2024年中国网络空间安全治理行业概览

网络安全前沿，
中国政策与技术进步护航数字经济

概念标签：网络空间、安全治理、安全生态

China Cybersecurity Governance Industry

中国サイバーセキュリティガバナンス産業

研究目标

研究目的

了解中国网络空间安全治理的发展演变、关键技术，分析中国网络空间安全治理的产业链、应用领域、行业市场规模以及未来发展趋势。

研究目标

- 了解中国网络空间安全治理的定义、分类、演变
- 分析中国网络空间安全治理的关键技术和应用
- 探析中国网络空间安全治理行业产业链情况
- 预判中国网络空间安全治理行业发展态势

本报告的关键问题

- 市场空间：中国网络空间安全治理行业市场规模情况如何？未来增长情况如何？
- 产业链情况：中国网络空间安全治理各类型厂商所在的产业链构成是怎样的？未来格局会如何演化？
- 核心技术：中国网络空间安全治理技术架构是怎样的？核心技术有哪些？

观点摘要

市场规模与增长预测

中国网络空间安全治理行业在2023年的市场规模为640亿元，预计到2026年将达到752亿元，并在2028年突破800亿元大关。这一增长主要得益于技术创新、政府支持及各行业对智能化解决方案需求的增加。

市场扩大的驱动因素

技术创新与发展推动了网络安全治理能力的提升，满足了大规模数据处理的需求；政府对高科技领域的大力支持和各行业对智能化解决方案的需求增长，加之5G网络和数据中心等基础设施的完善，共同促进了市场的快速发展。

未来发展方向与关键技术

网络空间安全治理行业将重点发展蜜点、蜜庭、蜜阵和蜜洞技术，构建更加主动和智能的安全防御系统。抗量子密码（PQC）作为新一代密码算法，是确保未来网络安全的关键技术之一，国内外都在积极推进其标准化和应用。

综合活动与多层面合作

网络空间安全治理涉及政策制定、技术研发、标准建立、风险评估与管理、教育培训及国际合作等多个方面，通过有效的政策引导、标准化建设、技术创新、风险管理、人才培养以及国际合作，构建一个健康有序且充满活力的网络空间安全环境，确保ICT基础设施的安全性和稳定性。

内容目录

名词解释

- **数字化转型：**是指组织、企业或社会采用数字技术来重新设计或优化其业务、流程、文化和客户体验的过程。这种转型旨在充分利用数字技术的威力，提高效率、创造价值、增强创新，并适应不断变化的市场和技术环境。
- **机器学习：**是一种人工智能（Artificial Intelligence，AI）的分支领域，它致力于通过构建和训练计算机程序，使其具有从数据中学习的能力，从而能够在面对新数据时做出预测或做出决策。机器学习侧重于开发算法和模型，让计算机系统能够通过学习经验数据而不是通过明确编程来完成特定任务。
- **算力度量：**算力度量是一种用于评估计算机系统、网络或硬件设备性能和能力的手段。其涵盖多个方面，包括浮点运算性能（FLOPS），整数运算性能（IOPS），数据传输速度（带宽），响应时间（延迟），处理能力（吞吐量），存储容量等。这些度量标准的选择取决于特定应用场景和需求，而在算力网络等领域，可能存在一些专门用于衡量分布式计算和网络性能的度量标准。
- **算力池化：**算力池化是一种依托云计算技术整合异构算力资源，实现资源集中调度和按需分配的技术。它的目标是提升资源效率、降低成本。算力池化通过物理成池和逻辑成池，实现算力资源的充分利用和碎片最小化，使得资源可以被极致利用。
- **预训练模型：**是指在大量数据上进行预先训练的机器学习模型，通常用于深度学习领域。这些模型在特定的任务上训练得到，能够学习到通用的特征表示，然后将这些学习到的知识和特征应用到其他相关任务上，从而减少对标注数据的依赖，加快训练速度，并提高模型的性能。
- **异构计算架构：**是一种结合了不同类型处理器的计算方式，这些处理器具有不同的体系结构和指令集。这种计算模式能够有效地利用各种计算资源，以满足不同的计算需求，并使代码能够以获取最大总体性能的方式执行。异构计算系统通常由以下几部分组成：一组异构机器、将这些机器连接起来的高速网络，以及相应的异构计算支撑软件。

