2020 年数字安全十大产业方向、十大技术赛道研究报告

指导单位：工业和信息化部网络安全管理局

编制单位：中国信息通信研究院

数字中国产业发展联盟

2020 年 12 月

引言

近年来，伴随着信息通信技术的快速发展，数字产业化和产业数字化的发展日新月异，数字技术与实体经济深度融合，传统产业的数字化和智能化水平不断提高，带来数字经济的快速发展和相关产业的转型升级，并助力国家治理体系和治理能力现代化。

数字经济的发展时刻面临着安全问题的挑战。一是网络技术层的问题，例如恶意程序、软件漏洞、黑客攻击等，伴随新一代信息技术升级，将呈现出更加多样化、精准化、规模化的态势。二是社会层面的问题，例如数据安全、隐私保护、不良信息等，涉及监督管理和标准规范，需要社会各界共同应对。三是经济层面的问题，随着数字经济融合程度加深，个人和各类组织机构的数字资产日益增长，伴随而来的经济风险随之提升。

数字经济高质量发展离不开数字安全产业的保障支撑。2019 年 12 月 26 日，在工业和信息化部网络安全管理局（以下称工信部网安局）指导下，中国信息通信研究院（以下称中国信通院）和数字中国产业发展联盟正式启动“2020 年数字安全十大产业方向、十大技术赛道”征集活动，受到社会各界的广泛关注。目前，已遴选出“数字安全十大产业方向与十大技术赛道”，为政府和企业在数字安全产业的布局和发展起到了良好的引领作用。

经过遴选，2020 年数字安全十大产业方向为**工业互联网安全、物**

联网安全、关键信息基础设施安全、云安全、人工智能安全、智慧城市安全、5G 应用安全、大数据安全、车联网安全、智慧医疗安全；数字安全十大技术赛道为人工智能安全技术、区块链安全技术、边缘计算安全技术、敏感数据识别技术、生物特征识别技术、软件定义安全技术、安全多方计算技术、量子通信安全技术、商用密码技术、网络切片安全技术。本报告围绕上述二十大主题，结合领域专家与企业代表的调研访谈，系统梳理了发展背景、产业环节、市场需求、典型案例和应用等关键内容，对数字安全产业的高质量发展提供参考和借鉴。

目录

第一章 数字安全产业发展概况

近年来，我国数字经济蓬勃发展，各行各业正处于数字化转型的关键阶段，数字经济相关的服务和产品不断涌现，数字安全产业快速发展壮大。**数字安全产业**指，面向政府和企业在数字化转型过程中，针对管理、决策、服务、运营、合作等环节潜在的安全风险和威胁，提供安全防控能力的产业。数字安全产业在国家政策引领、数字经济高质量发展、新型基础设施建设等驱动因素带动下，从网络空间向经济社会各领域加快延伸，边界不断拓展。

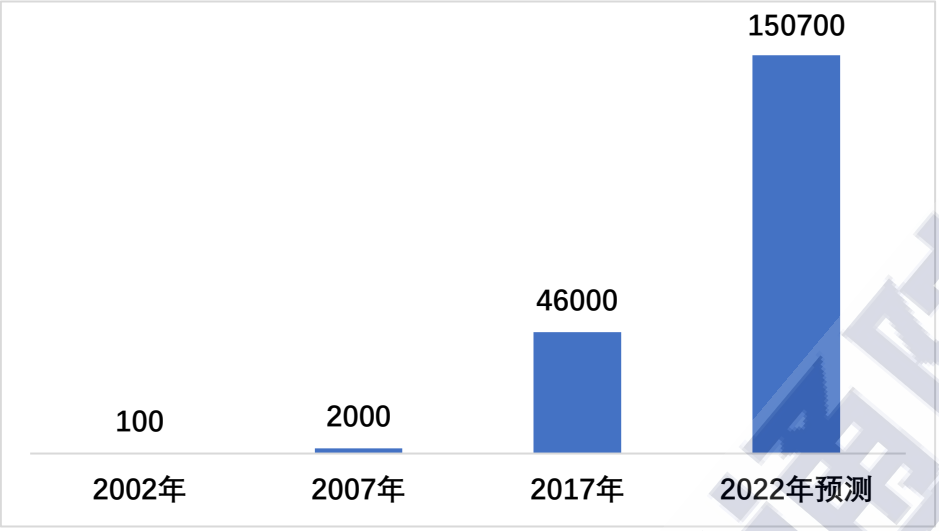
（一）国家政策引领发展路径

数字安全产业受到全球各国政府高度关注，并表现出不同的政策侧重。美国从国家安全角度出发，聚焦关键基础设施层面的安全，2018 年 5 月发布的《国家网络安全战略》明确提出“要保护关键基础设施免于遭受网络攻击，至 2023 年，提升国家政府网络和关键基础设施的安全和可靠性”。2020 年 3 月发布《2020 年 5G 安全及超越法案》要求“保障美国第五代和未来几代通信系统和基础设施的安全”。欧盟强调对用户隐私数据的保护和对企业合规的监管，2018 年 5 月生效的《通用数据保护条例》全面提出了各项用户数据权益，保障隐私安全；2019 年 6 月生效的《网络安全法案》要求欧盟机构在处理个人用户、组织和企业网络安全问题的过程中加强网络安全结构、增强对数字技术的掌控、确保网络安全应当遵守的法律规制。

我国政策从战略高度出发，引领数字安全产业高质量发展。党的十八大以来习近平总书记关于网络安全与信息化发表了系列重要讲话，党的十九大提出“坚持国家总体安全观”，党的十九届四中全会提出“推进国家治理体系和治理能力现代化”、“完善国家安全体系”及“建立健全网络综合治理体系”等要求。近年来，工信部、发改委、网信办等相关部门落实党中央、国务院相关要求，围绕工业互联网、5G、人工智能、云计算、大数据等新一代信息技术，密集发布了系列政策文件，综合推动数字安全产业的市场应用、技术创新和社会治理协同快速发展，为数字安全产业创造了良好的政策环境。2020 年 6 月，全国人大常委会首次对《数据安全法（草案）》进行审议，并就该草案面向社会公开征求意见；《个人信息保护法》也已列入第一类立法规划同步制定中。意味着我国自《网络安全法》实施以来，针对数据安全和个人信息保护的推动工作再上新台阶。

（二）数字经济发挥数字化转型促进作用

数字经济在全球经济中的重要性日益提升。据联合国《2019 年数字经济报告》测算，2019 年数字经济的规模估计最高占到世界国内生产总值（GDP）的 15.5%，到 2022 年代表全球互联网协议(IP)流量将达每秒 150700 千兆字节。同时，数字经济已成为推动传统产业转型升级、实现经济高质量发展的关键动力，各领域的数字化转型速度得到极大提升，数字化正在以不同的方式改造价值链，持续带来技术应用创新和生产力增长。



数据来源：联合国贸易与发展会议

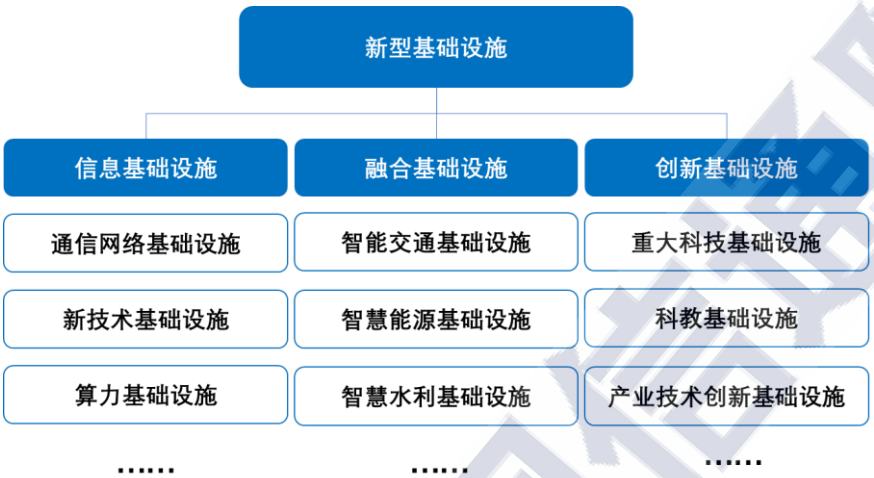
图 1-1 全球互联网协议(IP)流量（单位：千兆字节/秒）

我国数字经济持续快速发展，为数字安全产业创造重大机遇。当前，我国数字经济规模占我国 GDP 比重超过 30%，数字产业化结构持续优化，产业数字化深入推进，数字化治理能力全面提升，工业、服务业、农业数字化转型案例不断涌现。同时，数字化可能引发数字安全风险的扩大升级，对企业安全能力的挑战加剧，数字化治理体系与能力亟待完善，数字安全产业对数字经济向更多领域更深层次发展意义重大。

（三）新基建带动数字安全产业规模发展

新型基础设施建设给数字安全产业规模发展带来了新机遇。2020 年政府工作报告中，首次写入“新基建”概念，要求“加强新型基础设施建设，发展新一代信息网络……激发新消费需求、助力产业升级。”“新基建”浪潮下，5G、云计算、大数据、物联网、人工智能等产业需求提升，激发企业数字化转型趋势。在“新基建”推进过程中，需要数字安全产业更广范围、更深层次的参与其中，数字安全产业也需要依

托于新基建的宏观部署尽快实现“自我提升”，在产业方向和技术创新两方面都找准定位，应对复杂多变的内外部安全环境，筑牢“新基建”安全底座，为高质量发展保驾护航。



来源：国家发改委

图 1-2 新型基础设施建设范围

（四）新一代信息技术进一步成熟应用

新一代信息技术的发展日新月异，以 5G、云计算、大数据、人工智能、区块链等为代表的新兴技术从早期的研究创新阶段，逐步进入了大规模商用阶段，相关应用进一步成熟，例如 5G 能力开放、人工智能算法、大数据监测预警、云服务安全保障以及区块链去中心化加密等系列安全产品和服务，全面提升了当前数字安全的技术保障能力，助力构建科学高效的网络综合治理体系。另一方面，不法分子的攻击手段和能力也因技术而不断提升，对数字安全的防护能力提出了较之以往更高的要求，需要加大数字安全技术创新和推广应用力度。

第二章 数字安全十大产业方向和十大技术赛道遴选结果

（一）遴选结果引领数字安全产业发展

由工业和信息化部网络安全管理局指导，中国信息通信研究院和数字中国产业发展联盟联合承办的“2020 年数字安全十大产业方向、十大技术赛道”征集活动已圆满完成。征集活动旨在通过及时反映当前数字安全产业发展趋势和科研攻关方向，引导企业优先布局、提前行动，构建数字安全技术产业体系，形成数字安全保障能力持续供给，加快数字经济发展和推进网络强国建设。

征集活动主要立足于重要程度、迫切程度、关注程度等三个指标，就数字安全十大产业方向、数字安全十大技术赛道两项主题分别进行征集。2019 年 11 月 15 日，工业和信息化部网络安全管理局组织数字中国产业发展联盟相关专家召开座谈会，确定备选范围。2019 年 12 月 26 日，启动评选活动，采用社会公开投票和专家定向投票两种方式进行投票，由汇总投票数得出最终征集结果。2020 年数字安全十大产业方向和十大技术赛道结果如表 2-1 和表 2-2。

表 2-1 2020 年数字安全十大产业方向

序号	名称
1	工业互联网安全
2	物联网安全
3	关键信息基础设施安全
4	云安全
5	人工智能安全
6	智慧城市安全
7	5G 应用安全
8	大数据安全
9	车联网安全
10	智慧医疗安全

表 2-2 2020 年数字安全十大技术赛道

序号	名称
1	人工智能安全技术
2	区块链安全技术
3	边缘计算安全技术
4	敏感数据识别技术
5	生物特征识别技术
6	软件定义安全技术
7	安全多方计算技术

8	量子通信安全技术
9	商业密码技术
10	网络切片安全技术

（二）数字安全产业热点方向特点突出

遴选活动引发社会广泛关注，反响热烈，从反馈情况来看，数字安全产业热点方向呈现以下特点：

一是凸显政策导向。工业互联网安全、关键信息基础设施安全、大数据安全等方向因受到国家各机关法律法规、产业发展纲要性和指导性文件的着重指引而成为热点方向，分别有75%、67%、56%的问卷投了以上三个产业方向。国家近年来倡导加强重点领域数字安全防护工作，鼓励数字安全产业健康有序发展。工信部出台多项措施，布局加快构建工业互联网安全保障体系，提升工业互联网安全保障能力。

二是市场指向显著。人工智能安全技术、云安全、智慧城市安全等方向因拥有巨大市场潜力而受到企业推崇,分别有75%、67%、56%的问卷投了以上三个方向。数字安全企业基于人工智能的智能检测引擎和海量威胁情报赋能，能够有效提升数字安全防御的精度和效率，数字安全领域的人工智能应用正被定义为可替代安全专家能力的自动化技术,成为数字安全企业的拳头产品。伴随云计算技术广泛普及，云安全日益受到重视，云安全市场持续快速增长，其支出在数字安全整体市场的占比快速提升。数字科技推动新型智慧城市加速落地，随

之而来的安全问题也日益严峻，构建智慧城市保障体系的需求为数字安全企业带来巨大商机。

三是突出技术驱动。面对数字安全新形势、新挑战，关键技术是有效支撑数字安全保障的重要一环，区块链安全技术、生物特征识别技术、量子通信安全技术等方向因其技术优势而成为热点方向，分别有79%、56%、49%的问卷投了以上三个技术方向。区块链安全技术作为点对点网络、密码学、共识机制、智能合约等多种技术的集成创新，提供了一种在不可信网络中进行信息与价值传递交换的可信通道。生物特征识别技术能弥补传统密码学身份认证方式的缺陷，在网络环境下能够保证用户数字身份与物理身份的统一。量子通信安全技术因其基于量子力学原理保证信息安全的技术优势，未来将对数字安全领域产生重大影响。

第三章 数字安全产业十大方向

1 工业互联网安全产业

一、基本背景

工业互联网是云计算、大数据、人工智能等新一代网络信息技术与现代工业融合发展的产物，是推动工业数字化、网络化、智能化转型发展的重要基础设施保障，已逐步应用于电力、交通、石油、制造业等国民经济命脉行业。近年来，工业互联网面临的安全威胁和挑战愈发严峻，工业互联网安全产业重要性愈发凸显。

全球主要国家和地区纷纷布局工业互联网，抢占新一轮工业革命战略制高点。如美国于 2018 年发布《美国先进制造领导力战略》，2019 年发布《未来工业发展计划》。欧盟于 2019 年发布《增强欧盟未来工业的战略价值链》，2020 年发布《欧洲新工业战略》。德国于 2019 年发布《国家工业战略 2030》。日本于 2018 年发布《日本互联工业价值链战略实施框架》。

我国政府高度重视工业互联网发展，加强战略指引统筹发展和安全。2017 年 11 月，国务院颁布《关于深化“互联网+先进制造业”发展工业互联网的指导意见》，明确我国工业与互联网融合的长期发展思路，提出“建立工业互联网安全保障体系、提升安全保障能力”的发展目标。2019 年 8 月，工信部等 10 部门联合印发《加强工业互联网安全工作的指导意见》，提出“到 2025 年，安全产业形成规模，基本建

立起较为完备可靠的工业互联网安全保障体系”的总体目标。2020 年 3 月，中共中央政治局常务委员会强调，要加快工业互联网等新型基础设施建设进度；同月工信部发布了《关于推动工业互联网加快发展的通知》，提出从多个层面推动工业互联网发展。2020 年 5 月，政府工作报告指出，要“发展工业互联网，推进智能制造”。

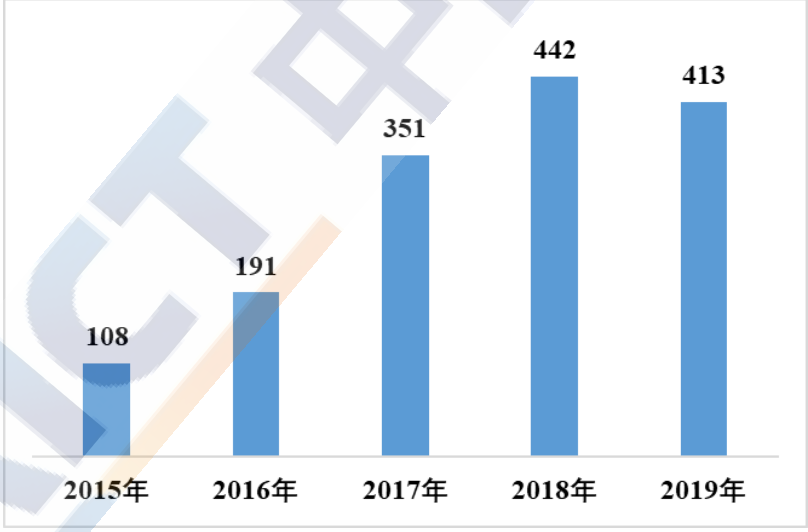
二、产业发展关键环节

工业互联网安全产业发展的关键环节包括设备安全、控制安全、网络安全、应用安全和数据安全五个方面。

设备安全方面，工业互联网的设备指工业生产现场的设备，包括单点智能器件以及成套的智能终端等，此类设备由嵌入式操作系统、微处理器、应用软件等构成，容易暴露在网络攻击之下。伴随工业互联网应用普及、设备规模扩大，其面临的攻击范围、扩散速度及带来影响将进一步扩大。工信部数据显示，截至 2019 年 7 月，我国重点工业互联网平台平均工业设备连接数达到 65 万台。国家互联网应急中心数据显示，2019 年上半年，我国境内暴露的联网工业设备数量共计 6814 个，34%存在高危漏洞隐患，嗅探事件高达 5151 万起。针对工业互联网设备安全问题，产业发展可围绕设备固件安全增强、 设备身份鉴权与访问控制、漏洞修复加固、补丁升级管理、安全漏洞披露、安全性评估评测等方面提供解决方案或服务。

控制安全方面，工业互联网的工业控制系统包括控制协议、控制软件、控制功能等关键要素，实现对工业自动化过程及相关设备的智

能控制、监测和管理。由于传统工业控制系统主要注重功能安全，在身份认证、传输加密、授权访问等安全防护功能方面有所弱化，导致当前主流工业控制系统普遍存在安全漏洞，日益成为黑客攻击和网络战的重点目标，带来远程操控、越权执行等安全威胁。据中国国家信息安全漏洞共享平台（CNVD）统计，截止到 2019 年 12 月，CNVD 收录的与我国工业控制系统相关的漏洞达 2306 个，其中，2019 年工业控制系统新增漏洞 413 个，中高危漏洞占比高达 92.8%，制造业、能源、水务、商业设施、石化行业新增漏洞位居前列。针对工业控制系统的安全问题，产业发展可以围绕身份认证、访问控制、传输加密、控制协议健壮性测试、软件防篡改、控制软件补丁升级更新、安全监测审计、安全意识教育培训等方面提供解决方案或服务。



数据来源：CNVD

图 3-1 2015 年~2019 年我国工业控制系统相关漏洞数量（单位：个）

网络安全方面，工业互联网的网络包括网络互联体系、标识解析体系等，是工业系统互联和工业数据传输交换的支撑基础。网络互联体系包括工厂内部网络和工厂外部网络，相关技术包括现场总线、工

业以太网、时间敏感型网络（TSN）、工业软件定义网络（SDN）、5G 等；由于工业互联网网络涉及多种网络融合，组网灵活复杂，传统的网络防护策略面临攻击手段动态化的严峻挑战。标识解析体系包括标识编码、标识解析系统和标识数据服务，是工业互联网实现互联互通的神经中枢；标识解析体系在标识解析架构、身份、数据、运营等诸多方面存在安全风险，面临挑战不断加剧。美国网络安全公司 Tenable 2019 年调查报告显示，来自 7 个国家工业、制造业、能源等关键行业的 700 多位 IT 安全决策者中，90%承认在过去两年间至少遭遇过一次破坏性网络攻击，半数称其运营技术（OT）基础设施经历过导致工厂和运营设备宕机的攻击。针对工业互联网网络安全问题，产业发展可以围绕网络结构优化、边界安全防护、接入认证、通信内容防护、通信设备防护、安全监测审计、网络安全评估、网络安全培训等方面提供解决方案或服务。我国工业互联网标识解析建设刚刚起步，安全保障能力建设相关工作相对滞后，亟需加快推进标识解析体系安全防控能力建设。

应用安全方面，工业互联网的应用包括工业互联网平台和工业应用程序两大类。工业互联网平台是基于云平台构建的海量数据采集、汇聚、分析服务体系,支撑制造资源泛在连接、弹性供给、高效配置的工业操作系统，由于其高复杂性、开放性、异构性，导致其面临的风险加剧；目前面临的安全风险主要包括数据泄露、篡改、丢失、权限控制异常、系统漏洞利用等。工业应用程序是基于工业互联网平台开发的、面向特定工业应用场景的智能化应用；目前面临的安全风险主

要包括开发过程中编码不符合安全规范带来的软件漏洞以及使用不安全的第三方库引起的漏洞等。国家互联网应急中心数据显示，2019年上半年，境内具有一定用户规模的大型工业云平台达40余家，其中部分平台持续遭受漏洞利用、拒绝服务、暴力破解等网络攻击，工业云平台已成为网络攻击的重点目标。针对工业互联网应用安全问题，产业发展可以围绕工业互联网平台安全审计、认证授权、DDOS攻击防护以及工业应用程序开发代码审计、定期漏洞检测、渗透测试、安全评估等方面提供解决方案。

数据安全方面，工业互联网的数据涉及数据采集、传输、加工处理、存储等各个环节，包括设备数据、业务系统数据、知识库数据、用户个人数据等。由于工业互联网数据形态种类多样、体量巨大、流向复杂、价值分布不均、安全防护需求不一、责任主体边界模糊，导致数据保护难度以及数据泄露风险加大。据美国电信运营商 Verizon 2020年数据泄露调查报告显示，与运营技术（OT）相关的数据泄露事件，主要集中在制造业、采矿、采石、油气开采相关垂直行业领域的公司。针对工业互联网数据安全问题，产业发展可以围绕数据防泄漏、数据加密、访问控制、业务隔离、数据脱敏、数据备份恢复、分类等级保护等方面提供解决方案。

三、典型案例

（一）安全风险监测领域

工业互联网安全风险监测是保障工业互联网安全的重要技术手

段。工信部等 10 部门 2019 年 7 月联合印发的《加强工业互联网安全工作的指导意见》指出，要求建设国家、省、企业三级协同的工业互联网安全技术保障平台。截止 2019 年 12 月，国家层面，国家级工业互联网安全监测与态势感知平台已基本建成；各省层面，已实现广东、山东、江苏等 12 个省级平台与国家平台系统对接，发现联网设备 800 多万、收录漏洞信息近 3700 条，形成工业互联网相关 IP、域名、企业等基础信息库；企业层面，重点行业的企业级安全监测平台正在快速构建。

