29.4%、16.4%。可见，学生对就业指导、实践锻炼、职业培训、招聘对接等直接赋能求职的活动，有着清晰且强烈的诉求，本质是想通过多元准备，应对就业挑战、抢抓就业机遇。

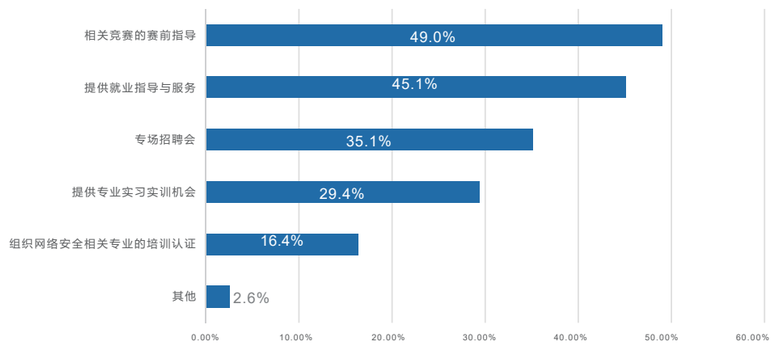


图50 在校生希望学校提供的指导或帮助

7．拥有实践实习经历，是提升自身就业竞争力的核心环节

根据图表数据显示，实践实习经历以47.6%的占比高居网络安全专业大学生就业竞争力要素之首，领先于其他指标。紧随其后的是专业知识技能（45%）和个人综合素质（36.4%），显示出专业技能与软实力的同等重要性。值得注意的是，竞赛获奖成绩以32.5%的占比位居第四，表明在网络安全这一实践性强的领域，实战经验和竞赛成果比传统学历背景更受重视。数据清晰地反映出，网安专业学生普遍认为：实践经历和竞赛成绩是提升就业竞争力的关键要素，这一分布特征凸显了网络安全行业重实践、重能力的用人导向。

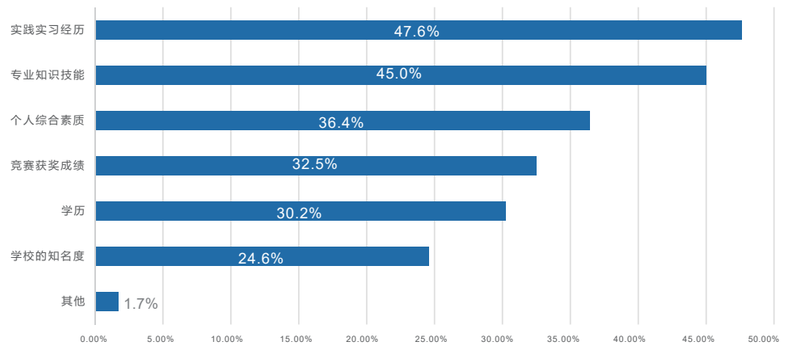


图51 在校生对未来求职过程中哪些条件会增加就业竞争力的看法

8．超四成学生已考取网络安全证书

从调查数据看，近半数（48.3%）学生“了解但未考取”相关证书，反映出他们对证书价值有认知，却因备考难度、时间分配等，暂未完成考取；超四成（44.3%）学生“了解并已考取”，说明部分学生行动力强，能将认知转化为成果，这类学生在专业实践与竞争中或有优势；仅7.4%学生“不了解且未考取”，占比低，表明网络安全证书的普及度已较高，多数学生关注行业资质要求。整体而言，学生对证书认知度高，但实际考取率仍有提升空间，院校可通过优化实践教学、开展备考指导，助力学生提升证书获取率，增强就业竞争力。