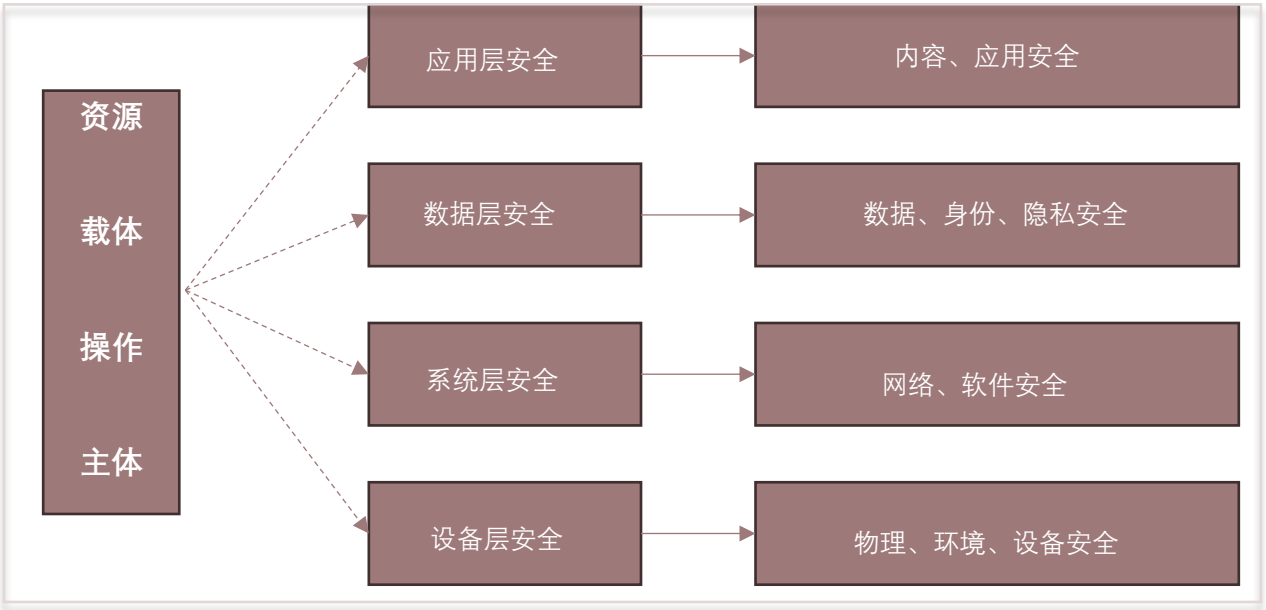
Chapter 1
行业综述

- 网络空间安全治理行业围绕保障信息和通信技术（ICT）基础设施的安全、保护数据隐私以及维护互联网服务的正常运行，涉及政策制定、技术研发、标准建立、风险评估与管理、教育培训及国际合作等多方面的综合活动，旨在确保网络空间的安全性、稳定性和可靠性，防止恶意行为对个人、企业乃至国家安全造成威胁。
- 2023年中国网络空间安全治理行业市场规模为640亿元，预计2026年将实现较大幅度增长，将达到752亿元，预计到2028年，中国网络安全市场规模将超过800亿元。这一增长不仅反映了市场对网络安全产品和服务需求的提升，也体现了国家和社会各界对网络安全重视程度的加深。随着技术的进步和应用场景的不断扩展，网络安全产业将迎来更加广阔的发展空间。

中国网络空间安全治理行业综述——定义

- 网络空间安全治理行业是一个多层次、多维度的复杂体系，各个层面相互依存、相辅相成，通过有效的政策引导、标准化建设、技术创新、风险管理等，才能构建一个健康有序且充满活力的网络空间安全环境

网络空间安全治理体系架构



■ **网络空间安全治理行业是一个多层次、多维度的复杂体系，各个层面相互依存、相辅相成**

网络空间安全治理行业围绕保障信息和通信技术（ICT）基础设施的安全、保护数据隐私以及维护互联网服务的正常运行，涉及政策制定、技术研发、标准建立、风险评估与管理、教育培训及国际合作等多方面的综合活动，旨在确保网络空间的安全性、稳定性和可靠性，防止恶意行为对个人、企业乃至国家安全造成威胁。

在政策法规层面上，由国家或国际组织发布的法律法规如《网络安全法》、《数据保护条例》等构成最高层次的指导框架；标准规范层面则包括国际、国家及行业标准，为网络安全产品和服务提供一致性要求和技术指南；

技术研发层面涵盖防火墙、入侵检测系统、防病毒软件等多项技术创新，并逐步融入人工智能、量子计算等新兴技术；风险评估与管理层专注于识别潜在威胁、评估现有防御措施并提出改进建议，同时进行安全审计和合规检查；教育培训层面提高全社会的网络安全意识和技术水平，培养专业人才；

