5G网络安全标准化白皮书

（2021版）

全国信息安全标准化技术委员会

通信安全标准工作组

2021年5月

5G 网络安全标准化白皮书

（2021 版）

全国信息安全标准化技术委员会

通信安全标准工作组

2021 年 5 月

编写单位

中国移动通信集团有限公司、中国电子技术标准化研究院、中国信息通信研究院、国家计算机网络应急技术处理协调中心、中国信息安全测评中心、华为技术有限公司、阿里云计算有限公司、中兴通讯股份有限公司、中国信息通信科技集团有限公司、大唐移动通信设备有限公司、亚信科技（成都）有限公司、高通无线通信技术（中国）有限公司、北京时代新威信息技术有限公司、北京百度网讯科技有限公司、杭州安恒信息技术股份有限公司

编写人员

李慧镝　张　滨　杨建军　赵　刚　袁　捷　上官晓丽　于生多　张　峰

邱　勤　孙　彦　王秉政　赵　蓓　李祥军　粟　栗　刘贤刚　徐思嘉

姚相振　江为强　于　乐　刘　畅　齐旻鹏　王国宇　刘胜兰　林美玉

舒　敏　杨红梅　贵　重　何　鹏　张弘扬　王光涛　韩晓露　武冰梅

王　军　张大江　陈　星　杜雪涛　张　晨　刘婧璇　王文磊　陈　悦

王　姣　吴　荣　林兆骥　游世林　毕晓宇　薛　辉　杜志敏　任若冰

柳　扬　樊洞阳　贾　强　彭伟营　王新杰　王连强　王海棠　唐佳伟

摘要 ABSTRACT

本白皮书介绍了5G的概念、关键技术和产业发展情况，梳理了国内外政策法规标准现状，分析了5G在终端安全、IT化网络设施安全、通信网络安全、行业应用安全、数据安全、网络运维安全等方面存在的安全风险和网络安全标准化需求，提出了5G网络安全标准框架和重点标准研制建议，旨在为5G技术安全应用、5G与产业融合安全有序发展提供标准化技术支撑。

全文结构如下：

第1章介绍了本白皮书编写的背景。

第2章介绍了5G概念与应用场景、5G关键技术与安全特性。

第3章介绍了国内外的5G网络安全法规与政策、5G网络安全标准化现状。

第4章介绍了5G网络安全风险，包括终端安全风险、IT化网络设施安全风险、通信网络安全风险、行业应用安全风险、数据安全风险和网络运维安全风险。

第5章基于5G网络安全标准化需求，给出了5G网络安全标准框架。

第6章给出了5G网络安全标准化工作推进建议。

第7章给出了本白皮书所引用的参考文献。

附录A介绍了国内外已发布及在研的相关标准。

附录B介绍了5G网络安全标准应用实践案例。

附录C给出了相关术语定义。

受编制时间、水平所限，疏漏在所难免。针对此版白皮书如有任何意见或建议，敬请联系 qiuqin@chinamobile.com。

目录 CONTENTS

1 引言

当前，以第五代移动通信技术（以下称 5G）为代表的新一轮科技和产业变革正在快速兴起，成为世界各国经济发展的重要技术支撑和全球产业竞争的战略高地。2019 年起，全球各大运营商竞相加快 5G 网络部署，各大机构积极探索 5G 与重点行业的融合创新。截至 2020 年底，全球 131 个国家的 412 家运营商采取各种方式投资 5G，59 个国家和区域的 140 个运营商已推动 5G 商用，全球共建成超 100 万个 5G 基站。其中，我国累计建成 5G 基站 71.8 万个，占比超全球总量的 70%，形成全球最大规模的 5G 网络，实现所有地级以上城市 5G 网络全覆盖。5G 凭借全新的架构，引入网络功能虚拟化、服务化网络架构、边缘计算等新型关键技术，大幅提升了移动网络业务能力，通过超高清视频、智能电网、工业互联网、智慧交通、智慧城市等应用，开启了万物广泛互联、人机深度交互的新时代，为产业数字化、生活智慧化、数字化治理提供有力支撑。