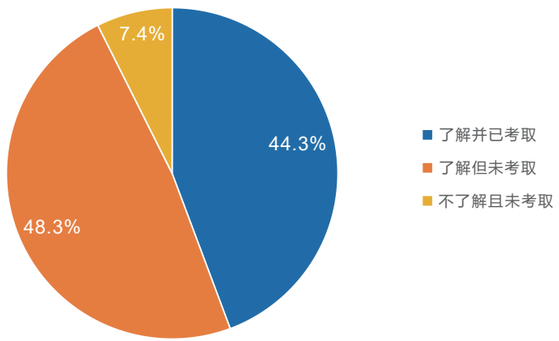


图52 在校生是否了解并考取了网络安全相关证书

9．AI驱动网络安全领域岗位革新与挑战升级

随着人工智能技术与网络安全行业的深度融合，当代大学生对这一技术变革带来的就业影响形成了较为全面的认知。约三分之一（33.5%）的学生表现出对技术替代的担忧，认为AI可能会取代部分传统网络安全岗位，从而加剧就业市场竞争；与之比例相近的32.5%的学生则持乐观态度，他们预见AI技术将创造全新的职业机会和岗位类型，为网络安全从业者开辟更广阔的发展空间；另有21.8%的学生关注到AI带来的职业转型需求，他们意识到未来的工作内容和技能要求将发生显著变化，需要从业者持续学习和适应。这些调研结果生动展现了当代大学生面对技术革新的理性态度：他们既能看到AI技术带来的就业机遇，又能清醒认识到其中蕴含的挑战。随着AI技术的持续演进，这种辩证的认知态度将帮助他们在未来的职业发展中更好地把握机遇、应对挑战。

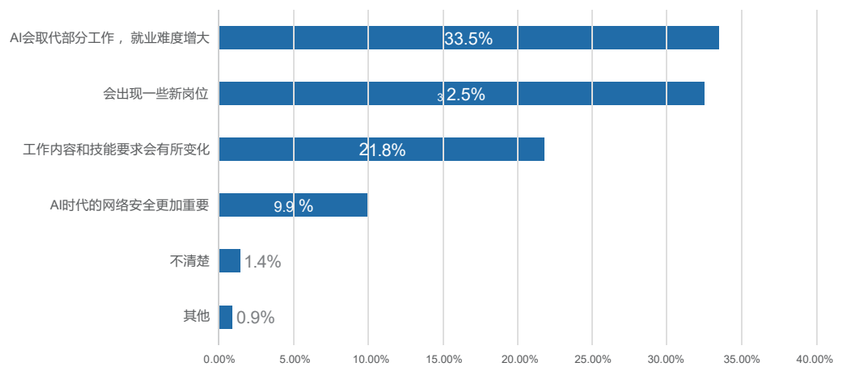


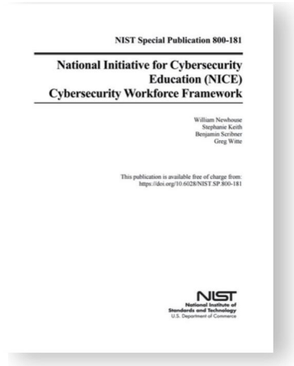
图53 在校生认为AI对网络安全专业未来就业趋势的态度

第四章

在岗人才成长

一、网络安全人才能力标准逐步实施

《网络安全劳动力框架》（NICE Cybersecurity Workforce Framework）是美国国家标准与技术研究院（NIST）主导制定的权威网络安全人才分类标准，旨在为政府、企业及教育机构提供统一的网络安全岗位描述和能力定义体系。 NCWF将网络安全劳动力分为7大类，33个专业领域、52个工作角色、630个知识要求、374个技能要求、176个能力要求及1007个任务，每一个专业领域包含多个工作角色，每一个工作角色需具备多个知识、技能及能力（KSAs），构建了网络安全人才的“能力地图”。


NIST Special Publication 800-181

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

William Newhouse
Stephanie Keith
Benjamin Scribner
Greg Witte

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-181

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

图54《网络安全劳动力框架》

GB/T 42446-2023《信息安全技术网络安全从业人员能力基本要求》由我国信安标委WG7工作组于2023年发布。标准定义了5大类16子类安全从业人员、20类工作任务，以及知识体系（10个知识领域36个知识点）、技能体系（1类通用技能+20类专业技能，共计72项技能），适用于各类组织对网络安全从业人员的使用、培养、评价、管理等。

网络信息安全领域的国家职业标准（原为国家职业技能标准）由人社部牵头不同重要部委进行制定。《标准》根据《中华人民共和国职业分类大典》,按照《国家职业标准编制技术规程》有关要求，相继发布了网络与信息安全管理员（4-04-04-02）、信息安全测试员（4-04-04-04）、密码工程技术人员（2-02-38-12）、密码技术应用员（4-07-05-06）、电子数据取证分析师（4-04-05-08）、数据安全工程技术人员（2-02-38-12）等多个国家职业标准，明确了各等级专业技术人员的工作领域、工作内容以及知识水平、专业能力要求。