（二）标识解析安全领域

工业互联网标识解析是工业互联网的重要网络基础设施，是支撑工业互联网实现身份管理、数据互联互通的枢纽，保障标识解析安全对于提升工业互联网安全能力具有重要意义。2017 年，国务院印发《关于深化“互联网+先进制造业”发展工业互联网的指导意见》，明确提出“重点突破标识解析系统安全”。在工信部指导下，中国信通院等单位落实建设工业互联网标识解析国家顶级和二级节点体系，部署安全风险防控手段，构建标识解析安全产业生态。2018 年底，北京、上海、广州、重庆、武汉五大国家顶级节点已实现上线运行，与 Handle 国际根节点、对象标识符（OID）国际体系等实现对接。截止 2019 年 11 月，已部署上线试运行的工业互联网标识节点达 34 个，涵盖 16 个行业，标识注册总量突破 12 亿，接入标识服务节点的企业超过 800 家。

（三）安全评估领域

工业互联网安全评估评测是推进工业互联网企业安全自查、开展第三方安全评估服务、支撑政府相关监管工作的重要手段。2018 年 11 月，工业互联网安全技术试验与测评实验室发布“工业互联网安全评测评估管理平台”；2019 年 4 月，平台亮相“2019 数字中国建设峰会”，该平台集成漏洞扫描、配置核查、网络流量采集与分析、病毒木马检测、无线 WIFI 安全检测等多种安全评测评估工具，通过对工业互联网安全管理和技术指标的评测、对系统或设备的技术检测，可实现对工业互联网业务对象的全面或针对性安全评估。

（四）工业数据安全领域

工业大数据是工业互联网的关键资源要素，是工业智能化、数字化转型发展的关键驱动，保障工业数据安全对于推动工业互联网健康有序发展至关重要。近两年，工信部分别启动了 2019 年、2020 年工业互联网创新发展工程，工业数据安全相关项目是其中重要组成部分，涉及“面向工业互联网平台的数据安全监测与服务系统”、“数据安全风险监测追溯与综合管理平台”、“工业互联网数据可信交换共享服务平台”等。其中，“工业互联网数据可信交换共享服务平台”项目旨在基于区块链等技术建立数据安全交换、安全共享、安全交易、安全下载等技术与公共服务能力，打造工业互联网数据可信交换、交易生态圈。

2 物联网安全产业

一、基本背景

物联网安全产业是为政府、企业在应用物联网推动数字化转型过程中有效应对各类安全风险，提升物联网安全保障能力，促进物联网产业安全健康有序发展，提供专用技术、产品和服务的重要产业。

各国政府高度重视物联网安全问题，出台战略、政策法规、技术规范等促进物联网安全产业发展。美国于 2016 年发布《保障物联网安全战略原则》白皮书，2017 年发布《物联网网络安全改进法案》，2019 年发布《物联网网络安全和隐私风险管理指南》报告。欧盟于 2017 年发布《关键信息基础设施领域的物联网安全基线指南》，2019 年出台《消费者物联网网络安全》标准。日本于 2017 年出台《物联网安全综合对策》,2019 年批准法案授权日本国家信息与通信研究院针对物联网设备安全开展监管。

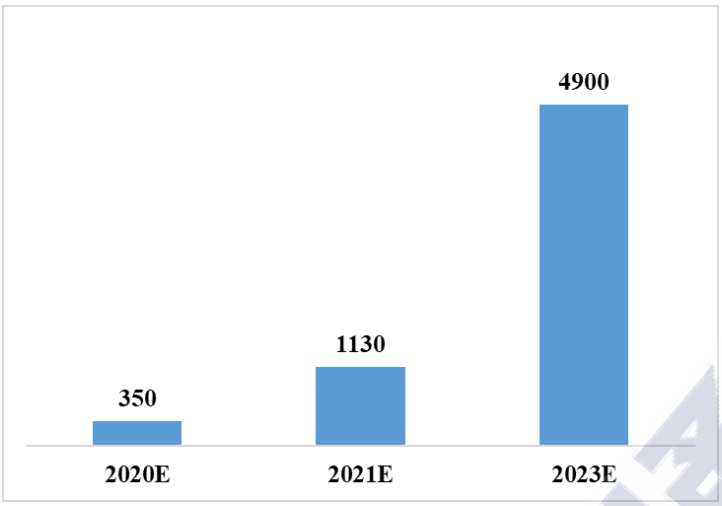
我国加强物联网发展战略规划指引，大力推动物联网安全产业发展。2016 年，国务院发布《“十三五”国家战略性新兴产业发展规划》，提出要“推动物联网、云计算和人工智能等技术向各行业全面融合渗透，构建万物互联、融合创新、智能协同、安全可控的新一代信息技术产业体系”。2017 年，工信部发布《关于全面推进移动物联网（NB-IoT）建设发展的通知》，提出要“建立健全 NB-IoT 网络和信息安全保障体系，提升安全保护能力”。2018 年底，中央经济工作会议提出加强物联网等新型基础设施建设；2020 年 5 月，国家发改委表示，我

国将加快布局支持新型消费的5G网络、物联网等新型基础设施建设。

二、产业发展关键环节

当前，物联网产业正与5G产业协同发展，形成了“物联网+5G”的安全产业发展新模式。物联网安全产业的关键环节包括感知层安全、网络层安全、应用层安全三个方面。

在感知层安全方面，5G时代物联网设备在安全上将得到提升，同时面临的安全威胁也日益增多。感知层由智能终端、传感器等各类终端节点设备组成，实现对信息的采集、识别。由于物联网设备的“轻量级”特点，导致其本身缺乏完备的安全防护能力，在隐私保护、授权、传输加密、软件保护等多方面都存在安全隐患，成为黑客攻击的主要目标。5G发展将带动物联网设备规模快速增长，也为网络攻击提供了丰富的目标环境，大量物联网设备可能被用于组成僵尸网络对网络基础设施发起DDoS攻击，造成网络堵塞甚至断网瘫痪。据高德纳咨询公司（Gartner）预测，从2020年到2023年，5G物联网终端将从2020年的350万台增长到2023年的近4900万台，并预测2021年全球物联网终端安全支出预计将达到6.3亿美元。针对物联网感知层的安全问题，应构建物联网设备安全的保障体系，发展设备安全测试、评估认证、漏洞披露、密钥管理、数据加密等解决方案。特别是在5G时代下，物联网终端设备需加速可信操作系统、安全芯片和特定安全服务的发展。



数据来源：Gartner, 2019

图 2-2 全球 5G 物联网终端数预测（单位：万台）

在网络层安全方面，5G 蜂窝物联网连接能提供更强的安全能力，以应对新的安全风险。物联网网络层由各类专用网络、互联网、有线和无线通信网等组成。由于网络类型多，传输处理的信息又是海量、多元异构的，其面临的网络安全威胁将更为复杂。与 4G 相比，5G 网络在海量数据上下行、隐私保护、认证授权等方面提供了更强的安全保障机制。据国外咨询机构 Ju-niper Research 预测，到 2023 年，所有企业的网络安全支出总额的 5%预计将用于物联网网络安全。针对物联网网络层安全问题，产业发展应提供网络节点身份认证及访问控制、网络态势感知、数据传输加密、数据完整性保护等方面的解决方案，同时 5G 网络集成了多无线接入、软件定义网络（SDN）\网络功能虚拟化（NFV）、云计算和边缘计算等诸多技术，物联网安全架构要适应虚拟化、云化的需要。

在应用层安全方面，5G 将带动物联网在车联网、工业互联网等关键领域的快速发展，应用层数据安全重要性愈发凸显。应用层包含

物联网中间件、物联网应用系统、云计算等部分，由于应用层集中存储着大量数据，应用系统自身也可能存在漏洞，易成为黑客攻击的目标；特别的，物联网应用层数据极为丰富，既有应用系统自身运行过程中产生的用户和业务数据，也有从感知层、网络层采集和收集的数据，一旦被窃取，有可能危及用户隐私、企业核心商业机密甚至有可能引发危及多人生命安全的严重公共灾难，保障应用层数据安全至关重要。随着 5G 应用的快速发展，物联网在医疗、交通、能源、电力等关键领域的应用将进一步拓宽，迎来“物联网+5G”应用的高速发展期。物联网安全产业在应用层，应充分利用 5G 架构的开放性和灵活性，构建相应的安全防护体系，在统一架构下为垂直行业应用提供定制性和差异化的安全能力，例如系统安全检测、操作用户身份认证、访问控制、行业信息加密及完整性保护等解决方案。

三、典型案例

（一）操作系统安全领域

操作系统是物联网产业底层基础设施，拥有自主产权的操作系统对于我国物联网产业生态安全具有战略意义。作为物联网产业的战略至高点，目前国内外企业主导物联网终端的操作系统。例如 ARM 公司、谷歌、微软等推出的物联网操作系统。从国内看，华为、阿里、腾讯等企业也推出了各自的物联网操作系统，如 AliOS Things、TencentOS-tiny、Huawei LiteOS、RT-thread、Ruff 等。国内物联网操作系统虽发展迅速，但仍存在各类产品规模较小、体系不完善等问题。

在国际 ICT 产业链竞争新形势下，我国亟需加强自主可控物联网操作系统的发展。

（二）芯片安全领域

作为物联网设备最主要的工作部件，保障芯片安全对物联网整体安全至关重要。2019 年，中国移动推出了针对物联网行业的和安芯系列产品“安全芯片及平台端到端解决方案”。该解决方案包含“芯片端”和“服务端”两部分，在芯片端推出了 SE-SIM 产品，该产品是将传统的 SE 芯片和 SIM 芯片高度集成的芯片，兼具安全与 SIM 两项能力，可以抵抗实验室级软件及物理攻击，提供通信加密、终端保护服务；在服务端形成了与 SE-SIM 配套的安全认证服务平台（和云盾）、IoT 平台、业务服务平台、安全产线等，具备端到端的物联网安全解决方案能力。目前，SE-SIM 解决方案已在智慧燃气、智能门锁、车联网、智慧城市等物联网应用领域实现商业落地，助力物联网行业应用安全。

（三）数据安全领域

物联网数据安全问题日益凸显，已逐步成为制约物联网发展的关键问题之一，亟需加强物联网“云管端”侧数据安全保障。2020 年 4 月，工信部发布了《网络数据安全标准体系建设指南》（征求意见稿），针对物联网领域，将加强在物联网云端数据安全保护、物联网管理系统数据安全保护、物联网终端数据安全保护等方面的标准建设布局。中国联通探索打造了“云管端”一体化的物联网安全解决方案，在终端侧，打造基于 SIM 卡的终端身份认证平台，提供数据加密功能，从

源头减少数据安全风险；在网络侧，重点关注终端业务异常和由物联网终端发起的 DDOS 攻击，根据策略进行告警和处置；在平台侧，建立物联网专有云安全环境，并在访问认证、数据加密、应急响应等方面做了优化和加强，旨在物联网企业客户提供更安全的物联网环境。

（四）安全监测领域应用

物联网对环境数据的广泛采集、传输和处理等特性，能在安全监测方面发挥重要作用。2015 年 6 月，自然资源部和水利部共同启动了“国家地下水监测工程”建设，通过运用物联网等技术，研发了集地下水水位、水温和大气压监测数据自动采集、实时传输、实时共享为一体的信息应用服务系统。2019 年 12 月底，完成工程验收，共建成国家级地下水专业监测站点 20469 个，实现对人口密集区、国家重大工程区、地下水超采区、地面沉降区的重点监测以及主要平原盆地和岩溶含水层地下水水位、水质的有效监测。两年试运行结果表明，水位水温自动监测数据到报率保持在 95%以上，每年产生近 9000 万条地下水水位、水温、水质数据，为保障我国生态安全提供重要支撑。

3 关键信息基础设施安全产业

一、基本背景

关键信息基础设施是指关系国家安全、国计民生、公共利益，一旦遭到破坏、丧失功能、或者数据泄露可能带来严重危害的信息设施，涵盖公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域。近年来，伴随重要行业和领域智能化、网络化程度的不断深化，关键信息基础设施的安全风险日益突出，关键信息基础设施安全产业重要性愈发凸显。

世界主要国家和地区将关键信息基础设施上升至国家安全高度，持续出台战略、规划、立法等加大保护力度。比如，美国于 2018 年 10 月通过《网络安全与基础设施安全局(CISA)法案》，2018 年 12 月通过《保护能源基础设施法案》，2019 年 1 月引入《管道和液化天然气设施网络安全预备法案》，2019 年 8 月引入《网络安全诊断和缓解增强法案》，2020 年 3 月签署《安全可信通信网络法案》等。欧盟于 2018 年 5 月生效实施《欧盟网络与信息系统安全指令》，2019 年 3 月通过《欧盟网络安全法案》。新加坡于 2018 年 2 月通过《网络安全法 2018》；日本于 2018 年 7 月发布第三版《网络安全战略》。

我国高度重视关键信息基础设施安全问题，正加快构建安全保护体系。自全国人民代表大会常务委员会 2016 年 11 月发布《中华人民共和国网络安全法》，对关键信息基础设施安全保护做了基本法层面的总体制度安排，我国关键信息基础设施保护相关配套政策、法规、

标准等制定加速推进。2019 年 5 月，国务院办公厅印发《国务院 2019 年立法工作计划》，明确提出拟制定《关键信息基础设施安全保护条例》。2020 年 4 月，国家互联网信息办公室、国家发展改革委等 12 部门联合发布《网络安全审查办法》，确保关键信息基础设施供应链安全。

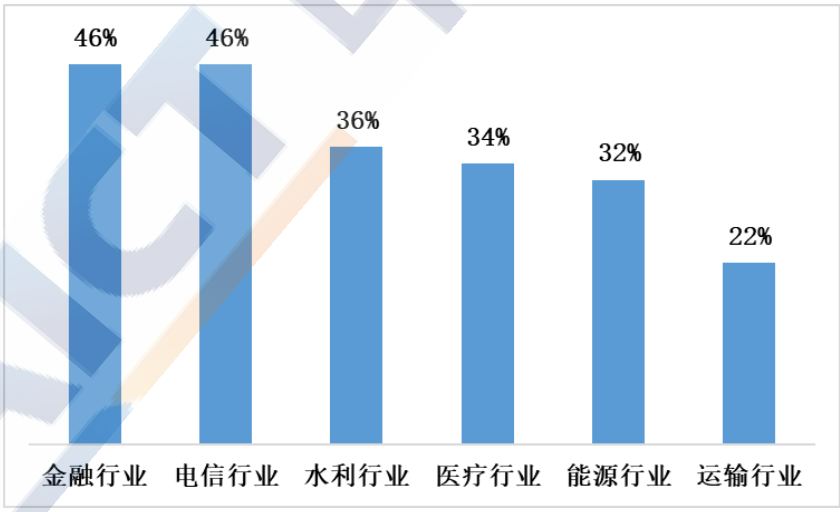
二、产业发展关键环节

关键信息基础设施安全产业发展的关键环节包括物理安全、运行安全、供应链安全三个方面。

物理安全方面，物理和环境安全是关键信息基础设施安全运行的基石。关键信息基础设施如遭受自然灾害、人为破坏、电磁环境、物理环境影响、操作管理不当等传统物理威胁，有可能导致关键信息基础设施宕机，从而引发严重后果。推进关键信息基础设施本身技术演进升级，确保关键信息基础设施配套放置环境安全可靠、运维能力扎实高效，将有效提升关键信息基础设施安全水平。围绕关键信息基础设施物理安全，产业可以围绕自动化监测、智能化运维、专业化托管等提供解决方案或服务。

运行安全方面，网络攻击严重威胁关键信息基础设施安全运行。关键信息基础设施遭受攻击、入侵等网络违法犯罪活动，可能造成物理破坏、服务中断、数据泄露等严重后果。由于关键信息基础设施广泛运用云计算、大数据、物联网、工业互联网等新技术，涉及系统大规模集成、联网，已成为网络攻击的主要目标，网络安全形势日趋严

峻复杂。德国安全公司 Greenbone Networks 2020 年调查报告显示，在英、美、德、法、日五国能源、金融、卫生、电信、运输和水利行业的 370 家大型企业中，平均仅 36%的公司具有很高的网络安全防护水平。德国西门子和美国 Ponemon 研究所 2019 年调查报告显示，全球 1726 名公用事业专业人士中，56%的受访者表示在过去一年中至少经历过一次网络攻击，64%的受访者表示复杂的攻击是最大的挑战，54%的受访者预计未来一年关键基础设施将遭受攻击。围绕关键信息基础设施的运行安全，产业可以从通信网络完整性保护、使用者身份验证、使用行为日志管理、应用程序完整性测试、数据访问控制、重要系统和数据的容灾备份、网络安全测试验证、监测预警、漏洞共享、应急演练、教育培训等方面着手，构建覆盖网络安全风险识别、防护、检测、预警、响应、处置等环节的解决方案。



数据来源： Greenbone Networks，2020 年

图 2-3 不同类型基础设施高安全防护水平企业占比

供应链安全方面，产品和服务供应链安全是关键信息基础设施保护的重要内容。关键信息基础设施使用的产品和服务如果存在后门、

漏洞、木马等安全缺陷或者供应渠道不可靠、供应中断等隐患，有可能带来关键信息基础设施被非法控制、遭受干扰或破坏、重要数据被窃取、泄露、毁坏的风险，甚至影响业务连续性等。我国在整机 CPU、高速内存、路由器、服务器及存储设备、操作系统、数据库等关键信息技术产品方面依赖国外企业，影响关键信息基础设施安全可控水平。围绕关键信息基础设施供应链安全，产业可围绕网络关键设备和网络安全专用产品安全认证、安全检测等提供解决方案或服务；此外，我国亟需加强在高性能存储设备、操作系统、数据库等产品领域的自主研发，加快推进在政府、通信、金融等重点领域国产化软硬件的应用推广，提升关键信息基础设施安全可控水平。

三、典型案例

（一）金融关键信息基础设施安全领域

征信系统是我国重要的关键金融信息基础设施之一，由中国人民银行征信中心负责征信系统的建设、运行和维护。2017 年 3 月，中国人民银行启动了二代征信系统建设，在信息采集、产品加工、技术架构和安全防护等方面进行优化改进。2020 年 1 月，二代征信系统正式切换上线。征信系统采用多种举措保障征信信息与公众用户隐私安全，一是提供数字证书、银行卡、问题、移动金融 IC 卡等多种验证方式，通过严格身份验证、多因子校验，确保查询申请由本人提交；二是经过身份验证，持有身份验证码，才能查看信用信息，确保查询结果由本人查看；三是从获得可以查询的反馈通知之日起，信用信息

仅在平台的互联网端存放 7 天，到期后会自动删除，确保信息保存安全。

（二）交通关键信息基础设施安全领域

数字交通是数字经济发展的重要领域，是以数据为关键要素和核心驱动，促进物理和虚拟空间的交通运输活动不断融合、交互作用的现代交通运输体系。2019 年 7 月，交通运输部印发《数字交通发展规划纲要》，部署数字交通建设，以兼顾创新发展和安全发展为原则，将健全网络和数据安全体系作为重要工作，防范化解数字化转型带来的信息安全风险，提升网络安全和数据安全保障能力，保障公共安全和国家利益。数字交通建设强调加强网络安全与信息系统同步建设，提高交通运输关键信息基础设施和重要信息系统的网络安全防护能力；推进重要信息系统国产密码应用、重要软硬件设备国产化应用；加强对交通数据全生命周期的管控，保护国家秘密、商业秘密和个人隐私。

（三）网络信息基础设施协议安全领域

加快推进 IPv6 规模部署，是我国构建高速、移动、安全、泛在新一代信息基础设施的关键举措。2019 年 5 月，工信部组织基础电信企业、云服务企业、终端设备厂商、互联网应用商店等，部署开展 IPv6 网络就绪专项行动，要求推进 IPv6 在网络各环节的部署和应用，提升对 IPv6 的支持能力，并同步升级防火墙/WAF、IDS/IPS、4A 系统等 IPv6 网络安全防护手段，同步改造僵木蠕监测处置系统、IDC/ISP

信息安全管理系统等网络安全监测处置系统等。伴随专项行动的开展，我国IPv6改造取得积极进展，IPv6网络安全保障能力得到有效强化。国家 IPv6 发展监测平台数据显示，截止 2020 年 3 月，我国已申请 IPv6 地址资源总量达 47859 块（/32），位居世界第二。

4 云安全产业

一、基本背景

云安全是指保护云计算环境免受外部和内部安全威胁，以及解决数字化过程中安全问题的一系列方案和技术。随着云计算产业的高速发展，政府、企业等各类组织的 IT 系统上云速度加快，对云安全的需求也不断提升，相关产业发展迅猛。

全球各国政府不断细化完善云计算安全政策和标准体系，着力提升云计算安全水平和整体网络安全防御水平。2011 年 2 月，美国联邦政府制定了“云优先”战略，2018 年 9 月，美国联邦政府发布了“云智能”战略，组成了美国政府的云计算管理委员会，同时制定了云安全的风险管控标准。2017 年，加拿大政府发布了《关于安全使用商业云服务的指导意见-安全政策实施通知》，旨在支持各部门在云计算下理解现有的安全政策要求，并指导协助各组织安全使用商业云服务。2018 年英国国家网络安全中心发布了《云安全指南》，规范了云服务商对云产品的安全定义和展示规则。

我国政府高度重视云计算安全防护，保障我国云计算安全发展，积极培育信息安全产业新业态。2015 年国务院发布《关于促进云计算创新发展培育信息产业新业态的意见》、2018 年工信部印发《推动企业上云实施指南（2018-2020 年）》、2019 年国家网信办、发改委、工信部、财政部联合发布《云计算服务安全评估办法》，落实强化安全管理和数据隐私保护，增强安全技术支撑和服务能力，建立健全安全防护体系，切实保障云计算信息安全。