在全球范围内 5G 广泛商用、规模快速扩大的背景下，5G 网络安全问题也成为各方关注焦点。5G 网络安全包括终端安全、IT 化网络设施安全、通信网络安全、行业应用安全、数据安全、网络运维安全等多个方面。虽然 5G 较 4G 拥有更为完善的安全特性，但随着 5G 融合应用的不断深入，又将面临的新网络安全威胁与风险。为促进 5G 与相关产业的健康安全发展，切实发挥标准在网络安全工作中的基础性、规范性、引领性作用，有效指导和体系化推进相关重点标准研究制定工作，本白皮书在充分调研国内外 5G 网络安全发展情况的基础上，针对 5G 典型应用场景和关键环节，研究提出 5G 网络安全标准框架，给出标准化工作推进建议。

2 5G 技术概述

2.1 5G 概念与应用场景

5G 即第五代移动通信技术（The 5th Generation Wireless communication），是继 2G、3G 和 4G 系统之后的延伸，其设计目标是高数据速率、低传输延迟、提升传输质量、节省能源、降低成本、提高系统容量和大规模设备连接。5G 不仅用于人与人之间的通信，还适用于人与物、物与物之间的通信，被视为促进各行业智能化升级、推动数字经济发展的关键技术之一。

2015 年发布的 ITU-R M.2083-0 建议书 IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond 提出了 5G（IMT-2020）的关键技术特征及指标建议，包括峰值数据速率、用户体验数据速率、频谱效率、移动性、延迟、连接密度、网络能效、区域业务容量等。基于全面提升的网络性能指标，ITU-R M.2083-0 建议书进一步定义了 5G 的三大应用场景：增强移动宽带（Enhanced Mobile Broadband,eMBB）、海量机器类通信（Massive Machine Type Communication，mMTC）和超可靠低时延通信（Ultra Reliable and Low Latency Communication,uRLLC），如图 1 所示。5G 结合其三大应用场景，与智慧家庭、智慧城市等社会生活领域结合，与超高清视频和 VR/AR 等多媒体应用、车联网和工业互联网等行业融合，渗透到生产和生活的各领域，为经济与社会发展注入强劲动力。

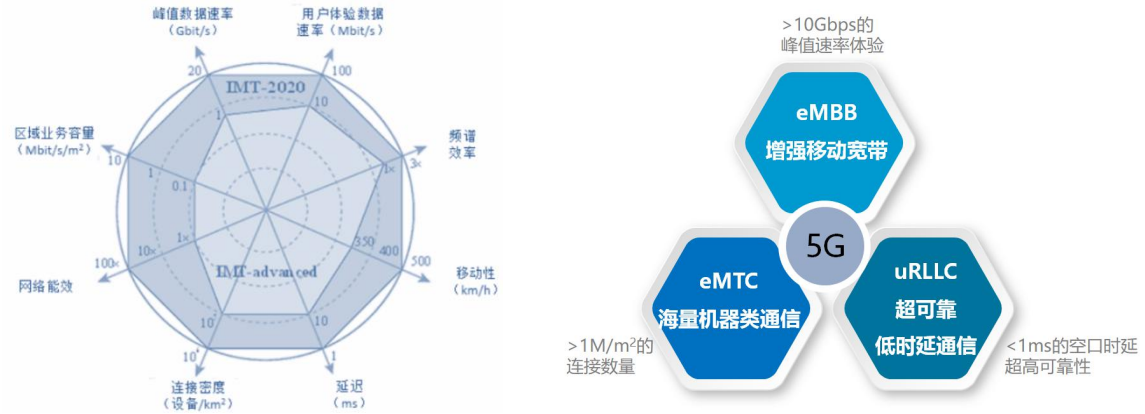


图1 ITU定义的5G关键指标和应用场景

- 增强移动宽带（eMBB）是以人为中心的应用场景，集中表现为超高的传输数据速率，广覆盖下的移动性保证。以常用的视频业务为例，4G 网络的平均用户体验速度下行为 30~50Mbps、上行为 6~8Mbps，能够满足一路高清视频的在线播放需求，无法满足高清直播、多路视频会议的需求；而 5G 网络