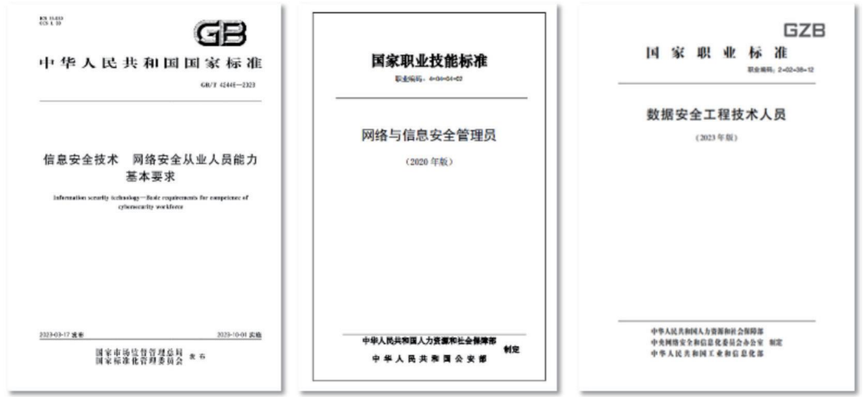


图55 网络信息安全领域的国家职业标准

其他已发布或待发布的行业及团体标准包括：

工信部人才交流中心及网络安全产业发展中心《网络安全产业人才岗位能力要求》

中国电力企业联合会《发电企业网络安全人员培训考核规范》、《电力行业职业技能标准电力网络安全员》

中国人民银行《金融行业网络安全等级保护实施指引第3部分：岗位能力要求和评价指引》

广东省网络空间安全协会《网络空间安全工程技术人才专业能力评价规范》

上海市汽车协会《智能网联汽车网络数据安全人才评价指南》

中国通信企业协会《网络与数据安全运营岗位职业能力规范》

……

此外，中国移动、中国电信等大型央国企也相继结合企业定位和人才发展规划发布了能力图谱、评价模型、技能等级要求等人才标准。

二、网络安全人才队伍建设加速落地

国家网络安全教育技术产业融合发展试验区（北京海淀）深度探索“机制牵引+赛事选拔+动态管理+激励奖励”的网络安全人才发展模式，基于破“四唯”、办“四赛”、建“四站”、立“四库”、推“四奖”的理念和运行机制，积极举办网信安全职业技能大赛、主动培育重点企业建立人才工作站、创新构建特殊人才评价体系、联合推出激励奖励计划，构建集人才发现、人才分类、人才评价、人才使用、人才激励架构为一体的网络安全人才选育用留路径。

国以才立，业以才兴。网络安全离不开专业人才的支持。在持续打造安全型企业过程中，中国电信高度重视网络安全人才的培养，积极引进人才，举办、参与各类网络安全大赛，培养高素质的人才队伍。2021年成立的天翼安全科技有限公司，人才数量已达千人规模，在福建、江苏等多地先后建设成立网络安全人才实训基地，将产、学、研紧密结合，建立多层次、多领域人才培养体系，服务于网络安全领域专业人才培养需求，打造懂业务、能实战的“安全铁军”，为产业、社会培养和储备大量专业人才[22]。

网络安全攻防实战是检验安全体系与防护能力的重要举措。近年来，南方电网公司坚持人才是第一资源，采取一系列举措夯实网络安全基础管理，提升网络安全人才队伍核心能力。目前，南方电网公司打造的这支“攻防兼备”的网络安全特种部队共有780余人，由于在重大活动保障、IPv6课题研究等工作中表现出色，多次受到中央网信办、国家能源局等部门通报表扬[23]。

作为农村金融的主力军，全国农信机构围绕网络安全工作需求设置网络安全岗位，建立了横向分类、纵向分级的多层次、立体化网络安全人才精细化培养体系，通过定期组织理论培训、专业认证、座谈交流、红蓝对抗等多样化竞赛，全面提升网络安全人才综合实战能力和岗位任职能力。自2019年起，农信银资金清算中心连续多年举办农信系统网络安全竞赛，福建社联、浙江农商联合银行、江苏联社等一批团队和人才不断涌现，推动了农信机构网络安全人才队伍建设。

[22]信息来源：《通信信息报》

[23]信息来源：《南方电网报》

三、提升网络安全从业者能力的多元化形式

从调研数据看，工作项目经验积累（41.1%）、工作之余自学（42.5%）占比突出，实际项目让技能落地，自学适配行业快速迭代，二者共同支撑从业人员应对日常复杂场景，是能力提升的“主引擎”。公司内部培训（39.8%）占比高于社会培训（12.8%），反映企业内部知识传承更直接、贴合业务，对员工能力基础构建作用显著。