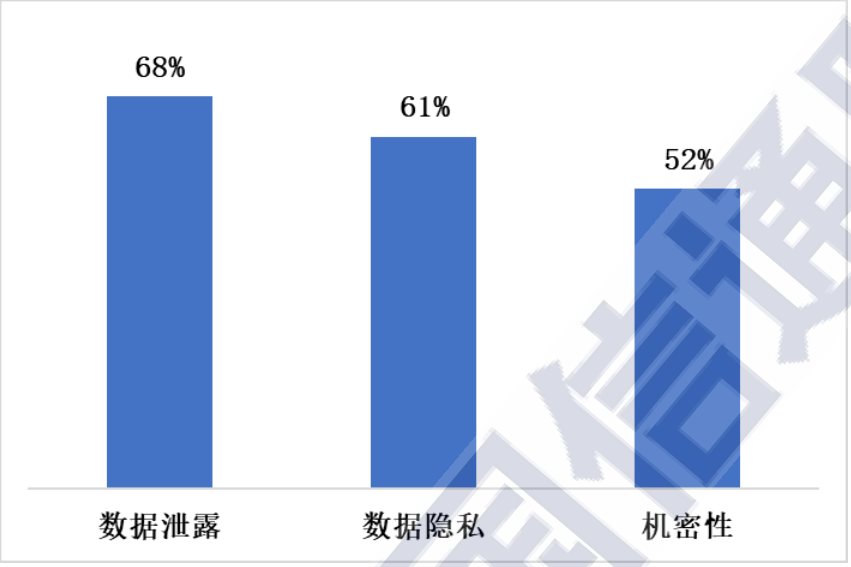
二、产业发展关键环节

云安全产业按照云计算运营模式主要分为私有云安全、公共云安全和混合云安全三大方面。

在私有云安全方面，私有云是通过互联网或专用内部网络面向特定用户提供的云计算服务，目前我国私有云正处于快速发展阶段，据国际数据公司（IDC）调查显示 2018 年中国企业在私有云平台投入同比增长达到 49.2%，市场规模达到 38 亿美元，并有望在 2023 年成为全球第一大市场。私有云安全风险主要包括云平台内部流量不可见，虚拟机间缺乏安全隔离，多云平台弹性扩展、动态迁移等风险。安全合规是私有云平台建设的必要条件，同时，随着越来越多的业务系统迁移到云平台，有效保障云端数据和业务的安全性和稳定性成为十分重要的刚性需求。为提升私有云安全防护能力，目前产业内发展出虚拟化防护边界、云安全管理系统基础防护、增强加密认证、安全可视化管理以及引入云安全访问代理等一系列私有云安全解决方案。

在公有云安全方面，公有云是指云计算基础设施由某一组织所有，通过网络向公众提供 IT 能力的服务模式。目前，中国公有云呈现稳步增长的态势，IDC 发布的《中国公有云服务市场(2019 下半年)跟踪》报告显示，2019 下半年中国公有云服务整体市场规模达到 69.6 亿美元。公有云安全问题备受关注，是云安全产业发展的焦点， IDC 在 2019 年对 400 家中国企业用户受访者的调查数据显示，安全是企业在选择公有云时主要顾虑之一。公有云的安全风险涉及众多方面，包括内外部威胁、网络攻击、数据泄露、业务连续性、隐私保护和监管

合规等多种类型。同时，2019 年亚马逊云安全报告提及，数据泄漏、数据隐私、机密性是客户关注云安全的最重要的三个问题，其中数据泄露尤其受到关注，占比 68%。



数据来源：亚马逊，2019

图 2-4 企业关注云安全最重要的三个问题占比

针对公有云安全问题，产业围绕保障云自身及其上各种应用的安全，建立云计算技术与安全基础设施资源协同的安全防护机制，基于云计算平台为用户提供的安全服务提供解决方案，同时完善云安全风险监管政策和数据保护政策，如开展第三方安全和质量认证、完善监管政策和制定技术标准推动公有云市场的规范发展。

在混合云安全方面，由于混合云部署模式是指用户在私有云的基础上进行扩展，利用公有云服务资源来扩展私有云的资源范围，其安全风险是复杂和广泛的，不同混合云组合模式对应的安全风险不同。针对混合云安全问题，目前围绕安全防护、隔离、监控和身份认证等措施展开。云服务提供商方面侧重于对自身提供环境下的安全防御、监视与应用级的安全保护，云平台软件提供商方面侧重于虚拟机环境

的兼容、通用性、迁移及安全性。

三、典型案例

（一）云网融合安全领域

5G 技术具有核心网全面云化的特点，正与云安全产业深度融合。进入 5G 时代，我国电信运营商积极发展云网融合业务，提供安全可信的云服务。2019 年 9 月，中国电信发布“5G + 天翼云 + AI”战略，将 5G 安全服务作为重要方向，发展云安全、网络安全和数据安全能力，提供云网融合的云安全服务。2019 年 11 月，中国移动推出“5G+移动云”，形成 5G 与云计算深度融合的新型能力体系，提供云主机安全、云堡垒机、云审计、云防火墙等安全服务，助力各行业应用安全发展。

（二）金融云安全领域

金融云安全能有效保障金融机构信息安全，是金融行业安全发展的重要内容。2018 年 8 月中国人民银行正式发布《云计算技术金融应用规范技术架构》《云计算技术金融应用规范安全技术要求》《云计算技术金融应用规范容灾》三项金融的云安全行业标准。2019 年 12 月，中国人民银行金融科技创新监管试点率先在北京市启动，今年 3 月首批 6 个项目“入箱”，涉及国有商业银行、全国性股份制商业银行、大型城市商业银行、清算组织、支付机构、科技公司等多家机构，主要聚焦云安全、大数据、人工智能、区块链、API 等前沿技术在金融领域的应用。促进金融活动的顺畅、安全运行，标志着我国在构建

金融科技监管体系方面迈出了非常关键的一步。2020 年 6 月 2 日第二批创新应用向社会公示，包括基于云安全的“多方数据学习‘政融通’在线融资项目”、“移动金融云签盾”、“智能云小店服务”等 11 个项目，作为积极探索金融企业和科技企业相结合的创新监管试点，为银行及相关机构积累经验，营造守正、安全、普惠、开放的金融科技创新发展环境。

（三）交通云安全领域

交通云安全对于提升出行信息安全系统防护能力，加强数据安全防护管理，构建全面高效的出行安全体系有重大意义。2016 年，交通部主导创建的综合交通出行大数据开放云平台“出行云”在论坛上正式上线。2016 年在交通运输部科技司推动下，“综合交通出行大数据开放云平台（出行云）”正式上线。截至 2019 年，出行云接入并共享了 15 个省市、5 所大学、3 家科研院所、12 家大型企业的 192 项共 10TB 开放数据集，数据累计查看量 130 万次，下载量近 2 万次。2019 年 12 月，出行云平台上新建设了“出行云交通旅游大数据平台（出行云交旅平台）”，实现交通与旅游行业大数据共享。

5 人工智能安全产业

一、基本背景

近年来，人工智能技术整体推进迅速，从基础支撑、核心技术到行业应用的人工智能产业链条逐步完善，新模式、新业态不断涌现，整体呈现蓬勃发展态势，推动经济社会各领域从数字化、网络化向智能化加速跃升。与此同时，产业的快速发展也带来核心基础技术安全需求旺盛、创新产品和服务安全能力亟待强化等诉求，人工智能安全产业重要性凸显，成为人工智能稳步发展的关键保障。

人工智能作为国际技术发展的新焦点，世界各国均加大对人工智能与安全问题的关注。2019 年 7 月，美国“国家人工智能安全委员会”向国会提交报告，提出未来要维持美国在人工智能国家安全应用领域的全球领先地位，重点包括研究美政府如何快速和大规模地采用人工智能应用程序来保护美国国家安全。2020 年 2 月，欧盟发布《人工智能白皮书—通往卓越和信任的欧洲路径》，6 月，欧盟发布《人工智能道德准则》，促进欧洲安全可信的人工智能发展。2018 年 12 月，日本科学技术振兴机构发布了《人工智能战略提案》，指出将通过新一代软件工程来确保人工智能应用系统的安全性和可靠性。

我国政府大力支持人工智能产业发展，探索构建人工智能安全管理体系。2017 年 12 月，工信部印发《促进新一代人工智能产业发展三年行动计划（2018-2020 年）》，提出完善发展环境，提升安全保障能力，实现产业健康有序发展；到 2020 年，完善人工智能网络安

全产业布局，形成人工智能安全防控体系框架。2019 年 2 月，科技部成立新一代人工智能治理专业委员会，并于 6 月发布《新一代人工智能治理原则—发展负责任的人工智能》，强调了“安全可控”等八条原则。2020 年 2 月，工信部发出倡议书，倡议充分发挥人工智能赋能效用，协力抗击新型冠状病毒感染的肺炎疫情。

二、产业发展关键环节

当前，人工智能安全产业已初具规模，主要包括基础设施安全、数据安全、算法安全、应用安全四个方面。

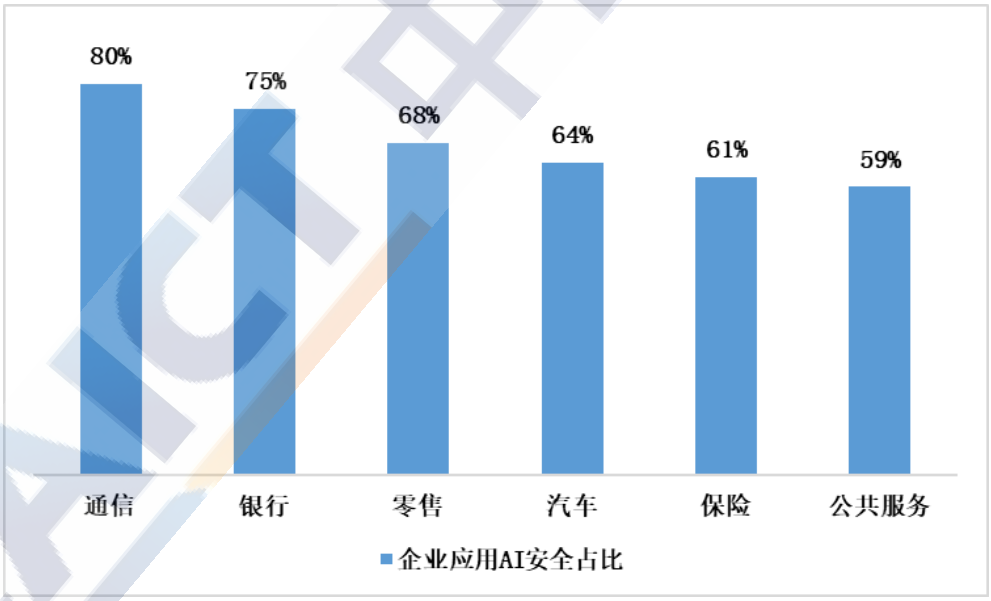
在基础设施安全方面，人工智能基础设施主要包括人工智能芯片、智能传感器、网络组件、存储设备等硬件基础设施，其中以提供计算能力的智能芯片为核心。据瑞银（UBS）预测，至 2021 年人工智能芯片市场将达至 350 亿美元。人工智能芯片在安全产业中扮演至关重要的角色，芯片级的安全漏洞能造成严重影响，整个信息系统都可能被黑客攻破，且修复难度很大。同时，高算力的芯片也是人工智能安全防护能力的必要支撑。目前，美国占据全球人工智能芯片的领先地位，在图形处理器（GPU）芯片方面有英伟达、AMD 等企业，在可编程逻辑门阵列（FPGA）芯片方面有 Xilinx 等企业，以及谷歌、英特尔、脸书、微软等科技企业都在人工智能芯片领域布局，IBM 则在美国国防高级研究计划局支持下开发类脑芯片“TrueNorth”。我国近年来涌现出不少芯片创新型企业，但仍存在一定差距。在当前国际竞争形势趋于紧张的环境下，人工智能安全产业应大力在芯片层级发力，

发展安全可信的人工智能芯片，对数字安全及国家安全都有十分重要的意义。

在数据安全方面，人工智能的深度学习、机器学习、神经网络等技术都依赖于海量的训练样本数据，数据安全风险已成为影响产业发展的关键因素。人工智能数据层面临着样本攻击、数据污染、异常、窃取、伪造、歧视以及隐私保护、数据权属、跨境流动等多方面的数据安全问题。目前，产业发展主要围绕人工智能数据的全生命周期，保障数据标注过程安全、数据质量，提升人工智能数据的安全管理和防护能力，重点应对因数据过度采集、逆向还原、数据滥用等造成的个人信息保护安全风险。

在算法安全方面，技术层主要由人工智能的算法模型、开发框架，以及基于前两者发展的机器视觉、智能语音、自然语言理解等具体应用技术组成，该层是是人工智能威胁识别、智能攻防、自动响应等安全能力的关键。其中，算法模型既是人工智能发展的突破，也是带来新安全威胁的因素，出现诸如算法的歧视、黑箱、伦理等安全新问题。而开发框架是通用算法模型的一种工程实现，主要安全风险一方面来自于开发框架本身的缺陷、漏洞等安全性问题，另一方面目前产业内的人工智能大部分基于国际开源框架项目，如 TensorFlow、Caffe 等，对于我国产业的安全自主发展不利。人工智能安全产业应着力加强算法的安全性、可靠性和稳定性，满足人工智能服务器侧、客户端侧、边缘侧等计算、运行框架等安全要求，强化针对人工智能开源框架的特定安全能力和自主掌控能力。

在应用安全方面，人工智能应用架构在基础设施层、数据层和技术层之上，在数字经济的各个领域快速发展，因此呈现出人工智能应用受到的攻击面更大、安全风险更突出的特点。据德国数据公司 Statista 预测，至 2025 年全球人工智能企业应用的收入预计将达 312 亿美元。此外，人工智能应用同时扮演了“安全保护者”和“威胁制造者”的双重角色，一方面用于安全防护，另一方面部分被滥用在了网络诈骗、不良信息传播、黑客攻击、生物特征伪造等违法领域，引发社会治理问题，亟待通发展人工智能的安全技术对抗。目前产业针对不同应用场景下的安全风险，发展出各领域不同产品服务的共性和特性安全解决方案，持续加强应用的安全规范，并提升对人工智能违法应用的防护治理能力。



数据来源：凯捷咨询公司（Capgemini），2019

图 2-5 各类企业中应用人工智能安全应对数字安全威胁的占比

三、典型案例

（一）网络和信息安全领域

人工智能安全产业在提供网络安全服务，保障数字经济相关信息技术应用安全中体现出高价值和重要性。2020 年 3 月，为做好工业互联网、远程医疗、在线服务、云办公等新型应用的安全保障支撑，充分发挥基础电信企业、网络安全企业作用，工信部网安局组织相关企业，依托网络安全公共服务平台，运用人工智能、云计算、大数据等技术，通过互联网远程方式，向党政机关、医疗机构、公共应急、教育教学等疫情联防联控单位以及重点工业互联网企业等用户提供在线网络安全服务，包括对分布式拒绝服务攻击（DDoS）、工业互联网安全、病毒木马、网络安全漏洞等开展实时监测与应急处置，提供威胁信息共享、数据安全防护等服务，最大程度降低企业系统遭受网络攻击的风险，为疫情防控和复工复产提供了坚实的网络安全保障。

此外，针对近年来网络诈骗活动，人工智能安全产业充分发挥了预防打击网络诈骗作用。2019 年，在工信部网安局指导组织相关单位建设部省两级互联网反诈系统，实现部系统与 19 个省系统对接联动，提升对基于人工智能技术的诈骗信息的拦截与处置能力，全年共汇聚涉诈域名 149 万个，涉诈网址 900 万个，涉诈互联网账号 13 万个。

（二）智能制造安全领域

智能制造是推动制造业转型升级、加快制造业高质量发展非常重要的工作抓手，人工智能、5G 通信等新兴技术实现了多点革命性的

突破，并加速融入到智能制造中。2019 年 9 月，中国电信联合天津海尔洗衣机互联工厂、青岛海尔工业智能研究院三方联合建设的 5G 智慧园区正式启动。借助 5G+人工智能技术，园区部署了无人巡逻机、无人巡逻车等巡逻机器人，从全域视角空间进行厂区巡逻，将高清视频信号回传至监控平台，高效发现生产安全及安保风险点并快速预警，确保园区安全。园区安监人员还可借助增强现实（AR）眼镜，实时采集现场图像，通过 5G 网络回传至统一图库比对，进行人工智能分析判断，对非准入人员的出现发出告警。人工智能安全能力极大提高了安全生产及园区安保风险点的监控和预警，提升了安防效率。

（三）公共卫生安全领域

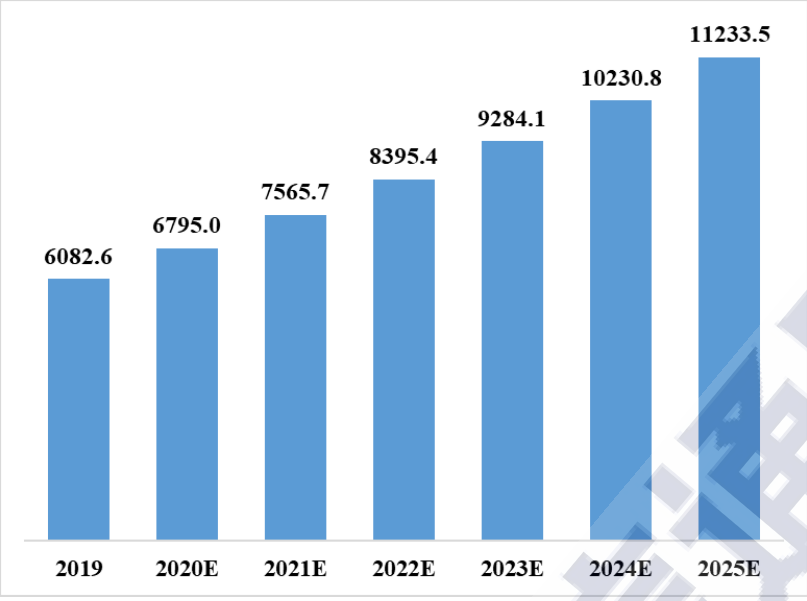
在抗击新冠肺炎疫情期间，人工智能技术发挥出了极大的优势，切实保护了人民群众生命安全和身体健康。2020 年 2 月，为支撑疫情防控的医疗物资保障工作，工信部充分应用人工智能、物联网、大数据等信息技术，紧急组织开发了国家重点医疗物资保障调度平台，主要用于搜集、统计、分析、监控、调度、过滤重点医疗物资企业的产能、产量、库存等情况，统筹线上线下，实现对防护服、药品和检测试剂、专用医疗设备等重点医疗物资供给能力的及时监控。截至 2020 年 4 月，平台共覆盖 9 个大类 116 个种类医疗物资产品，收入企业 2656 家，基本实现了对医用防护服等重点医疗物资生产企业的全覆盖；实现了分区域、分类别的企业产能、产量、库存、周转、保供情况监测，为重点医疗物资保障科学决策提供了信息窗口，在疫情防控中发挥了重要作用。

6 智慧城市安全产业

一、基本背景

智慧城市是新一代信息技术变革和数字经济进一步发展的产物，基于工业化、城市化与数字化的深度融合，具备互联互通、数字整合、协同运作、创新发展等新型城市数字化发展特点。近年来，人民群众对城市服务水平的期望日益提升，城市管理趋于复杂，针对物理和信息的新数字安全风险不断增多，可能从根本上影响智慧城市的发展，智慧城市安全产业凸显出重要地位。

以数字经济为基础的智慧城市作为最具创造力的城市形态，已成为全球城市发展的战略选择。目前，全球共有超过 50 多个国家和地区已经制定智慧城市战略布局、引导市场发展，相关行业企业积极参与开展智慧城市项目和工程建设，例如美国“智慧城市挑战（Smart Cities Challenge）”计划、欧盟“城市变革（+CityxChange）”项目、日本“编织之城（Woven City）”项目、韩国《智慧城市综合规划（2019~2023）》等。全球智慧城市产业正在快速发展，据德国数据公司 Statista 预测，到 2025 年全球智慧城市建设支出将达 1.1 万亿美元。



数据来源：Statista，2020

图 2-6 全球智慧城市建设支出（单位：亿美元）

我国政府高度重视新型智慧城市建设，推进国家治理现代化，助力数字中国稳步发展。党的十八大以来，党中央、国务院以及各级部门陆续出台新型智慧城市建设的相关政策、规划、标准及评价指标体系等。2016 年 4 月，习近平总书记在网信工作座谈会上指出，要“分级分类推进新型智慧城市建设”。我国陆续发布的《“十三五”国家信息化规划》《关于继续开展新型智慧城市建设评价工作 深入推动新型智慧城市健康快速发展的通知》《2020 年新型城镇化建设和城乡融合发展重点任务》等系列政策文件明确将建设智慧城市作为我国国家规划的内容之一，提出了相关发展目标、建设方向和关键环节等重点要求。

二、产业发展关键环节

智慧城市安全产业发展的关键环节包括终端安全、网络安全、数

据安全与应用安全四个方面。

在终端安全方面，智慧城市的终端分为智能手机等用户使用终端（2C）和传感器、控制器、执行器等企业应用终端(2B)两大类。这些边缘区域终端具备多样的接入方式、复杂的接入条件和庞大的接入数量，容易成为安全威胁的载体，会导致恶意行为进入智慧城市系统，危害城市的关键基础设施，扰乱城市服务的正常运作。据国际数据公司(IDC)预测，至 2023 年 20%的智慧城市网络与信息安全事件会由部署的物联网设备而引发。针对智慧城市终端安全问题，产业发展可围绕构建智慧城市终端安全的保障体系，提供终端安全检测与评估、终端身份认证和实名化管理、数据加密和存储保护、安全策略统一配置管理等解决方案。

在网络安全方面，通信网络覆盖智慧城市的各个角落，是信息流通的基本通道，由网络基站、承载网、接入网、核心网以及网络切片等网络部件组成。智慧城市在建设和运营网络过程中，面临数据传输泄露、DDoS 攻击、垃圾信息泛滥以及物理设施损坏等一系列安全威胁。其中 5G 网络是智慧城市的网络安全重点，据 IDC 预测，至 2024 年，三分之一的智慧城市应用将由 5G 驱动，75%的大型城市将基于 5G 规模部署服务。目前，智慧城市在网络安全方面围绕 5G 网络增强移动宽带（eMBB）、超高可靠低时延（uRLLC）、海量机器类通信（mMTC）三大场景，由网络运营商、设备供应商等广泛参与，推动安全防护能力升级，建立配套安全管理机制，以及构建智能攻防的通信场景安全模型。

在数据安全方面，智慧城市体系涵盖了各类智能计算、分析与流程功能，包括了人工智能平台、大数据平台、安全中台等。各类平台之间存在大量的信息交互与数据流动，而且经常需要将新技术与传统系统集成，面临大多数传统系统不具备新型安全能力的问题。目前，在整合城市不同系统的条件下，智慧城市的数据安全一方面保障不同平台的数据对接安全，如加强 API 接口安全管理和加密通信，另一方面保障平台存储数据的安全，如采取数据冗余、数据验证、数据库审计等技术，以及开发部署“城市大脑”等新型智慧城市平台，整体提升城市数字化过程中的数据保密性、完整性和连续性。

在应用安全方面，城市各行业的智能应用是支撑智慧城市管理与运行的具体表现，其安全保障包括了软件安全与运营管理两大方面。智慧城市应用广泛分布于能源、通信、交通、医疗、教育等各行业，面对数据泄露、身份伪造、软件漏洞、黑客攻击等网络风险，以及行业领域的特定安全威胁。据国际信息系统审计协会（ISACA）2018 年的一项全球调查显示，71%的受访者认为，智慧城市能源应用最容易受到安全攻击，其次是通信（70%）和金融服务（64%）应用。智慧城市安全产业面向应用层面，具备漏洞扫描、安全升级、灾备恢复等基本应用安全保障能力，构建对应用使用者的接入、权限及信任等多方面的安全管理机制，解决智慧城市不同部门在阶段性建设中的应用升级协同，实现应用的操作性和安全性之间均衡。