的平均用户体验速度下行为 100Mbps、上行为 50Mbps，用户体验会有明显的提升。

- 海量机器类通信（mMTC）以大规模物联网为应用场景，支持密集环境下的海量机器类通信，使得人与机器、机器与机器的大规模通信成为可能。mMTC 的海量体现在两个方面：首先，5G 网络可连接的物联网设备量远大于 4G，每平方公里可支持 100 万个连接；其次，联网设备和业务的种类也大大丰富了，支持多种使用不同通信模式的终端，比如：仅作为主叫不作为被叫被寻址的终端、仅在固定时间间隔激活和通信的终端。大部分物联网终端具有资源受限的特点和低功耗工作要求，5G 在架构和协议设计上做了优化，简化了连接建立和管理模型，可最大限度降低物联网终端的功耗。
- 超可靠超低时延通信（uRLLC）以无人驾驶、远程医疗、智能制造等关键通信为应用场景，必须严格满足业务需求的时延和可靠性。4G 网络时延最小只能达到 20ms 左右，但是 5G 系统本身可将端到端时延降低到 1~10ms、且在高速移动（500KM/H）情况下保持高可靠性（99.999%）连接。同时，5G 系统架构支持边缘计算，可进一步降低业务时延，确保时延敏感场景下高速通信、及时执行命令和发送反馈。

2.2 5G 关键技术与安全特性

2.2.1 IT 化网络设施

传统移动通信网络基于网元设备实现网络功能。5G 在网络基础设施层面引入了包括网络功能虚拟化（Network Function Virtualization，NFV）、软件定义网络（Software Defined Network，SDN）等 IT 技术，并支持通过网络切片将网络划分为虚拟专网，从而能够低成本、灵活快速地满足行业应用对网络的高安全性和可定制化需求。

- 网络功能虚拟化：NFV 技术实现了计算和存储资源的虚拟化，实现了软件与硬件的解耦，使网络功能不再依赖于专有通信硬件平台、专用操作系统，实现了 5G 网络基础设施的云化，支持资源的集中控制、动态配置、高效调度和智能部署，缩短网络运营的业务创新周期。
- 软件定义网络：SDN 技术实现了通信连接的软件定义，将数据通信设备拆分为控制面和数据面，控制面集中控制并提供可编程接口，实现了根据组网和业务需要灵活定义网络传输通道，可灵活调度流量并编排安全能力。

- 网络切片：网络切片是为满足垂直行业对网络能力可定制化、通信及信息安全可控化的需求而出现的，它可将一个物理网络切分成功能、特性各不相同的多个逻辑网络，同时支持多种业务场景。基于网络切片技术，可以隔离不同业务场景所需的网络资源、提高网络资源利用率。

2.2.2 服务化网络架构

传统移动通信网络架构基于固定网元、固定连接，网络功能的可扩展性受限。为了满足5G时代灵活部署的需要，5G采用了服务化架构（Service-based Architecture, SBA），将原有的网元按照“微服务”的理念拆分为松耦合、细粒度的网络功能（Network Function，NF），通过服务调用、服务组合的方式实现核心网的基本功能。5G核心网内的应用功能（Application Function,AF）指应用层的各种服务，它既可以是运营商内部应用，也可以是第三方应用，其他网元可通过AF的服务化接口Naf对其进行访问。

