中国网络安全产业分析报告

（2024 年）

中国网络安全产业联盟

2024 年 10 月

版 权 声 明

前　言

党的十八大以来，习近平总书记深刻把握全球科技革命和产业变革的大趋势，对网络安全和信息化工作作出一系列重大部署和重要论述，是新时代做好网络安全工作的根本遵循。党的二十届三中全会审议通过的《中共中央关于进一步全面深化改革、推进中国式现代化的决定》提出，加强网络空间法治建设，健全网络生态治理长效机制，健全未成年人网络保护工作体系。网络安全是总体国家安全观的重要组成部分，切实维护网络空间安全，筑牢国家网络安全屏障，已成为关系我国发展全局的重大战略任务。近年来，我国网信相关部门深入推进网络安全治理，网络安全政策法规体系更加健全，各项长效机制不断完善，治理效能持续提升，全社会网络安全意识和能力显著提高。同时应该看到，近年来我国网络安全威胁和风险日益突出，国际宏观环境变乱交织，全球网络攻击活动持续升级，网络安全逐步向政治、经济、国防、社会等领域传导渗透，防范网络安全风险、维护网络空间安全，已经成为我们必须面对和解决的重大安全问题。

本报告是中国网络安全产业联盟（CCIA）连续第七年发布。CCIA 以网络安全行业调研数据为基础，按照客观中立原则展开了数据收集整理和分析研究工作。

本报告的市场规模采用收入法统计，统计范围为在国内

销售网络安全产品或提供网络安全服务的企业，不包括产业链上游硬件供应商和下游销售渠道（代理商和分销商）。

本次调研延续前六次产业调研模式，仍然以具备网络安全产品、服务和解决方案销售收入的我国网络安全企业为目标研究对象，调研企业数量近300家，最终收集到160家企业有效数据，基本覆盖了国内主要的网络安全企业。

本报告首先介绍了2024年我国网络安全产业面临的总体形势，既面临全球网络安全产业增势明显、多国战略布局持续加快、技术集成加大垂直赋能、政策法规体系持续完善、发展新质生产力及加快推进新型工业化对产业提出更高要求等发展机遇，也遭遇国际宏观环境变乱交织、网络攻击活动持续升级、开源软件供应链风险加剧、国内网络安全市场需求转弱等挑战。

在产业发展情况分析部分，报告从国际和国内两个视角透视网络安全产业发展脉络。全球视角，重点关注网络安全支出、重点企业图景和行业投融并表现。国内视角，以网络安全产业调研数据为基础，面向产业链结构的供需两侧探求市场全貌。供给侧维度，报告对2023年我国网络安全产业规模进行了测算，分析了我国网络安全企业的总体构成及分布情况，并对行业集中度、市场区域分布、集群化发展情况等内容进行了分析；需求侧维度，对客户行业分布等进行了分析。

在资本市场部分，报告基于采集的样本公司经营数据，对2023年我国网络安全主要企业经营情况进行了综合分析，刻画了总体现金流量画像。同时，报告评价了我国网络安全产业资本市场表现，回顾了2023年以来的IPO动态和投融并情况。

在产业发展热点部分，报告从网络安全技术、服务、治理以及重点行业应用四个维度，重点列举了10个发展热点，分别是人工智能安全技术、移动目标防御技术、量子加密通信技术、深度伪造检测技术、隐私增强技术、持续威胁暴露管理、安全访问服务边缘、数据安全态势管理、智能网联汽车安全和低空经济网络安全。

在产业发展趋势部分，报告提出对网络安全产业未来发展的四大趋势研判，展望了网络安全产业的发展前景，为网络安全企业业务拓展、产业规划布局等提供参考。

鉴于产业全口径统计数据获取实际情况，本报告中涉及网络安全产业规模及增速、网络安全企业经营数据等分析所用数据截至2023年底。产业基本情况以及资本市场分析涉及的数据均为CCIA基于调研或公开资料整理。本报告观点及数据仅供参考，不作为投资依据。

目 录

图目录

表目录

一、2024 年网络安全产业发展面临的新形势

2024 年，延续近年来宏观政治经济发展底色，全球局势变乱交织，百年变局加速演进，安全形势错综复杂，经济下行压力加大，全球产业链供应链深度调整，网络安全产业发展面临的国际形势依然严峻。从国内看，我国经济回升向好，高质量发展扎实推进，全面建设社会主义现代化国家迈出坚实步伐[1]，新型工业化建设稳步推进，新质生产力加快培育，网络安全产业迎来全球增势回暖、技术集成赋能、政策法规精细务实等发展机遇，也面临安全合作“阵营化”凸显、网络攻击持续升级、国内市场需求转弱等挑战。与此同时，我们也要看到在不稳定、不确定性上升的全球经贸环境中，2024 年上半年中国经济顶住压力，发挥了“稳定器”和“动力源”的重要作用，为我国网络安全产业快速发展奠定了坚实基础。

（一）发展机遇

1.全球持续加快网络安全战略布局

近年来，随着地缘政治不稳定不确定因素日益增多，技术发展日新月异，全球各国不断加强网络弹性建设，通过加强立法、技术创新和国际合作等手段加速网络安全战略布局，80%以上的国家颁布网络安全法规政策，140 多个国家设立了网络安全事务协调机构，110 多个国家出台个人数据与隐私保护法规，60%以上的国家通过外资审查、市场许可

[1] 《确保同向发力、形成合力——从中央经济工作会议看 2024 年中国经济高质量发展》。https://www.gov.cn/yaowen/liebiao/202312/content_6919861.htm

证等方式管理网络安全产品准入[2]，以应对不断演变的网络安全挑战。2023 年下半年以来，美国相继发布《2023 年网络战略》《2024 财年国防授权法案》《关键与新兴技术清单（2024 年更新版）》《国际盟友合作伙伴标准指南》《2023 年网络安全监管协调草案》《网络访问安全的现代方法》《供应链网络安全原则》等法规政策，从加强网络安全资金支持、促进关键技术研发、保障供应链网络安全、联合盟友强化战略合作等方面提出更加全面细化的措施要求；欧盟陆续推出《欧盟网络安全条例》《网络弹性法案》，针对数字产品、工业网络等领域规定了更加完备、更具约束力的网络安全要求和治理框架。全球主要国家和地区持续优化网络安全战略布局，为我国洞察和把握全球网络安全形势变化、强化我国网络安全产业顶层治理提供参考。

2.人工智能技术为代表的技术集成加大赋能网络安全

2023 年，人工智能、量子计算、区块链等前沿技术加快迭代、集中涌现，应用领域呈现多方向、融合性、集群式发展，网络安全产业所蕴含的巨大的发展潜力进一步充分释放。随着机器学习、深度学习、自然语言处理等人工智能技术深度应用正在颠覆网络安全底层逻辑和运营体系，一方面网络攻击通过应用人工智能技术实现“升维”，另一方面“人工智能+安全”技术将实现对网络攻击及威胁的“免疫性防御”，

[2] “剖析宏观经济波动下的网安产业及 2024 年走向”，http://www.cww.net.cn/article?id=587162。

2024 年，“人工智能+安全”正在朝向更高性能、更强算力以及智能化运营的发展方向演进。量子计算技术发展进入“实用量子模拟机”阶段，两款新型量子芯片“秃鹰”和“苍鹭”亮相，全球首个模块化量子计算机“量子系统二号”推出，量子计算凭借超大算力将在复杂网络威胁识别、加固密钥安全等网络防御领域实现更广泛应用；区块链技术由单点应用逐步发展为可信基础设施，我国“星火·链网”、欧盟区块链服务基础设施（EBSI）等项目持续推进，促进政府、民生等领域数据要素安全可信流转的规模化应用[3]，多元化跨界融合的技术创新活力和应用潜力正在激发网络安全产业新的经济增长点和群体化应用浪潮。

3.网络安全治理相关政策走深且要求向实

近一年来，网络安全政策体系更加完善，网络空间法治根基不断夯实，主要涵盖战略规划、法规条例、治理规范、行业监管机制和人才资金保障等方面的政策法规，总体上看发布的系列政策法规更加注重实操层面的具体要求，在各细分行业领域的网络安全保护实践中谋求安全与发展的平衡。党的二十届三中全会审议通过的《中共中央关于进一步全面深化改革、推进中国式现代化的决定》提出，加强网络空间法治建设，健全网络生态治理长效机制，健全未成年人网络保护工作体系。法规方面，《未成年人网络保护条例》《中

[3] 穆琳.2023 年网络安全领域新兴技术的发展特点.中国信息安全, 2024-02

华人民共和国保守国家秘密法》陆续发布，健全未成年人网络保护体制机制，完善了网络信息、数据保密管理规定；《网络数据安全管理条例（草案）》审议通过，作为行政法规对《网络安全法》《数据安全法》和《个人信息保护法》等上位法的有关规定进行落实、细化、补充，将对网络数据实行分类分级保护，明确各类主体责任，落实网络数据安全保障措施。政策方面，围绕数字政府、数据资产管理、数据安全、数据要素、数据跨境流通、关键信息基础设施安全保护、安全应急预案等方面发布系列政策规定，同时在工业和信息化领域、新兴技术、寄递服务、民用航空、保险、电力系统、教育行业等细分应用领域提出网络安全和数据安全管理要求。可以看到，我国网络安全政策立法总体呈现不断优化调整、细化落实现有政法体系的趋势，同时紧跟新兴技术发展伴随的网络防御新特点新形势，提出具有前瞻性、突破性的网络安全治理理念，更加多元、审慎的政法体系为网络安全产业健康有序发展营造了良好环境。

4.培育发展新质生产力为网络安全产业注入新动力

新发展阶段，党中央创新性的提出要培育发展新质生产力，加快推进新型工业化，是我们推动构建现代化产业体系，实现高质量发展的必由之路。数字经济时代，无论是发展新质生产力，还是实现新型工业化都离不开网络这一关键基础设施。网络安全是加快培育发展新质生产力，加快推进新型

工业化的重要底座，网信事业代表着新的生产力、新的发展方向，网络安全本身就具有“新质”特征[4]。随着网络化、数字化、智能化加速推进，新质生产力加快培育发展，推进实现新型工业化对数据安全和网络安全的需求将日益提高，新质生产力所蕴含的新技术、新模式、新理论也为网络安全发展提供了新的思路和方法，新时期网络安全工作需要开辟产业链协同、跨领域联动、价值链延伸等新路径，及时完善新技术创新发展伴随的数据权属、算法监管等网络安全新领域的政策法规，增强关键基础设施安全防护，提升软硬件系统安全可靠性，强化企业网络安全管理制度，发展新质生产力将极大促进网络安全产业快速发展。

（二）面临挑战

1.国际宏观环境变乱交织，安全合作“阵营化”趋势凸显

近年来，世界经济增长乏力，全球主要国家“阵营化”发展趋势日益明显，“以政制经”图谋甚嚣尘上，单边主义、保护主义持续上升，加剧了全球产业链供应链恶性竞争，政治、经济、产业等方面的博弈对抗扩散至网络空间领域，对全球战略合作产生巨大影响。美国对华“脱钩断链”，从构筑“小院高墙”发展为“大院铁幕”，高科技领域的竞合博弈更具网络效应，关键技术涉及的网络和信息安全问题比以往任何时候都更具风险且更加敏感。同时，美国持续加大对现有盟友、新

[4] 杨力群.以新质生产力打造高质量发展强劲引擎.《新华日报》,2024-04-02（10）.