三、典型案例

（一）能源安全领域

智慧能源是智慧城市重要应用分支，对于保障能源网络安全、提升能源行业数字化水平、构建安全高效能源体系具有十分重要的意义。2019 年 4 月，工信部、国资委、国家能源局联合推进网络安全及能源智慧信息平台建设工作，平台的建立是保证我国能源网络安全的重要举措。截至 2019 年 9 月，共有 12 家中央企业和 44 家地方国有企业参与平台建设,完成了重点能源企业六大类 64 个经营指标的数据接入，230 个厂站的安全网络态势感知平台的接入,实现了对全国所有省份以及所有能源类型（包括风电、光电、水电、火电、核电）的全覆盖，并不断推进建设横向到边、纵向到底的全国能源网络安全与智慧能源体系。

（二）电子政务安全领域

“互联网+政务服务”是国家推进智慧城市的一项重要建设工作。2018 年，为深入推进“放管服”改革，全面提升政务服务规范化、便利化水平，更好为企业和群众提供全流程一体化在线服务，推动政府治理现代化，国务院发布指导意见加快推进全国一体化在线政务服务平台建设。在平台建设中坚持安全可控，积极运用安全可靠技术产品，推动安全与应用协调发展，筑牢平台建设和网络安全防线，确保政务网络和数据信息安全，强化各级政务服务平台安全保障系统的风险防控能力，构建全方位、多层次、一致性的防护体系，切实保障全国一

体化在线政务服务平台平稳高效安全运行。2019 年 11 月，平台整体上线试运行，联通 31 个省（区、市）及新疆生产建设兵团、40 余个国务院部门政务服务平台，接入地方部门 300 余万项政务服务事项和一大批高频热点公共服务。

（三）交通安全领域

新一代信息技术与交通运输深度融合发展的趋势加快，智慧城市在保障交通安全领域的作用日益凸显。2018 年，交通运输部启动了关于加快推进新一代国家交通控制网和智慧公路试点工作，涵盖交通基础设施安全状态综合感知、分析及预警，公路信息交互、风险监测及预警，车路协同安全辅助服务，面向城市公共交通及复杂交通环境的安全辅助驾驶等系列智慧交通安全应用。试点工作在北京、河北、吉林、江苏、浙江、福建、江西、河南、广东等省份开展，以高速公路和城市内道路相结合，重点解决交通领域一系列的安全、拥堵、污染等问题。2019 年 5 月，首个国家交通控制网智慧高速试验段在江西省建成。2020 年 1 月，连接北京市和河北省，作为国家交通控制网与智慧公路示范工程、冬奥会重大交通保障项目的“延崇高速”正式通车。

7 5G 应用安全产业

一、基本背景

5G 应用是以第五代移动通信技术（IMT-2020，通常称 5G）为基础服务各领域的新一代信息技术应用，具有高速率、低时延、大容量的特点。5G 应用因技术本身以及应用场景特点，面临新的复杂安全风险，有效实现 5G 应用安全是产业高质量发展的重要前提和保障。

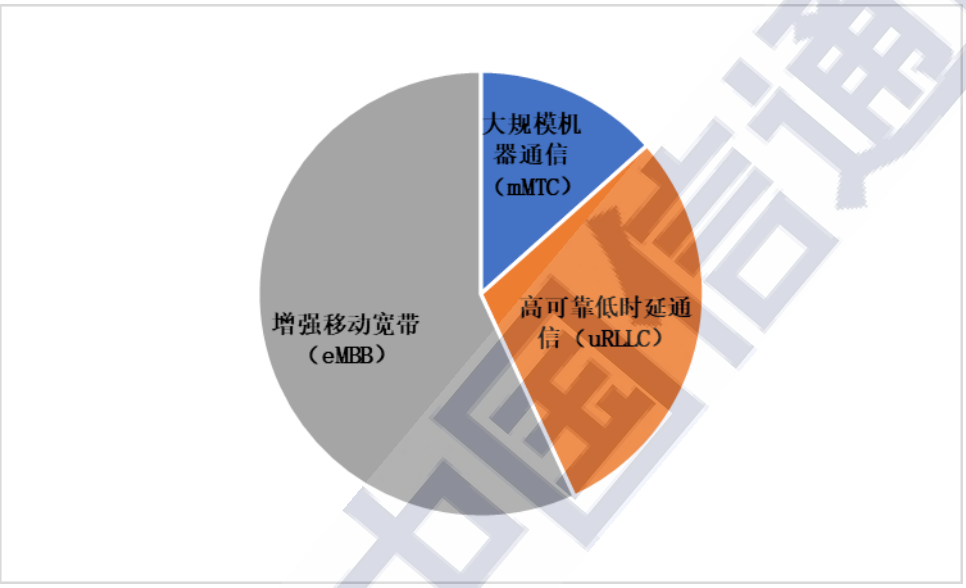
5G 已成为各国数字经济战略的焦点，各国普遍关注 5G 的安全发展。美国于 2020 年 3 月发布《2020 年 5G 安全保障法》，欧盟于 2 019 年 10 月发布《欧盟 5G 网络安全风险评估报告，2020 年 1 月发布《在欧盟确保 5G 的安全部署——实施欧盟工具箱》。韩国于 2019 年 6 月推出全球首个商用 5G 七年增长计划。

我国高度重视 5G 应用发展，将 5G 作为实施国家创新战略的重点之一。2019 年 11 月，工信部印发《“5G+工业互联网”512 工程推进方案》，从技术产业、创新应用、资源供给等方面提出细化发展目标和发展路径，加速推动“5G+工业互联网”512 工程落地实施。2020 年 3 月，工信部发布《关于推动 5G 加快发展的通知》，对于加快 5G 建设及应用、推动产业创新发展、助力经济平稳运行具有重要意义。2020 年 3 月，发改委、工信部下发《关于组织实施 2020 年新型基础设施建设工程（宽带网络和 5G 领域）的通知》。

二、产业发展关键环节

5G 应用安全产业按场景分为增强移动宽带(eMBB)安全、海量机

器类通信(mMTC)安全、高可靠低时延(uRLLC)安全三个方面。 根据中国信通院《全球 5G 发展数据跟踪报告》，关于 5G 试验应用的监测样本数据显示，增强移动带宽 5G 应用占比最高，达到 56.9%；高可靠低延时通信占比其次，为 29.7%；大规模机器通信占比最低，为 13.4%。



数据来源：中国信通院

图 2-7　三类 5G 应用场景试验分布状况

在增强移动宽带安全方面，增强型移动宽带场景将带动 5G 手机、VR/AR、超清视频、超清直播等应用的落地，同时超大流量对于现有网络安全防护手段形成挑战。首先，由于 5G 数据速率最高可达 10 Gbit/s，需要更高的安全处理性能，在流量检测、链路覆盖、数据存储等方面满足超大流量下的安全防护需求；其次 5G 需要支持外部网络二次认证，更好地与业务结合在一起；最后需要解决目前发现的已知漏洞的问题。构建云化或服务化的安全基础设施，进行网络或业务策略的访问控制，通过服务间的配合与协同机制来实现高性能的安全处理能力，是增强移动宽带安全的主要途径。

在海量机器类通信安全方面，海量物联网通信场景将带动低功耗广域物联网、智慧家居、智慧城市等应用的落地。国际数据公司(IDC)预计到 2025 年全球物联网设备联网数量将达到 252 亿。其中大量功耗低、计算和存储资源有限的终端难以部署复杂的安全策略，一旦被攻击容易形成僵尸网络，成为攻击源，进而引发对用户应用和后台系统的网络攻击，带来网络中断、系统瘫痪等安全风险。对低功耗网络来说，一是需要轻量化的安全机制以适应功耗受限、时延受限的物联网设备的需要；二是通过群组认证机制，解决海量物联网设备认证时所带来的信令风暴的问题；三是依靠抗 DDOS 攻击机制，应对由于设备安全能力不足，攻击者对网络基础设施发起攻击的危险。目前，针对海量物联网通信场景安全风险，可采取深度挖掘垂直行业应用在网络层的安全服务需求，构建基于大规模机器类通信场景的安全模型等措施，建立智能动态防御体系应对网络攻击，防止网络安全威胁横向扩散。

在高可靠低时延安全方面，高可靠低时延主要支持车联网与自动化辅助驾驶、远程医疗以及工业自动化控制等应用。对于关系到人身安全或高额经济利益的应用，其安全防护机制要求更加严苛，而安全机制的部署会增加时延，不能满足低时延业务的要求。为提升低时延条件下安全防护能力，目前产业内发展出建立面向低时延需求的安全机制、加强与应用服务提供商在安全保障能力的协作、统筹优化业务接入认证、数据加解密等一系列解决方案。

三、典型案例

（一）能力开放安全领域

随着 5G 应用在各领域的丰富扩展，5G 的安全能力开放也将作为电信运营商面向各行业提供的安全服务能力。2018 年以来，中国移动联合包括国内外运营商、设备提供商以及终端和芯片厂商在内的产业各方，全面研究了基于 5G 网络安全机制为上层业务提供认证和密钥分发能力的关键问题及解决方案，形成了适配 5G 网络服务化的高安全性认证与密钥分发架构，及可适用于物联网、车联网、工业互联网等多种 5G 应用场景的轻量级协议。2019 年 12 月，中国移动基于该成果在国际标准组织 3GPP 主导完成首个 5G 安全能力开放项目。

（二）无人机安防领域

搭载 5G 技术的警用无人机在自动巡检监控中，可实现 4K 画质的图像传输，便于警务人员识别犯罪嫌疑人特征；无人机可在制高点观测整个事件，对目标进行全面全程跟踪及拍摄；根据不同案件和事件，无人机可在不同角度、不同距离和不同光线条件下作业，准确传递现场信息。2019 年 12 月，中国电信发布了天翼无人机使能平台，提供低延时、高带宽中国电信 5G 实时通信服务、安全可靠的天翼云数据存储服务，保障警务数据安全，运用 5G 和人工智能技术接入各种警务终端，有效打击犯罪，维护社会秩序稳定。2020 年 1 月，中国移动完成全球首个无人机 5G 高空基站应急通信测试，进一步验证 5G 高空基站方案的可行性及落地性，为今后的警务工作提供更加优质的

应急通信方案。

（三）金融安全领域

5G 为金融行业提供泛在智能的移动互联基础设施，提升金融服务的可得性与安全水平，实现巩固金融系统稳定性、提升金融服务效能。2019 年 4 月，工商银行与中国电信合作推出的首个基于 5G 网络的营业网点正式落地，为确保网络传输的安全性，5G 接入端设备采用了加密算法，对金融交易数据进行端到端安全加密传输。2019 年 5 月，中国银行 5G 智能+生活馆在北京正式开业，是银行业首家深度融合 5G 元素和生活场景的智能网点，为了保障数据安全，搭建了 5G 网络专用数据通道，将重要业务加密传输。

（四）智能电网安全领域

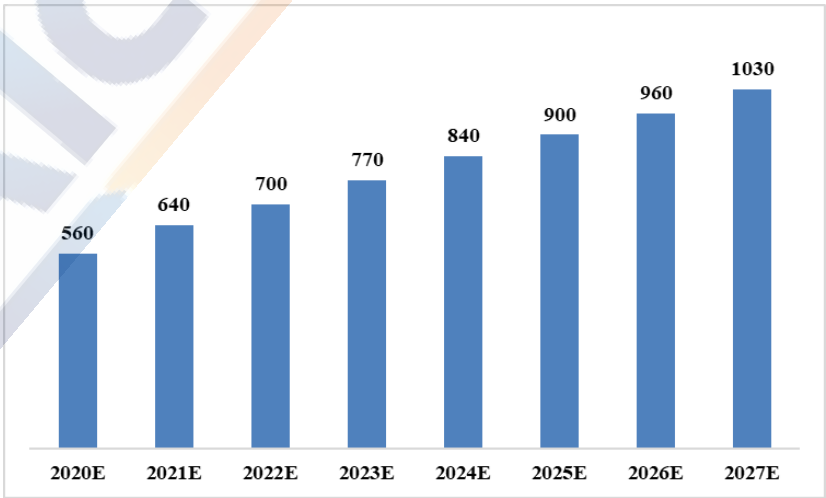
智能电网是在传统电力系统的基础上，集成新技术形成的新一代电力系统。智能电网安全的核心是电网的监控系统安全，包括该系统的技术安全、信息安全、结构安全和应用安全。2020 年 5 月，国家能源局在发布的《关于建立健全清洁能源消纳长效机制的指导意见》中明确提出，要持续推进智能电网建设，通过融合应用 5G，实现电力能源领域高质量发展。2019 年 10 月，国家电网联合产业链生态合作伙伴在青岛建成了全国最大规模 5G 智能电网实验网，对独立存在的电网系统与互联网建立安全可靠的连接，实现数据信息的流动提供了解决方案。

8 大数据安全产业

一、 基本背景

大数据是利用新一代信息技术形成的，以容量大、类型多、存取速度快、应用价值高为主要特征的数据集合。大数据安全是用于保护大数据免受攻击、盗窃或其他可能对其造成伤害或负面影响的恶意活动的措施和工具的总称。

全球高度重视大数据所蕴含的战略价值，相继出台大数据战略规划和配套法规促进大数据应用与发展。2019 年 12 月，美国发布《联邦数据战略与 2020 年行动计划》。2020 年 1 月，欧盟发布针对个人数据保护的比例原则的指南，2019 年 6 月，英国政府为《国家数据战略》公开征集意见，2020 年 1 月，韩国国会通过了《个人信息保护法》、《信息通信网络利用和信息保护促进法》和《信用信息使用和保护法》。据 Gartner 预测，全球大数据产业 2027 年可规模达 1030 亿美元。



来源：Gartner，2018

图 2-8 全球大数据产业收入规模（单位：亿美元）

我国政府高度重视大数据安全发展，积极推动相关政策制定，推动经济发展、完善社会治理、提升政府服务和监管能力。2020 年 4 月国务院发布的《中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见》明确指出要加快培育数据要素市场，推进政府数据开放共享，提升社会数据资源价值，加强数据资源整合和安全保护，2019 年 12 月交通运输部印发《推进综合交通运输大数据发展行动纲要(2020—2025 年)》，2019 年 5 月，网信办发布《数据安全管理办法(征求意见稿)》。

二、产业发展关键环节

大数据安全产业分为大数据采集安全、大数据处理和存储安全和大数据使用和共享安全三个方面。

在大数据采集安全方面，大数据采集安全是数据安全生命周期的第一个过程，来自大量终端设备和应用的超大规模数据源输入，对鉴别大数据源头的真实性提出了挑战。除数据来源是否可信，源数据是否被篡改是需要防范的风险外，还面临从数据源到数据库的传输需要各种协议相互配合，缺乏专业数据安全保护机制的协议可能给大数据带来安全风险，数据传输过程中的泄漏、破坏或拦截会带来隐私泄露、谣言传播等安全管理失控的问题。目前，行业内主要围绕大数据传输中信道安全、数据源防伪造和篡改、以及数据采集设备终端安全等提供产品和服务。

在大数据处理和存储安全方面，大数据平台一般是处理和存储功能的整合，大多数大数据框架将数据处理任务分布在许多系统中，以加快分析速度。例如 Hadoop 是一种流行的用于分布式数据处理和存储的开源框架，但 Hadoop 最初的设计没有考虑到足够的安全性，引发了诸多隐患。大数据处理和存储的安全风险涉及众多方面，包括分布式计算在安全攻击和非授权访问防护方面比较脆弱、平台访问控制存在安全隐患、数据滥用和数据挖掘导致隐私泄露等。在存储和计算上，大数据安全侧重于分布式系统安全、隐私保护技术、动态静态数据加密机制、异地容灾备份、数据镜像和快照保护等。

在大数据使用和共享方面，大数据使用和共享安全主要涉及大数据结果的输出方式和对象的安全。大数据的分析结果通常输出到应用程序、报表和仪表板等应用层出口，这为威胁入侵提供了丰富的目标，对输出进行安全防护至关重要。同时，大数据使用和共享还涉及到数据的权属问题，与用户个人信息和隐私保护密切相关。目前，在保障大数据使用和共享安全方面，行业主要围绕数据传输的加密、应用账户的访问控制安全、大数据个人隐私保护以及大数据流动的监管合规性等方面展开。

三、典型案例

（一）大数据基础设施安全领域

大数据是我国开展新型基础设施建设的重要组成部分，数字化基建的运转会产生大量数据，来自政府、企业及生产生活各个环节的数

据，汇聚在众多大数据中心，其安全保障尤其重要。围绕“新基建”发展，可发挥大数据安全顶层设计、全局感知的重要能力，全网采集安全大数据，建立全视角安全感知能力，即时输出威胁情报，实现全局升级基础上的单体安全能力提升。2020 年 5 月，国家发改委表示将在 2020 年制定加快新型基础设施建设和发展的意见，并实施全国一体化大数据中心建设重大工程，将在全国布局 10 个左右区域级数据中心集群和智能计算中心。

（二）大数据个人信息安全领域

用户个人信息和隐私保护是大数据安全的重要内容之一。自 2013 年起中国移动即开始采用“金库模式”保护客户信息。该模式严格执行多人验证授权的数据查询，对涉及用户敏感信息的关键操作，采取“关键操作、多人完成、分权制衡”的原则，实现操作与授权分离，确保所有敏感操作都有严格的控制。2016 年，针对加速推进电话“实名制”工作，中国移动依托敏感信息模糊化等技术手段，深化“金库模式”，不断强化用户信息保护能力。2019 年，针对 APP 违法违规收集使用个人信息的问题，中国移动将“金库模式”覆盖到全网，严格把关自有及合作 APP 的数据权限范围。

（三）大数据应用安全领域

大数据在交通领域应用，与综合交通运输深度融合，保障交通大数据安全，是加快我国交通强国建设的有力支撑。2019 年 12 月，交通运输部部署相关行动，深入推进国家综合交通运输信息平台建设，

推动基于大数据的综合交通运输安全生产全流程监管，强化大数据安全保障，推进交通运输领域数据分类分级管理，加强重要数据和个人信息安全保护，制定数据分级安全管理、数据脱敏等制度规范以及推进重要信息系统密码技术应用和重要软硬件设备自主可控，推进国家交通运输的关键数据资源全面实现异地容灾备份，推进去标识化、云安全防护、大数据平台安全等数据安全技术普及应用。交通运输部明确，到 2025 年力争实现综合交通大数据中心体系基本构建，大数据安全得到有力保障。

9 车联网安全产业

一、 基本背景

车联网是借助新一代信息通信技术，实现车、人、路、服务平台等全方位网络连接和信息交互，提升汽车智能驾驶水平、社会交通智能化服务水平的信息物理系统。伴随着汽车智能化、网联化的快速推进，暴露出的安全问题日益增多，安全已成为关系车联网快速发展的重要因素，车联网安全产业地位日益凸显。

以欧美日为代表的汽车强国纷纷加强车联网发展战略规划指引，抢占未来汽车产业竞争战略制高点。欧盟 2018 年 6 月发布《通往自动化出行之路：欧盟未来出行战略》，2019 年 8 月发布新版的《网联自动驾驶路线图》，2019 年 11 月发布第二版《智能汽车网络安全最佳实践研究报告》。美国于 2018 年 10 月发布指导文件《为未来交通做准备：自动驾驶汽车 3.0》，2020 年 1 月发布《自动驾驶 4.0 计划》。日本于 2018 年 3 月提出《自动驾驶相关制度整备大纲》，2018 年 9 月发布《自动驾驶汽车安全技术指南》，2019 年 8 月通过《道路运输车辆法》修正案。

我国政府高度重视车联网发展，加强顶层设计促进汽车产业转型发展。2018 年 12 月，工信部印发《车联网(智能网联汽车)产业发展行动计划》，推动形成深度融合、创新活跃、安全可信、竞争力强的车联网产业新生态。2020 年 2 月，国家发改委、网信办、工信部等 11 部门联合印发《智能汽车创新发展战略》，明确提出战略愿景，即到 2025 年，中国标准智能汽车的技术创新、产业生态、基础设施、法

规标准、产品监管和网络安全体系基本形成。2020 年 4 月，工信部发布《2020 年智能网联汽车标准化工作要点》，加快推进智能网联汽车标准体系建设。

二、 产业发展关键环节

车联网安全产业发展的关键环节包括终端安全、网络安全、服务平台安全以及数据安全四个方面，涉及覆盖车联网的“云、网、端”三级技术框架体系。

来源：工信部、国标委《国家车联网产业标准体系建设指南》

图 2-9 车联网产业（信息通信）标准体系技术结构图

终端安全方面，车联网终端包括智能网联汽车、移动智能终端，智能网联汽车是搭载先进车载传感器、控制器、执行器等装置的新一代汽车，面临芯片、外围接口、传感器、车载操作系统、车载中间件、车载应用软件以及远程升级等方面的安全风险；移动智能终端是实现

人与智能网联汽车、车联网服务平台等交互的载体，面临终端系统、APP 方面的安全隐患。针对车联网终端安全问题，产业发展可围绕智能网联汽车的设计、研发、测试、认证评估，硬件安全芯片的研发、设计、部署，软件远程升级更新、传感器控制系统干扰智能监测以及移动智能终端的应用加固、渗透测试等方面提供解决方案或服务。

网络安全方面，车联网的网络涉及车内网络、车际网络、车载移动互联网络等，由于车联网通信场景具有联网汽车高速移动、网络种类多样、网络拓扑结构复杂等特点，面临通信协议破解、中间人攻击、恶意节点入侵、认证机制破解等安全威胁，带来通信数据被监听、敏感数据被窃取、汽车动力系统被非法控制、路况信息传递受影响等严重后果。针对车联网网络安全问题，产业发展可围绕通信加密、分段隔离、接入鉴权认证、车云通信双向认证、入侵检测、异常流量监测等方面提供解决方案。

服务平台安全方面，车联网服务平台是提供车辆管理与信息内容服务的云端平台，是车联网数据汇聚与远程管控的核心，一方面，面临着传统的云平台安全问题，安全威胁涉及平台操作系统漏洞、SQL 注入攻击、访问控制、拒绝服务攻击等方面；另一方面，目前较多车联网管理平台访问控制策略偏弱，面临攻击者通过伪造凭证方式访问平台，进行网络攻击的问题。针对车联网服务平台安全问题，产业发展可围绕安全加固、安全检测、漏洞远程更新、身份校验、威胁情报共享等方面提供解决方案。