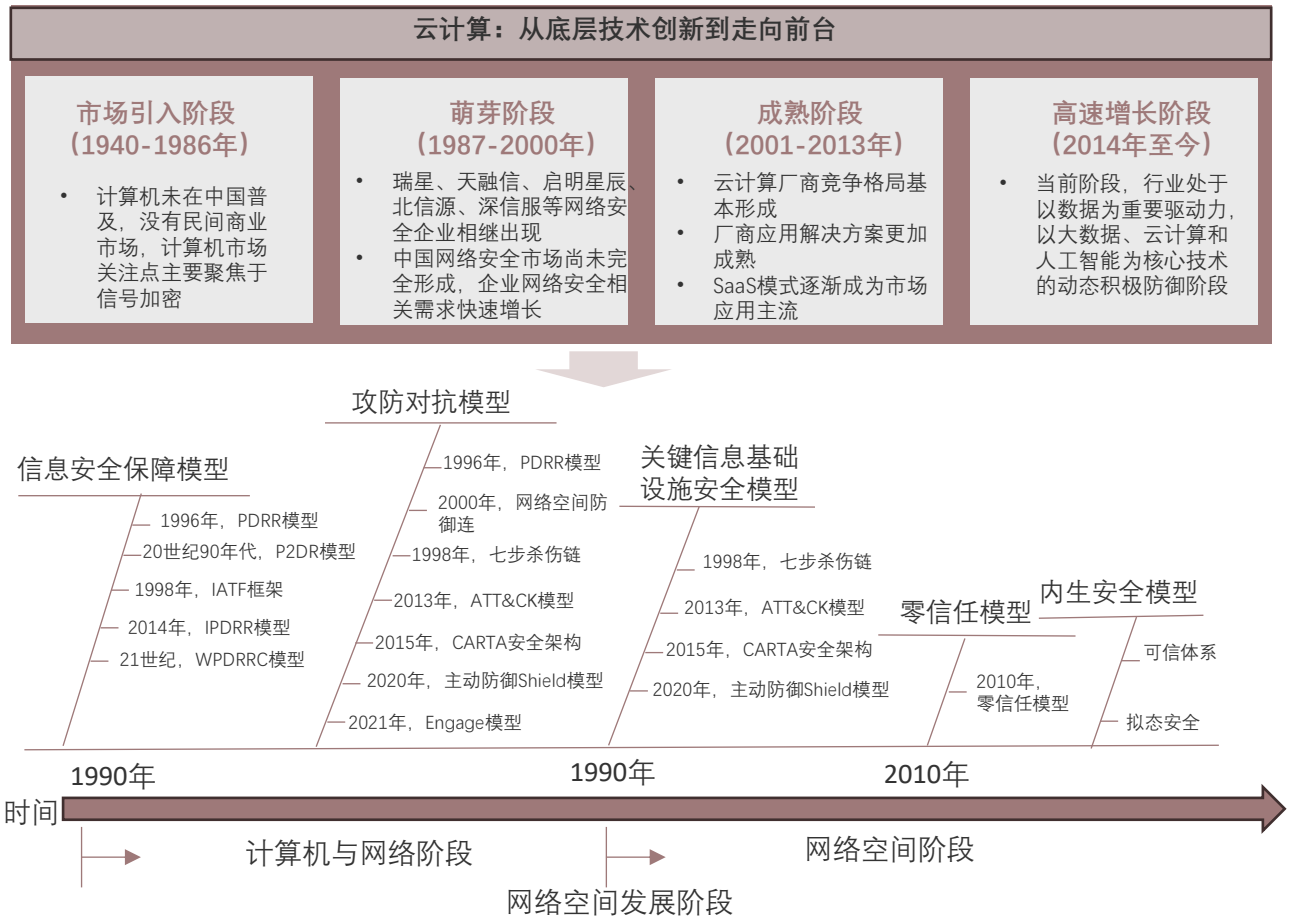
国际合作层面促进各国政府和企业间的交流协作，共同应对全球性挑战；市场服务层面则由各类商业机构提供的定制化安全解决方案和服务组成。通过有效的政策引导、标准化建设、技术创新、风险管理、人才培养以及国际合作，各个层面相互依存、相辅相成，构建一个健康有序且充满活力的网络空间安全环境。

来源：通信世界，头豹研究院

中国网络空间安全治理行业综述——发展历程

- 网络空间安全治理的发展历程经历了从概念萌芽到概念形成，再到快速发展和高速发展的几个阶段。每个阶段都有其特定的发展特点和标志性事件，反映了网络空间安全治理从无到有，再到成熟应用的过程

中国网络空间安全治理的发展历程，1940年至今



■ **网络空间安全治理的发展历程可大致分为四个阶段**

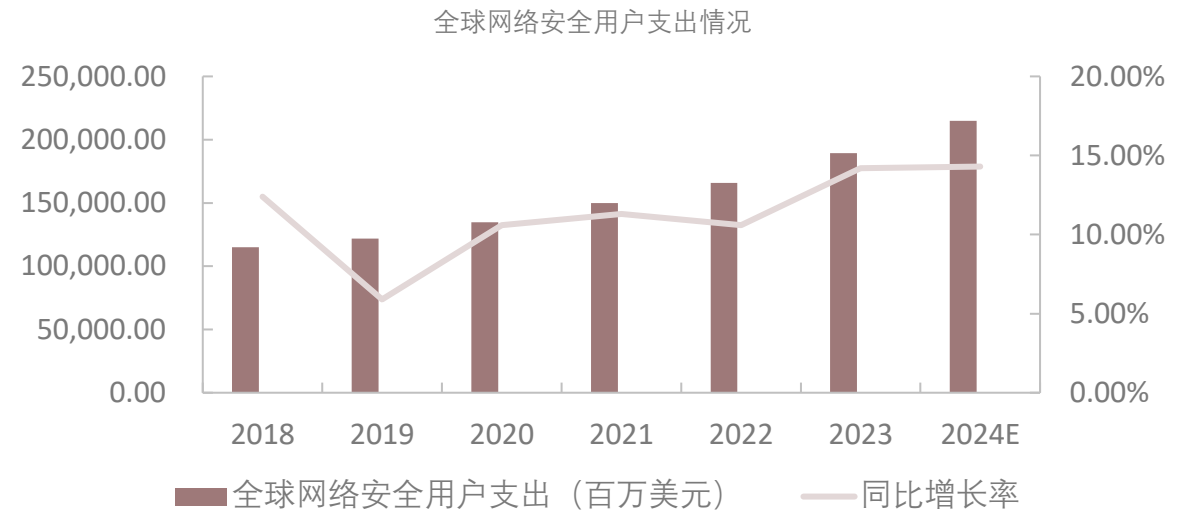
从1940年至1986年的市场引入阶段，当时计算机技术和互联网开始萌芽，主要用于军事、政府和科研机构，网络安全主要集中在物理安全性和数据保密性；随后进入1987年至2000年的萌芽阶段，随着互联网商业化和个人使用量增加，网络安全问题逐渐显现，标志性事件如1988年的莫里斯蠕虫促使人们重视网络安全，期间出现了防火墙、入侵检测系统（IDS）、SSL/TLS加密协议等基础性技术和协议；自2014年起进入高速增长阶段，云计算、大数据、物联网（IoT）、5G通信等新兴技术的应用使网络安全挑战更加复杂多样，高级持续性威胁（APT）、零日漏洞利用、勒索软件等新型攻击手段层出不穷，各国政府纷纷出台严格的网络安全政策和法规，时人工智能、机器学习等先进技术也被应用于网络安全领域，提高了威胁检测和响应的速度与准确性。