兴经济体及更多发展中国家的拉拢渗透，如恢复美欧跨境数据流动，推动亚太经济合作组织（APEC）构建跨境隐私规则（CBPR），扩大四方安全对话（QUAD）印太布局打造以日本为核心的网络情报合作网，加强美韩数字身份领域合作研讨以及积极吸纳阿尔巴尼亚、哥伦比亚、埃及等国家网络信息共享等措施，建立“遏华”“排华”国际网络协作阵营，打压、剥夺我国发展网络科技、深化全球网络安全合作等正当权利。

2.网络攻击活动持续升级，开源软件供应链风险加剧

2023 年以来，网络攻击活动呈现组织化程度高、攻击目标明确、攻击数量增多、隐蔽性增强、攻击效率提高等趋势，高级持续性威胁（APT）攻击、勒索软件攻击、数据窃取、零日攻击等网络攻击手段近年来已演化为结合社会工程学攻击、应用人工智能等前沿技术的综合体，网络空间安全威胁越来越严峻。据 Statista 网站统计显示，全球 72%的企业成为勒索攻击受害者。2024 年上半年发生多起严重的网络攻击事件，例如，美国 Ivanti VPN 设备零日漏洞受到攻击、美国医疗处方公司 Change Healthcare 遭受网络攻击、XZ Utils 软件供应链攻击、美国国家环境保护局数据泄露[5]及 7·19 微软蓝屏事件造成全球近千万台设备宕机等，极大地暴露了网络安全防护的薄弱环节。开源软件漏洞造成的供应链攻击的

[5] 安全内参.盘点：2024 年上半年典型网络攻击事件.
https://www.secrss.com/articles/67655

频率不断升高，据安全评估公司 Verocode 研究结果显示，开源组件仓库中 70.5%的代码库存在安全漏洞，超 96%的产业组织机构在开发软件应用中使用开源组件; OwnCloud、Sierra Wireless 等公司的 OT/IoT 路由器均发现严重漏洞，网络边界模糊引起的多源异构身份互信互认问题、海量数据储存及应用造成的数据泄露以及 APT、供应链威胁等带来的新型网络安全问题等。开源软件被广泛应用在涉及产业安全、社会民生的方方面面，不仅对网络安全产业本身产生影响，对经济社会系统安全也具有不容忽视的重要性，其安全风险事关重大，风险挑战不断升级，需要高度重视。

3.国内政企数字化建设放缓，网络安全市场需求转弱

2024 年，受宏观经济环境结构性问题与周期性矛盾交织叠加等因素影响，我国网络安全市场增速延续较低趋势，政企信息化、数字化建设的节奏放缓，企业经营压力增大，降本增效需求明显[6]，对网络安全产品需求转弱。从上市公司发布的业绩情况看，不少企业出现业绩下滑、亏损等情况，除一些头部企业仍保持较高增速外，多数企业营收增长相对乏力，部分中部网络安全企业滑落至尾部，失去生态配套主导权。此外，传统合规市场逐渐趋于饱和，新的增量市场尚未形成规模，网络安全企业纷纷调整战略布局和发展策略，网络安全产业发展空间受到一定限制。

[6] 关键基础设施安全应急响应中心.透过现象看本质，深度剖析宏观经济波动下的网安产业及 2024 年走向，2024-02.

二、网络安全产业发展情况

（一）全球网络安全产业整体情况

受益于网络安全政策加码以及新技术、新业态安全需求不断释放，全球网络安全产业逐步复苏回暖，网络安全企业积极加强业务布局，加速技术迭代创新，人工智能、零信任、量子信息等前沿技术为网络安全产业发展注入新活力，从供需两侧促进全球网络安全投入持续增长，全球网络安全产业发展长期向好的基本面没有改变。

全球网络安全市场支出不断攀升。据 Gartner 统计预测数据显示，2019 年至 2024 年全球网络安全支出同比增速呈现上升趋势，预计 2024 年将达到 2149.5 亿美元，同比增长 14.3%（图 1），全球网络安全需求仍然强劲。细分领域看，安全服务、基础设施保护、网络安全设备支出占比最高，2024 年将分别达到 41.9%、15.5%、11.3%。

数据来源：Gartner

图 1　2018—2024 年全球网络安全支出及同比增长率

网络安全产业规模稳中有升。根据世界经济论坛（WEF）与埃森哲联合发布的《2024 年全球网络安全展望》，2023 年，全球网络安全经济的增长速度达到世界经济增速的 4 倍[7]；据全球市场调研机构 Markets and Markets 预计，全球网络安全市场规模预计将从 2023 年的 2200 亿美元增长到 2027 年的 2662 亿美元，年复合增长率（CAGR）达 3.9%。

主要网络安全企业相对稳定。根据 QYResearch 头部企业研究中心调研数据显示，全球网络安全企业主要包括 Palo Alto Networks、Cisco、IBM、Fortinet、Check Point、McAfee、Trend Micro、Broadcom (Symantec)、RSA Security、奇安信等，头部企业竞争格局较为稳定。从主要国家地区看，北美

[7] The World Economic Forum. Global Cybersecurity Outlook 2024. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

汇集了众多国际头部企业，成为全球最大的市场，约占 45%的市场份额，其次是欧洲和亚太，分别占比 25%和 23%。

全球网络安全企业投融并活动较活跃。据 Crunchbase 统计，网络安全并购热度不减，2023 年，海外共发生 130 多起并购事件，并购总金额超 430.5 亿美元[8]。2023 年以来，全球网安融资活动呈现先降后升态势，去年全球共发生 692 笔融资交易，总融资金额为 82 亿美元，与 2022 年的 163 亿美元相比，融资规模同比下降近 50%; 2024 年融资迎来复苏反弹，根据 Pinpoint Search Group 报告显示，2024 年第二季度 98 轮融资和 22 笔并购交易总额为 33 亿美元，融资额同比上涨 71%，且早期阶段的融资（包括种子轮和 A 轮融资）占二季度融资总量的 55%，表明全球企业对网络安全产品和服务的需求保持增长态势，且资本市场对于应对当前和未来网络安全业务挑战的初创公司的投资信心不断增强。

（二）我国网络安全企业总体表现

截至 2024 年 6 月 30 日，我国已公开上市的网络安全企业共有 29 家（见表 1）。29 家上市网络安全企业数据的统计分析结果显示，2023 年网络安全上市公司营业收入保持正增长的公司有 15 家（见图 2），相较对比 2022 年同期数据，保持持续正增长的企业数量进一步下滑，网络安全企业收入持续承压。

[8] 计算机与网络安全.2024 年网络安全产业走向，2024-02。

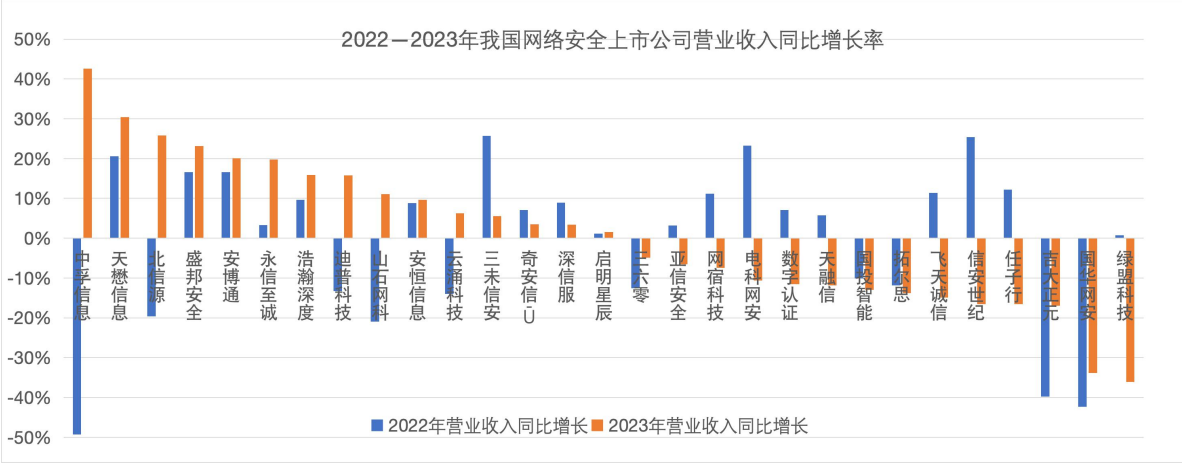

图 2　2022—2023 年我国网络安全上市公司营业收入同比增长率

从我国上市企业的营业收入情况来看，29 家上市公司 2023 年营业收入总和为 562.33 亿元，较 2022 年同比下降 3.4%。其中，2 家公司收入增速超过 30%，7 家公司收入增速在 10%—20%之间，14 家网络安全上市公司收入增速为负值，增速为负值的企业数量较 2022 年进一步增加。从网络安全企业营业收入及增速来看，网络安全行业发展减缓甚至停滞态势仍在延续。

表 1 2023 年网络安全上市企业经营数据

序号	公司	营业收入（亿元）	营业收入同比增长 %	扣非净利润（亿元）	扣非净利润同比增长 %
1	三六零	90.6	-5%	-7.6	59.5%
2	深信服	76.6	3%	1.1	10.0%
3	奇安信-U	64.4	4%	-1.0	68.4%
4	网宿科技	47.1	-7%	4.1	132.1%
5	启明星辰	45.1	2%	4.7	-9.6%
6	天融信	31.2	-12%	-4.2	-371.3%
7	电科网安	30.7	-11%	3.0	14.5%
8	安恒信息	21.7	10%	-3.9	-29.9%
9	国投智能	19.8	-13%	-3.4	-464.3%

序号	公司	营业收入（亿元）	营业收入同比增长%	扣非净利润（亿元）	扣非净利润同比增长%
10	绿盟科技	16.8	-36%	-10.1	-9106.9%
11	亚信安全	16.1	-7%	-3.2	-2159.9%
12	迪普科技	10.3	16%	1.2	-12.3%
13	数字认证	9.7	-12%	-0.5	-157.2%
14	中孚信息	9.2	43%	-2.2	53.6%
15	山石网科	9.0	11%	-2.5	-20.9%
16	拓尔思	7.8	-14%	0.0	-97.0%
17	飞天诚信	7.4	-15%	-1.8	-45.9%
18	北信源	6.8	26%	0.0	101.6%
19	任子行	6.1	-17%	-1.2	-507.7%
20	信安世纪	5.5	-17%	0.1	-93.9%
21	安博通	5.5	20%	0.1	125.8%
22	浩瀚深度	5.2	16%	0.5	1.7%
23	吉大正元	4.1	-17%	-1.7	-356.0%
24	永信至诚	4.0	20%	0.1	-72.3%
25	三未信安	3.6	6%	0.6	-41.4%
26	盛邦安全	2.9	23%	0.3	-18.6%
27	云涌科技	2.8	6%	-0.1	-158.4%
28	天懋信息	1.2	30%	0.3	29.8%
29	国华网安	1.1	-34%	-1.4	76.6%

（三）我国网络安全产业规模及增速

根据国内网络安全主要企业调研数据分析，2023 年，我国网络安全市场规模约为 640 亿元，同比增长 1.1%，增速较 2022 年下降 2 个百分点。近三年行业总体保持增长态势，但受宏观经济等因素影响，政企信息化、数字化建设的节奏暂缓，网络安全行业增速持续放缓（见图 3）。根据重点企业

调研数据，国内百家网络安全主要企业的从业人员数量达91798人。

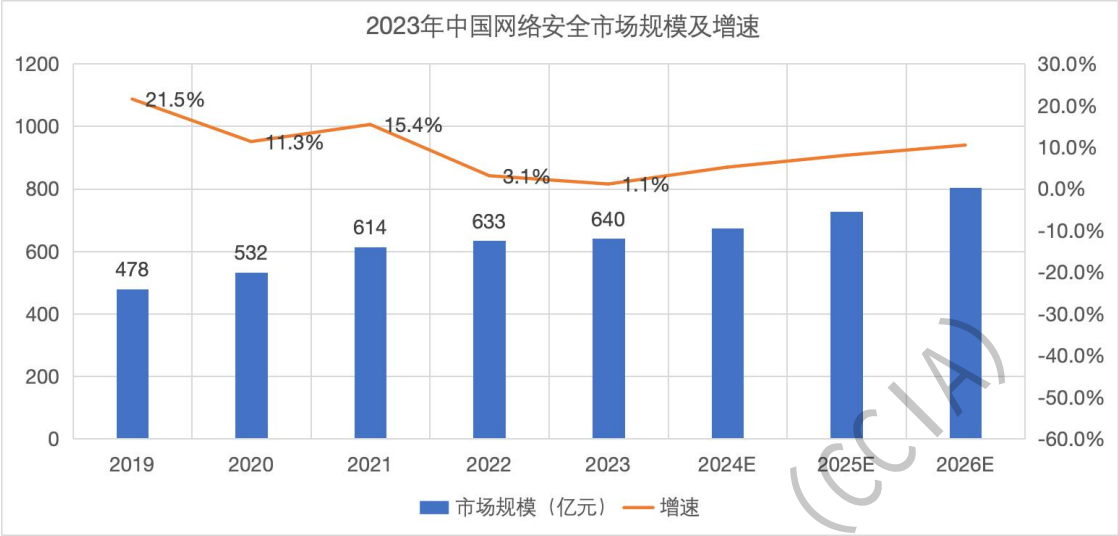

图 3　2023年中国网络安全市场规模及增速

展望未来，网络安全产业发展顶层设计更加完善，促进行业发展的政策基础愈加稳固，数字经济加速发展等正向激励将给网络安全产业注入新动力，网络安全生态逐步拓展，运营商、IT厂商、集成商纷纷投入网络安全业务板块，其他软件产业的细分领域也将逐步涉及网络安全业务，在多方面利好条件的影响下，网络安全产业将逐步改善发展较为稳滞的状态，网络安全产业增速将逐步增大，预计到2026年市场规模将超过800亿元。