数据安全方面，车联网数据来源于用户、电子控制单元（ECU）、

传感器、车载信息娱乐系统（IVI）及操作系统、第三方应用及车联网服务平台等，种类不仅包括车辆速度、行驶里程和位置等固有信息，还涉及车主、乘客出行时间、途径地点、行车轨迹、目的地甚至样貌、行为等隐私信息，这些数据一旦泄露或被滥用，不但影响车辆安全性，用户个人隐私也将受到侵犯。目前，在传输和存储环节，存在能因访问控制不严、数据存储不当等原因导致数据被窃风险；在采集和使用环节，存在因车联网数据采集、利用、共享等管理要求不明确，导致数据过度采集、越权使用等侵犯用户隐私的风险。针对车联网数据安全问题，产业发展可围绕数据分级管理、敏感数据加密传输、数据共享管理等方面提供解决方案。

三、典型案例

（一）认证安全领域

证书安全配置是加强车联网身份认证管理、保障终端通信安全的有效手段。2019 年 10 月，中国移动联合多家通信设备厂商、车载终端生产企业和安全芯片生产企业，推出 C-V2X 证书安全配置方案，该方案将运营商通用引导架构（GBA）技术应用于车载 LTE-V2X 终端，打通从车载终端和 USIM 卡到无线接入网、核心网、GBA 平台、CA 服务器的端到端流程，完成了车联网 C-V2X 证书安全配置能力验证。该成果在 2019 年世界智能网联汽车大会展出，展示了在车规级通信模组及车载单元（OBU）终端上实现设备安全“一键配置”，支持 GBA 初始安全配置机制的车载 LTE-V2X 终端使用配置证书对 C-

V2X 广播消息进行安全保护的真实场景。

（二）网络安全领域

网络安全能力提升是有效抵御车联网网络攻击、保障信息安全传输的前提。2019 年 9 月，中国联通展示了其车联网网络安全解决方案“车联网安全系统”，该系统为 V2X 通信提供安全的基础网络支持，为车联网业务建立专属低时延的网络切片，配合 V2X 形成车联网专属的 5G 安全数据链，为车辆提供“高并发、低时延、抗干扰、强加密、高可靠”的网络服务，有效保证车与车之间通信加密不被篡改，防止车辆被黑客攻击造成交通事故，保护乘客的安全。

（三）车路协同安全领域

云网融合为车路协同安全实践提供了创新技术保障。2020 年 6 月，中国电信携手中兴通信在雄安新区绿色交通先行示范区成功打造了国内首个城市级车路协同示范应用边缘计算节点，是云网融合在车联网场景的首次实践。此次发布的边缘计算节点汇聚 5G、MEC 边缘云、云计算、云边协同、AI 技术，为车路协同示范应用提供融合高性能计算服务、边缘计算服务、云平台服务、信息管理服务于一体的分布式、弹性算力网络，可有效支撑交叉路口碰撞预警、安全辅助信息推送、区域交通指引等低时延驾驶安全服务，保障车内产生的信息安全、可靠、高效的连接到云端，提供多源交通数据的边缘融合处理服务，实现统一安全的网络接入、各种终端灵活适配、海量数据的采集分析。

10 智慧医疗安全产业

一、基本背景

智慧医疗指通过信息化实现患者、医务人员、医疗数据、医疗设备之间互动，从而在整个医疗服务圈中达成数据的高效运用的技术。伴随着智慧医疗系统的更广泛应用，政府、医疗体系、保险公司必然进行更多信息的收集、处理、分析工作，这对智慧医疗安全的需求也不断提升，相关产业发展迅猛。

全球智慧医疗市场在移动医疗、智慧医疗设备、远程医疗等医疗新模式的带动下快速发展。美国联邦通信委员会（FCC）于 2020 年 4 月发布《COVID-19 远程医疗计划》。德国于 2019 年 2 月，在柏林建立“健康创新中心”。韩国 KT 公司与三星医疗中心 2020 年 1 月宣布共同开发创新型智慧医疗服务，建议 5G 智慧医院。日本厚生劳动省 2017 年 5 月制定《健康信息系统安全指引》。

我国政府大力支持以智慧医疗助推健康中国建设，加大基层健康领域科技支撑力度。2018 年 4 月，国务院办公厅印发《关于促进“互联网+医疗健康”发展的意见》；2018 年 9 月，国家卫生健康委员会（以下简称卫健委）引印发了《国家健康医疗大数据标准、安全和服务管理办法（试行）》。2019 年的《健康中国 2030 规划纲要》提到，要实现医保智能监控。2019 年 12 月，卫健委发布《关于落实卫生健康行业网络信息与数据安全责任的通知》。2020 年 5 月 21 日，国家卫健委发布《关于进一步完善预约诊疗制度加强智慧医院建设的通

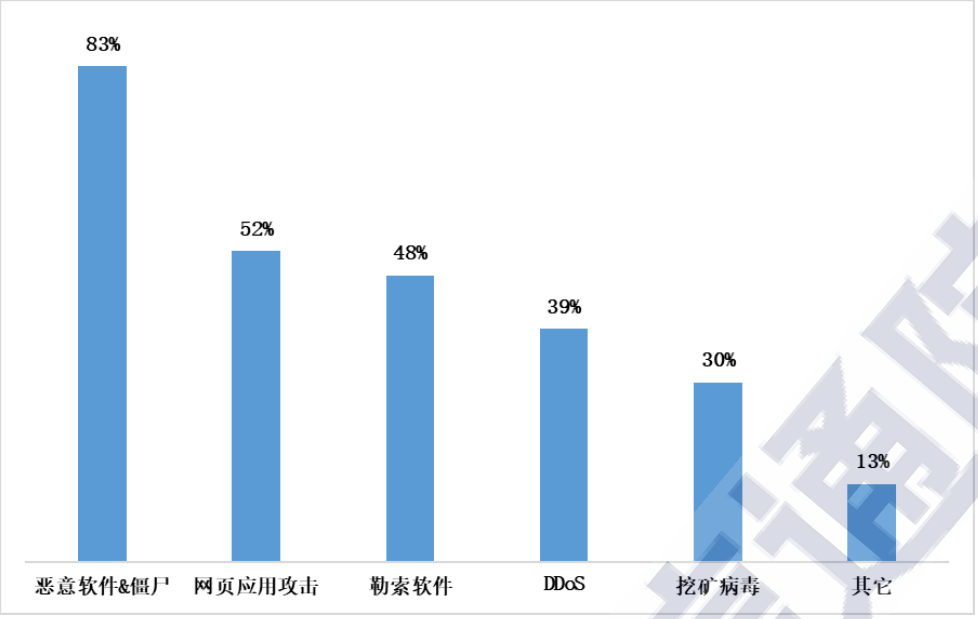
知》。

二、产业发展关键环节

智慧医疗安全产业发展的关键环节包括医疗设备安全、网络安全、数据安全三个方面。

在医疗设备安全方面，智能化医疗设备随物联网发展更好的保障市民安全健康，同时也面临更多安全挑战。智能医疗终端、视频终端、可穿戴传感器可打破时间空间限制协助医生进行医疗服务或对患者进行实时监控，但智慧医疗设备本身由于其“轻量级”特点，导致其本身缺乏完备的安全防护能力，在隐私保护、授权、传输加密、软件保护等多方面都存在安全隐患。应构建物联网医疗设备安全的保障体系，发展医疗设备安全测试、评估认证、漏洞披露、密钥管理、数据加密等解决方案。

在网络安全方面，随着国家智慧医疗信息化的建设，患者信息等医疗数据实时、可靠、安全的网络传输当得到进一步保障。但网络建设与运营中也同样面临着以勒索软件为代表的恶意网络攻击等一系列安全挑战。根美国网络安全咨询公司 Radware 2020 年的医疗解决方案报告显示，2019-2020 年间因网络攻击而受损失的医疗机构中 83%遭受了恶意软件与僵尸设备的攻击。面对智慧医疗中的网络安全问题应采用适当的安全系统，包括构建网络架构协议层面的安全审计，分别针对居民健康数据区和服务区限制非法访问，从而达到限制不安全数据传递的目的。



数据来源：Radware，2020

图 2-10　2019 年全球医疗机构遭受的网络攻击

数据安全方面当实现智能准确的数据管理。云端互通电子病例的数据采集工作可以有效地整合入日常的医疗服务，患者自身也可以有效的参与进数据管理之中。同时，医疗信息由于其隐私与敏感性很容易成为网络犯罪分子的目标，2019 年 RSA 数据与隐私安全调查，在欧洲和美国的消费者中 61%的受访者担心他们的医疗数据被泄露，根据德勤《新冠病毒相关数据隐私保护网络安全简报》报告，暗网上非医疗个人信息的平均价格是 0.1 美元每条，而医疗个人信息则超过 5 美元每条。近年来，在推广电子病历信息化工作的过程中，着重强调了电子病历管理相关的标准与规范，处理医疗信息的人员采取更严格的保密措施，包括但不限于应用电子签名验证执行程序、多因素验证远程登陆用户。

三、典型案例

（一）智慧医院安全领域

为保障医疗专网和相关网络、医疗设备数据的传输服务质量，确保医患敏感信息安全保密，2019 年 9 月，在国家卫生健康委指导下，全国 30 余家省部级医院及多个运营商联合启动《基于 5G 技术的医院网络建设标准》制定工作，促进 5G+医院网络规模建设的同时保障质量和安全，提升医疗健康行业的技术和服务。方案最终要求设备医院 5G 无线接入网络的设备支持安全启动和安全存储；支持安全 O&M 通道、安全用户管理机制、安全告警、事件日志。要求传输支持采用无线接入设备与网管、核心网直接基于数字证书的双向认证。2019 年 11 月中国电信发布了“5G+云+AI”智慧医疗解决方案。2020 年 1 月，火神山医院的建设中，中国电信天翼云为医院 HIS、PACS 等核心系统部署提供计算与存储能力，并提供内网区、互联网区及运维区的安全防护。搭建了高速、稳定和安全的基础网络，承载两家医院全部病区的医疗数据和信息共享与安全、保障各种医疗软件应用正常运转。

（二）远程医疗安全领域

远程医疗平台可以促进医疗资源的有效利用，同时因医疗业务特点，具备完整性、连续性、稳定性等多方面的安全要求。2018 年 6 月，国家卫健委指导，由中国移动联合中日友好医院建设的国家级远程医疗协同平台上线，在提升安全防护的基础上，促进医疗数据互联互通，建立规范有序的“互联网+健康医疗”。中日友好医院基于满足网络安

全等级保护制度2.0标准的基础上，创新应用了人机共智安全运营模式，通过全面梳理业务资产，建立漏洞管理机制，实时监测整体网络进行，建立威胁管理机制，提升业务系统强壮性，并持续规避高级威胁。安全系统根据安全事件发展进程动态调整安全策略，逐步提升安全状态，由原本“检测”为主的“被动运维”安全体系，转向“检测和响应”并举，从而建立紧急机制及时止损，为平台构建持续的安全保护能力。2020 年 2 月，远程医疗协同平台承担新冠肺炎重症、危重症患者远程会诊任务，新入驻医院数130多家，并有效开展远程指导武汉雷神山医院部署、新冠疫情防控科普直播等工作。

（三）医疗数据安全领域

智慧医疗系统大规模建立的电子病历、电子健康档案等健康信息的数据安全保障尤其重要。2018 年 12 月，国家卫健委印发了《电子病历系统应用水平分级评价管理办法（试行）》和《电子病历系统应用水平分级评价标准（试行）》，将电子病历系统应用水平划分为9个等级，提出了医疗安全质量管控、健康信息整合，医疗安全质量持续提升等高等级要求，面向全国范围医院推动电子病历升级。2020 年 5 月，卫健委发布《关于进一步完善预约诊疗制度加强智慧医院建设的通知》，明确以“电子病历”为核心，确保医疗数据安全有效应用，实现诊疗服务全流程闭环覆盖，加强互联网医疗服务中的患者隐私保护，完善隐私保护有关制度和措施。

第四章 数字安全十大技术赛道

1 人工智能安全技术

一、基本背景

人工智能安全技术是以机器学习、深度学习、神经网络等人工智能技术要素为基础，与网络、数据、终端、身份验证、应用、云和物联网等安全领域技术广泛融合，实现防护、检测、响应及预测等多方面安全能力的技术集合。

在国家战略驱动下，人工智能安全技术已逐步成为数字安全产业各领域的基础性技术之一。自 2013 年以来，全球已有美国、欧盟、英国、日本等 20 余个国家和地区发布了人工智能相关战略、规划或重大计划。**我国大力加强人工智能的发展引导，并将其上升至国家战略。**2015 年 7 月，国务院出台《关于积极推进“互联网+”行动的指导意见》。 2017 年 7 月，国务院发布《新一代人工智能发展规划》，人工智能首次加入国家战略规划。2017 年 10 月，党的十九大报告进一步强调“推动互联网、大数据、人工智能和实体经济深度融合”。2020 年 4 月，国务院常务会议提出，要加快推进包括人工智能在内的新型基础设施建设。

二、市场需求

人工智能安全技术是适应当前数字安全智能攻防形势的必然要求。近年来，网络攻击日益增多且越来越自动化、智能化，黑客的攻

击手段日趋复杂与多样，新型威胁层出不穷，自动化传播形成规模冲击，传统防御策略和安全能力难以及时识别和应对威胁。与之对应，安全防守方亟需人工智能技术加持以提升自动化防御水平，进行基于机器智能的攻防对抗，促进自动系统和人类在安全领域中的有机结合，推动数字安全领域向智能化全面迈进。

人工智能安全技术是数据安全防护手段的重要发展方向。在数据安全领域，更多的传统防御方式需要依赖人工策略部署和判别，通过对用户访问数据的行为方式分析甄别，如非授权账户访问、陌生 IP 访问、异常流量等信息以及 0-day 攻击、APT 等新型威胁，通过人工从海量数据中分析甄别数据安全风险行为，难以适应当前迅速变化的安全威胁形式。通过利用人工智能安全技术，利用人工智能的算力，通过大量的样本学习，形成智能化、自动化的识别能力，可以有效地发现异常的数据访问行为，及时进行响应和防御。

人工智能安全技术是新型基础设施安全发展的必备保障。加快建设人工智能等技术演化和深度应用、创新形成的新型基础设施，是当下助力产业升级、培育新动能、带动创业就业，实现“一业带百业”的重要内容。伴随新基建的发展，安全威胁击将从数字空间延伸到物理空间，人工智能安全技术在同步构建新型基础设施安全保障体系中将发挥重要作用，包括网络、终端、数据、应用、传感器、芯片等不同的新基建维度，都需要人工智能安全技术的有效保障。

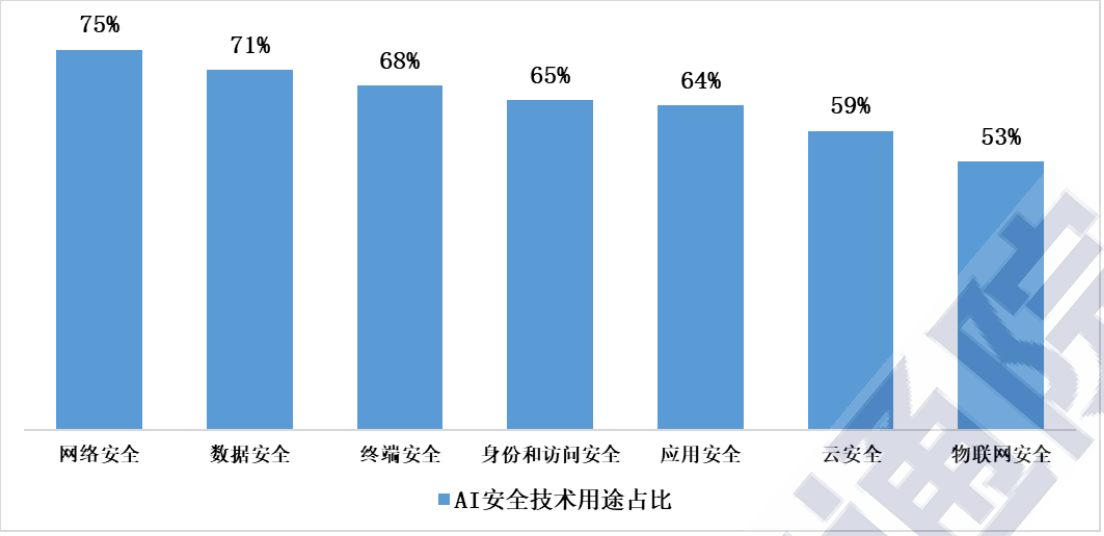
人工智能安全技术是社会治理现代化的关键驱动力。人工智能安

全技术应用场景不断丰富，在社会治理的教育、社保、养老、保障、医疗、卫生等领域广泛应用，有力支撑社会治理体系和治理能力现代化的需要。人工智能安全技术能实时监测社会经济运行中出现的各类威胁和风险，感知和判断安全态势，及时溯源发布预警，采取有效的防控举措，智能化应对社会治理中的安全问题，变革社会治理的方式，提升社会治理服务水平和治理效率。

三、典型应用

（一）网络与信息安全领域

人工智能安全技术广泛应用于网络与信息安全领域，例如在安全数据层面，人工智能安全技术能过滤无效信息，产生精准的安全情报、规则或者签名，减少人工分析提高工作效率。在安全检测层面，一方面可基于监督学习，建立分类模型，有效识别威胁的真实性。另一方面可基于无监督学习，建立行为基线，检测未知威胁。在安全认知层面，人工智能可基于安全攻防知识、资产的脆弱性和重要性、情报等知识进行推导，实现高级威胁识别和决策处置，同时可加快响应速度，减少系统受损程度和增加对 APT 攻击的预判。



来源：凯捷咨询公司（Capgemini）企业调查报告，2019

图 3-1 企业组织人工智能安全用途类型占比

（二）社会治理安全领域

我国经济社会正处在数字化转型的关键阶段，人工智能安全技术能对社会治理、服务、运营等环节存在的安全风险和威胁提供安全防控能力。例如在骚扰电话治理方面，骚扰电话问题黑灰色产业鱼龙混杂，呼叫规模大，呼叫类别广泛，参与主体众多，利用传统技术手段难以实现有效的管控。在工信部指导下，中国信通院、三大基础电信企业等单位共同参与建设了全国谢绝来电综合服务。全国谢绝来电服务依托于 VoLTE 网络，在 IP 化网络中基于人工智安全技术实现实时的、主被叫两端的监测拦截防护，扩展智能化、精准化的识别和拦截手段，为用户提供智能接听、数据保护等有效防护。

（三）公共卫生安全领域

人工智能安全技术在抗击新型冠状病毒肺炎疫情总体战中，发挥了重要作用。为支撑疫情防控相关部署，人工智能与大数据技术向结

合， 诞生了“健康码”、“健康宝”等防疫应用，将健康状态结果分类为“集中观察”、“居家观察”、“未见异常”三种状态，并分别用红色、黄色、绿色三种颜色进行标识，解决了地域间流动人员的个人健康状态查询问题，为抗击疫情提供数字化安全管理模式，为各行业复工复产提供有力支撑。

2 区块链安全技术

一、基本背景

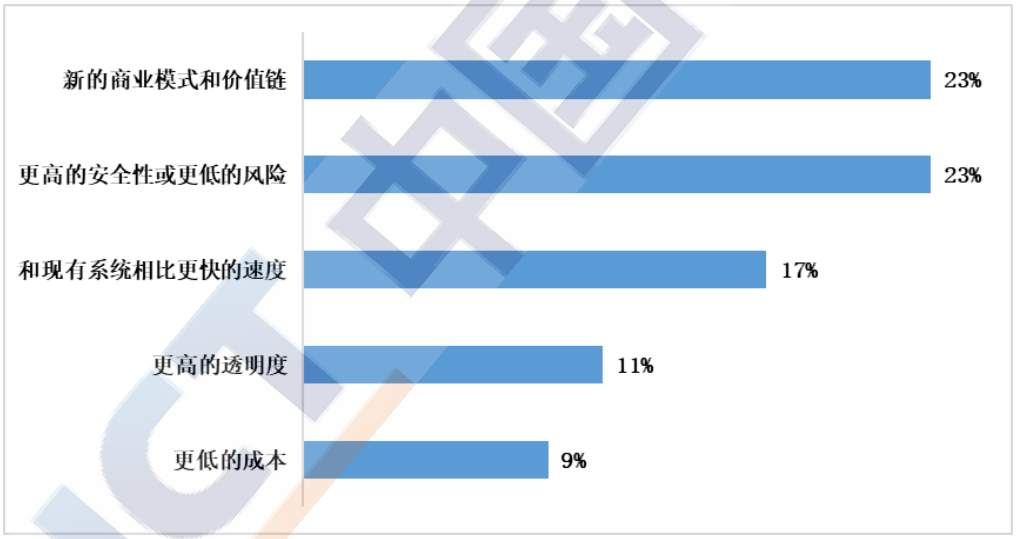
区块链安全技术以区块链技术为基础，具备去中心化、透明性、开放性、自治性、不可篡改、可追溯等特性，是旨在解决经济社会各领域安全性问题的技术解决方案。

世界各国广泛关注区块链，多措并举加速推进区块链安全技术在本国的发展布局。如英国 2016 年 1 月发布报告《分布式账本技术：超越区块链》，瑞士 2018 年 12 月发布《瑞士分布式账本技术和区块链的法律框架：以金融部门为重点视角》，澳大利亚 2019 年 3 月发布国家区块链战略路线图，美国 2019 年 7 月批准《区块链促进法案》，德国 2019 年 9 月发布《德国国家区块链战略》等。

我国高度重视区块链发展，加强对区块链安全技术发展的规划引导。2016 年 10 月，工业和信息化部发布《中国区块链技术和应用发展白皮书（2016）》，提出我国区块链技术发展建议。2016 年 12 月，国务院印发《“十三五”国家信息化规划》，鼓励针对区块链等战略性前沿技术进行提前布局。2019 年 1 月，国家互联网信息办公室发布《区块链信息服务管理规定》，促进区块链技术及相关服务的健康发展。2019 年 10 月，习近平总书记在主持中共中央政治局第十八次集体学习时强调，要把区块链作为核心技术自主创新重要突破口，加快推动区块链技术和产业创新发展。2020 年 4 月，国家发改委正式将区块链技术纳入新基建范畴。

二、市场需求

区块链安全技术为解决数字安全问题提供创新性思路。区块链安全技术能够解决传统领域信任和安全问题，具备更好的安全优势、变革创新业务模式，在数字金融、物联网、智能制造、供应链管理、数字资产交易、社会治理和民生服务等多个领域发挥重要作用，有效支撑虚假金融交易、商品假冒伪劣、食品污染、资金截留挪用等安全风险管理，促进经济社会持续健康发展。据高德纳咨询公司（Gartner）预测，到 2023 年，区块链将支持每年 2 万亿美元的商品和服务的全球流动和跟踪。