3GPP将5G核心网定义为一个可分解的网络体系结构，引入了控制面和用户面分离，其中核心网用户面采用传统架构和接口，用户面功能（User Plane Function，UPF）负责数据包的路由转发、与外部数据网络的数据交互等，核心网控制面网元采用服务化架构设计，彼此之间通信采用服务化接口，从而提供多个网络功能服务。5G服务化架构中，将网络功能以服务的方式对外提供，不同的网络功能服务之间通过标准接口进行互通，支持按需调用、功能重构，从而提高核心网的灵活性和开放性。如图2所示，5G核心网将控制面拆分为多个网络功能：

- 接入和移动性管理功能（Access and Mobility Management Function,AMF）主要负责终端接入和移动性管理，对应的服务化接口为 Namf；
- 会话管理功能（Session Management Function,SMF）负责会话管理，对应的服务化接口为 Nsmf；
- 策略控制功能（Policy Control Function，PCF）负责策略管理，对应的服务化接口为 Npcf；
- 网络切片选择功能（Network Slice Selection Function，NSSF）负责判断应该为 UE 提供何种网络切片服务，对应的服务化接口为 Nnssf；
- 网络开放功能（Network Exposure Function，NEF）负责开放网络能力给 AF，对应的服务化接口为 Nnef；
- 网络存储功能（Network Repository Function，NRF）负责 NF 以及 NF 上提供的服务的统一管理，包括注册、发现、授权等功能，对应的服务化接口为 Nnrf；

- 统一数据管理（Unified Data Management,UDM）负责用户数据管理等，对应的服务化接口为 Nudm。

5G独立组网架构中，SBA化的核心网控制面及用户面对外交互时所涉及的业务接口包括：

- N1：控制面与用户终端之间的接口。
- N2：控制面与无线接入网之间的接口。
- N3：用户面和无线接入网之间的接口。
- N4：控制面和用户面之间的接口。
- N6：用户面和数据网络之间的接口。
- N9：用户面的漫游接口。