（四）我国网络安全市场区域分布情况

综合对比分析国内网络安全企业调研数据和网络安全上市公司的公开数据，2023年，华北、华东、华南地区网络安全市场份额分别为38%、23%及14%，华北、华南等地区对网络安全的投入进一步加大，区域市场占比有所提升（见

图 4）。同时，近年来网络安全企业逐步实现技术和资本积累，为其“出海”打下坚实基础。奇安信、深信服、绿盟科技等领军企业海外业务发展良好，创新型企业积极尝试突破，2023 年取得一定成绩，海外市场占比延续小幅提升的趋势。据公开数据显示，我国网络安全企业在新加坡及其他东南亚地区布局安全业务的企业数量达 50 多家，中东地区布局业务的约有 20 家左右，拉美、欧洲等地区也将成为“出海”热门地区。预计未来海外市场将成为中国网络安全企业新的业务增长点。

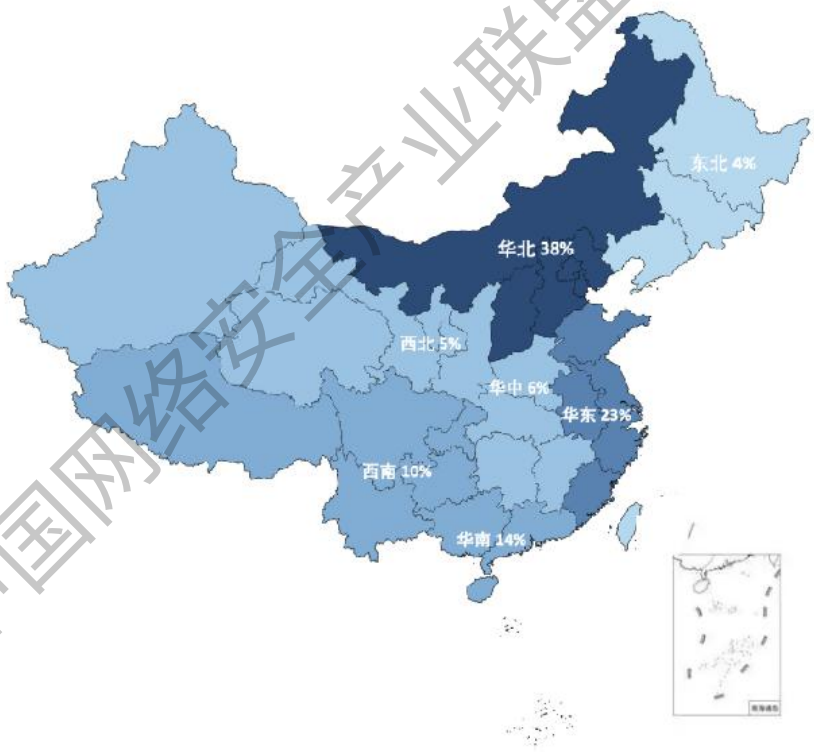

图 4　2023 年中国网络安全市场区域分布

（五）我国网络安全客户所属行业分布情况

从网络安全客户所属行业分布来看，政府部门因政策监管严格，其信息系统涉及国计民生和国家安全等重要业务，

对网络安全项目的需求较大，近年来一直占据最大份额；能源、企业、金融、电信、军工、公检法司、医疗、交通、教育等与国计民生紧密相关的领域紧随其后，作为密集数据源生产、持有和使用方，网络安全需求和投入均十分可观（见图 5）。

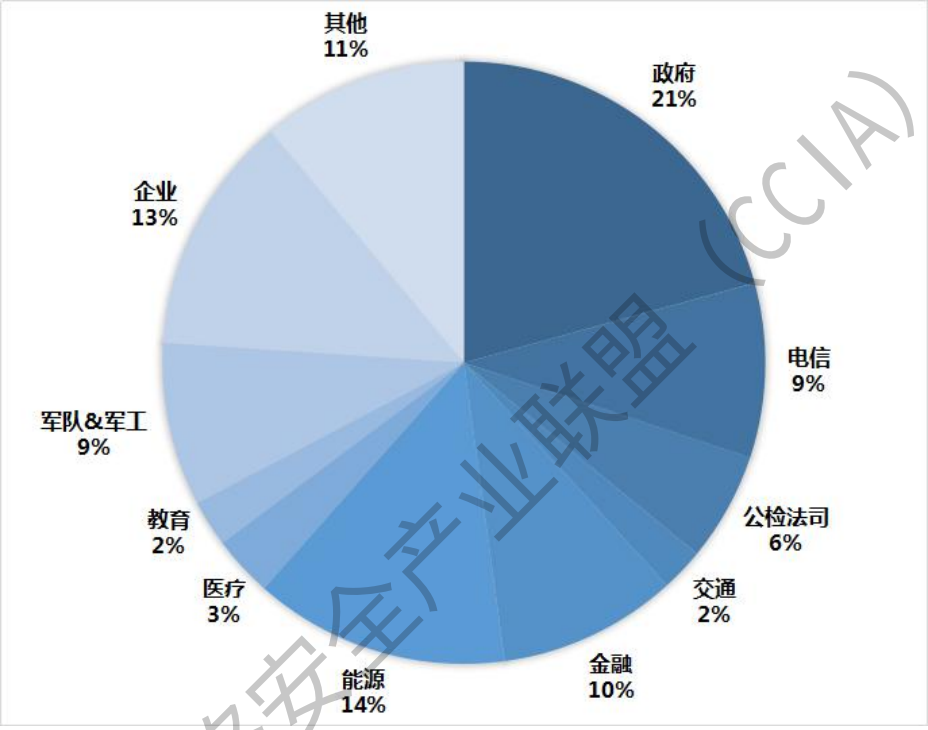

图 5 2023 年中国网络安全项目数量行业分布

（六）我国网络安全产业集群化发展情况

近年来，国内很多省市开始立足地方产业实际，培育发展网络安全产业集群，既有致力于打造世界级产业集群的“先锋队”，如在第一批 66 家国家级战略性新兴产业集群中，唯一一个网络信息安全产品和服务产业集群——天津滨海高新区网络安全产品和服务产业集群、国家级先进制造业集群——长沙市新一代自主安全计算系统产业集群、国内首个跨

省域的国家级网络安全产业园区——国家网络安全产业园区（成渝）等优秀代表，也有专心深耕县域经济的集群“新生力量”,如国家级中小企业特色产业集群——湖北省武汉市东西湖区网络安全产业集群。需要注意的是，尽管有这些网络安全产业集群的优秀代表，但在国家级战略性新兴产业集群、先进制造业集群、新型工业化示范基地，以及中小企业特色产业集群等中，以网络安全产业为核心主导产业的集群数量仍然十分有限。受限于网络安全产业整体规模相对较小，就观察来看，国内以网络安全产业作为主导产业的产业园区、集群、基地等数量较少、规模相对较小。目前，网络安全产业多作为数字经济、新一代信息技术等相关产业集群的二级甚至三级产业板块存在，或者在制造业等相关产业集群中作为辅助性产业板块存在。随着国家大力倡导推动产业集聚化发展，实现“串珠成链、集链成群”，在可预期的未来，越来越多的网络安全产业集群将相继出现。

三、我国网络安全资本市场分析

（一）我国主要网络安全企业经营情况分析

我国网络安全资本市场分为一级市场和二级市场。报告选取 2023 年已上市的 29 家网络安全企业中的 23 家作为分析样本，通过对其经营数据进行分析，以了解我国网络安全资本市场总体情况，原因如下：一是部分企业为混业经营，上市主体中包含非安全业务且占比较高，因此未列入本次数

据选取范围（见表 2）；二是与一级市场的网络安全企业数据相对不透明不同，二级市场的企业经营数据定期公开，数据可获得性高；三是样本企业在 2023 年的收入占国内网络安全市场份额超过 60%，在一定程度上可反映网络安全企业总体经营状况[9]。

表 2 公开上市的网络安全企业 2023 年经营情况

交易所	证券代码	证券简称	上市板块	营业收入（亿元）	扣非净利润（亿元）	是否选为样本企业
上海	601360.SH	三六零	主　板	90.5542	-7.5586	否
深圳	300454.SZ	深信服	创业板	76.6217	1.1044	是
上海	688561.SH	奇安信-U	科创板	64.4249	-0.9667	是
深圳	300017.SZ	网宿科技	创业板	47.0550	4.0788	是
深圳	002439.SZ	启明星辰	主　板	45.0691	4.7107	是
深圳	002212.SZ	天融信	主　板	31.2449	-4.1702	是
深圳	002268.SZ	电科网安	主　板	30.7278	3.0146	是
上海	688023.SH	安恒信息	科创板	21.7016	-3.8782	是
深圳	300188.SZ	国投智能	创业板	19.8372	-3.3520	否
深圳	300369.SZ	绿盟科技	创业板	16.8078	-10.0517	是
上海	688225.SH	亚信安全	科创板	16.0809	-3.2494	是
深圳	300768.SZ	迪普科技	创业板	10.3397	1.1904	是
深圳	300579.SZ	数字认证	创业板	9.7247	-0.5480	是
深圳	300659.SZ	中孚信息	创业板	9.1858	-2.1722	是
上海	688030.SH	山石网科	科创板	9.0104	-2.4859	是
深圳	300229.SZ	拓尔思	创业板	7.8168	0.0243	否
深圳	300386.SZ	飞天诚信	创业板	7.3855	-1.7788	否
深圳	300352.SZ	北信源	创业板	6.8272	0.0308	是
深圳	300311.SZ	任子行	创业板	6.0874	-1.2387	否
上海	688201.SH	信安世纪	科创板	5.4923	0.0947	是
上海	688168.SH	安博通	科创板	5.4828	0.0556	是
上海	688292.SH	浩瀚深度	科创板	5.2050	0.4568	是
深圳	003029.SZ	吉大正元	主　板	4.0796	-1.6571	是
上海	688244.SH	永信至诚	科创板	3.9587	0.1103	是
上海	688489.SH	三未信安	科创板	3.5860	0.5795	是
上海	688651.SH	盛邦安全	科创板	2.9083	0.3456	是
上海	688060.SH	云涌科技	科创板	2.8236	-0.0900	是

[9] 网络安全市场和企业收入呈现较为突出的季节性分布特征，下半年收入占全年比例较高，因此，为更加科学准确地分析企业经营情况，报告选取 2023 年全年企业经营数据进行分析。

交易所	证券代码	证券简称	上市板块	营业收入（亿元）	扣非净利润（亿元）	是否选为样本企业
新三板	874151.NQ	天懋信息	新三板	1.1923	0.2666	是
深圳	000004.SZ	国华网安	主　板	1.1005	-1.3828	否

从营业收入来看，2023 年，样本企业安全业务营业收入合计 429.6 亿元，同比下降 1.8%。其中，网络安全业务收入超过 10 亿元的有 10 家；超过 20 亿元的有 7 家，分别是深信服、奇安信、网宿科技、启明星辰、天融信、电科网安和安恒信息（见图 6）。