来源：存储随笔，专家访谈，头豹研究院

中国网络空间安全治理行业综述——发展现状

- 网络空间安全治理行业正迅速发展以应对数字化转型带来的海量数据处理需求，算力成为国家竞争力的关键，推动着智慧城市和AI产业化的进步

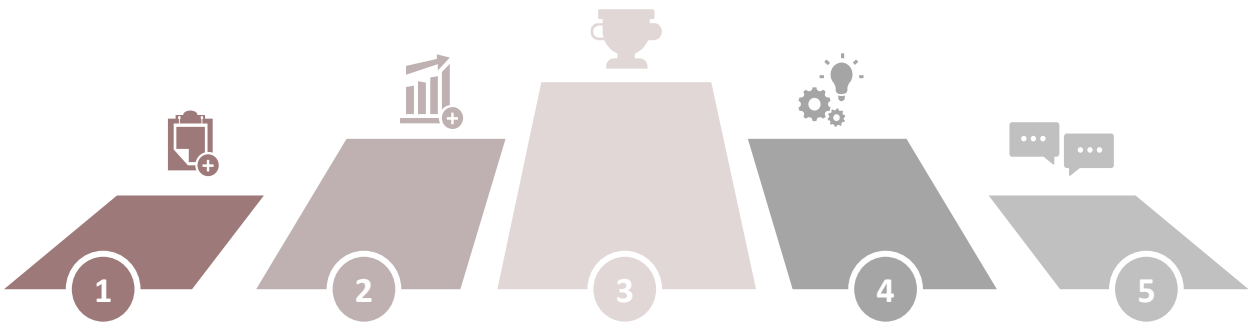
全球网络空间安全治理发展现状



全球网络安全市场支出不断攀升

从2019年至2024年，全球网络安全支出同比增速持续上升，预计2024年将达到2149.5亿美元，同比增长14.3%，显示出全球范围内对网络安全的强劲需求。在细分领域中，安全服务、基础设施保护和网络安全设备的支出占比最高，2024年预计将分别占总支出的41.9%、15.5%和11.3%。这表明企业在增强网络安全防护能力的同时，更加重视综合性的安全服务和关键基础设施的安全保障

2022-2023全球网络空间安全发展态势特征



1. 网络军事和网络冲突：全球网络冲突加剧，战争和冲突思维充分蔓延到网络空间
2. 各国正以反垄断、数据安全及隐私保护为由强化其数字领域的法律法规
3. 数字冷战路线崛起，国家安全、意识形态、地缘政治冲击数字经济和数字贸易
4. 威胁演化与防护升级：网络犯罪持续增加，各国积极监管网络空间
5. 虚假信息在全球加速蔓延：各国持续推进网络信息内容监管，虚假信息治理武器化显现

来源：中国信通院，大数据产业联盟，头豹研究院

中国网络空间安全治理行业综述——行业市场规模

- 虽然短期内宏观经济等因素对网络安全产业造成了影响，但从长远来看，随着政策环境的优化和技术应用的深化，网络安全产业将继续保持稳健的增长态势，并逐步迈向高质量发展的新阶段

中国网络安全产业市场规模，2019年-2026年预测

单位：[亿元]

首席分析师：oliver.yuan@leadleo.com

主笔分析师：ruowei.lin@leadleo.com

从业人员总数达到91,798人。

展望未来，随着国家对网络安全产业顶层设计的不断完善，相关政策基础愈加稳固，数字经济的加速发展将为网络安全产业注入新的动力。预计在政策支持、技术创新和市场需求的多重驱动下，网络安全生态将进一步拓展。运营商、IT厂商、集成商等各方纷纷加大在网络安全业务板块的投入，其他软件产业的细分领域也将逐步涉足网络安全业务。这些积极因素有望改善当前行业发展较为滞缓的局面，推动网络安全产业增速逐步回升。

具体而言，预计到2028年，中国网络安全市场规模将超过800亿元。这一增长不仅反映了市场对网络安全产品和服务需求的提升，也体现了国家和社会各界对网络安全重视程度的加深。随着技术的进步和应用场景的不断扩展，网络安全产业将迎来更加广阔的发展空间，成为保障国家信息安全和社会经济稳定的重要力量。