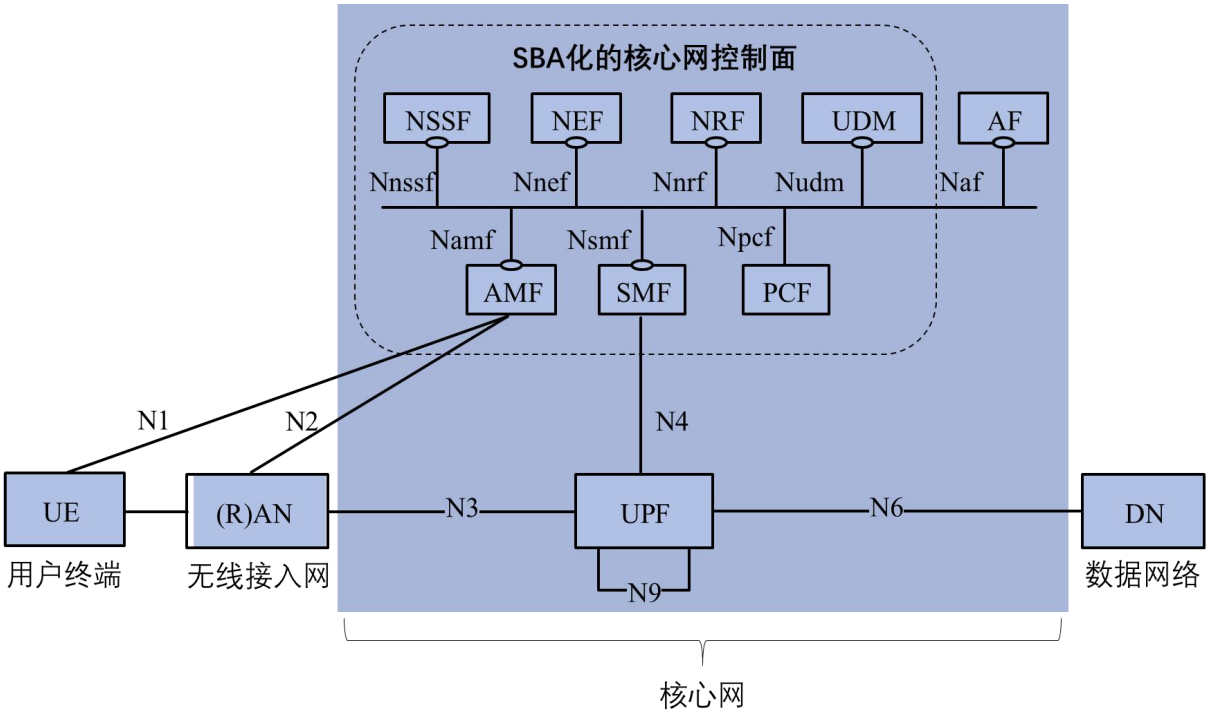


图2 5G独立组网架构

2.2.3 边缘化计算资源

3G/4G 时代，网络服务普遍采用云端协同的方式，即远端的云计算或者云数据中心和终端相互配合完成网络服务的提供和访问。5G 时代，大量高可靠低时延业务出现，对网络传输和服务计算的时延效率提出更高需求，边缘计算（MEC,Multi-access Edge Computing）的应用需求更为广泛。5G 网络本身也支持更加灵活的边缘计算服务。

- 边缘计算作为 5G 网络新型网络架构的主要特征之一，部署在无线基站、接入机房等网络边缘，通过将计算能力和 IT 服务环境下沉，就近向用户提供服务，从而构建一个具备高性能、低时延与高带宽的电信级服务环境。
- 边缘计算平台在网络边缘靠近用户的位置上，提供 IT 服务和云计算的能力，降低核心网的负载开销和用户业务时延，为用户提供本地视频、位置定位、视频质量优化、流量分析等低时延和高带宽业务。
- 边缘计算采用开放应用编程接口（API）、网络功能虚拟化（NFV）等技术，通过边缘节点上应用程序 APP 对外提供服务。

2.2.4 增强的安全能力

基于前几代移动通信演进过程中发现的安全问题和积累的运维经验，5G 网络对安全机制考虑更加充分，具有以下特点：

（1）更全面的数据安全保护

在数据安全保护方面，5G 相对于之前的通信网络对用户数据的完整性保护要求更严格，5G 不仅只是对网络信令进行完整性保护，还增强了对用户数据的完整性保护。

从 3G 到 4G，系统的设计要求主要是保证系统空口的吞吐效率最大化和时延最小化，通信系统对网络信令进行完整性保护、避免被恶意篡改，对用户数据并未进行完整性保护。

在 5G 通信中，数据应用越来越广泛，对用户数据的完整性保护要求更严格，需要进行更全面的数据安全保护。除信令外，5G 通信中对用户数据也可进行完整性保护，确保用户数据在空中接口传输时不会被恶意篡改。

（2）更丰富的认证机制支持

在认证机制支持方面，5G 相对于之前的通信网络具有更丰富的认证机制支持，不仅增强了归属网络对认证的控制，还具有更加灵活的可扩展框架。

在 3G 至 4G 网络中，所使用的认证与密钥协商（Authentication and Key Agreement，AKA）认证机制具备很高的安全性。AKA 协议是 3GPP 在研究 2G 安全脆弱性的基础上，针对 3G 接入域安全需求提出的，其使用挑战应答机制完成用户和网络间的身份认证，同时基于身份认证对通信加密密钥进行协商，通过认证和加密手段更好地预防攻击行为。

5G 支持多种接入技术（如 4G 接入、WLAN 接入以及 5G 接入），为了使用户可以在不同接入网间实现无缝切换，5G 网络认证一方面继承了 AKA 框架，在机制和能力上进行增强并形成了 5G-AKA，增强归属网络对认证的控制，不仅提供对用户的认