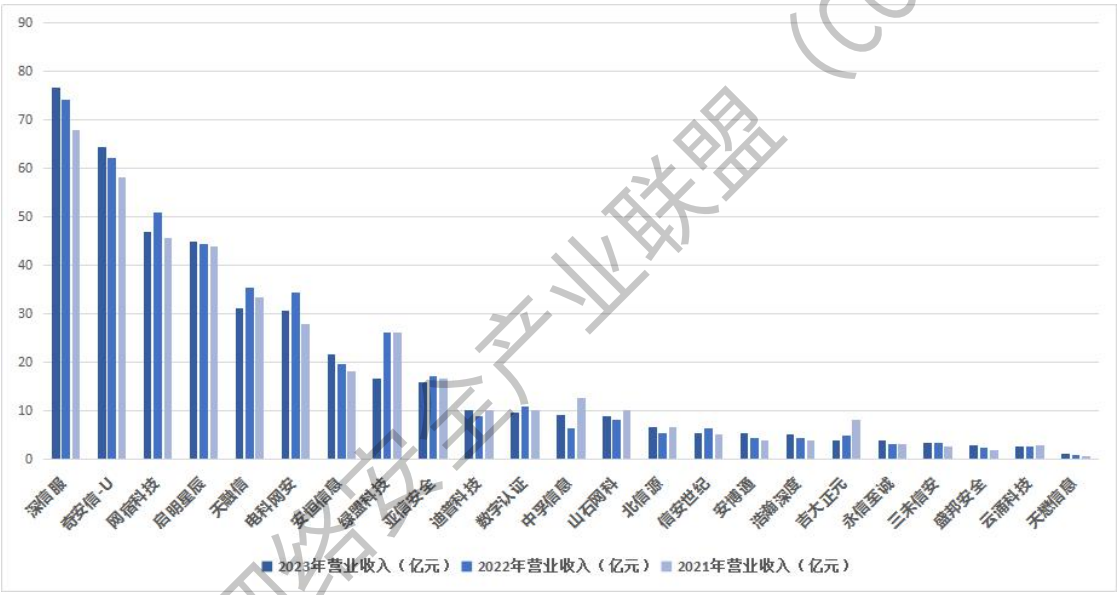

图 6　2021—2023 年样本网络安全企业安全业务营业收入

从营收增长情况来看，2023 年，样本企业中 15 家收入增速为正，8 家收入出现负增长。实现收入正增长的企业中，9 家收入同比增长超过 10%，增速最高的五家企业分别为中孚信息、天懋信息、北信源、盛邦安全和安博通（见图 7）。

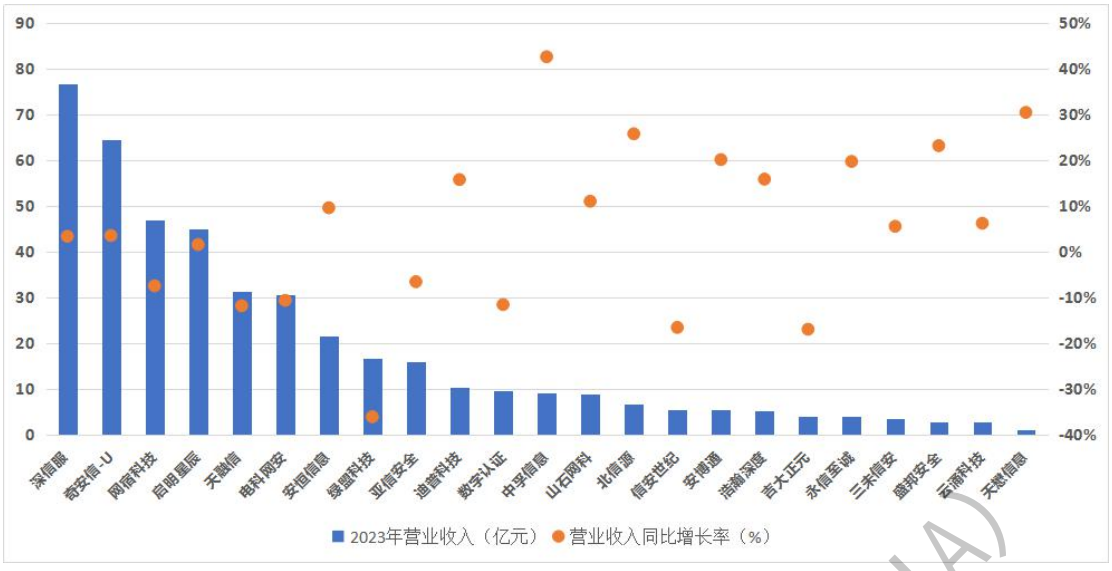

图 7　2023 年样本企业安全业务营业收入及营收增长情况

从盈利能力来看，2023 年，样本企业盈利能力持续下滑，23 家企业中有 13 家盈利，盈利企业中扣非净利润不足 1 亿的企业有 7 家，16 家亏损（见图 8），较 2022 年亏损情况更加突出。

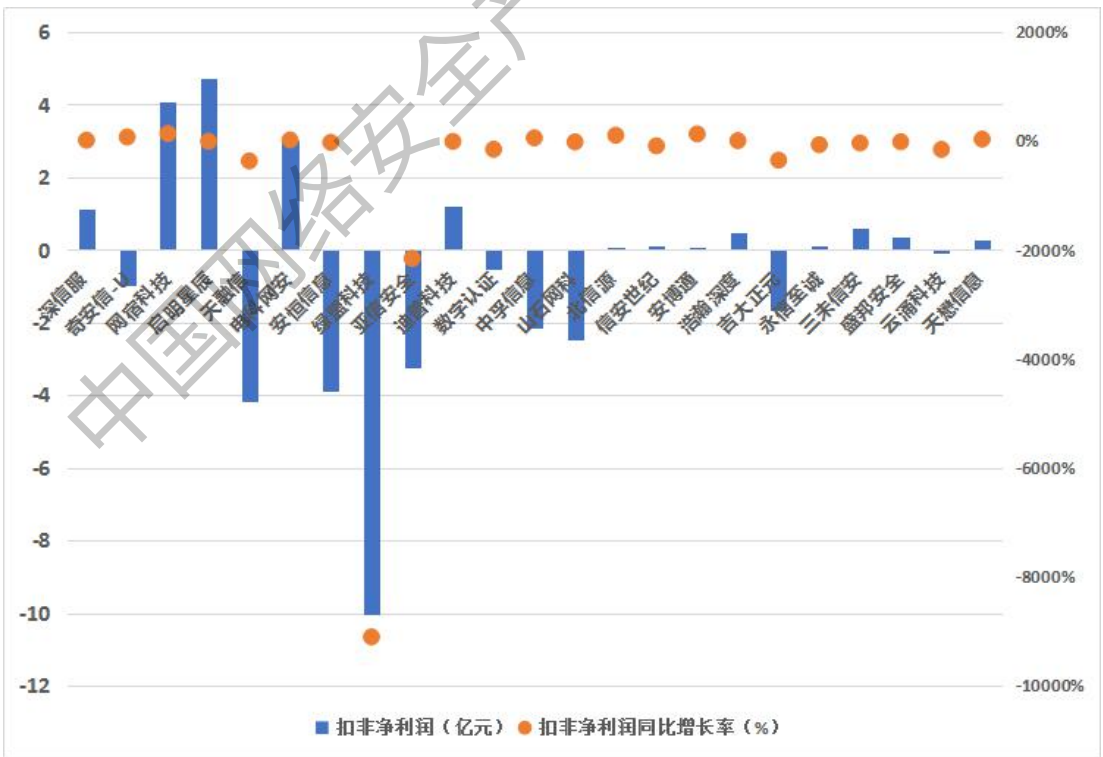

图 8　2023 年样本网络安全企业安全业务盈亏状况

从四项费用构成看，2023 年，样本企业中，有 20 家四项费用率（销售费用率+研发费用率+管理费用率+财务费用率）超过 60%（见图 9），相较于 2022 年的 8 家，有大幅上升，这反应出越来越多的企业或运营成本不断上升，或企业收入显著降低，盈利空间受到较大挤压。但也需注意，样本企业研发和销售投入也在持续增大，两项费用合计达 219 亿元，占企业营业收入的 51.0%。其中，销售费用为 118.4 亿元，同比增长 10.9%；研发费用达到 100.6 亿元，同比增长 4.4%，反映出企业一方面希望通过技术创新开辟新赛道，另一方面希望扩大销售渠道，开辟市场“蓝海”，成为 2023 年网络安全企业逆境图存的两个主要思路。

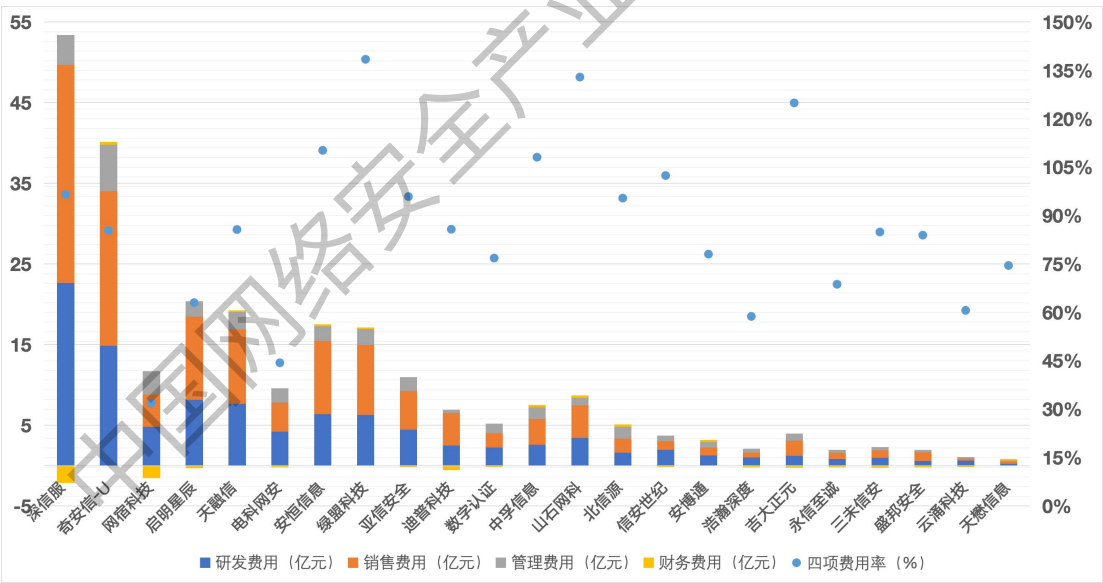

图 9　2023 年样本企业费用以及四项费用率构成

进一步分析样本企业研发情况，可以看出，样本企业中研发投入达 5 亿元以上的企业有 6 家，分别是深信服、奇安信、启明星辰、天融信、安恒信息和绿盟科技；6 家企业研

发投入保持正增长，分别是亚信安全、电科网安、绿盟科技、网宿科技、山石网科和深信服（图 10）。可以看出，网络安全头部企业仍然坚持“技术为王、创新图存”的发展理念，坚持扩大技术研发投入，为提高未来产业竞争力增强技术储备。

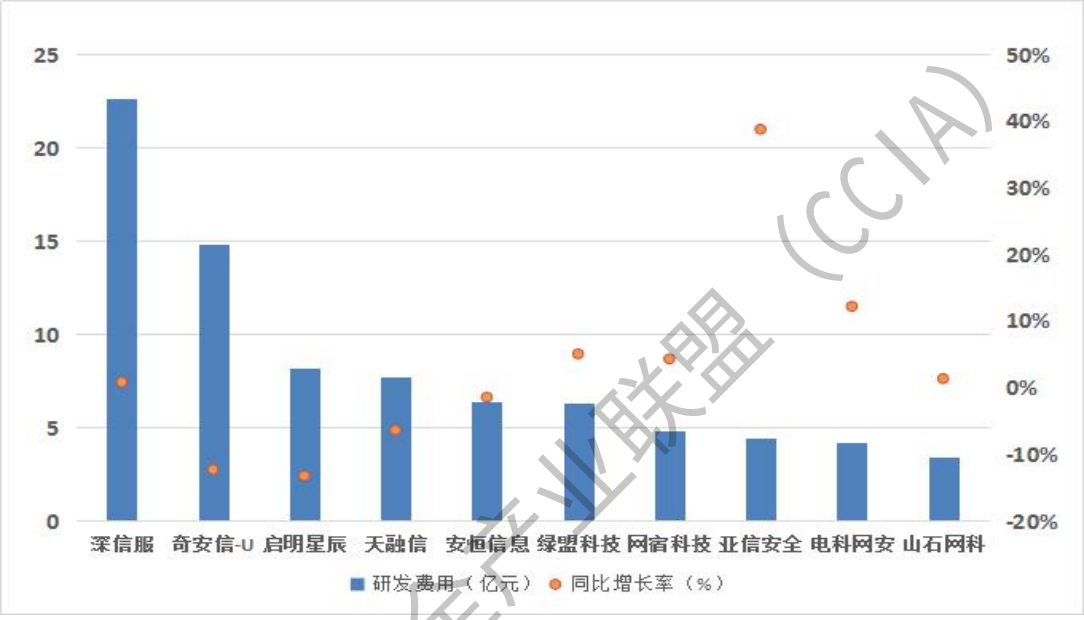

图 10　2023 年样本企业前 10 研发投入及增速

研发人数位列前三的企业分别是奇安信、深信服、启明星辰，研发人员数量占员工总数比例居前三名的企业分别是数字认证、网宿科技、天融信（图 11），仍以头部企业为主，与研发投入形势相符。