来源：专家访谈，头豹研究院

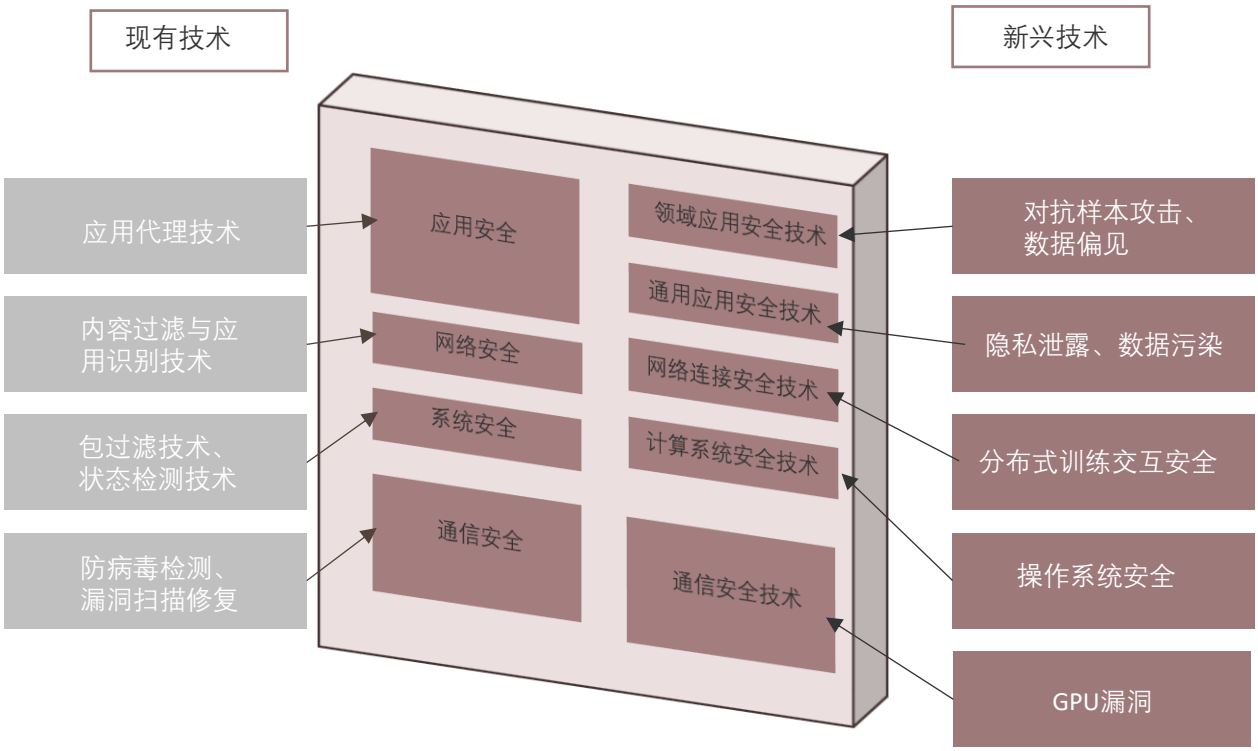
Chapter 2
产业链分析

- 网络空间安全治理正面临多重复杂挑战，涵盖技术发展、不同年龄群体的数字素养差异、平台治理和用户信息保护不足以及网络舆情治理机制的不完善
- 综合对比分析中国网络安全企业的调研数据和上市公司的公开财务信息，2023年华北、华东和华南地区的网络安全市场份额分别为38%、23%及14%。华北和华南地区对网络安全的投入进一步加大，使得这两个区域的市场占比有所提升。与此同时，近年来网络安全企业在技术和资本积累方面取得了显著进展，为其国际化扩展奠定了坚实基础。

中国网络空间安全治理行业产业链分析——技术路线

- 网络空间安全治理的技术路线涵盖了从基础防御到高级威胁检测的一系列方法论和技术手段。随着新的挑战不断涌现，技术路线也在持续演进，旨在构建一个更加坚固、灵活且具有前瞻性的网络安全体系