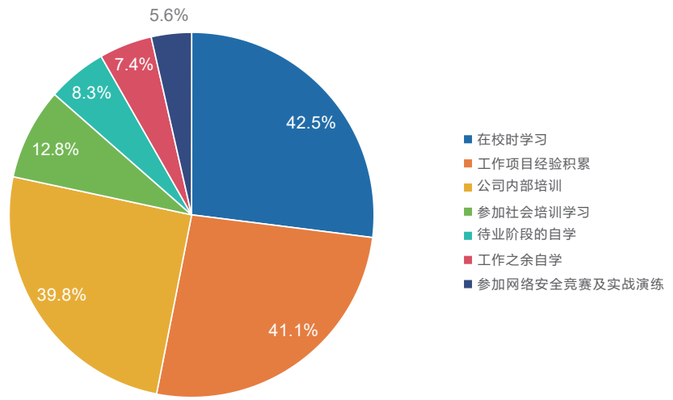


图56 网络安全从业者能力提升形式占比

整体而言，针对安全从业人员的能力提升以“实践+自学”为核心，企业强化内部培训体系、院校优化知识衔接性、社会培训聚焦细分领域、竞赛补足实战短板，形成“学-练-赛-用”闭环，适配网络安全行业动态需求。

培训方面，调研数据体现出从业人员对安全管理、安全运营、安全技术等方向培训需求较高，同时反映出对新兴技术安全、实战能力等方面的关注。

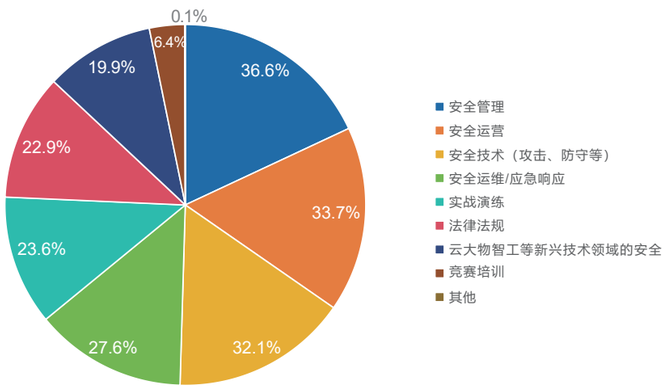


图57 从业人员的培训需求

竞赛方面，本次数据反映出超六成的从业人员有参赛经历（经常参加26.9%、偶尔参加40.9%），相比2023年时我们发布的数据（经常参加10.6%、偶尔参加23.7%），参赛参与度提升明显，这表明网络安全从业人员对竞赛的参与热情在增加，参赛频率有所提高。因为近两年各行业举办的网络安全竞赛数量和参赛人数也逐年提升，网络安全竞赛的形式更加多样化，除了传统的CTF竞赛，还出现了模拟实战、攻防演练等多种形式，更贴近企业实际安全需求，企业也逐渐意识到网络安全竞赛在人才培养、技术提升和品牌建设方面的价值，开始鼓励和支持员工参赛。