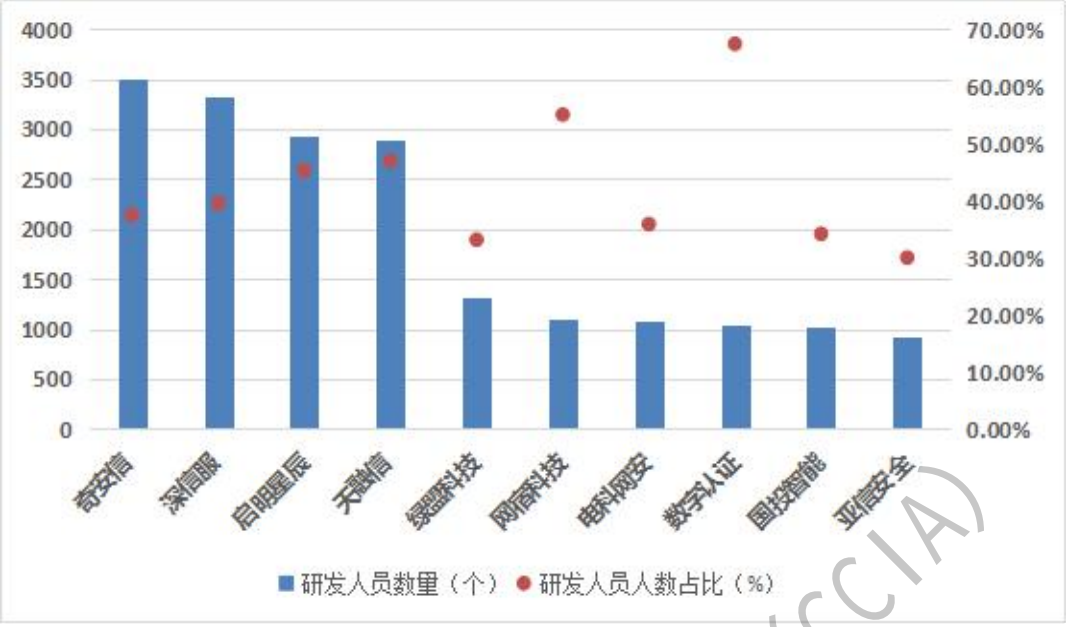

图 11　2023 年样本企业前 10 研发人员情况

从研发成果情况看，网络安全领域有效专利数量位列前三的企业分别是深信服、奇安信和迪普科技（图 12）。

图 12　样本企业前 10 有效专利情况

从企业现金流量来看，如图 13 所示，2023 年，样本企业的经营性现金流净额合计为 9.88 亿元，相较于 2022 年同期的-17.24 亿元，呈现大幅回升的状态。投资活动产生的现

金流净额合计为-66.11 亿元，筹资活动产生的现金流净额合计为 71.38 亿元。这反映出在产业整体发展处于“瓶颈”且不确定性增强的大形势下，企业在积极加强财务风险防控，坚持“现金为王”的同时，也在寻求通过多样化的资本运作方式，为未来产业振兴储备力量。

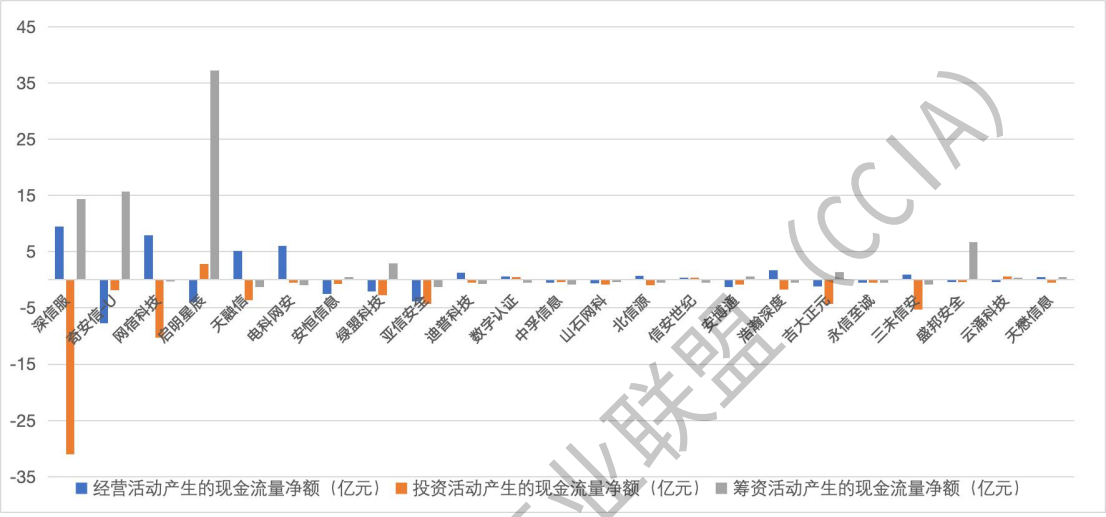

图 13　2023 年样本企业现金流净额

（二）我国网络安全企业 IPO 动态

近年来，网络安全企业在科创板的 IPO 申报趋势趋于平稳，在经历了 2019 年到 2021 年的申报高峰期后，2022 年和 2023 年逐渐回归常态。科创板网络安全企业平均上市历经天数 287 天。2023 年，盛邦安全成功登陆科创板。

表 3 2019—2023 年网络安全企业上市进程情况

序号	企业名称	当前状态	板块	受理时间	上市时间	上市历经天数	上市首日市值（亿元）	最新市值（亿元）
1	奇安信-U	上市	科创板	2020-07-22	2020-05-11	72	908	152
2	安恒信息	上市	科创板	2019-11-05	2019-04-09	210	59	29
3	亚信安全	上市	科创板	2022-02-09	2021-03-12	334	156	43

序号	企业名称	当前状态	板块	受理时间	上市时间	上市历经天数	上市首日市值（亿元）	最新市值（亿元）
4	山石网科	上市	科创板	2019-09-30	2019-04-09	174	81	18
5	信安世纪	上市	科创板	2021-04-21	2020-06-29	296	38	23
6	安博通	上市	科创板	2019-09-06	2019-04-04	155	92	18
7	浩瀚深度	上市	科创板	2022-08-18	2021-12-22	239	31	23
8	吉大正元	上市	主板	2020-12-24	2019-06-25	548	29	33
9	永信至诚	上市	科创板	2022-10-19	2021-06-30	476	28	24
10	三未信安	上市	科创板	2022-12-02	2021-12-21	346	91	29
11	盛邦安全	上市	科创板	2023-07-26	2022-06-28	393	41	19
12	云涌科技	上市	科创板	2020-07-10	2019-12-20	203	152	18
13	联软科技	退市	科创板	n/a	2021-06-23	n/a	n/a	n/a
14	齐治科技	退市	科创板	n/a	2020-11-05	n/a	n/a	n/a
15	溢信科技	退市	科创板	n/a	2020-06-23	n/a	n/a	n/a

（三）我国网络安全产业投融并情况

2023 年，受宏观环境影响，网络安全一级市场投资热度延续下滑态势，国内网络安全产业融资事件共有 65 起，同比下降 47.6%；融资额约为 36.9 亿元，同比下降 45.6%（见图 14），2023 年 8 月 27 日证监会提出“阶段性收紧 IPO 节奏”，投资机构对于网络安全项目投资更加谨慎。

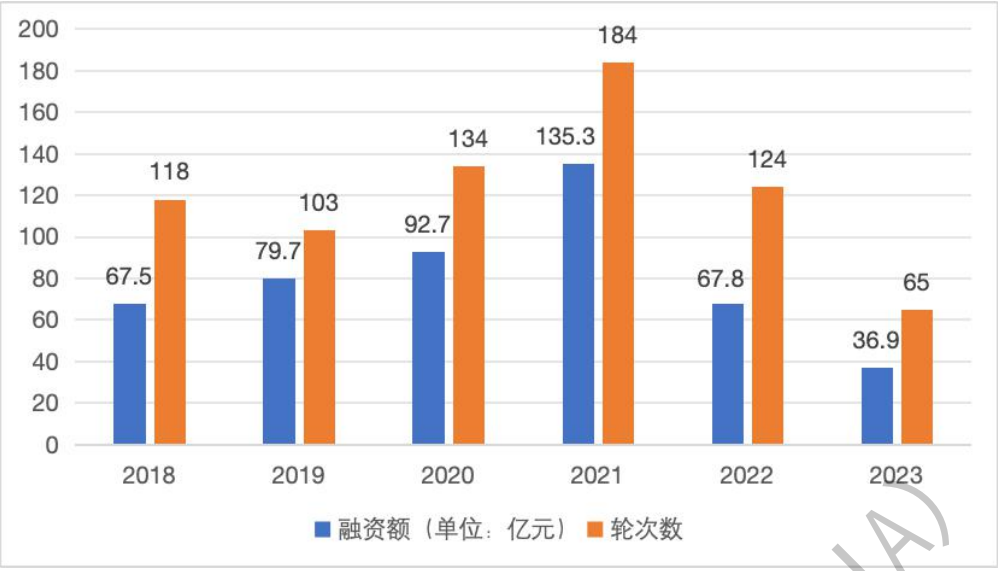

图 14　2018—2023 年中国网络安全领域融资事件数量金额比较

2023 年，单笔融资额达到亿元以上的融资有 14 起，千万级的有 44 起，千万级以上融资事件数量占全年融资数量为 89.2%。与 2022 年相比，千万级以上融资事件占比有所增大。2023 年以来包括“827 新政”阶段性收紧 IPO 节奏，“315 新政”压实中介机构责任，沪深交易所优化上市条件，北交所辅导指引规范监管，出台科创板八条加强全链条监管等一系列政策措施的出台，表明 IPO 市场监管体系正在不断完善和强化，网络安全一级市场投融资的质量和安全性将得到更好保证，促进各利益相关方的投融资活动更加规范有序。

表 4 2023 年网络安全企业融资（亿元级）情况

时间	公司简称	轮次	交易金额	投资方
2023.01	云天安全	A 轮	1.22 亿元	山东发展投资集团、泰山创投、乐知基金、高华投资
2023.01	烽台科技	B 轮	2.5 亿元	中网投、毅达资本、贵州创新赋能大数据投资基金、元起资本、中信建设资本、火山石资本、贵阳创投

时间	公司简称	轮次	交易金额	投资方
2023.02	观安信息	E 轮	3 亿元	国鑫创投、国家制造业转型基金、卓戴资本
2023.02	炼石网络	A+轮	近 1 亿元	重庆科技转投
2023.03	华瑞指数云	Pre-A 轮	近 1 亿元	明势资本领投、奇安投资、同创伟业
2023.04	翼方健数	B++轮	数亿元	未披露
2023.05	领信数科	B 轮	超亿元	晨壹并购基金
2023.05	银基科技	B+轮	2 亿元	奇安投资、华控基金、博将资本、合方资本
2023.06	烽台科技	B+轮	1.2 亿元	中化基金、中移北京基金
2023.07	赛博昆仑	A 轮	近 1 亿元	达晨财智、红杉中国
2023.08	全宇工业	A 轮	近 1 亿元	未披露
2023.08	众智维科技	A 轮	近 1 亿元	奇安投资领投、苏州相城金控、海邦投资跟投
2023.10	金睛云华	B 轮	近 1 亿元	未披露
2023.11	鼎茂科技	B 轮	超 1 亿元	未披露

四、我国网络安全产业发展热点分析

基于对行业领军企业、研究机构，以及权威的网络安全领域专家进行问卷调查和深度访谈，结合对国内外网络安全技术发展趋势的综合研判，从网络安全技术、服务、治理和行业应用四个维度，提出以下 10 项网络安全产业发展热点：