网络空间安全体系框架的应用分析



网络空间安全治理的技术路线涵盖了从基础防御到高级威胁检测的一系列方法论和技术手段

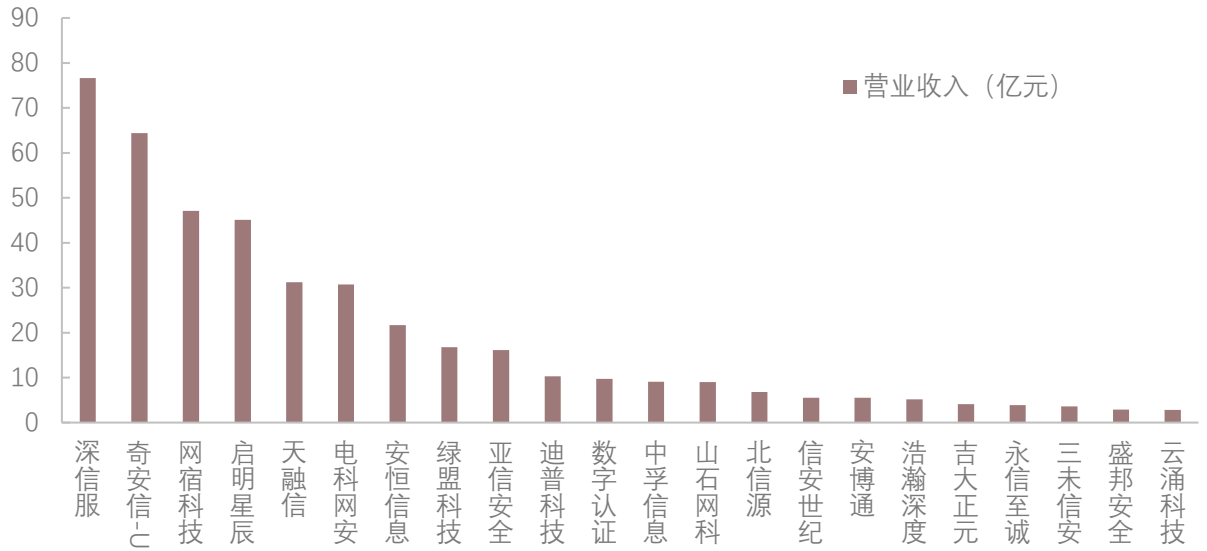
网络空间安全治理的技术路线是一个综合性的框架，结合了多种技术、工具和策略来保障信息系统的安全性。这包括边界防护（如防火墙、入侵检测/预防系统IDS/IPS）和端点保护（如防病毒软件、端点检测与响应EDR），以及应用安全措施（如Web应用防火墙WAF、代码审计和漏洞扫描）。在加密与认证方面，采用数据加密（如传输层安全协议TLS/SSL、磁盘加密）和身份验证与访问控制（如多因素认证MFA、单点登录SSO、权限管理）。威胁情报与态势感知技术，例如威胁情报平台TIP、自动化情报交换格式STIX/TAXII、安全信息和事件管理SIEM、网络安全运营中心CSOC，用于收集分析情报并提供实时监控。应急响应与恢复能力涵盖事件响应计划（如计算机应急响应团队CERT、事故响应手册）和备份与灾难恢复措施。安全意识教育与培训通过员工培训和模拟钓鱼攻击测试构建安全文化。新兴技术如人工智能与机器学习应用于智能威胁检测和自适应安全架构ASA，而区块链技术则用于分布式账本和去中心化身份管理，减少单点故障风险。综上所述，这些技术路线不仅涵盖了从基础防御到高级威胁检测的方法论和技术手段，而且随着信息技术的发展持续演进，旨在构建一个更加坚固、灵活且具有前瞻性的网络安全体系。

来源：华为官网，头豹研究院

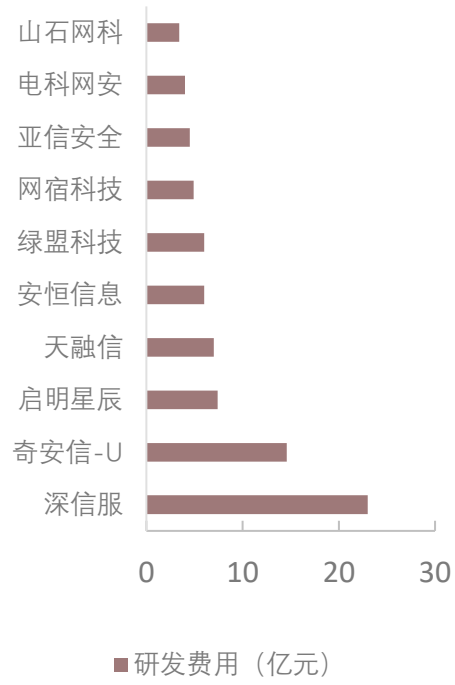
中国网络空间安全治理行业产业链分析——厂商情况

- 随着技术实力的不断增强和国际市场的进一步开拓，中国网络安全企业有望在全球范围内占据更加重要的位置，形成具有国际竞争力的安全产业生态

中国网络空间安全治理厂商情况



2023年代表企业前10研发投入及增速



网络空间安全治理的主要参与者较多，其在网络空间安全治理生态系统中扮演着不同的角色

综合对比分析中国网络安全企业的调研数据和上市公司的公开财务信息，2023年华北、华东和华南地区的网络安全市场份额分别为38%、23%及14%。华北和华南地区对网络安全的投入进一步加大，使得这两个区域的市场占比有所提升。与此同时，近年来网络安全企业在技术和资本积累方面取得了显著进展，为其国际化扩展奠定了坚实基础。

具体而言，奇安信、深信服、绿盟科技等领军企业在海外业务上的表现尤为突出，创新型企业也在积极尝试突破国际市场，2023年取得了一定的成绩。数据显示，海外市场占比延续了小幅提升的趋势。根据公开资料，目前已有50多家中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，而在中东地区布局的企业数量约为20家左右。此外，拉美和欧洲等地区正逐渐成为中国网络安全企业“出海”的热门目的地。

展望未来，随着中国网络安全企业技术实力的不断增强和国际市场的持续开拓，海外市场有望成为中国网络安全企业新的业务增长点。预计这些企业将进一步深化在东南亚、中东、拉美和欧洲等重点区域的业务布局，通过提供定制化的安全解决方案和服务，满足不同市场的多样化需求，从而在全球竞争中占据有利位置。