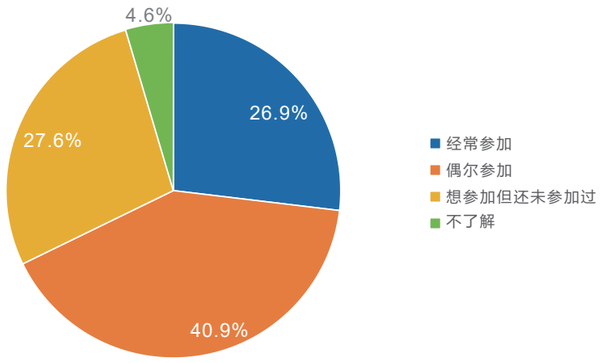


图58 网络安全从业者竞赛参与度占比

持证方面，在本次参与调研的群体中， CISP持证人数最多，占比58.2%。注册信息安全专业人员CISP系列作为国内最早推出、覆盖“管理+技术”的体系化认证，在行业内的知名度和影响力一直较大，尤其受政企、传统行业安全团队认可，是从业者证明其网络安全能力与经验的首选。由中国网络安全审查认证和市场监管大数据中心推出的CCRC、CISAW系列（本次调研占比41.2%），在合规性、专项技术领域也具备较高的权威性。例如，涉及关键信息基础设施的企业，常要求员工持有CCRC证书。CNCERT（国家互联网应急中心）在网络安全应急处理方面权威性高，其CCSC系列证书在应急响应、安全保障等细分领域受认可，因此选择考取这两类证书的人员也有一定数量。随着“多云架构、云原生安全”普及，云安全联盟（CSA）的证书在互联网企业、云服务商中需求上升，反映新兴技术对证书体系的拉动。 CISSP、Security+、ISO27000系列认证占比相对较低（占比15.8%），这些证书源自国外，考试难度较大、费用较高，且部分内容与国内实际网络安全环境适配度存在一定差异，导致选择考取的人员相对较少。

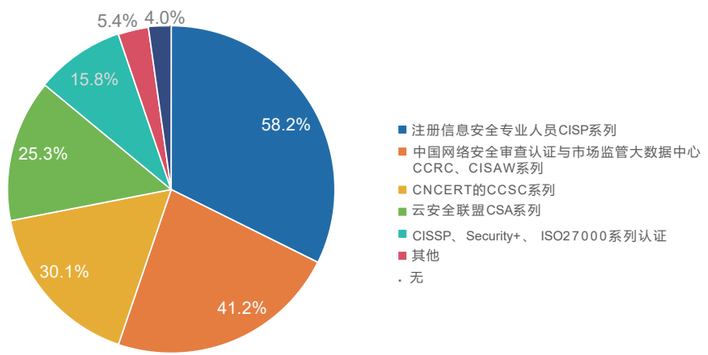


图59 网络安全证书市场占比情况

四、影响网络安全从业者职业能力发展的因素

政策与环境主导性（占比59%最高），说明行业从业人员普遍认为“政策支持（如人才补贴、职业晋升通道）、企业激励（如薪资竞争力、发展规划）”是影响能力发展的核心，从业者会因“看不见成长价值”而缺乏提升动力，组织/企业需通过优化政策扶持（如专项人才计划）、搭建“技术+管理”双晋升通道等，激活从业者成长意愿。

个人基础与资源制约（占比42.4%），体现安全从业者存在“专业底子弱、学习资源少”的问题。组织/企业可增加内部培训（如实战演练、专家分享）、建设学习平台（如免费课程库、技术社区），帮从业者“补基础、拓视野”。

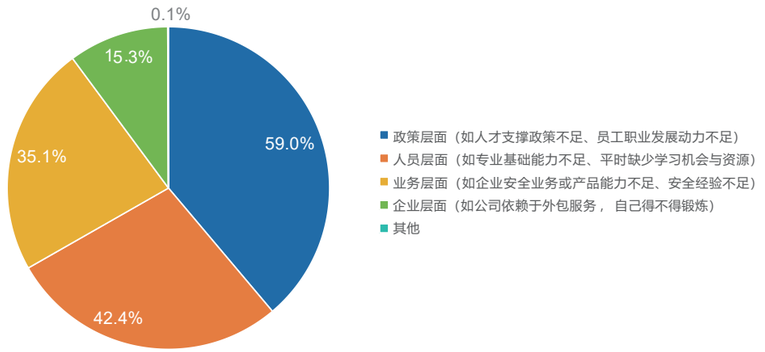


图60 网络安全从业者职业能力发展制约因素占比

业务与实践场景不足（占比35.1%），反映企业安全业务/产品“创新少、场景单一”，从业者因接触不到复杂场景（如高级APT攻防、多云安全架构），能力难突破。企业需主动引入新兴业务（如AI安全、数据跨境合规）、参与行业攻防演练（如护网行动），让从业者在“真场景”中积累经验，避免“纸上谈兵”。

外包依赖的隐性影响（占比15.3%）虽占比低，但体现部分企业“过度外包安全业务”的问题——从业者因“无实操机会”陷入“能力停滞”。企业需平衡外包与自研：核心安全业务（如数据中心防护）保留自研团队，外包非核心业务（如基础安全巡检），既控成本又给员工成长空间。

职业能力发展是“政策（方向）+企业（土壤）+个人（种子）+业务（养分）”的协同结果：组织/企业需先“给动力”（如补贴、晋升），再“给资源”（如培训、场景），从业者才能“主动学、扎实练”，形成“个人成长-企业安全-行业发展”的正向循环。