数据来源：Deloitte，2019 年

图 1 受访者关注的区块链前五位技术优势

区块链安全技术成为各类组织推动数字化转型的战略性选择。鉴于区块链在保障及解决安全性问题等方面的技术优势，针对区块链安全技术的投资已逐步成为企业、组织机构的重要选择之一。2019 年德勤全球高管调查数据显示，71%的受访者认为区块链提供了比传统 IT

解决方案更好的安全性。2019 年 Gartner 调查显示，全球有 60%的企业期望在未来三年内部署区块链技术及应用，另据 2020 年国际数据公司（IDC）报告预测，2020 年全球区块链市场整体支出规模将达到 42.8 亿美元。

区块链安全技术是保障用户个人信息和数据安全的重要支撑。区块链安全技术一方面解决链上数据被篡改、未被授权访问等问题，保障数据安全，防范用户隐私泄露，另一方面其解决数据共享规则、匿名化等问题，打通数据共享和使用壁垒，促进业务协同，保障数据要素的安全、有序、高效流动。据世界经济论坛预测，到 2025 年全球 GDP 总量 10%的相关信息将基于区块链技术保存。

三、典型应用

（一）网络与信息安全领域

区块链安全技术被广泛应用于网络与信息安全领域，典型用例涉及多个方面。一是支持攻击发现和防御，使用区块链技术识别黑客对关键基础设施重要数据库的网络攻击，并追踪黑客攻击的来源；使用区块链技术建立分散式平台系统，允许用户出租空余带宽，并共享给遭受分布式拒绝服务攻击（DDoS）攻击的网络节点，帮助其缓解遭受的攻击。二是支持更安全的 DNS 架构，使用区块链技术的域名服务器，能支持域名管理，防止域名服务器缓存投毒。三是保护边缘计算设备，使用区块链技术给物联网边缘计算终端设备分发数字证书或提供身份认证体系，确保数据传输、运算和存储的安全。四是提高公

钥基础设施（PKI）安全性，使用区块链作为域名及其公钥的分发账本，或者基于区块链创建无秘钥签名基础设施，杜绝虚假秘钥的传播。五是保障通信安全，利用区块链创建外来攻击无法渗透的安全消息服务、保护即时聊天工具和社交媒体上流转的隐私信息。六是保障数据安全，基于区块链技术提供可审计、合规的物联网数据完整性保障服务。

（二）新型基础设施安全领域

区块链安全技术应用于基础设施领域，可提供安全、可靠、可扩展的基础设施服务载体。2019 年 10 月，国家信息中心、中国移动、中国银联等机构正式发布“区块链服务网络（BSN）”，基于区块链技术构建跨云服务、跨门户、跨底层架构的全球性基础设施网络，能够为开发者提供公共区块链资源环境，极大降低区块链应用的开发、部署、互通和监管成本，具有安全可控可监管、完全自主创新、开放包容可持续等特点。2020 年 4 月，BSN 正式商用，已建成 128 个公共城市节点，其中海外节点 8 个，囊括了主流云服务商，打造了全球性区块链底层公共基础设施网络，并通过建立五级安全机制确保全网全链数据安全，同时还催生了公益慈善、物品溯源等创新应用，在新冠肺炎疫情防控中发挥了积极作用。

（三）金融安全领域

区块链安全技术广泛应用于金融风险管理及监管，保障金融交易的安全稳定。例如，在贸易金融方面，中国人民银行发起、联合多家

上市公司共同打造上线的“中国人民银行贸易金融区块链平台”，是基于区块链技术为贸易金融提供公共服务的金融基础设施，能推动银行机构贸易金融业务办理无纸化，实现对供应链应收账款多级融资、跨境融资、国际贸易账款等的系统监管，防控重复融资、虚假融资、虚假交易等业务风险。在数字货币方面，中国人民银行组织研发、测试中的数字货币和电子支付工具（DCEP)，是基于区块链技术的加密电子货币体系，DCEP 的后续正式落地，将有利于人民币的流通和国际化，有助于捍卫我国数字主权，阻止其他数字货币对我国货币安全的威胁，同时，也将有助于降低纸币匿名伪造、洗钱、非法集资和融资等风险。

3 边缘计算安全技术

一、基本背景

边缘计算安全技术是边缘计算的重要安全保障，是通过综合利用多种安全技术手段，以满足各应用领域对于边缘计算网络、数据、应用、设备等层面的安全需求为目标，形成的一系列安全技术、安全协议和防护体系的总称。

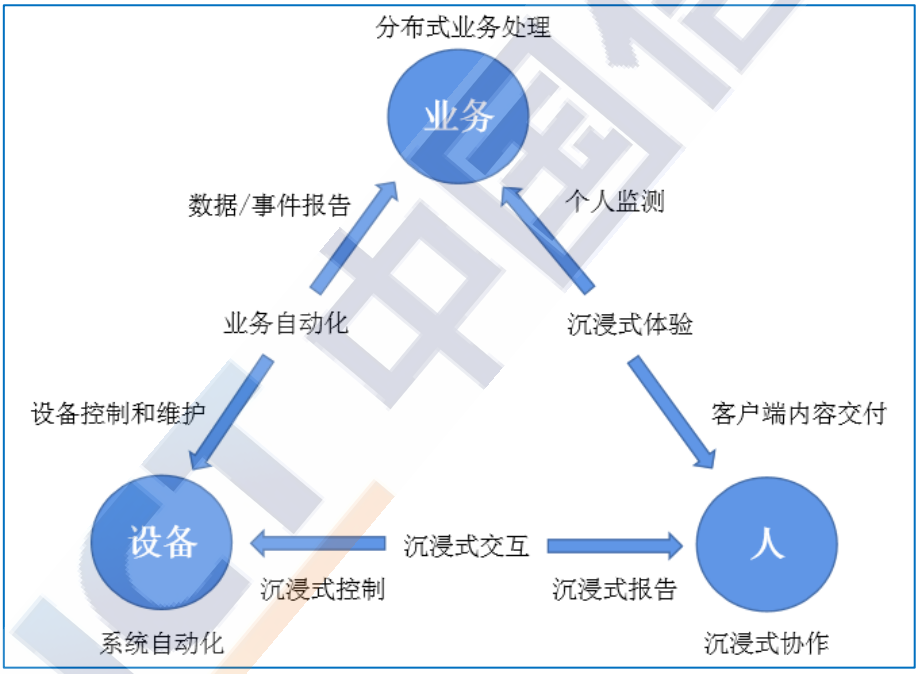
国际主流巨头公司纷纷参与边缘计算安全技术与应用的研究和投资。2017 年，亚马逊携 AWS Greengrass 进军边缘计算领域，将 AWS 扩展到设备上，实现本地处理数据，同时在云端进行管理、分析数据和持存储；谷歌已实现硬件芯片 Edge TPU 和软件堆栈 Cloud IoT Edge，旨在改善边缘联网设备的开发；微软公司计划截止到 2021 年，向包括边缘计算项目的物联网领域投入 50 亿美元；惠普公司计划截止到 2022 年，向边缘计算领域投资 40 亿美元。**国际标准化组织成立相关工作组，开展边缘计算标准化工作，逐步完善标准体系。**2014 年，欧洲电信标准化协会（ETSI）成立移动边缘计算标准化工作组。2017 年，国际标准化组织（ISO）成立了边缘计算研究组。2018 年，国际电联标准化组织 ITU-T SG20 完成了首个物联网领域边缘计算项目立项。

我国高度重视边缘计算发展，从顶层设计、技术布局等方面推动边缘计算产业规范、安全发展。2016 年 12 月，国务院印发的《“十三五”国家信息化规划》提出“到 2020 年，新一代网络技术体系、云计

算技术体系、端计算技术体系和安全技术体系基本建立”的目标。2020 年 5 月，工业和信息化部发布的《关于工业大数据发展的指导意见》中指出“推动人工智能、区块链和边缘计算等前沿技术的部署和融合”。

二、市场需求

边缘计算的潜在应用场景是非常多样、广泛和复杂的，Gartner 基于人、设备和业务之间的交互结构和关系，定义了 12 个边缘计算的应用场景，这些场景普遍需要边缘计算安全技术的参与。



来源：Gartner

图 3-3 边缘计算技术前沿应用场景

边缘计算安全技术为 5G 安全发展提供有力保障。边缘计算作为 5G 网络采用的新技术，可有效改善网络拥塞和响应时延长等问题，赋能 5G 高速发展。但是，边缘计算作为新技术也面临着如空口监听、非法访问存储数据、边缘节点数据损毁、应用安全漏洞等新的安全问

题。面对这些不利于“5G+边缘计算”发展的安全问题，需要通过边缘计算安全技术完善边缘计算服务的安全防护能力，为面向 5G 的边缘基础设施、边缘网络的部署和应用提供有力的安全保障。

边缘计算安全技术成为物联网应用的重要安全防护手段。当前，全球物联网应用正高速发展部署，但物联网应用节点分布广、环境复杂、计算存储能力有限等特点，带来了多方面的安全威胁与挑战。边缘计算安全技术能在边云协同、边缘网络、边缘数据、边缘基础设施安全等层面提供安全防护，为解决物联网应用安全提供了重要手段。据高德纳咨询公司（Gartner）公司预测，至 2021 年，全球超过 50%的大型企业将部署至少一个边缘计算应用来支持物联网或沉浸式系统。

边缘计算安全技术有效支持对隐私数据的保护。边缘计算将数据处理从云端迁移到临近终端、用户的一侧，使得边缘计算设备、节点可以获取到大量用户数据，涉及的数据也将更为私密，如个人生物识别数据、私人场所活动或关键工业数据等。边缘计算安全技术能通过处理、存储或丢弃适当的数据来满足保护隐私的需求，从而减少数据泄露风险。根据 Gartner 预测，到 2025 年，至少 75%的数据将在云或数据中心之外处理。

三、典型应用

（一）网络与信息安全领域

边缘计算安全技术能够在移动通信网络和行业应用中为边缘基础设施、网络、平台、应用、管理等层面提供安全防护支撑，助力企业应对各类数字安全风险。中国移动联合产业合作伙伴于 2019 年共同发布了边缘计算“Pioneer 300”先锋行动，面向 5G 及工业互联网等新兴领域，中国移动将在全连接的网络平面之上，依托边缘计算打造面向全行业的算力平面，构建 “连接+计算”新型智能基础设施；中国联通已于 2018 在 15 个省市开展了 Edge-Cloud 规模试点，打造智慧港口、智能驾驶、智慧场馆、智能制造等 30 余个试商用样板工程，到 2020 年，计划能达到真正的边缘 DS 云化资源池的构建，以及多网元共平台的实现。

（二）公共安全领域

边缘计算安全技术在公共安全领域的应用显著提升了数据处理效率和及时性，大幅节约了数据传输资源，在消防、安防、治安等诸多公共安全保障场景下发挥着良好的作用。2015 年至今，国家高度重视的以县、乡、村三级综治中心为指挥平台的“雪亮工程”持续推进建设，“雪亮工程”是以综治信息化为支撑、以网格化管理为基础、以公共安全视频监控联网应用为重点的群众性治安防工程，通过应用边缘计算安全技术，使得边缘智能设备对人、车、物等数据进行更全面、精准、实时的采集和处理，实现对重点人员、车辆的感知和预警，真正实现治安防控“全覆盖、无死角”。

（三）能源安全领域

边缘计算技术助力我国能源企业提升能源安全数据的感知、处理能力，成为保障能源安全的新举措。2019 年，国家电网公司全面部署泛在电力物联网建设，在其“云-网-边-端”的泛在电力物联网发展体系中引入边缘计算，提升电力数据的感知和处理能力。以智能精准运检场景为例，当前，以人工巡检为主的运检方式，效率较低，监控范围有限。在边缘计算技术支撑下，电网企业应用智能设备、高清摄像头等边缘自动化巡检设备，以自动化设备替代人工巡检。通过边缘自动化巡检设备采集的线路、变压器、电表信息，可快速识别故障隐患，提升故障抢修效率，保障电力能源安全，助力构成能源流、业务流、数据流“三流合一”的安全能源互联网。

4 敏感数据识别安全技术

一、基本背景

敏感数据识别技术是通过综合利用数据挖掘、语义扩展、特征识别、机器学习等技术，在特定的敏感数据发现机制下，实现对个人财产信息、健康信息，生物特征信息、证件信息等敏感数据精准识别和定级的一系列技术的集合。

世界主要国家和地区已普遍出台了敏感数据保护相关法案。2019 年，美国加州、缅因州、内华达州等多州均陆续出台了敏感数据保护相关的法案[1]。2020 年 1 月，欧盟发布的《数据保护与科学研究的初步意见》再次强调了遵循《通用数据保护条例》的重要性。印度于 2019 年 12 月发布了《2019 个人数据保护法案》草案，该法案界定了个人敏感数据范围，并对数据处理提出了明确的要求。

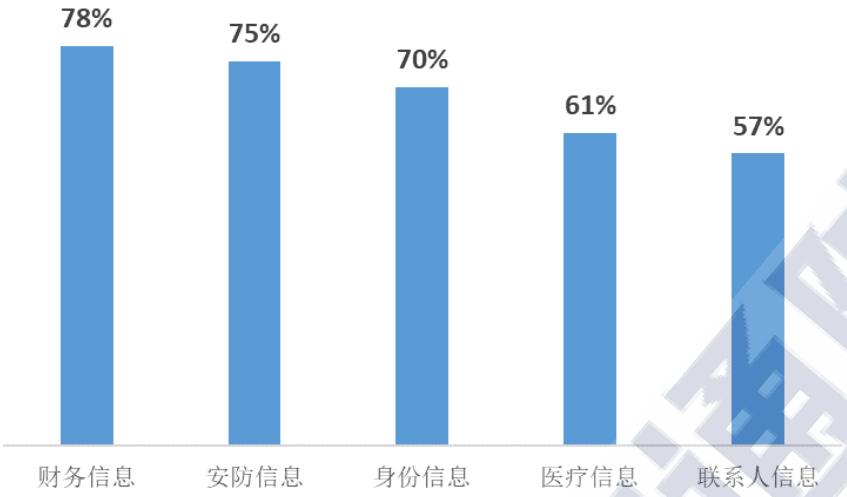
我国高度重视敏感数据保护工作，加快推进相关立法。2019 年 11 月，网信办、工信部、公安部、市场监管总局联合印发了《App 违法违规收集使用个人信息行为认定方法》。2020 年 4 月，央行发布的“2020 年规章制定工作计划”中涉及《个人金融信息（数据）保护试行办法》的修订。2020 年 5 月，十三届全国人大三次会议审议通过的《民法典》中对隐私权和个人信息保护的定义范围、个人信息保护要求等进行了规定。

[1] 2019 年 5 月，美国内华达州出台了新《内华达州数据隐私法》；2019 年 6 月，美国缅因州通过了《保护在线消费者信息隐私法案》；2019 年 10 月，美国加州通过了《加利福尼亚州消费者隐私法案》修正案。

二、市场需求

敏感数据识别技术提升差异化数据安全管理能力。当前，大数据、云计算技术快速发展，数据价值得以有效挖掘和利用，在为用户提供个性化服务体验的同时，也对敏感数据保护提出了挑战。目前企业、机构主要采取数据加密、数据库防火墙等传统安全防护手段保护敏感数据。但传统安全防护手段无法对数据的敏感程度做出区分，管理模式单一，多以全部加密、隔离等“强管控”模式为主。敏感数据识别技术可基于正则表达式、机器学习等技术精确识别敏感数据，对不同敏感程度的静态数据进行分级分类管理，在防止敏感数据泄漏的前提下，有效提升敏感数据管理效率。

敏感数据识别技术为安全使用动态数据提供有力支撑。敏感数据在调用过程中的动态安全是当前敏感数据安全防护的重要环节之一。在研发测试、数据分析等敏感数据使用过程中，为了防止开发及分析人员私自倒卖用户敏感数据，对企业及个人在经济、声誉等层面造成损失和影响，需要利用基于敏感数据识别的数据脱敏技术对开发测试、数据分析环境中的敏感数据进行精确识别和脱敏处理，从而在确保数据可用性的前提下，规避敏感数据泄露风险。据美国安全公司（RSA）发布的《2019 数据隐私和安全调查报告》显示，金融数据、安全信息、身份信息、医疗信息、联系人信息是受访者认为最需要保护的五类敏感数据。



数据来源：RSA，2020

图 3-4　受访者最关注的五类敏感数据

敏感数据识别技术有效强化数据安全事件溯源能力。当出现敏感数据安全事件时，为尽量降低安全事件所产生的负面影响，涉事机构必须及时采取全面的事件还原和严肃的追责处理。但往往因为数据访问者众多，数据泄露途径不确定，导致定责模糊、取证困难，溯源追责工作难以推进。引入敏感数据识别技术可实现敏感数据精确识别，通过在识别出的敏感数据集上嵌入隐式数字水印，实现对泄露人和泄露时间的定位，为快速完成溯源追责提供有力支撑。据美国安全公司（Risk Based Security）统计，2020 一季度，数据泄露量达到 84 亿条数据，同比增长 273%。

三、典型案例

（一）金融安全领域

随着银行业金融机构信息化技术的不断深入，应用水平的不断提高，银行业金融机构对敏感数据保护的要求日益提升，如何防止

用户金融信息、证件信息等敏感信息泄漏，避免敏感数据安全事件对银行声誉和经营造成的严重影响，是目前银行业金融机构安全工作面临的严峻挑战。敏感数据识别技术可助力银行业金融机构高效精准定位敏感数据，进而采取针对性安全保护措施，有效提升敏感信息数据的防护能力。2019 年 7 月，中国银行启动"数据中心网络安全能力提升专项"办公终端信息安全审计工具项目，该项目旨在通过敏感数据识别技术对终端数据进行识别及分析,监测敏感数据资产,建立精细化的敏感数据泄露安全防护系统，实现对行内终端的敏感信息数据的管控和防护。

（二）能源安全领域

能源数据安全是关系到国计民生的大事，随着世界网络空间局势日益复杂化，能源行业面临的终端安全威胁也在不断变化和扩大。如何对能源企业在传输、交易、消费过程中产生、使用的敏感数据进行有效保护，是当前能源行业安全管理面临的主要问题之一。敏感数据识别技术可高效发现能源企业在传输、交易、消费过程中涉及的敏感数据，实现分级分类管理，强化能源敏感数据安全防护能力。2019 年 1 月，中国石油天然气集团启动“信息内容审计平台 2.0 建设项目”终端敏感数据审计系统的建设工作。该系统基于敏感数据识别技术可实现对终端上的敏感数据自动识别，对各类型数据进行分级分类管控，能够有效降低系统敏感数据外泄，并抵御从外部对中石油集团体系内的各种敏感数据的窃取。

（三）物流安全领域

邮政快递业作为现代服务业的重要组成部分，在经济新常态下保持了快速发展的良好态势，业务规模不断扩大。但与此同时，寄递渠道安全形势日益严峻，收寄信息、用户信息等敏感数据面临的数据安全风险持续增大。针对当前寄递渠道安全监管面临的突出问题，为有效规避敏感数据泄露风险，2019 年国家邮政局推动建设了邮政寄递渠道安全监管‘绿盾’工程项目。该项目利用敏感数据识别技术，通过识别终端敏感数据，进而采取对敏感数据的加密保护、及时阻断外传、溯源水印嵌入、邮件告警等安全防护措施，保障物流数据和用户隐私安全。

5 生物特征识别技术

一、基本背景

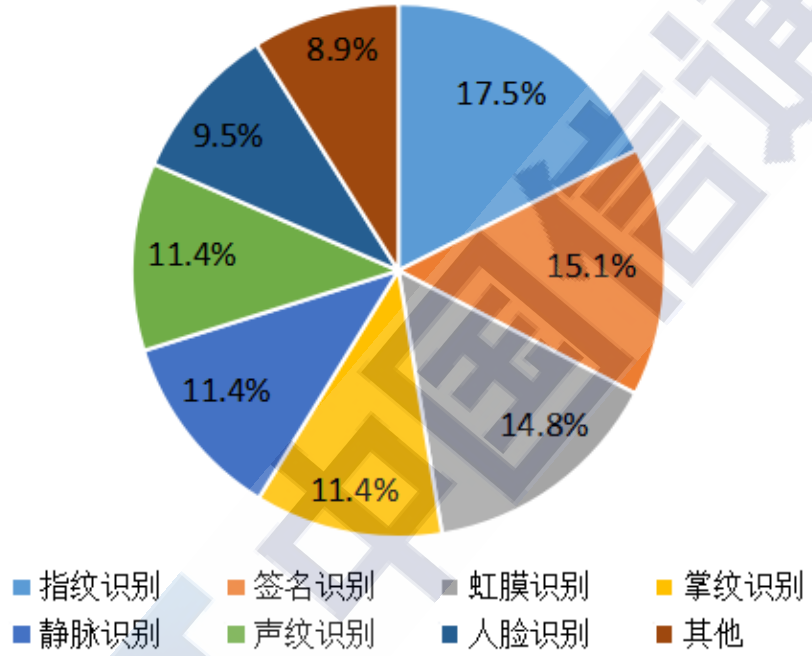
生物特征识别技术是通过计算机技术与光学、声学、生物传感器等科技手段结合，利用人的虹膜、人脸、指纹等生理特征或笔迹、声音、步态等行为特征，来进行个人身份鉴定的一系列技术的集合。

国际上广泛应用生物特征识别技术保护公共安全。美国于 2018 年 9 月发布了《2018 年生物识别迁移预警计划授权法案》。2019 年 9 月，美国情报高级研究项目局（IARPA）启动了“从高处和远处进行的生物特征识别和辨认”项目。2019 年 4 月，欧盟投票同意建立通用身份资源库，该资源库将收集 3.5 亿人的生物特征信息，并允许出入境控制、移民及执法系统调用。2019 年 7 月，日本法务省在主要机场部署了基于面部识别技术进行出境审查的通关门。

我国立足于人工智能发展，聚焦生物特征识别技术研发与应用。2017 年 12 月，工信部印发的《促进新一代人工智能产业发展三年行动计划（2018-2020 年）》提出，支持生物特征识别等技术创新，拓展在安防、金融等重点领域的应用。2019 年 7 月，银保监印发的《 关于推动供应链金融服务实体经济的指导意见》指出，鼓励银行业金融机构运用生物识别等技术，完善风控技术和模型，创新发展在线金融产品和服务。

二、市场需求

当前，生物特征识别技术正处于稳健发展与应用阶段，主要生物特征识别技术包括：指纹识别、签名识别、虹膜识别、掌纹识别、静脉识别、声纹识别、人脸识别等。据德国数据公司 Statista 统计预测，到 2022 年，指纹识别、签名识别、虹膜识别将成为市场收入规模排名前三的生物特征识别技术。