（一）人工智能安全技术

2022 年以来，随着通用大模型的广泛应用，人工智能技术进入发展爆发期，资本、技术涌入新赛道。特斯拉 Optimus

机器人、开源通用人形机器人“青龙”、百度萝卜快跑无人出租车等人工智能产品不断涌现，以全新形式进入人类生产、生活，人工智能发展潜力持续释放。与此同时，生成式人工智能和大型语言模型技术越来越多的被运用到网络攻防两方，不仅在网络攻击、网络诈骗等应用愈多，同时也越来越深刻地成为网络安全守卫者手中的技术“利剑”。日常的网络安全维护中，生成式人工智能不仅被用于识别安全威胁，还被应用在网络风险评估和合规性分析等领域。一方面，通过自动生成威胁报告和警报，生成式人工智能能够帮助安全团队更好地理解和应对各种安全威胁，有效提升了安全团队对风险的响应和处置效能。另一方面，生成式人工智能还可以辅助识别合规性风险，帮助企业确保遵循相应的法律、法规、政策、标准等规定。此外，生成式人工智能还可以用于安全配置的优化，确保系统和应用始终遵循最佳的安全配置标准。虽然生成式人工智能技术仍在快速迭代演进的进程中，其可靠性、有效性和成本可控性仍有待检验，但其价值和潜力不容忽视。今年 7 月，OpenAI 的技术负责人 Ilya 离职创立了 SSI 研究院，专门研究安全超级智能；在世界人工智能大会上，浦江实验室的新任掌门周伯文启动了 45 度 AI 计划，研究以 AI 安全优先，又能保证 AI 性能长期发展的技术体系。在可预见的未来，生成式人工智能将越来越多地被应用于网络安全领域，人工智能安全技术具有巨大的发展潜力和广阔

前景。

（二）移动目标防御技术

移动目标防御（MTD）技术是一种以主动预防为主的网络防御技术，通过动态排列、变形、变换或混淆应用访问入口，不断转移攻击表面等方式对抗攻击，实现主动防御。MTD技术主要包括三类：一是动态调整IP地址、网络端口以扰乱攻击目标；二是随机化指令集、数据和地址空间，动态改变数据在内存中存储的位置、将指令集和数据异构后再存储等方式达到扰乱攻击者的目的；三是提供数据、服务和节点等方面的多个副本，判断系统是否遭受攻击后能够适时将运行环境还原。此外，MTD能够设置陷阱捕捉威胁者的行为，以达到防范未来攻击的效果。MTD技术可以有效阻止勒索软件和其他高级零日攻击，成为有效提升内存、网络、应用程序和操作系统安全的关键技术之一，是从静态、被动防御逐步向动态、主动防御理念转变的具体体现。通过动态改变设备的网络配置和属性，MTD技术在面对未知、复杂的网络攻击方面较静态防御技术具备显著的优势，其在电子政务、军事、电子商务等领域具有广阔的应用前景。

（三）量子加密通信技术

量子通信是基于量子叠加、量子纠缠等物理特性进行信息传输或密钥分发的通信技术，主要包括量子密钥分发（Quantum Key Distribution，QKD）、量子安全直接通信

（Quantum Secure Direct Communication，QSDC）等应用形式，是唯一被称为“无条件安全”的通信方式[10]。量子密钥分发是指通信双方通过传送量子态实现对称密钥生成的方法，是当前实用化程度最高的通信技术。量子加密通信技术是利用量子不可分割、量子态不可克隆等特性对传输的信息进行一次一密的加密方法，是一种绝对安全的通信技术。通过应用密钥分发技术和对称密码技术，能够抵御量子计算对主流公钥密码体系和现有信息安全体系的威胁，克服经典加密技术的安全隐患。2023 年 3 月，美国量子安全公司首次利用“星链”卫星实现了能够抵御量子计算攻击的端到端加密通信，其通信过程由“量子安全层”软件进行数据保护，该软件采用端到端“量子安全即服务”架构，运用抗量子计算攻击加密技术，能在存储、使用、传输等全生命周期对数据进行充分保护。我国通过运用量子加密通信“京沪干线”和“墨子号”量子科学实验卫星，构建全球首个星地量子通信网，实现跨越 4600 公里的多用户量子密钥分发。可以预见，量子加密通信技术未来将在国防军工、电子政务、应急指挥、金融证券、智能制造等多个领域发挥作用，其未来发展空间十分广阔。

（四）深度伪造检测技术

深度伪造技术（DT）是指应用人工智能技术篡改图像、音频和视频内容生成虚假信息的技术。近年来，大量深度伪

[10] 郭苗苗，王峰生. 量子保密通信技术及应用组网分析.中移智库，2023-08。

造技术发展演进，在教育、娱乐、社交媒体等领域广泛应用，同时在政治舆论、司法刑侦等领域造成较大的负面影响。图像视频的深度伪造检测技术主要分为针对伪造痕迹进行取证的检测方法和数据驱动的检测方法，前者主要检测图像处理取证、生物信息、融合痕迹、时序连贯和模型指纹等图像伪造痕迹，后者利用卷积神经网络检测常规的人脸伪造方法，得到相关特征向量后，利用神经网络根据特征向量判断输入图像是否经过伪造。语音深度伪造检测技术主要从音频中提取声学特征，并利用高斯混合模型、神经网络等分类模型，根据声学特征对目标音频进行分类，从而判断语音是否经过伪造[11]。目前针对单个数据集或伪造方式的深度伪造检测技术已较为成熟，但现有的深度鉴伪模型仍存在较多问题，其泛化性能较差，检测模型的鲁棒性有待提升，且难以应对现实世界中不同压缩率、噪声等复杂条件[12]。近年来，英特尔、微软、OpenAI 等公司相继推出深度伪造检测工具产品，深度伪造检测技术在人工智能、机器学习等技术加持下快速发展，检测深度伪造内容的准确率大大提升，误报率大幅度降低。深度伪造检测技术将更多应用于社交媒体、政府机构、国防军事等领域，以预防关键信息的恶意操纵和虚假宣传。

（五）隐私增强技术

[11] 全球技术地图. 深度伪造技术的风险、挑战及治理，2023-04。

[12] 李泽宇, 张旭鸿, 蒲誉文, 伍一鸣, 纪守领. 多模态深度伪造及检测技术综述. 计算机研究与发展, 2023, 60(6)。

隐私增强技术（Privacy-enhancing Technologies，PETs）是一系列收集、处理、分析和共享信息同时保护个人数据隐私的数字技术和方法的集合。PETs 主要包括三类技术：一是为敏感数据处理分析提供可信环境，具体通过利用硬件或软件的可信执行环境（TEE），在隔离空间内执行加密的数据和代码，防止外部攻击或窥探，如 Intel SGX、ARM Trust Zone、AMD SEV 等均是硬件可信执行环境的具体应用。二是在不泄露数据的情况下对数据进行本地处理分析，通过本地节点进行分布式数据计算，并通过安全协议汇总结果，避免数据直接传输或集中存储，如安全多方计算、差分隐私等均应用了此类技术。三是在处理数据前对数据和算法进行转换，利用数学方法对数据和算法进行加密或扰动，从而在计算过程中不会泄露原始信息，同时保持计算结果的正确性，如同态加密、零知识证明等。当前，隐私增强计算技术已广泛应用于政务、金融、教育、医疗、能源、工业等领域，实现跨机构数据协作、云端数据服务等应用，促进跨行业、跨部门数据共享和分析，有效提升隐私数据泄露风险防控能力。可以预见，隐私增强计算技术将与量子计算、物联网、5G、区块链等前沿技术融合应用，实现更快速、更安全、更复杂、更智能的数据处理。

（六）持续威胁暴露管理

攻击面管理（ASM）、外部攻击面管理（EASM）、网

络资产攻击面管理（CAASM）、数字风险保护服务（DRPS）和资产风险管理技术一直以来是重要的技术热点。随着政府、企业、个人的资产更多接入网络，“云大物移智”等多种技术深度融入企业等各类组织运营各环节中，企业等组织对于安全风险的暴露面和攻击面范围更大、影响更广，而网络攻防天然的不对等使攻击者在攻击时机、资源等方面占据主动，因此，亟需采取技术创新，以综合性、体系性考虑如何管控数据资产的网络安全风险。因此，暴露面智能运营的理念在过去几年被提出，并引起广泛重视。持续威胁暴露管理技术（Continuous Threat Exposure Management，CTEM）便是在这一背景下产生发展的。Gartner 将其列入 2024 年十大网络安全战略技术趋势。

CTEM 并不是单一的一项技术，而是一整套用于减轻组织数字环境中风险的流程和能力。通过采用这一策略，各种规模的组织都可以通过持续监控和管理其面临的潜在攻击，从而增强其整体安全防御能力。Gartner 将其分为 5 个阶段：Scoping（资产范围界定）、Discovery（风险发现）、Prioritization（风险优先级排序）、Validation（风险验证）和 Mobilization（修复动员）[13]。通过这五个阶段的工作，CTEM 以一种动态的主动防御的思路，利用多个自动化技术组合去解决安全问题，以实现企业业务的持续性、稳定性和安全性。目前，

[13] 绿盟科技研究通讯. 应对攻击面的未来之路：持续威胁暴露管理（CTEM），2024-01。

我国的持续威胁暴露管理主要通过动态且持续的开展实网攻防演习，在演习过程中，政企机构综合运用渗透测试、威胁情报管理和漏洞扫描、资配漏补管理等多种工具和服务，了解潜在风险全景，并对潜在的关键风险和威胁进行管控[14]。在未来数年，持续威胁暴露管理技术一直是企业安全管理能力的建设重点。

（七）安全访问服务边缘

伴随边缘计算、云服务和混合网络的逐渐兴起，传统网络安全架构已无法适用，常常产生延迟、联网盲点、管理开销较大等问题，安全访问服务边缘（SASE）架构能够帮助解决以上问题，可以为企业提供全网流量的可见性，并对流量进行安全检测和路由转发，实现企业全流量的网络威胁检测与控制，同时能够根据应用优先级进行路由分类，确保用户访问体验和安全合规得到保障[15]。SASE 架构集成了多种网络安全功能，主要包括软件定义广域网（SD-WAN）、云原生安全服务、零信任网络访问（ZTNA）、边缘计算、全球就近接入点（PoPs）以及集中化策略管理等，对云服务进行了架构简化，降低企业对于硬件采购、维护和管理等成本，同时提供了包括加密、多因素身份验证、威胁保护和数据泄露防护等功能于一体的全面的集中化的安全防护措施。根据 Markets and Markets 公司测算，2023 年全球 SASE 市场规模

[14] 计算机与网络安全.2024 年十大安全技术趋势，2024-02。
[15] 云安全联盟大中华区. 《SASE 安全访问服务边缘白皮书》，2022-03。

约 19 亿美元，并将以 25%的复合增长率快速发展。随着数字化转型加速，移动设备和远程工作的普及使得边缘安全性和远程访问管理成为关键问题，促进了 SASE 在国内的应用和发展。预计未来 SASE 将进一步发展壮大，越来越多的企业网络架构将转向 SASE 技术。

（八）数据安全态势管理

数据安全态势管理（DSPM）是一种保护云数据的方法，最早由 Gartner 在 2022 年提出，指的是通过对本地和云上数据资产进行全面评估、分级分类以及漏洞修复，识别多个云环境和服务中的敏感数据并评估数据风险，是一种规范性的数据优先方法。随着数据量在云上激增，大量中间数据的位置和内容未知，数据安全风险大大增加。根据 IBM 发布的 2023 年数据泄露成本报告显示，82%的数据泄露涉及云环境中的存储数据。这些数据风险大多涉及“影子”数据，即备份、复制数据或复制到数据存储的数据。DSPM 通过创建和分析数据图和数据流以识别数据的具体位置以及用户访问情况，跟踪发现“影子”数据，并将这些数据纳入整体数据安全治理策略中。DSPM 的主要功能包括：数据安全策略实施、数据风险评估、数据分类、数据泄漏保护、数据访问监控、数据发现、数据风险补救、数据风险排序、数据所有者标识、数据合规性报告、数据流映射以及数据沿袭识别等[16]。目前国

[16] 安全牛. 如何做好数据安全态势管理，2023-08。

内 DSPM 产品落地实践仍有一段距离，随着未来云计算加速向各行各业渗透，云上数据交互使用将越来越频繁，越来越多云安全企业相继涌现，DSPM 及类似 DSPM 产品的落地应用将进一步提速。