来源：专家访谈，头豹研究院

中国网络空间安全治理行业产业链分析——行业应用

- 各关键行业对网络安全项目的重视程度和投资力度不断加大，旨在构建全面且高效的网络安全防护体系，以应对日益复杂多变的网络威胁环境

2023年网络安全的行业应用

首席分析师：oliver.yuan@leadleo.com

主笔分析师：ruowei.lin@leadleo.com

作为信息传输的主要通道，其安全性至关重要；军工行业涉及国家安全的核心部门，需防范各种威胁；公检法司的信息系统存储大量案件资料和个人隐私，完善的网络安全措施是保障司法公正的前提；医疗行业需保护患者隐私和医疗数据安全；交通行业直接影响公众出行的安全性和效率；教育行业则需确保学生个人信息和技术资源的安全。

随着全球数字化转型的加速，网络空间安全治理在各行业的应用正迎来前所未有的发展机遇与挑战。各国政府日益重视网络安全，不断出台严格的法律法规，推动企业加大安全治理投入以确保合规性。与此同时，人工智能（AI）、机器学习（ML）、区块链等新兴技术正在重塑网络安全治理方式，提高防护水平并促进跨行业合作；而量子计算的发展也促使抗量子密码学成为研究热点。不同行业因其特有的业务流程和技术需求，对网络安全治理有着不同的侧重点，未来的安全治理将更加注重提供针对性强、适应性强的定制化解决方案。零信任安全模型主张“永不信任，始终验证”，预计将在更多行业中广泛应用，特别是在远程办公常态化和云计算普及的背景下。

来源：深圳市云计算技术与应用协会，头豹研究院

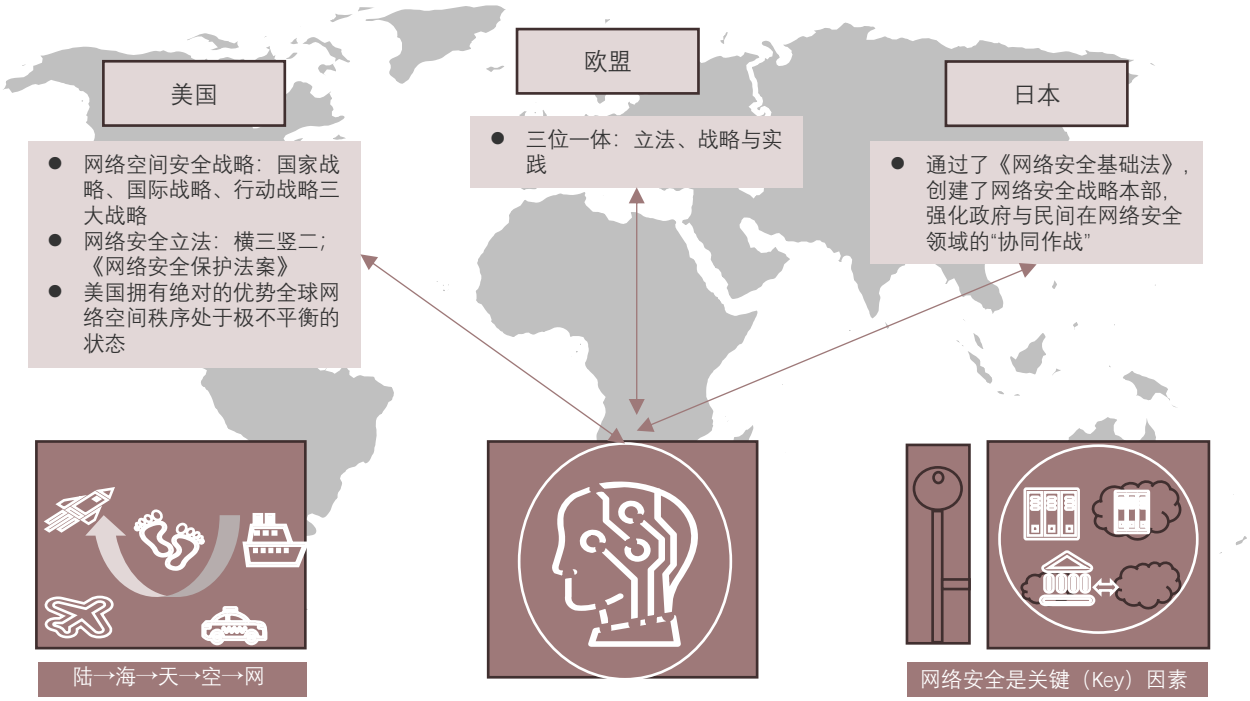
Chapter 3
行业发展分析

- 中国网络空间安全治理行业政策分析
- 中国网络空间安全治理行业发展趋势
- 中国网络空间安全治理行业竞争格局

中国网络空间安全治理行业分析——政策分析（1/2）

- 全球网络空间安全治理行业政策的主要目标是通过鼓励投资、创新和合作，支持人工智能算力的建设，以满足不断增长的技术应用需求

全球网络空间安全治理行业相关政策机制与分析



各国发布指导文件和措施支撑网络空间安全发展

美国

- ✓ 白宫发布《国家网络安全战略》
- ✓ NIST发布《对联邦漏洞披露指南的建议》
- ✓ 白宫发布《国家网络安全战略实施计划》
- ✓ 白宫发布《国家网络人才和教育战略》
- ✓ 国防部发布《2023年国防部网络战略》
- ✓ 网络安全和基础设施安全局发布《为供水公司提供免费的网络漏洞扫描》情况说明书
- ✓ 网络安全和基础设施安全局发布《CISA开源软件安全路线图》
- ✓ 网络安全和基础设施安全局宣布修订《国家网络事件响应计划》