五、网络安全从业者的AI能力提升

当前，人工智能通过技术渗透、模式创新与治理重构，深刻改变着经济社会的运行逻辑。网络安全从业者应加速顺应这一轮科技革命与产业变革所带来的挑战，拥抱AI、学习AI、应用AI以提高职业竞争力。本次调研发现，有超过97%的参与调研者接受过关于网络安全领域AI技术的培训或学习，而《2024年网络安全产业人才发展报告》的相关数据仅为47.7%，这说明AI在网络安全领域的能力培训正从“局部覆盖”向“全面普及”推进。

然而，本次调研数据在能力提升满意度上反映出，“完全不满足（14%）+不太满足（37.5%）”合计占比超51%，说明超半数参与者认为现有AI安全培训未达到预期，凸显“学了但没用好”的矛盾。

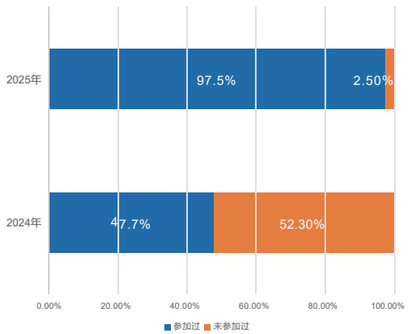


图61 网络安全从业者参与培训情况

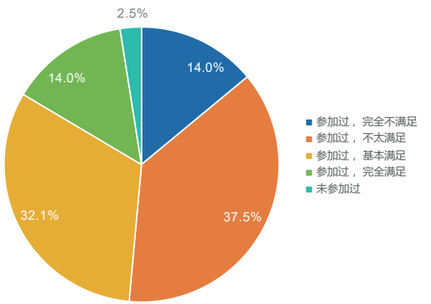


图62 网络安全从业者AI能力培训满意度占比

那么，在受访参与调研的人员中，他们更期待哪类AI+安全主题的培训或学习呢？从需求优先级来看，“对抗新型威胁”与“实战应用”最迫切。应对AI新型威胁的学习需求占比最高（55.8%），说明从业者发现如模型投毒、深度伪造等新型威胁逐渐成为实际工作中的核心痛点。 AI实战技术应用的学习需求占比42.4%，体现从业者希望将AI工具（如异常行为检测、攻击链分析）落地到日常运营（如SOC团队用AI提升威胁狩猎效率），需培训强化“技术+业务”融合，如AI在云安全、工业控制系统中的实战部署。

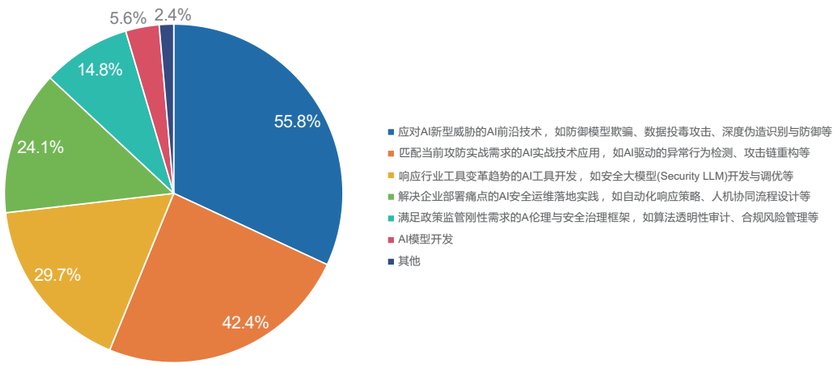


图63 网络安全从业者AI安全培训需求占比

AI时代的网络安全，正从“传统攻防”转向“AI驱动的新型攻防”，培训则需要帮助从业者跨越“AI安全能力鸿沟”。调研数据展示了AI工具使用（48.8%）、AI攻防技术（47.7%）、数据与算法理解（42.8%） 占比远高于其他选项，说明从业者已清晰意识到AI时代的安全能力，需要围绕“AI工具运用-AI攻防对抗-AI决策优化”构建新的能力体系。