数据来源：Statista，2018

图 3-5　2022 年全球生物特征识别技术系统市场收入规模预测（单位：美元）

生物特征识别技术在各行业得到广泛应用。当前，随着经济社会数字化转型持续推进，各行业数字化进程不断加快，数字化服务能力不断提升。同时，用户在使用数字化服务的过程中，对数据安全、信息安全保障的需求日益增强。生物特征识别技术作为一种平衡安全与便捷的身份安全验证手段，具有识别精度高、速度快、防伪性强等特点，已在金融、零售、社保、安防等多个领域得到广泛应用，市场规模不断扩大。据美国市场研究机构（MarketsandMarkets）预测，全球

生物识别系统市场规模将从 2019 年的 330 亿美元增长到 2024 年 653 亿美元，预测期内的年复合增长率为 14.6%。

生物特征识别技术助力强化安全访问控制能力。目前，办公场所、社区、实验室、校园等多是采用基于特定物理介质（电子工牌、钥匙、校园卡等）和特定知识（密码、口令等）的传统方法进行流动人员的安全访问控制，但特定物理介质和知识存在被窃取、伪造的风险。生物特征识别技术具备难窃取、防伪性强等特点，无需物理介质或密码口令即可快速完成身份安全验证，有效弥补了传统访问控制方式的缺陷。据美国透明度市场研究咨询公司（Transparency）预测，到 2025 年，生物识别门锁系统将占数码锁系统市场份额的 73%。

生物特征识别技术逐步成为智能终端的必备安全功能之一。随着 5G 网络发展，智能终端设备数量快速增长，在智能家居、移动办公等领域得到了普遍应用。为确保用户信息安全、财产安全，智能终端设备需引入生物特征识别技术提升身份安全验证的准确性。智能终端可通过搭载生物识别传感器提取用户指纹、人脸、声纹特征，运用生物特征识别算法准确完成用户身份安全验证。据 Transparency 预测，到 2023 年，全球生物识别传感器市场将达 18 亿美元。

生物特征数据具有特殊性需重视数据保护问题。随着生物特征识别技术在诸多领域得到广泛应用，越来越多的生物特征数据被采集、储存和使用。生物特征数据具有无法修改、难以再生等特点，这就意味着生物特征数据一旦被泄露，不仅会对用户信息财产安全造成危害，

还会导致用户的该生物特征可能再也无法被使用，给用户个人信息安全造成“永久性”的损失。因此，生物特征数据保护尤为重要。据俄罗斯安全厂商卡巴斯基（Kaspersky）统计，在 2019 年第 3 季度，用于收集、处理和存储生物特征数据的计算机中，有 37%面临恶意软件感染的风险。

三、典型应用

（一）公共卫生安全领域

随着疫情防控进入常态化，做好机场、车站等人员密集公共场所的防控工作显得尤为重要。生物特征识别技术可以在口罩遮挡和非接触的条件下有效完成个人身份核验。在实现体温筛查、重点人群甄别和追踪的同时，大幅提升人员通行效率。2020 年 2 月，北京西站部署了移动式双光快速温测智能识别系统，该系统基于人脸识别技术，实现对通行人员进行快速准确、非接触式的体温检测，为开展快速体温筛查提供新技术支撑。2020 年 2 月，广州市交通运输部门在市内公交车上部署了人脸识别测温仪，支持乘客在乘车支付的同时系统自动完成测温。2020 年 3 月，长沙地铁上线无感红外人体热成像测温系统，该系统利用人脸识别技术，实现乘客异常体温声光报警、是否佩戴口罩告警等能力。

（二）金融安全领域

随着经济社会发展，金融服务场景和应用愈加多元化。为满足客户对更安全、便捷、高效金融服务的需求，我国银行业金融机构陆续

引入生物识别技术，在远程开户、审核管理、支付结算等场景下，为用户提供更方便、安全、快速的身份认证体验。2019 年 10 月，中国银联联合工商银行、农业银行、中国银行、建设银行、交通银行、邮政储蓄银行六大国有银行在内的 60 余家机构，正式发布了基于生物特征识别技术的全新智能支付产品“刷脸付”。“刷脸付”通过人脸识别实现交易路由，用户完成银联卡绑定后，在商超、餐饮、自助售货机等场景结算时，无需使用任何物理介质，只要完成“刷脸”操作并输入支付口令，即可完成付款，显著提升了客户支付体验，增强了金融服务获得感。

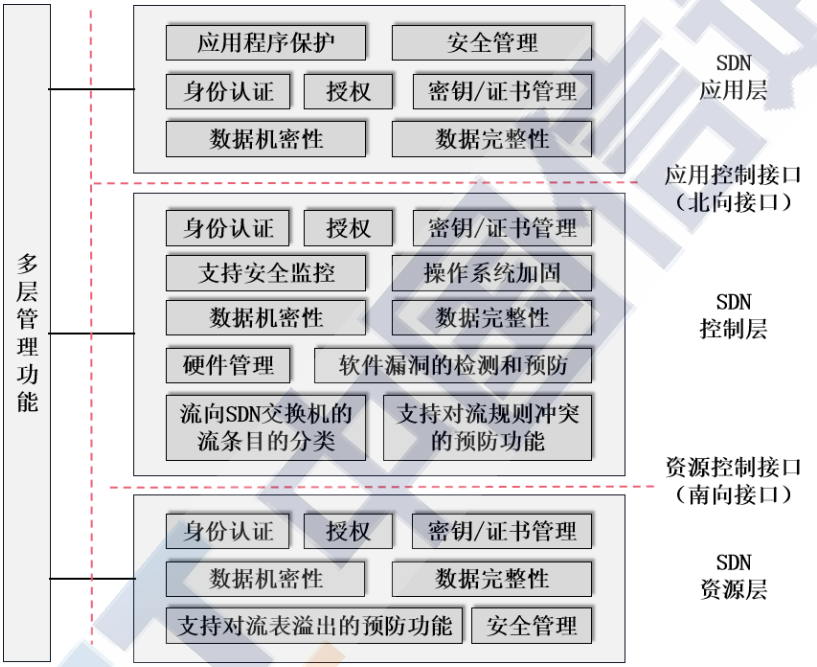
（三）校园安全领域

校园安全建设是教育管理工作中的重要组成部分，是各项教育工作正常开展的前提和基础。为扎实做好校园安全建设工作，筑牢校园安全防线，我国高校纷纷借助生物特征识别技术完善技术安全防护手段建设。中国移动针对校园安全领域推出了“和识”5G 智慧校园解决方案，该方案利用人脸识别技术，提供刷脸安全出入、访客线上管理等多项功能，增强了图书馆、实验室等重要场所的安全性。截止 2019 年，中国移动“和识”5G 智慧校园解决方案已在北京邮电大学、北京师范大学、江苏启东中学、浙江多元艺术幼儿园等多个院校落地，全面覆盖各层级教育场景。

6 软件定义安全技术

一、基本背景

软件定义安全技术是以提升软件定义网络（简称 SDN）安全性为目标，重点从保障 SDN 控制层安全、应用层安全、资源层安全、接口安全等方面入手，综合运用多种安全技术手段，形成的一系列安全技术、安全架构和安全机制的总称。



来源：ITU-T

图 3-7 软件定义安全技术参考框架

国际普遍关注 SDN 安全性保障工作，优化基于 SDN 的安全防护能力。2018 年 9 月，美国陆军研究实验室、新西兰坎特伯雷大学和韩国光州科学技术研究所共同研发了基于软件定义网络的移动目标防御技术（MTD），以抵御网络攻击。2019 年 12 月，美国国家科学技术委员会（NSTC）发布的《联邦网络空间安全研发战略计划》提出，为虚拟化无线接入网络以及核心网络的软件定义网络的安全性，开发软件保障解决方案。欧洲网络与信息安全局(ENISA)于 2019 年 11 月

发布的《5G 网络威胁图谱》中将 SDN 安全威胁归类为影响 5G 网络安全的因素之一。

我国高度重视 SDN 应用发展，从完善技术标准、鼓励落地应用等方面推动 SDN 产业安全发展。2019 年 1 月，工信部印发的《工业互联网网络建设及推广指南》强调，制定工业软件定义网络等新型网络技术标准。2019 年 5 月，工信部、国资委联合发布的《关于开展深入推进宽带网络提速降费 支撑经济高质量发展 2019 专项行动的通知》指出，鼓励基础电信企业积极开展试点示范，利用 SDN、NFV（网络功能虚拟化）等多种技术，持续提升网络效率和服务能力。

二、市场需求

软件定义安全技术为 5G 网络安全发展提供有力保障。5G 网络架构通过引入 SDN 可以在提高系统的灵活性、可扩展性和效率的同时，有效降低成本。但是，由于 SDN 打破原有网络封闭状态、使得安全边界模糊化，传统网络中依赖于物理安全设备隔离来提供防护的安全机制在 5G 网络中难以适用，故需通过软件定义安全技术为面向 5G 网络的 SDN 提供有力的安全保障。美国智库布鲁金斯学会（Brookings Institution）发布的《5G 需要新的网络安全方法》指出，5G 网络架构由传统的集中式、基于硬件的网络变成了分布式的 SDN，更易受到网络攻击。

软件定义安全技术助力工业互联网安全发展。伴随着工业互联网向着 IP 化、扁平化、灵活组网的方向演进发展，SDN 正逐步成为工业互联网网络技术发展的重要方向。SDN 赋能工业互联网显著扩

展了网络空间的边界和功能的同时，也使得工业系统与互联网的安全边界日益交叉，在工业控制、工业数据、业务应用等层面面临诸多安全风险与挑战。软件定义安全技术可有效保障 SDN 控制层、数据层、应用层的安全，助力工业互联网安全发展。

软件定义安全技术为云计算搭建安全防护体系。随着云计算技术的广泛应用，以及分布式拒绝服务攻击（DDos）、高级可持续威胁攻击（APT）等网络攻击日益频繁，传统网络安全模式面临着巨大挑战。在云计算环境中，传统网络安全模式难以按需提供弹性的安全功能，无法满足云计算环境灵活的业务发展需求和安全防护要求。软件定义安全技术通过将控制层与数据层的分离，可形成一套自动化、动态弹性、可按需扩展的云安全防护体系，从而实现在提升云计算网络资源动态管理效率的同时，强化安全防护能力和用户安全体验。

三、典型应用

（一）5G 网络安全领域

5G 网络建设通过引入 SDN 技术对网络架构进行了重构，在实现更好地支撑多样化行业应用的同时，也借助软件定义安全技术提供了更灵活的安全架构，即可实现共性安全的统一考虑，又能为具体行业应用按需配置安全机制。2019 年 5 月，中国移动、中国电信、中国联通与安全公司和科研机构联合成立了 5G 安全协同创新中心，重点推进 SDN 控制器安全防护等方面的研究。SDN 控制器

可以将原先离散的、异构的设备形成统一的逻辑安全资源池，并通过全局视野，对所有安全资源进行统一、灵活调度，实现分布式安全设备的协同工作，有效提升面向 5G 网络安全的防护效率。

（二）云计算安全领域

随着 SDN 技术在云计算网络、数据中心建设中得到广泛部署，作为保障 SDN 安全性的技术软件定义安全技术也在云计算安全领域得到了重点应用。软件定义安全技术可以在安全组网、安全服务编排、云虚拟机审计、安全运维等方面为云计算安全提供有效的安全保障。在软件定义安全技术的有力保障下，电信运营商纷纷引入 SDN 技术开展云计算建设，提升云计算的安全性。2019 年 8 月，中国移动完成了云能力中心华南节点 SDN 的升级工作，通过新增分布式防火墙功能，优化了 SDN 系统的安全性。2020 年，中国联通持续推进基于 SDN 的云服务产品“云联网”的应用，该产品依托基于 SDN 的 IP 骨干网，实现安全故障自愈、统一安全运维管理、访问控制等安全功能，从而可面向各行业提供安全可靠的多云连接及组网服务。

（三）工业互联网安全领域

当前，随着工业企业利用 SDN 对外网开展升级改造工作的逐步推进，软件定义安全技术在工业物联网安全领域发挥的作用日益凸显。2019 年,工信部印发的《工业互联网网络建设及推广指南》指出，要建立一批工业互联网网络新技术标准符合性试验验证系统。

2020 年 5 月，中国信息通信研究院启动了基于 SDN 的工业互联网网络试验验证系统建设工作。该系统通过引入软件定义安全技术，可实现对跨品牌安全设备的统一管理、构建基于业务按需提供防护的安全资源池，有效提升了试验验证系统的安全服务能力。

7 安全多方计算技术

一、基本背景

安全多方计算是现代密码学为解决安全计算问题提出的一系列安全协议的集合，其目的是为了使多个计算参与者在不泄露各自原始数据的前提下，完成分布式协同计算，并提取计算结果输出的价值。

世界各国普遍关注安全多方计算技术在数据隐私保护中的应用。当前，全球已有近 90 个国家和地区制定了个人信息保护的法律法规。随着国际社会对隐私数据保护的要求日趋严格，国际科技公司纷纷采用安全多方计算技术解决协同计算过程中的数据隐私保护问题。2018 年 10 月，美国科技公司 Unbound Tech 推出基于安全多方计算的无绑定加密资产安全平台，可为银行提供具备安全性的加密交易和钱包服务。2019 年 8 月，谷歌推出新型安全多方计算开源库，以隐私安全的方式帮助组织与数据集协同工作。

我国高度重视隐私保护工作，带动产业各方发展安全多方计算技术。2020 年 5 月，全国人大常委会工作报告在下一步主要工作安排中指出，围绕国家安全和社会治理，制定个人信息保护法。我国产业各方积极探索安全多方计算技术发展，标准化组织持续推进安全多方计算应用标准体系建设。中国通信标准化协会推动多项安全多方计算相关标准的制定，并于 2019 年 6 月发布了《基于安全多方计算的数据流通产品标准》。

二、市场需求

安全多方计算技术助力区块链提升隐私数据保护能力。当前，区块链技术快速发展，与众多垂直领域深度融合并落地应用。区块链具备不可篡改、可追溯、透明开放等特点在保证数据完整性的同时，也使得隐私数据保护成为制约区块链在部分行业应用的主要问题。安全多方计算技术可以在区块链的隐私智能合约、跨链交易、密钥管理、随机数生成等技术中发挥作用，提升区块链的隐私数据保护能力。据高德纳咨询公司（Gartner）预测，到 2021 年，75%的公共区块链可能发生将隐私数据添加到公有链上而导致违反隐私法的现象。

安全多方计算技术为人工智能隐私数据安全管理提供支撑。海量的数据资源促进了人工智能技术的蓬勃发展,但人工智能模型的训练集在数据采集、模型训练等环节中存在的隐私泄露风险,为人工智能的隐私安全管理提出了挑战。安全多方计算支持在不公开各参与方隐私数据的同时,保证计算结果的正确性,可与联邦学习等由多方参与、共同训练的模型结合，为其提供隐私数据安全管理支撑。据 Gartner 预测，到 2023 年，超过 75%的大型组织将雇用调查员进行人工智能行为取证以及隐私和客户信任专家，以降低品牌和声誉风险。

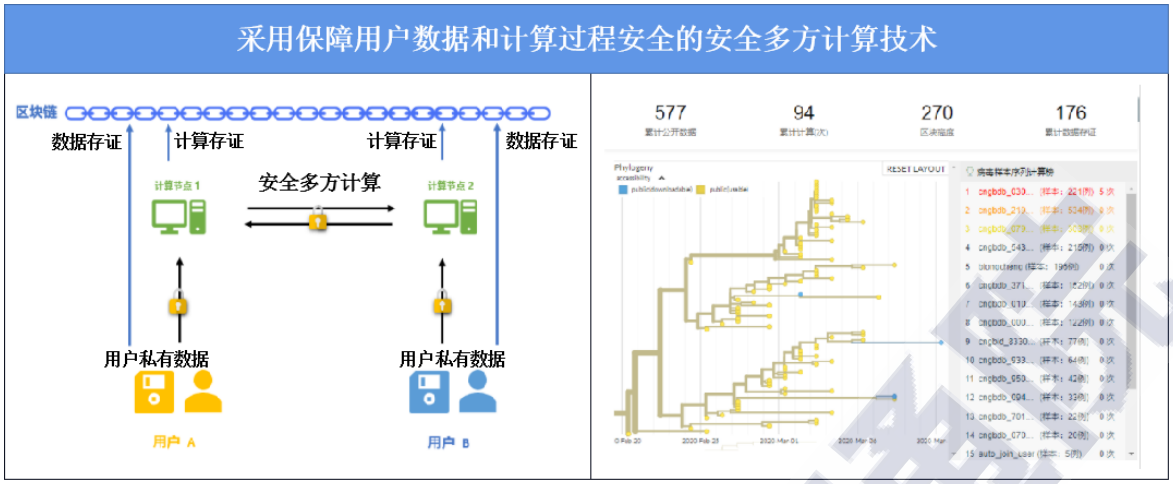
安全多方计算技术可在大数据分析中对隐私数据进行有效保护。随者大数据技术迅速发展，大数据处理、挖掘、分析场景愈加复杂，越来越多的大数据分析工作需要多方合作完成。在进行协同大数据分析任务时，各参与方普遍希望在保护自身隐私数据的情况下，获取协

同分析的结果。安全多方计算具有输入隐私性、计算正确性、去中心化等特点，可以在保护各参与方隐私数据的前提下，提取基于数据分享、挖掘分析的价值。从而在协同大数据分析场景下，有效满足各参与方对数据隐私保护的需求。

三、典型应用

（一）公共卫生安全领域

新冠肺炎疫情发生以来，党中央高度重视，始终把疫情防控工作作为最重要的工作来抓。在疫苗尚未研制成功、暂无针对新冠病毒的特效药的当前，推动病毒基因组数据共享，为抗疫提供科学依据和支撑尤为重要。为做好疫情防控工作，推动病毒基因组数据安全共享，由国家发改委、工信部、卫健委、财政部四部委指导建设的国家基因库生命大数据平台于 2020 年 3 月正式上线了新型冠状病毒基因组分析平台。该分析平台基于安全多方计算技术允许用户在不公布己方数据的前提下，以数据“可用不可见”的方式，与其他用户、科研人员联合进行多方协同计算并共享结果。实现实时追踪病毒流行病学情况、预测未来毒株演化，为评估新冠疫情风险、启动公共卫生应对措施提供更全面、有效的数据支撑。



来源：国家基因库生命大数据平台

图 3-7 安全多方计算在新型冠状病毒基因组分析平台中的应用

（二）金融安全领域

安全多方计算技术在金融科技领域得到重点应用，有效提升金融机构的风险识别和控制能力。2020 年 1 月，中国人民银行启动金融科技“监管沙盒”工作，通过推动金融科技创新试点应用，打造新型监管工具，引导金融机构和科技公司守正创新、规范发展。2020 年 6 月，中国人民银行将“多方数据学习‘政融通’在线融资项目”纳入金融科技创新监管试点应用（2020 年第二批）。该项目利用基于安全多方计算的联邦学习技术，在保障数据安全和个人隐私的前提下，使用互联网、政务、金融大数据联合建模，向金融机构提供风控产品，增强金融机构风控能力。

（三）政务安全领域

安全多方计算技术助力政府治理能力现代化，为政府部门与企业等各方数据的协同计算提供隐私保护，推动数字政府建设。2019 年 5 月，北京市海淀区政府建设了政务大数据加密融合共享平台。该平台

基于安全多方计算技术，可以在保证政务数据安全共享、规避数据泄露风险的同时，规定分享政务数据的用途和用量，助力海淀区政府推动政务大数据深度挖掘分析。

8 量子通信安全技术

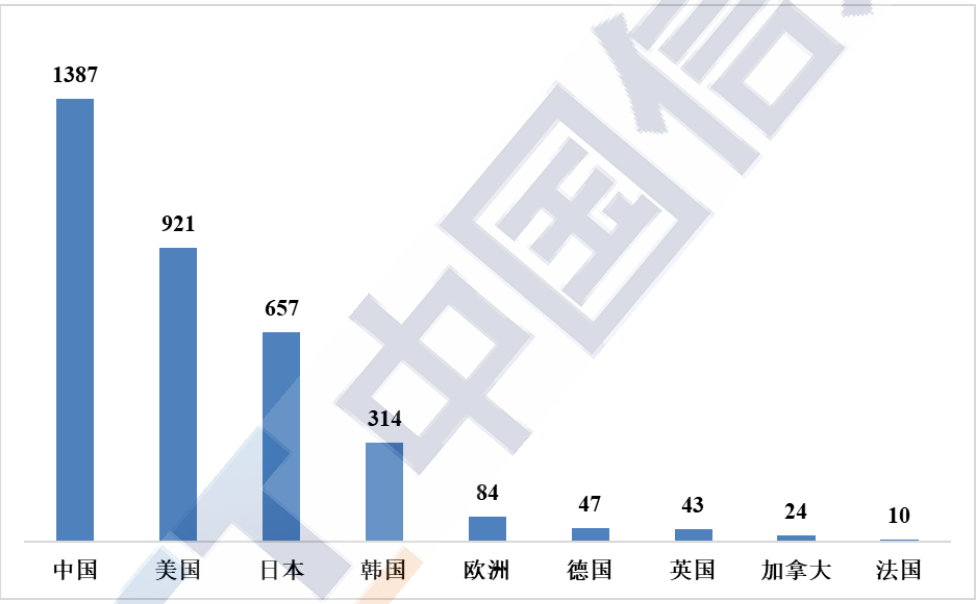
一、基本背景

量子通信安全技术基于量子力学原理，是利用量子态作为信息载体，并依据量子叠加态和量子纠缠效应进行信息和密钥传输的新型安全通信技术。量子通信安全技术作为量子信息技术领域的重要分支，在网络信息安全领域产生了重大影响，目前已经逐步进入产业化应用阶段。

近年来，为强化通信和信息安全保障能力，全球各国均加快量子通信安全技术的研究与应用。英国 2014 年设立了“国家量子技术计划”。德国 2018 年 9 月提出“量子技术-从基础到市场”框架计划。美国 2018 年 12 月通过了《国家量子计划（NQI）》立法，同期发布了《量子信息科学国家战略概述》。欧盟 10 国于 2019 年 7 月签署量子通信基础设施（QCI）声明，目前已有超过 20 个欧盟成员国加入该建设倡议。

我国高度重视和支持量子通信相关领域的研究探索，加快推进其发展与应用工作。量子通信安全技术在我国关于“十三五规划”的建议中明确被列为体现国家战略意图的重大科技项目。在国务院发布的《“十三五”国家科技创新规划》《“十三五”国家战略性新兴产业发展规划》等文件中，明确量子通信领域的顶层发展布局规划。2018 年 3 月，在政府工作报告中将量子通信列为重大科技创新成果之一。2018 年 5 月，习近平总书记在两院院士大会上的讲话中指出，“以人工智

能、量子信息、移动通信、物联网、区块链为代表的新一代信息技术加速突破应用。”2019 年 12 月，国务院发布的《长江三角洲区域一体化发展规划纲要》提出，加快量子通信产业发展，协同建设新一代信息基础设施。**我国在发展量子通信安全技术方面处于全球领先地位，**据 2019 年 3 月，日本科学技术振兴机构（JST）发布《从全球专利地图看量子技术 2.0》调查报告显示，1990 年至 2018 年我国量子通信相关公开专利数自以 1387 件居世界首位，其次是美国、日本。