（九）智能网联汽车安全

据公安部统计，截至 2023 年底，全国机动车保有量达 4.35 亿辆，其中汽车 3.36 亿辆；机动车驾驶人达 5.23 亿人，其中汽车驾驶人 4.86 亿人，车辆已经成为最重要的交通工具之一。随着数字技术的快速迭代和互联网的全面覆盖，汽车智能网联功能逐渐成为当前新车的标配。据中国汽车工业协会、共研产业咨询预测，智能电动汽车[17]的销售量将从 2023 年的 583.9 万辆增长至 2027 年的 2896.9 万辆。百度旗下的“萝卜快跑”无人驾驶网约车服务在武汉实现落地，投放车辆突破 400 辆，订单量快速增长。智能网联汽车的快速发展和正式商用使得汽车信息安全将成为继主动安全、被动安全、功能安全之后的第四大安全问题[18]。云端业务系统漏洞、数据泄露事件频发，车端复杂的功能形成更多的网络攻击面，严重的远程控车漏洞和近场通信漏洞时时出现[19]。对相关网络安全服务的需求加速爆发。根据虎符智库的分析数据，在过去一年中进入车联网安全领域的网络安全厂商数量同比上升

[17] 智能电动汽车指通过搭载先进传感器、控制器、执行器等装置，运用信息通信、互联网、大数据、云计算、人工智能等新技术，局域部分或完全自动驾驶功能，逐步成为智能移动空间的汽车。
[18] 虎符智库. 透过现象看本质，深度剖析宏观经济波动下的网安产业及 2024 年走向，2024-02。
[19] 绿盟科技研究通讯. 车联网安全技术现状、突破及趋势，2024-07。

18%，并且在近三年呈现了持续增长的趋势。车联网安全的核心能力涉及汽车专业领域的威胁分析与风险评估、渗透测试、漏洞管理、车辆安全运营中心、供应链安全及数据安全等，其中，车联网漏洞挖掘技术和车联网数据安全技术在近年来引起越发广泛的关注。漏洞挖掘技术可谓“双刃剑”，既可被黑客用于盗取敏感信息、攻击联网车辆等，也可被车联网安全“守门人”用于网络风险的预先检测修复。与传统的互联网云端服务基本类似，车联网的漏洞挖掘大多数也是对WEB、数据库、认证登录、邮件收发、文件传输、MQTT 等多类服务进行漏洞挖掘，进而获取管理员权限或关键业务系统数据[20]。车联网数据安全是在对相关数据进行科学的分类分级的基础上，综合运用隐私保护、数据脱敏、数据溯源、隐私计算等技术对数据的安全运营和合规使用进行保护。随着智能网联企业的更多商用落地，对相关网络和数据安全技术、产品和服务的要求将更高更广泛，进而带动技术、产品和服务供给的全面提升。

（十）低空经济网络安全

随着新兴技术飞速发展和社会需求日益多样化，低空经济作为一个新兴的经济形态，正逐步成为推动经济社会发展的新引擎。低空经济指的是在一定高度范围内，通过航空器、无人机等空中交通工具进行的经济活动。2024 年 3 月，“低

[20] 绿盟科技研究通讯.车联网安全技术现状、突破及趋势，2024-07。

空经济”首次写入政府工作报告；7 月 21 日，《中共中央关于进一步全面深化改革 推进中国式现代化的决定》对健全推动经济高质量发展体制机制作出部署，明确提出“发展通用航空和低空经济”。随着我国低空领域“云”“网”“端”的安全边界不断延展，接入终端数量、种类呈现指数级增长，网络攻击面将会越来越广、攻击手段越来越多样，传统“被动式”网络安全防护手段难以实现“结构性安全”的全面保障[21]。此外，低空经济市场需求进一步释放，其所需的算力、数据规模也会相应扩大，低空飞行器在执行测绘、航拍、取证、物流等任务时，装置搭载的摄像头、传感器将涉及大量数据处理行为，对于低空网络体系的各类关键信息基础设施的数据安全提出了更加严苛的要求。可以预见，探索低空经济网络和数据安全合规制度建设、引导低空飞行器生产者和运营使用者采取技术手段保护网络和数据安全等工作将加速提上日程。

五、我国网络安全产业发展展望

基于多年来对网络安全产业发展动向和趋势的深入分析研究，我国网络安全产业未来几年的发展态势作出如下展望：

（一）网络安全从风险防控、危机应对为主向全面提升网络安全弹性韧性转变

2023 年 7 月，中央网络安全和信息化工作会议传达了习

[21] 视联战略研究院. 打造低空智联网，护航低空经济安全发展，2024-08。

近平总书记对网络安全和信息化工作的重要指示，坚持党管互联网，坚持网信为民，坚持走中国特色治网之道，坚持统筹发展和安全，坚持筑牢国家网络安全屏障，坚持发挥信息化驱动引领作用，坚持推动构建网络空间命运共同体等，大力推动网信事业高质量发展，以网络强国建设新成效为全面建设社会主义现代化国家、全面推进中华民族伟大复兴作出新贡献。这体现了大网络安全工作格局的任务要求，将网络安全事业推向更高的战略位置，提出了更高更全面的工作要求。未来一段时间，清朗健康的网络环境建设、更细化更实操性的网络安全规则体系完善、攻防能力一体提升协同推进、开放合作的网络空间命运共同体构建将成为大网络安全工作的重要立足点。在此背景下，网络安全从风险防控化解向提高网络“弹性”和“韧性”转变，这也紧密贴合了全球网络安全治理的大趋势。欧盟《网络弹性法案》在欧盟理事会及欧洲达成临时协议，美国动态更新《国家网络安全战略》，通过将网络安全工作前置、网络安全责任下移、促进多方合作和承担共同责任、增强基础设施安全韧性等推动提升网络安全鲁棒性。未来，我国也将在构建大网络安全工作格局的指导下，进一步统筹发展和安全，持续提升网络安全弹性和韧性，为相关的技术攻关、产品研发、应用服务等提供了良好的发展空间。

（二）网络安全产品和服务的定制化需求越发凸显，产

业整合仍在继续

合规要求与安全需求是长期影响我国网络产业布局和企业投入的关键因素，法律规定、政策导向、标准规制仍将在很大程度上影响网络安全产业布局和企业投入方向。同时，数字经济纵深发展，各行各业数字化升级方兴未艾且行业化属性更加明显，因此，网络安全需求的专业化、碎片化更加明显，从而对定制化产品和服务的需求日益增长，特定行业的特定安全需求，需要由专业的团队持续跟踪、精深研究、长期投入，这给技术能力强的专业化创新企业提供了足够的生存空间，但也在一定程度上，导致网络安全中小企业往往难以摆脱单一业务的局限性，受市场波动影响明显，业务抗风险能力偏低。网络安全中小型创业企业往往会在做大做强和待价而沽之间权衡选择，因此，产业内部一直不乏合纵连横。无论从全球范围还是国内来看，网络安全行业巨头立足企业长远规划和业务发展定位，往往采用“产品收购”“企业并购”等多元方式来构筑“市场防波堤”，巩固提升行业领先地位和竞争优势。全球范围内，Palo Alto Networks、Crowdstrike、Fortinet、ZScaler、Check Point 等市值数百亿乃至过千亿的网络安全企业不断出现，IBM、Cisco 等电子信息技术巨头在网络安全领域也迅速占据主导地位，显著影响着全球网络安全市场结构和风险投资方的投资策略。从国内看，传统网络安全企业继续深耕，电信运营商、IT 厂商、数

字化服务商和集成商纷纷入局网络安全领域，持续扩大相关资源投入和业务拓展，产业整合仍在继续，产业集中度不断提高。可以看到，在可预见的未来，网络安全产业将形成行业龙头“顶天立地”，小美企业“遍地开花”的发展格局。

（三）网络安全问题泛化、杂糅等趋势将越来越突出

一是网络安全问题呈现泛化的特点。当前网络各类信息、数据、社交关系等存在被不法分子、敌对势力利用的可能性，网络意识形态背后映射的国家安全问题不再是国家主权、军事等面临威胁的战争状态，而是演变成一种更加日常、普遍、泛在的现象。与此同时，基于社交媒体平台的高度连结性、基于移动互联网的实时讯息传播、基于资讯聚合平台算法推荐造成的信息茧房，正在加速网络安全问题的发展过程。二是网络安全问题呈现面状发展、领域杂糅等特点。现阶段围绕互联网黑灰产业正以极快的速度发展蔓延，恶意绑定、病毒传播、撞库攻击、精准广告、隐私倒卖、网络诈骗等问题，形成了信息安全、经济安全、科技安全、社会安全、政治安全等多种安全问题杂糅的特点，如在作案模式方面，主要利用手机恶意广告推送或捆绑恶意软件，出售用户隐私实现广告变现；在发展趋势方面，从消费者端延伸到企业端，通过提供假的实名认证信息觅得市场，“刷票党”“羊毛党”“刷粉党”等现象频发；黑产觊觎信用建设等领域，各类买卖公民个人信息和篡改学历的案件高发；在技术手段方面，传统病

毒木马和电话诈骗等模式向更为先进的数据库撞库拖库、精准诈骗等模式发展。在这个过程中，网络安全问题成为杂糅了各类安全问题的复杂议题，经济的、社会的、文化的、信息的因素塑造着国家安全问题朝向更为总体的、动态的安全实践转化。

（四）企业维度的集中度提升与产品服务维度的模块化并存

一直以来，网络安全产业企业大多深耕具体细分领域，尤其是网络安全中小企业往往围绕有限的几个特定行业、特定安全需求开发和部署产品及服务。过去很长一段时间，网络安全产品和服务呈现出碎片化的现象。随着网络安全需求更加复杂，原来碎片化的安全能力建设开始向集约化、整合化、平台化转变，并且呈现出愈发模糊的网络安全边界。在这一背景下，一批大型综合性的网络安全企业成长壮大起来，并引发一系列企业间并购重组，越来越多的“一站式”网络安全解决方案提供商涌现出来，行业格局持续处在重构整合进程中。另一方面，出于对成本控制、效率提升、专业度增强等方面的考虑，企业不断推进网络安全服务 SaaS 化、工具化和模块化进程，亦即聚焦于解决某一种通用场景的安全问题，将网络安全需求进行分解，进而将满足相关需求的产品和服务分解为具有一定通用性、标准化的安全组件或服务模块，通过网络安全业务平台的搭建，将离散、碎片的安

全能力最小化、组件化集成于平台之中，更好地匹配用户企业业务逻辑和特性[22]，在降低安全企业运营成本的同时，提升产品服务的交付效率，从而实现安全研究、技术攻关、产品开发、服务运营等协同推进。

[22] 赛迪顾问. 2024 年网络安全行业趋势洞察——面向数智时代的网络安全：融合创新、回归本质，2024-01。

附件一 2023 年 9 月至今网络安全相关法律法规和政策列表

文件名称	发布部门	发布时间
《数字政府网络安全合规性指引》	国家信息中心	2023 年 9 月 6 日
《科技伦理审查办法(试行)》国科发监〔2023〕167 号	科技部、工业和信息化部等 10 部门	2023 年 9 月 7 日
《信息安全技术 网络安全保险应用指南（征求意见稿）》信安秘字〔2023〕132 号	全国信息安全标准化技术委员会	2023 年 9 月 13 日
《关于进一步加强网络侵权信息举报工作的指导意见》	中央网信办	2023 年 9 月 15 日
《未成年人网络保护条例》（国令第 766 号）	国务院第 15 次常务会议通过，2024 年 1 月 1 日起施行	2023 年 9 月 20 日
《关于依法惩治网络暴力违法犯罪的指导意见》（法发〔2023〕14 号）	最高人民法院、最高人民检察院、公安部	2023 年 9 月 25 日
《商用密码应用安全性评估管理办法》(国家密码管理局令第 3 号）	国家密码管理局	2023 年 9 月 26 日
《工业和信息化领域数据安全风险评估实施细则（试行）（征求意见稿）》	工业和信息化部网络安全管理局	2023 年 10 月 9 日
《电子政务电子认证服务管理办法(征求意见稿）》	国家密码管理局	2023 年 10 月 17 日
《全球人工智能治理倡议》	中央网信办	2023 年 10 月 18 日
《工业互联网安全分类分级管理办法(公开征求意见稿）》	工业和信息化部网络安全管理局	2023 年 10 月 24 日
关于做好《商用密码检测机构管理办法》和《商用密码应用安全性评估管理办法》实施工作的公告	国家密码管理局	2023 年 10 月 31 日
《工业和信息化领域数据安全行政处罚裁量指引（试行）（征求意见稿）》	工业和信息化部网络安全管理局	2023 年 11 月 23 日
《网络安全标准实践指南——网络安全产品互联互通 告警信息格式》	全国信息安全标准化技术委员会	2023 年 11 月 28 日
《网络安全事件报告管理办法（征求意见稿）》	国家互联网信息办公室	2023 年 12 月 8 日
《工业和信息化领域数据安全事件应急预案（试行）（征求意见稿）》	工业和信息化部网络安全管理局	2023 年 12 月 14 日
《铁路关键信息基础设施安全保护管理办法》	交通运输部	2023 年 12 月 17 日
《铁路关键信息基础设施安全保护管理办法》（中华人民共和国交通运输部令 2023 年第 20 号）	交通运输部	2023 年 12 月 17 日
工业领域数据安全标准体系建设指南（2023 版）》（工信部联科〔2023〕250 号）	工业和信息化部、国家标准化管理委员会	2023 年 12 月 19 日