欧盟

- ✓ 国防部发布《2023年国防部网络战略》
- ✓ 欧洲议会和理事会发布了《欧盟数字十年网络安全战略》
- ✓ 欧盟提议将网络安全认证作为法定要求，并加强关键基础设施领域的标准和认证制定

来源：国务院，头豹研究院

中国网络空间安全治理行业分析——政策分析（2/2）

- 中国网络空间安全治理行业政策的主要目标是通过鼓励投资、创新和合作，支持网络空间安全体系建设，以满足不断增长的技术应用需求

中国网络空间安全治理行业相关政策机制与分析，2023-2024年

国家互联网信息办公室	2024-06	《网络暴力信息治理规定》 网络暴力信息治理不仅是对特定问题的回应，更是整体网络空间安全治理体系不可或缺的一部分。
工信部	2024-05	《工业和信息化领域数据安全风险评估实施细则》 既为企业提供了具体的指导方针，也为政府监管部门设定了清晰的工作边界。
国家信息中心	2023-9	《数字政府网络安全合规性指引》 不仅是指导数字政府建设的重要文件，也为整个网络空间安全治理行业指明发展方向，带来了积极而持久的影响。
科技部、工业和信息化部等10部门	2023-9	《科技伦理审查办法（试行）》国科发监[2023]167号 不仅为中国科技伦理治理提供了详细的指引和支持，也对网络空间安全治理行业产生了积极的影响。
全国信息安全标准化技术委员会	2024-08	《信息安全技术 网络安全保险应用指南》 不仅是指导网络安全保险业务操作的技术文件，更为网络空间安全治理行业注入了新的活力。
中央网信办	2024-08	《关于进一步加强网络侵权信息举报工作的指导意见》 不仅是指导网络侵权信息举报工作的重要文件，也为网络空间安全治理行业指明了发展方向。
国务院	2024-08	《未成年人网络保护条例》 网络暴力信息治理不仅是对特定问题的回应，更是整体网络空间安全治理体系不可或缺的一部分。
最高人民法院、最高人民检察院、公安部	2024-08	《关于依法惩治网络暴力违法犯罪的指导意见》 强调利用先进技术手段如人工智能、大数据分析等进行监测预警和识别处置。这将激励科技公司加大研发投入。
国家秘密管理局	2024-08	《商用密码应用安全性评估管理办法》 不仅提升了商用密码应用的专业化水平和服务质量，还促进了技术创新和社会各界的广泛参与。

来源：云计算开源产业联盟，专家访谈，头豹研究院

Chapter 4
典型厂商分析

- 任子行
- 奇安信
- 美亚柏科

方法论

- 头豹研究院布局中国市场，深入研究19大行业，持续跟踪532个垂直行业的市场变化，已沉淀超过100万行业研究价值数据元素，完成超过1万个独立的研究咨询项目。

- 研究院依托中国活跃的经济环境，研究内容覆盖整个行业的发展周期，伴随着行业中企业的创立，发展，扩张，到企业走向上市及上市后的成熟期，研究院的各行业研究员探索和评估行业中多变的产业模式，企业的商业模式和运营模式，以专业的视野解读行业的沿革。

- 研究院融合传统与新型的研究方法，采用自主研发的算法，结合行业交叉的大数据，以多元化的调研方法，挖掘定量数据背后的逻辑，分析定性内容背后的观点，客观和真实地阐述行业的现状，前瞻性地预测行业未来的发展趋势，在研究院的每一份研究报告中，完整地呈现行业的过去，现在和未来。

- 研究院密切关注行业发展最新动向，报告内容及数据会随着行业发展、技术革新、竞争格局变化、政策法规颁布、市场调研深入，保持不断更新与优化。

- 研究院秉承匠心研究，砥砺前行的宗旨，从战略的角度分析行业，从执行的层面阅读行业，为每一个行业的报告阅读者提供值得品鉴的研究报告。

法律声明

业务合作

会员账号

可阅读全部原创报告和百万数据，提供PC及移动端，方便触达平台内容

定制报告/词条

行企研究多模态搜索引擎及数据库，募投可研、尽调、IRPR等研究咨询

定制白皮书

对产业及细分行业进行现状梳理和趋势洞察，输出全局观深度研究报告

招股书引用

研究覆盖国民经济19+核心产业，内容可授权引用至上市文件、年报

市场地位确认

对客户竞争优势进行评估和证明，助力企业价值提升及品牌影响力传播

行研训练营

依托完善行业研究体系，帮助学生掌握行业研究能力，丰富简历履历

报告作者

袁栩聪
首席分析师
oliver.yuan@leadleo.com

莫舒棋
行业分析师
kay.mo@leadleo.com

业务咨询

- **客服电话：400-072-5588**
- **官方网站：www.leadleo.com**

深圳办公室

广东省深圳市南山区粤海街道华润置地大厦E座4105室

邮编：518057

上海办公室

上海市静安区南京西1717号会德丰国际广场 2701室

邮编：200040

南京办公室

江苏省南京市栖霞区经济开发区兴智科技园B栋401

邮编：210046