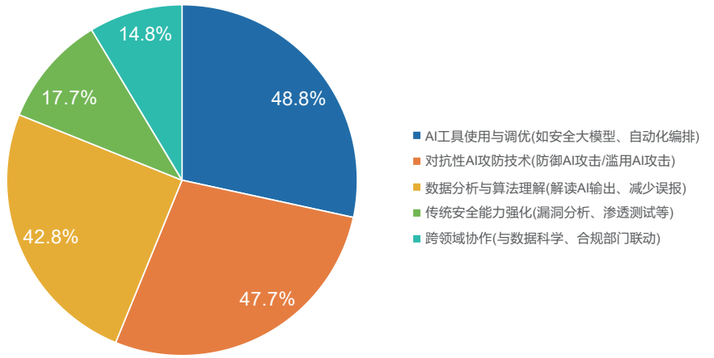


图64 网络安全从业者AI时代能力需求占比

第五章

AI时代：网络安全人才的挑战与转型路径

人工智能正深刻重塑网络安全的防御范式，推动安全能力从“被动响应”向“智能免疫”跃迁。这一变革催生了“AI in security”与“AI for security”双轨并重的能力体系：前者以人工智能为“效能倍增器”，提升威胁感知、决策响应与协同治理能力；后者以安全为“基石守护者”，应对大模型投毒、对抗攻击、数据泄露、算法偏见等内生风险。在此背景下，网络安全人才的角色正经历根本性重构——从传统运维者进化为人机协同指挥官、系统韧性测评师与智能防御总设计师。这一转型不仅是技能升级，更是思维范式与战略定位的跃迁，要求人才兼具驾驭智能工具的效率革新能力与守护AI系统安全的原生架构能力。

然而，AI与网络安全深度融合带来了前所未有的人才挑战。一方面，技术复合性显著提升：从业者不仅需掌握传统安全知识，还需深入理解大模型微调、生成式AI、智能体开发、知识工程等AI核心技术，并能将其应用于威胁建模、自动化响应与风险预测等场景。另一方面，新兴场景安全需求激增：在金融RWA、智能网联汽车、低空经济、数据要素流通等前沿领域，AI安全与行业合规交织，岗位门槛不断提高，亟需既懂AI原理又通安全架构的复合型人才。此外，隐私计算、抗量子密码、无密码认证等非AI类新兴技术的广泛应用，进一步拉高了入行门槛，加剧了人才供需的结构性矛盾。

面对这一挑战，政府、高校与企业需深度融合，以岗位能力模型为核心，共同开展基于真实应用场景的高应用型技能课程设计。政府应发挥政策引导与资源统筹作用，推动建立跨领域的网络安全人才标准体系；高校需依托产业实际岗位需求，重构课程内容与教学流程，强化项目式、沉浸式教学实践；企业则应深度参与课程开发，提供前沿技术案例、实战化训练平台及双师型导师支持，确保教学内容与岗位技能要求无缝对接。通过共建联合实验室、订单式培养项目和动态更新的课程机制，多方形成“需求共定、课程共建、人才共育、成果共享”的协同育人生态，为AI时代的网络安全产业持续输送具备实战能力与创新思维的高素质技术人才。加速构建AI与网络安全创新融合型人才队伍，需各方协同发力精准施策：

一、主管部门与监管机构：强化战略引领与制度供给

1． 纳入国家战略体系：将AI+网络安全复合型人才发展上升至国家安全战略高度， 明确其在关键信息基础设施 、人工智能产业治理中的核心地位， 统筹制定中长期人才发展规划 。

2． 推动标准与认证动态演进：加快建立覆盖 "AI in security" 与 "AI for security" 全链条的能力标准与职业认证体系， 引导人才培养方向与产业需求精准对接， 弥合代际鸿沟 。

3． 构建跨区域协同机制： 打破地域壁垒， 推动人才 、技术 、数据资源的跨区域共享与流动， 支持中西部地区通过远程实训 、联合实验室等形式参与高水平能力建设 。

4． 激励产教融合创新：设立专项基金， 支持龙头企业牵头建设国家级AI安全实训平台与开源社区， 鼓励企业开放真实场景与数据用于教学与研究 。

二 、教育与科研机构：推动课程体系革新与教学范式转型

1． 加快AI安全课程普及与实战化：在网络安全专业中系统融入大模型安全 、对抗样本防御 、联邦学习隐私保护 、生成式AI风险治理等前沿内容， 推动 "理论+沙箱+红蓝对抗" 一体化教学 。