数据来源：日本科学技术振兴机构（JST）

图 3-8　1990 至 2018 年各国公开量子技术专利数占比图

二、市场需求

以量子通信安全技术为基础的量子保密通信，是未来保障信息通信安全的关键技术，是网络和信息安全的战略制高点。量子通信安全技术主要分为量子隐形传态和量子密钥分发两类，其中，基于量子密钥分发技术的量子保密通信是未来提升信息安全保障能力的可选技

术方案之一。量子保密通信通过量子密钥分发产生密钥，与传统保密通信技术相结合完成经典信息的加解密和安全传输，提供了不再依赖于数学计算复杂度的新型密钥分发方法，使得密钥分发过程的防窃听和防破译的能力得到加强，使得量子通信本身成为了实现安全、保密通信的关键技术。

量子通信安全技术在新型基础设施建设中发挥重要作用，广泛应用于数字化发展的各个领域。当前，量子通信安全技术正助力新型基础设施的建设与发展，量子保密通信骨干网、城域网、星地一体化网络建设不断完善，全球化的广域量子通信网络部署提速，未来可作为电信网络、企业网络、个人与家庭等领域的重要组成部分，为各类数据安全提供有效保障，并在电子政务、金融行业、电力行业等多个领域实现大规模应用，在发展壮大数字经济、助力产业升级等方面发挥更大作用。

量子通信安全技术为移动终端用户数据安全问题提供新的解决方案。移动终端的数据安全问题被各界广泛关注，用户依靠智能终端处理和存储大量的个人数据，移动应用程序也收集了越来越多包括密码在内的敏感信息。利用量子通信技术的安全性，结合现有的经典加密技术，可将量子密钥分发技术生成的量子密钥应用于移动终端的安全防护，搭载量子芯片的量子智能终端能生成不可预测且无模式的纯随机数，帮助用户安全地使用特定服务，在移动办公、移动支付、移动作业等领域广泛应用。

三、典型应用

（一）骨干网安全领域

量子通信安全技术可用于为电信网络的骨干网节点之间通信提供安全服务，量子保密通信骨干网建设和相关试点应用项目在我国广泛开展。2017 年，由中国科学院牵头，中国科学技术大学承建的国际上首条千公里级量子保密通信骨干网络“京沪干线”正式开通。干线采用可信中继方式，连接北京和上海，贯穿济南、合肥等地，可满足上万用户的密钥分发业务需求，为沿线金融机构、政府部门等提供高安全等级的通信服务。2018 年底，国家广域广域量子保密通信骨干网络建设一期工程开始实施，在“京沪干线”基础上，增加武汉和广州两个骨干节点，新建北京—武汉—广州线路和武汉—合肥—上海线路。2020 年，中国科学技术大学与清华大学、山东济南量子技术研究院等机构合作，实现了 500 公里级真实环境光纤量子通信传输，为大幅减少骨干光纤量子通信网络中的可信中继数量、显著提升光纤量子保密通信网络的安全性打下坚定基础。同时，基于骨干网体系，我国已经具备了为多行业、多领域提供量子保密应用服务的能力。如在金融领域，依托于“京沪干线”，量子保密通信技术正逐步运用于金融业的数据信息传输交换、数据备份存储、网上银行加密、人民币跨境收付系统应集报送等多方面，进一步强化金融行业系统信息安全性。

（二）星地网安全领域

量子通信安全技术与基于卫星等飞行器的无线通信系统相结合，可实现星地之间高度安全的量子保密通信。2016 年 8 月，在中科院战略性先导科技专项的支持下，由中国科学技术大学牵头研制的世界上首颗量子科学实验卫星“墨子号”于酒泉成功发射，并配合多个地面站，在国际上率先实现千公里级的星地高速量子密钥分发、星地双向量子纠缠分发、和星地量子隐形传态。2017 年 9 月，结合“京沪干线”与“墨子号”的天地链路，成功实现了洲际量子保密通信。2019 年 12 月，我国研制的全球首个可移动量子卫星地面站与“墨子号”卫星完成对接，并成功接收到了足以加密大量数据进行长距离传输的量子密钥。

（三）专网安全领域

量子通信安全技术保障政企专网基础设施及其服务的安全性，为用户和数据间的交互提供高等级的安全防护。在我国，量子通信安全技术被应用于重要活动的通信安全保障，如抗战胜利 70 周年阅兵、中国共产党第十九次全国代表大会等。2017 年 9 月，济南党政机关量子通信专网正式投入使用。2019 年 4 月，合肥市政府新一代政务云体系投入使用，其构建了独立的量子通信传输通道，对重要政务业务数据采用了量子加密技术，保障信息通信安全。

9 商用密码技术

一、基本背景

商用密码技术是指基于商用密码算法，对不属于国家秘密的信息实现加密、解密和认证等功能的密码技术。商用密码技术作为商用密码的核心，在信息的加密和完整性保护、实体身份和信息来源的安全认证等方面发挥关键作用。

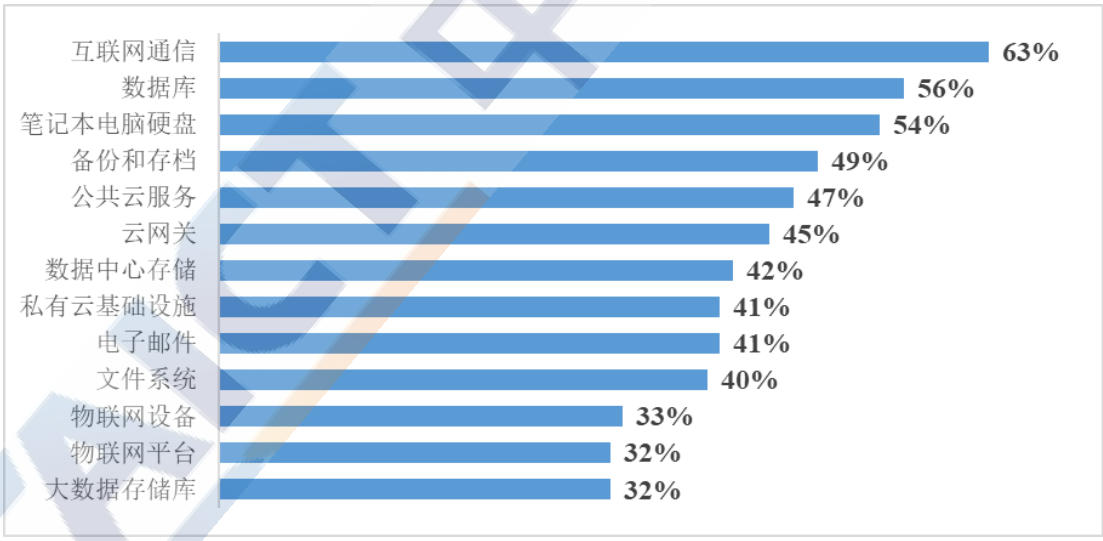
各国高度重视密码技术在信息安全中的重要作用，国际上密码技术和密码算法发展较早，已经形成了较为成熟的国际密码算法标准。美国于 2020 年 5 月，由国家标准与技术研究院（NIST）更新有关标准，指导管理密钥材料的指南和实践应用，其开展的美国联邦信息处理标准认证（FIPS）是目前应用最为广泛的密码模块安全评估体系之一。欧盟 2018 年 5 月生效的《通用数据保护条例》对个人信息的加密做出了要求。韩国 2019 年 4 月于发布了《国家网络安全战略》，要求加强基于密码技术的信息安全系统的使用，保障政府机密信息安全。

我国商用密码技术起步较晚，但发展速度较快，目前商用密码管理逐步规范、技术不断进步、产业日益繁荣、应用初见成效。2016 年 12 月，在国务院关于印发的《“十三五”国家信息化规划》中明确指出，要优先推进密码法等法律法规的立法工作，加强密码在重要领域应用推广。2019 年 6 月，国家标准《信息安全技术 信息系统密码应用基本要求》进入全国征求意见稿阶段，该标准对商用密码的合规、正确、

有效使用具有指导性作用。2020 年 1 月 1 日，《中华人民共和国密码法》正式施行，在保障网络信息安全和国家安全的同时，对促进我国商用密码产业的发展具有里程碑意义。2020 年 3 月 26 日，国家市场监管总局、国家密码管理局发布《关于开展商用密码检测认证工作的实施意见》，加强检测认证工作的组织实施、监督管理和结果采信，对营造商用密码发展的良好市场环境具有积极作用。

二、市场需求

当前，密码技术作为网络信息安全的核心技术，被广泛应用于多种业务领域，以保障重要数据信息安全。跟据德国数据公司 Statista 的全球调查数据显示，在 2019 年，全球多种 IT 业务领域均广泛采用了密码技术，如 63%的企业均在互联网通信使用密码技术。



数据来源：Statista

图 3-9　2019 年全球企业密码技术使用情况

商用密码技术的创新应用需求日益迫切。商用密码技术作为密码技术的重要组成，其产业发展日益壮大，在金融、电子政务、交通、

能源、通信等重大领域的信息安全保障工作中已经得到广泛应用，2019 年 IDC 报告预测，到 2023 年全球网络安全支出规模将达到 1512 亿美元，并将以 9.4%的年复合增长率持续增长。但是，随着云计算、大数据、人工智能、区块链为代表的新一代信息技术迅猛发展，网络和信息安全保障工作正面临着极大挑战，商用密码技术与物联网、大数据和云计算等新技术新业态的融合创新应用需求正日益迫切。

构建基于密码的安全防御体系是新型基础设施数据安全的重要保障。“新基建”相对于传统的基础性设施建设而言，主要表现为数字化、信息化，本质上是信息数字化的基础设施。随着大数据与人工智能技术的发展与广泛应用，保障隐私和数据安全成为在“新基建”的建设过程中面临的新问题与新挑战，密码技术作为保障基础信息网络和信息系统的数据安全核心支撑，在“新基建”中发挥着重要安全保障作用。

密码智能化已经成为密码技术的新发展方向。基于可信计算，密码技术已经实现智能化发展，可实现身份识别、状态度量、保密存储等功能，密码从传统的被动挂接调用转变为主动度量，转变了传统计算机的被动防御方式，在计算运算的同时进行安全防护，确保主机安全执行，有效降低安全风险。密码智能化可解决新时期网络信息安全所面临的新问题、新挑战。

三、典型应用

（一）个人信息安全领域

国产商用密码技术在北京 2022 年冬奥会和冬残奥会组织委员会面向全球招聘志愿者、工作人员云系统中得到有效应用。该云系统采用统一密码服务系统，向保护系统资源的应用提供加密、解密、签名、认证等基础密码应用服务，保障云系统中的重要信息系统安全运行和关键数据的安全存储和使用，其中，采用统一密钥管理平台提供密钥管理、数字证书管理等功能所需的基础支撑。该系统运行至今已经完成了两轮大规模招聘，有利维护了云上应聘者个人手机号、身份证号、护照信息、宗教信仰等个人敏感信息安全。

（二）政务信息安全领域

目前，我国正在快速推进商用密码技术在政务信息系统的使用，保证政务信息系统安全可靠运行。2018 年 3 月，基于商用密码技术的北京市“一证通”统一身份认证入选国家政务信息系统整合共享应用试点典型案例。北京市计划到 2020 年底，全面推广电子证照应用，该系统的身份认证、数字签名、电子签章等功能服务均广泛使用商用密码技术，如在身份认证功能服务模块采用密码云技术，为证照签发部门、证照使用部门、电子证照中心发放数字证书，解决电子证照参与各方的身份可信，该系统在新冠肺炎疫情防控期间，提高了北京市政务事项的网上实办率，进一步推动了网上办事全程电子化。

（三）金融信息安全领域

密码技术在身份认证、信息完整性和保密性、电子合同不可抵赖性等方面发挥着关键性的作用，有效防止了敏感信息泄露、财产损失

或业务中断，在金融领域得到广泛应用，包括网上银行、网上证券交易、网上投保等各种系统。如银行的统一密码认证平台，通过统一用户、认证通道，为金融行业提供一套集统一的用户管理、密码认证管理、客户端安全保护、端到端传输安全、渠道推广为一体的综合服务，用于登录、交易、远程开户、电子合同签署、电子回单查询、身份验证确认电子票务真实性等多种应用场景进行身份认证和鉴别。截至2019年，该系统在在北京银行、哈尔滨银行、上海银行、郑州银行、浙江农信、宁波银行等十多家银行广泛使用。

10 网络切片安全技术

一、基本背景

网络切片安全技术是5G安全领域的关键保障，通过实现切片安全隔离、切片安全管理、用户设备接入切片安全和切片之间通信安全等主要方式，防范因网络切片带来的切片间信息泄露、干扰和攻击等安全威胁，是保障网络切片安全和5G安全的核心技术手段。

各国企业高度重视网络切片安全技术，并开展相关领域应用研究工作。2017年6月，18家公司在欧盟委员会资助下成立欧洲新5G联盟（5G-Transformer），专注5G网络切片研究。2019年10月，爱立信在实时5G独立组网上实现网络切片突使客户能够设计和创建具有超可靠的低延迟通信服务的网络切片。2020年2月，德国电信与诺基亚、高通等公司基于多厂商平台，在两个网络切片中测试了首个端到端数据传输。同时，国际标准化组织加快推动开展网络切片安全标准化研究部署工作。2018年10月，第三代合作伙伴计划标准化组织（3GPP）开始接入特定网络切片的认证、密钥隔离、安全隐私等网络切片安全相关标准的深入研究。

我国高度重视网络切片安全技术研究工作，加快部署推进在5G安全等重要领域的应用。2020年3月，工业和信息化部发布《关于推动5G加快发展的通知》要求着力构建5G安全保障体系，加强网络切片等新对象的网络安全防护，2020年5月，发布《关于深入推

进移动物联网全面发展的通知》，要求加强网络切片等新兴关键技术研究实验工作。

二、市场需求

网络切片安全技术为网络切片带来的安全威胁提供解决方案。目前 5G 网络切片安全成为业界研究的热点，网络切片通过构建不同的逻辑网络来满足不同业务之间差异化服务需求的同时，也带来了新的安全问题，如切片间的信息泄露、干扰和攻击等。网络切片安全技术可通过切片隔离、切片接入认证、安全机制差异化等方式，确保网络切片实例资源相互独立，满足网络切片对安全的特定要求，防止非授权用户访问切片资源，切实保障网络切片安全。

网络切片安全技术已经成为 5G 赋能垂直行业应用的重要安全保障。网络切片是 5G 关键技术，具备灵活性，满足工业互联网、车联网等重要领域对于 5G 网络超大带宽、超低时延、超高可靠性的能力，在进一步促进产业型互联网发展方面具有重要作用，根据全球移动通信系统协会（GSMA）预测，到 2025 年底，中国 5G 连接数将达 4.6 亿。但是，在车联网、物联网等一些重要领域，对网络和信息安全需求较高，网络切片安全技术作为 5G 赋能垂直行业的重要技术，可为底层的 5G 网络提供良好的安全支持和技术保障，在 5G 垂直行业应用安全领域发挥着重要作用。

表 3-1　网络切片技术主要应用场景

应用场景	场景描述
娱乐和媒体	VR、AR、增值和视频直播、多人游戏-要求高带宽、低延迟
海量物联网	具有连接数百万台设备的潜力-依据设备的不同需求定制切片，为每种应用场景提供服务
工业	要求超可靠低时延通信和关键监控控制
车联网	娱乐、物联网和关键服务的需求组合，灵活组合网络切片来满足所有汽车应用场景

来源：IHS Markit

网络切片安全技术为新型基础设施建设提供有效防护手段。当前，新型基础设施建设快速推进，其中 5G、数据中心和工业互联网在面对大量有不同业务需求的客户时，会采用网络切片方式按需提供相应服务，通过网络切片安全技术可有效保证新型基础设施建设的网络信息安全，如通过在切片间采取有效隔离机制，防止因某个网络切片受到攻击后造成其他网络切片损伤，从而保护切片的数据信息安全。

网络切片安全技术为切片网络的数据安全提供首要保障。当前，网络切片面临的数据安全问题主要包括切片管理数据安全、切片隔离数据安全、切片使用数据安全等三方面安全风险。要解决网络切片面临的数据安全威胁，首要条件就是通过网络切片安全技术建立认证、隔离、管理等安全机制，确保切片网络自身安全可控，才能进一步保障数据的安全性。

三、典型应用

（一）电力安全领域

5G 网络切片技术满足电力业务的安全性、可靠性和灵活性需求，在智能电力系统的发电、输电、变电、配电、用电的各个环节有不同程度的应用。2020 年 4 月，由中国移动牵头联合南方电网等企业，完成全球移动通信系统协会（GSMA）首个网络切片 PoC（Proofof Concept）案例-5G 智能电网项目。基于 5G 网络切片技术的智能电网项目在为不同业务提供差异化网络服务能力的同时，还可为电网不同分区业务提供高度可靠的安全隔离，为不同分区业务提供物理资源、虚拟逻辑资源等不同层次的安全隔离能力，满足不同生产、管理大区电力业务不同的安全隔离要求，为智能电网的业务承载提供更好的安全保障。

（二）工业安全领域

5G 网络切片技术作为工业互联网建设的重要支撑，在工业安全领域发挥重要作用。2019 年 10 月，中国电信等企业合作推出了中国首个端到端 5G 切片和智能制造解决方案，对 5G 网络切片和智能制造等技术进行了试验测试，建立基于 5G 切片的智能工厂平台。该平台采用切片存储、无线切片感知、切片安全隔离、动态切片迁移等方式，支持机器视觉切片的快速部署和视频流的快速回程，降低视频数据传输的延迟、抖动和丢包率。同时，平台通过结合切片安全隔离机制，各切片之间共享物理网络通道但却互不干扰，保障

切片之间的隔离性，从而保证业务流传输数据的完整性，在一定程度上提高了业务的安全性和可靠性。

（三）警务安全领域

基于 5G 网络切片安全技术的 5G 智慧警务专网，可为警务工作提供高品质业务保障。2020 年 5 月，中国电信基于 5G SA 网络切片技术，为深圳市公安局建立全球首个 5G 智慧警务应用。该应用通过实现不同业务间的物理隔离，避免其他业务抢占警用业务的网络带宽，保障了高清视频回传等警用业务大带宽的要求。通过切片隔离，避免了其他突发流量对警用业务的冲击而带来的网络拥塞，满足警用业务的稳定低时延要求，实现秒级人脸识别，助力现场警员快速、准确抓捕。同时，通过网络切片可实现警务业务与公众业务之间硬隔离，实现数据安全隔离，保障警务数据安全。

第五章 数字安全产业发展建议

当前我国数字安全产业发展正迎来重要的战略机遇期，全行业要坚持总体国家安全观，坚持一手抓住“产业发展”，一手抓住“技术创新”，用产业的实际需求来促进技术能力的演进，继而带动我国数字安全技术的自主创新能力以及合作模式的创新，着力推广先进安全技术、产品和服务，提升安全产业创新能力，充分发挥政、产、学、研、用各方面的积极性、主动性和创造性，推动安全产业集聚发展，强化安全产业国际合作，优化安全产业发展环境。

（一）完善法律法规制订，优化产业政策引领

法律法规及产业政策在数字安全产业发展中起到重要的引领作用。近年来全球各国在数字安全领域均加强了法律法规的制订，同时我国《网络安全法》《电信和互联网用户个人信息保护规定》《网络安全等级保护条例》等系列法律法规极大助力了数字安全产业的规范发展，数字经济、“互联网+”等政策文件为产业明确发展方向、创造了有利条件。我国正围绕数据安全、个人信息保护、“新基建”等重点，持续完善法律法规、发布重要产业政策，从顶层设计角度引领数字安全产业的新方向、新进步。

（二）发挥市场配置作用，激发产业主体活力

依托当前有利的政策指引，面向产业范畴、应用领域、市场需求等发展方向，促进市场要素和资源的有效配置，让市场在资源配置中

起决定性作用，同时要更好发挥政府作用，激活产业发展动能。健全激励创新、包容开放的产业发展体系，带动产业的创造力和活力，通过建立园区、提供资金支持等方式，让企业能够更好地接受和发展数字化转型。充分发挥企业主体作用，激发创新活力，探索利用投资助力，孵化、投资一些创新创业的中小微主体，为产业经济发展注入新的活力。

（三）释放数据要素价值，筑牢数字安全产业底座

作为数字技术的关键要素，全球数据爆发增长，海量集聚，成为实现创新发展、重塑人们生活的重要力量，事关各国安全与经济社会发展。2020 年 9 月，我国提出《全球数据安全倡议》，欢迎政府、国际组织、信息技术企业、技术社群、民间机构和公民个人等各主体应秉持共商共建共享理念，齐心协力促进数据安全，积极维护全球信息技术产品和服务的供应链开放、安全、稳定。数字安全产业各方应当切实保障重要数据和个人信息安全、筑牢安全防护的底座，秉持发展和安全并重的原则，推动数字安全产业和平、安全、开放、合作、有序的发展。

（四）加快新兴技术研发，驱动数字安全创新变革

数字安全领域的新技术新业态不断涌现，伴生新的安全风险和挑战，必须牢牢抓住科技创新这个“牛鼻子”。新一代信息通信技术在更广范围、更深层次、更高水平与实体经济融合，数字安全风险和挑战也不断渗透、扩散、放大，要坚持创新引领，加强基础性、通用性、

前瞻性技术创新，持续强化工业互联网、5G、人工智能、云计算、区块链、大数据等产业方向和技术赛道的研究力度，构建多领域、多层次网络安全技术创新体系，应针对前沿技术提早谋划，预先布局，有效防范不断变化的数据、个人信息、关键基础设施等安全风险。

（五）推动产学研深度融合，促进技术向市场转化

基于自主创新、激励相容、均衡发展的原则，建立以企业为主体、市场为导向、产学研深度融合的数字安全产业协同体系，面向数字化转型的关键安全问题，深度挖掘数字安全技术的应用新模式，形成多角色、多阶段、分层次的技术产业链条，优化知识产权和无形资产保护，实现创新技术向产品、服务、整体解决方案以及成熟商业模式的落地，促进数字安全技术向市场的有效转化。

（六）坚持多方合作共赢，共建数字安全产业生态

坚持合作共赢的产业发展方向，综合发挥政府、企业、科研院所及国际组织等各方作用，加强相关各方在数字安全领域交流合作，深化数字安全有效实践的经验交流，强化数字安全人才培养和队伍建设，构筑协同合作的产业链条，共同发挥出数字安全在国家治理能力和治理体系现代化中的积极作用，鼓励企业积极走出去，合力应对全球数字安全威胁与挑战，维护数字经济的安全秩序。