文件名称	发布部门	发布时间
《区块链和分布式账本技术标准体系建设指南》（工信部联科〔2023〕260 号）	工业和信息化部、中央网信办、国标委	2023 年 12 月 28 日
《国家汽车芯片标准体系建设指南》（工信厅科〔2023〕80 号）	工业和信息化部办公厅	2023 年 12 月 29 日
《关于加强数据资产管理的指导意见》（财资〔2023〕141 号）	财政部	2023 年 12 月 31 日
《“数据要素 X”三年行动计划（2024—2026 年）》	国家数据局等、中央网信办、科技部、工业和信息化部、中国人民银行等十七部门	2024 年 1 月 4 日
《工业控制系统网络安全防护指南》（工信部网安〔2024〕14 号）	工业和信息化部	2024 年 1 月 30 日
《寄递服务用户个人信息安全管理办法(征求意见稿）》	国家邮政局	2024 年 2 月 1 日
《自然资源数字化治理能力提升总体方案》（自然资发〔2024〕33 号）	自然资源部	2024 年 2 月 5 日
《工业领域数据安全能力提升实施方案（2024-2026 年）》（工信部网安〔2024〕34 号）	工业和信息化部	2024 年 2 月 23 日
《中华人民共和国保守国家秘密法》（中华人民共和国主席令第 20 号）	2024 年 2 月 27 日第十四届全国人民代表大会常务委员会第八次会议第二次修订	2024 年 2 月 27 日
《生成式人工智能服务安全基本要求》（信安秘字〔2023〕146 号）	全国网络安全标准化技术委员会	2024 年 3 月 1 日
《民航数据管理办法》《民航数据共享管理办法》（征求意见稿）	中国民航局	2024 年 6 月 4 日
《促进和规范数据跨境流动规定》（国家互联网信息办公室令第 16 号）	国家网信办	2024 年 3 月 22 日
《数据出境安全评估申报指南（第二版）》、《个人信息出境标准合同备案指南（第二版）》	国家网信办	2024 年 3 月 22 日
《自然资源领域数据安全管理办法》（自然资发〔2024〕57 号）	自然资源部	2024 年 3 月 22 日
《银行保险机构数据安全管理办法(征求意见稿）》	国家金融监督管理总局	2024 年 3 月 22 日
《反保险欺诈工作办法（征求意见稿）》	国家金融监督管理总局	2024 年 4 月 11 日
《会计师事务所数据安全管理暂行办法》（财	财政部、国家网信办	2024 年 4 月 15 日

文件名称	发布部门	发布时间
会〔2024〕6 号）		
《关于规范移动互联网应用程序中登载使用地图行为的通知》（自然资办函〔2024〕972 号）	自然资源部办公厅、工业和信息化部办公厅	2024 年 4 月 24 日
《工业和信息化领域数据安全风险评估实施细则（试行）》（工信部网安〔2024〕82 号）	工业和信息化部	2024 年 5 月 10 日
《互联网政务应用安全管理规定》	中央网络安全和信息化委员会办公室、中央机构编制委员会办公室、工业和信息化部、公安部	2024 年 5 月 15 日
《电力网络安全事件应急预案》（国能发安全〔2024〕34 号）	国家能源局	2024 年 5 月 16 日
《关于建立碳足迹管理体系的实施方案》（环气候〔2024〕30 号）	生态环境部等十五部门	2024 年 5 月 22 日
《网络暴力信息治理规定》	国家网信办等四部门	2024 年 6 月 12 日
《国家智慧教育平台数字教育资源入库出库管理规范》	教育部	2024 年 6 月 16 日
《个人求助网络服务平台管理办法(征求意见稿）》	民政部	2024 年 6 月 19 日
《关于印发国家人工智能产业综合标准化体系建设指南（2024 版）的通知》（工信部联科〔2024〕113 号）	工业和信息化部、中央网络安全和信息化委员会办公室、国家发展和改革委员会、国家标准化管理委员会	2024 年 7 月 2 日
《电力监控系统安全防护规定》(征求意见稿）	国家发展和改革委员会	2024 年 7 月 25 日
《国家网络身份认证公共服务管理办法(征求意见稿）》	公安部、国家互联网信息办公室	2024 年 7 月 26 日

附件二 2024 年中国网安产业竞争力 50 强、成长之星、潜力之星

2024 年 5 月 11 日，中国网络安全产业联盟（CCIA）面向网络安全企业发布《关于开展我国网络安全产业现状调研的通知》（CCIA 秘〔2024〕008 号），组织开展我国网络安全产业现状调研工作。本次调研延续前六次产业调研模式，以具备网络安全产品、服务和解决方案销售收入的我国网络安全企业为目标研究对象，调研企业数量近 300 家，最终收集到了 160 家有效数据（数据周期区间为 2023 年 1 月 1 日至 2023 年 12 月 31 日）。依据调研数据，延续使用“资源力”和“竞争力”两个维度进行评估，最终得出 2024 年代表成熟期企业的中国网安产业竞争力 50 强、代表成长期企业的 10 家成长之星以及代表初创企业的 10 家潜力之星。

（一）评估指标

“资源力”指企业所拥有的资本、技术、人力等相关资源的多寡程度，资源的多寡会对企业的经营表现有直接而重要影响。主要参考指标包括是否为上市公司、公司收入规模、市值与估值、人员规模与人才质量、安全业务营收占比（新增指标）。

“竞争力”是指企业在当前商业模式下呈现出的总体能力，是企业所拥有的资源到经营成果的转化。竞争力强的企业，通常能高效地调动和运用相关资源，形成较高的竞争壁

垒，在市场中不断获得可观的经营回报。从我国网络安全企业的运营特点来看，对企业竞争力的量化评估从品牌、营销、产品、研发、服务和经营这六个维度展开。主要评估指标包括公众号影响力、官网影响力、百度品牌指数、安全业务营收和毛利、安全业务增长率、净利润率、收入构成情况、员工构成分布、服务资质、应急响应单位级别、销售许可证数量与级别、研发投入情况、专利情况、客户数量等。

（二）分析方法

针对成熟期企业，企业的经营数据能基本反映出企业运营情况，以及在市场中竞争力的强弱和发展潜力。因此在分析方法上，采取了定量分析的原则，主要基于企业公开数据，或者在调研过程中获得的企业经营数据进行评选。成熟期企业具体评价指标主要依据“资源力”和“竞争力”两个维度定量分析。

针对成长期企业，鉴于处于这一阶段的企业商业模式相对成熟，未来的业务重点和经营策略也基本确定。但是，由于企业处于高速增长阶段，经营数据不足以全面反映企业在市场竞争中的地位及未来的发展潜力，因此在分析方法上，采用了定量分析和定性分析并重的原则。在数据基础上从企业竞争力和成长性 2 个维度对企业综合能力进行画像。成长性指企业成长周期、人员规模和业务规模增长情况。

针对初创期企业，鉴于这一阶段的企业商业模式还处于

探索阶段，除企业经营数据之外，创始人及团队、公司市场定位和技术发展趋势等难以定量分析的因素对企业竞争力和发展潜力有着重要影响。因此，采用了定性分析为主，定量分析为辅的方法。在数据基础上从企业竞争力、成长性和资本热度 3 个维度对企业综合能力进行画像。资本热度主要从融资时间、融资轮次和企业估值等多个方面来考量企业的资本能力。

2024 年中国网安产业竞争力 50 强

序号	公司中文简称	公司中文全称
1	奇安信	奇安信科技集团股份有限公司
2	启明星辰	启明星辰信息技术集团股份有限公司
3	深信服	深信服科技股份有限公司
4	华为	华为技术有限公司
5	天融信	天融信科技集团股份有限公司
6	新华三	新华三信息安全技术有限公司
7	安恒信息	杭州安恒信息技术股份有限公司
8	亚信安全	亚信安全科技股份有限公司
9	绿盟科技	绿盟科技集团股份有限公司
10	三六零	三六零安全科技股份有限公司
11	电信安全	天翼安全科技有限公司
12	电科网安	中电科网络安全科技股份有限公司
13	迪普科技	杭州迪普科技股份有限公司
14	山石网科	北京山石网科信息技术有限公司
15	中孚信息	中孚信息股份有限公司
16	数字认证	北京数字认证股份有限公司
17	长亭科技	北京长亭科技有限公司
18	北信源	北京北信源软件股份有限公司
19	信安世纪	北京信安世纪科技股份有限公司
20	联通数科	联通数字科技有限公司
21	安天	安天科技集团股份有限公司
22	安博通	北京安博通科技股份有限公司
23	观安信息	上海观安信息技术股份有限公司
24	青藤云安全	北京升鑫网络科技有限公司
25	永信至诚	永信至诚科技集团股份有限公司
26	盛邦安全	远江盛邦（北京）网络安全科技股份有限公司

序号	公司中文简称	公司中文全称
27	威努特	北京威努特技术有限公司
28	恒安嘉新	恒安嘉新（北京）科技股份公司
29	格尔软件	格尔软件股份有限公司
30	微步在线	北京微步在线科技有限公司
31	长扬科技	长扬科技（北京）股份有限公司
32	三未信安	三未信安科技股份有限公司
33	吉大正元	长春吉大正元信息技术股份有限公司
34	默安科技	杭州默安科技有限公司
35	美创科技	杭州美创科技股份有限公司
36	网宿科技	网宿科技股份有限公司
37	明朝万达	北京明朝万达科技股份有限公司
38	安华金和	北京安华金和科技有限公司
39	天地和兴	北京天地和兴科技有限公司
40	南瑞信通	南京南瑞信息通信科技有限公司
41	国投智能	国投智能（厦门）信息股份有限公司
42	斗象科技	上海斗象信息科技有限公司
43	联软科技	深圳市联软科技股份有限公司
44	梆梆安全	北京梆梆安全科技有限公司
45	任子行	任子行网络技术股份有限公司
46	中睿天下	北京中睿天下信息技术有限公司
47	瑞数信息	瑞数信息技术（上海）有限公司
48	指掌易	北京指掌易科技有限公司
49	珞安科技	北京珞安科技有限责任公司
50	芯盾时代	北京芯盾时代科技有限公司

2024 年中国网安产业成长之星

序号	公司中文简称	公司中文全称	业务领域
1	海云安	深圳海云安网络安全技术有限公司	开发安全/数据安全
2	万物安全	深圳万物安全科技有限公司	物联网安全/网络资产测绘
3	华云安	北京华云安信息技术有限公司	攻击面管理/威胁管理
4	六方云	北京六方云信息技术有限公司	工业互联网安全
5	保旺达	江苏保旺达软件技术有限公司	数据安全/数据分类分级
6	安芯网盾	安芯网盾（北京）科技有限公司	内存安全/端点安全
7	烽台科技	烽台科技（北京）有限公司	工控安全靶场/工控安全咨询
8	中信网安	福建中信网安信息科技有限公司	数据安全/安全服务
9	赛宁网安	南京赛宁信息技术有限公司	网络靶场/攻防演练
10	小佑科技	北京小佑科技有限公司	云原生安全/容器安全

2024 年中国网安产业潜力之星

序号	公司的中文简称	公司的中文全称	业务领域
1	亿格云	杭州亿格云科技有限公司	SASE/零信任
2	丈八网安	北京丈八网络安全科技有限公司	网络靶场/攻防演练
3	知其安科技	北京知其安科技有限公司	安全有效性验证/BAS
4	数安行	北京数安行科技有限公司	数据安全/个人隐私保护
5	矢安科技	上海矢安科技有限公司	BAS/攻击面管理
6	观成科技	北京观成科技有限公司	加密流量检测
7	安全玻璃盒	杭州孝道科技有限公司	DevSecOps/软件供应链安全
8	软安科技	软安科技有限公司	软件供应链安全/开发安全
9	魔方安全	深圳市魔方安全科技有限公司	攻击面管理/漏洞管理
10	齐安科技	浙江齐安信息科技有限公司	工业互联网安全