2． 实现产业技术向教学语言转化：引入企业专家共建课程， 将产业中的AI安全实践案例 、工具链与攻防日志转化为教学资源， 缩短教学与实战之间的 "技术时差" 。

3． 强化跨学科融合培养：推动计算机科学 、人工智能 、法学 、伦理学等学科协同， 培养具备技术穿透力 、合规领导力与战略洞察力的复合型人才 。

4． 对接国家战略工程：鼓励高校与科研机构参与国家AI安全重大专项， 将高端人才培养与核心技术攻关深度融合， 提升学术前瞻性与工程责任感 。

三、用人单位：深化实战赋能与生态共建

1. 主导产教融合实体建设：

头部企业应牵头建立AI安全联合实验室、人才孵化基地，提供真实攻防场景、数据集与工具平台，推动人才培养从“纸上谈兵”向“人机协同实战”转型。

2. 建立动态能力评估机制：

依据岗位需求设计AI安全能力图谱，定期评估员工在模型鲁棒性测试、AI日志智能分析、生成式内容鉴伪等方面的实际能力，实现精准用人与持续赋能。

3. 推动内部角色转型：

支持传统安全人员向“AI安全运营工程师” “AI系统韧性评估师”等新角色演进，提供专项培训与项目实践机会，打破技术执行与AI整合的壁垒。

4. 参与开源与标准共建：

鼓励企业贡献AI安全工具、数据集与最佳实践，积极参与行业标准制定，提升整体生态的协同效率与创新能力。

四、从业与准从业人员：构建可持续发展能力范式

1. 树立终身学习与行动学习理念：

主动追踪AI与安全融合的前沿动态，通过权威认证（如AI安全专项资质）构建职业成长通道，持续更新知识图谱。

2. 提升三维核心能力：

技术穿透力：深入理解AI模型训练、推理与部署流程，掌握对抗攻击、后门检测、隐私泄露分析等核心技术；

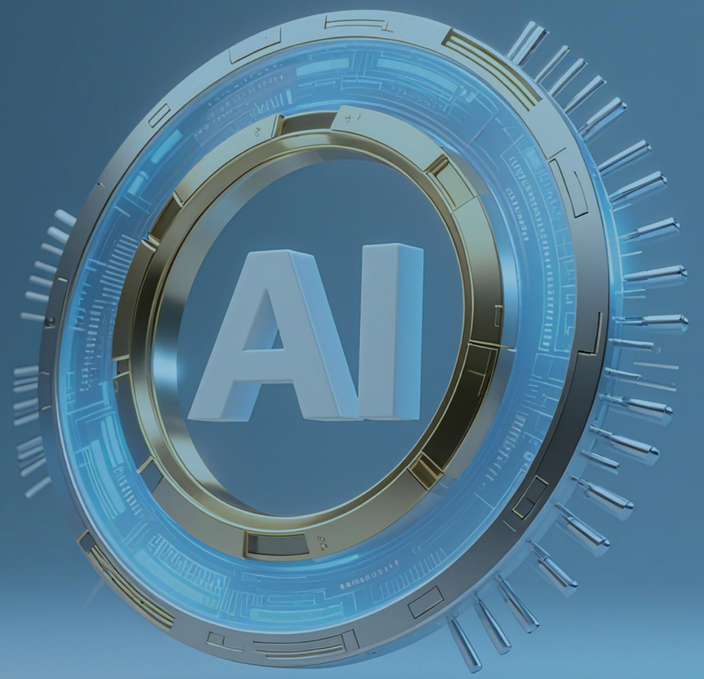
合规领导力：熟悉AI法案、数据安全法等法规要求，具备算法审计、风险评估与治理落地能力；

战略洞察力：能够将AI安全风险转化为业务影响，参与企业级安全架构设计与战略决策。

3. 勇于实现价值跃迁：

从被动执行转向主动设计，积极参与AI原生安全架构建设、生成式AI攻防演练与智能防御体系规划，完成从“技术操作者”到“智能防御架构师”的角色进化。

AI与网络安全的深度融合，既是技术革命，更是人才范式的重构。唯有主管部门强化引领、教育机构重塑体系、用人部门深化实战、个人主动进化，方能构建起支撑智能时代安全底座的创新融合型人才队伍，真正实现 “让安全更智能，让智能更安全”的双重目标。



特别提醒

行业交流分享群

分享：可获取人资行业的报告、方案及其他学习资源，上新群内通知

交流：求职、找人、找资源、找供应商

客服

交流群

免责声明

第三方声明：本报告所有内容（数据/观点/结论）整理于网络公开渠道，均不代表我司立场，我司不承担其准确性、完整性担保责任。

侵权处理承诺：如报告内容涉嫌侵权，请立即联系客服微信，我司将在核实后第一时间清理相关内容并配合处理