证，还提供对访问网络的认证，防止访问网络虚报用户漫游状态、产生恶意扣费等情况。另一方面，5G 网络采用统一的认证框架，引入了扩展认证协议（Extensible Authentication Protocol，EAP），其具有较好的灵活性和可扩展性，既可运行在数据链路层上，也可以运行于 TCP 或 UDP 协议之上，不仅支持多种认证协议和各种应用场景下的双向身份鉴权，还支持垂直行业的多种已有应用，扩展适配垂直行业应用所需的新认证能力。

（3）更严密的用户隐私保护

在用户隐私保护方面，5G相对于之前的通信网络具备更严密的加密措施，能在更大力度上保护用户隐私不受侵犯。

在2G至4G网络中，通信网络和终端通常使用临时移动用户识别码（Temporary Mobile Subscriber Identity，TMSI）交互，用于避免国际移动用户识别码（International Mobile Subscriber Identity，IMSI）被攻击者窃取。但当终端初始接入网络，TMSI和IMSI未能同步时，通信网络会请求终端发送IMSI进行认证，IMSI会短暂出现在信道上，攻击者可能获取IMSI并进一步攻击或追踪用户。

5G通信网络利用用户卡上存储的归属运营商的公钥对永久用户标识进行加密，不再明文传输国际移动用户识别码。为抵御中间人攻击，归属运营商的公钥直接预置在用户卡内，有效地保护了用户的隐私。其次，在5G通信网络中，切片选择辅助信息NSSAI（Network Slice Selection Assistance Information）可区分不同类型的5G网络切片，在用户初始接入网络时，NSSAI知识基站及核心网网元将其路由到正确的切片网络，5G网络可对NSSAI敏感信息进行隐私保护。

（4） 更灵活的网间信息保护

在网间信息保护方面，5G新增了安全边界保护代理（Security Edge Protection Proxy，SEPP），能有效保护在网络中互联互通信息的机密性和完整性。

在3G/4G系统中，运营商的数量和网络部署规模也在不断扩大，为防止信令在网络间传输过程中被窃听、篡改甚至伪造，3GPP制定了基于域划分的网络域/IP层安全机制、基于公钥基础设施提供认证服务的认证框架协议，以保护网间信息互联互通。

在5G网络中引入了SEPP，其作为运营商核心网控制面之间的边界网关，所有跨运营商的信息传输均需要通过SEPP进行处理和转发，SEPP在运营商之间建立TLS安全传输通道，对传输的信息中需要进行保护的字段进行机密性和完整性保护，从而有效防止数据在传输过程中被篡改和窃听。

表 2-1 5G 网络与 4G 网络的安全能力对比

能力类型	4G	5G
数据安全保护	对网络信令进行完整性保护。	对网络信令和用户数据进行完整性保护。
认证机制支持	使用 AKA 认证机制。	使用增强的 5G-AKA 认证机制，并引入 EAP 构建更灵活的可扩展框架。
用户隐私保护	通信网络和终端通常使用临时移动用户识别码 TMSI 交互。	利用用户卡上存储的归属运营商的公钥对永久用户标识进行加密。
网间信息保护	基于域划分的网络域/IP 层安全机制、基于公钥基础设施提供认证服务的认证框架协议。	新增了安全边界保护代理 SEPP，对传输信息进行机密性和完整性保护。

3 5G 网络安全政策与标准现状

3.1 5G 网络安全法规和政策

3.1.1 美国

美国力图在5G技术创新、应用发展、安全生态建设等方面占据全球领导地位。2018年9月，美国联邦通信委员会（FCC）发布了“5G加速计划”，主要从频谱资源投入、基础设施建设、修订法规三个方面提出了促进5G发展的举措。2018年10月，白宫发布《关于制定美国未来可持续频谱战略的总统备忘录》，提出“美国必须率先实现第五代无线技术（5G）”。2018年12月，国际战略研究中心（CSIS）发布《5G将如何塑造创新和安全》报告，指出5G技术是下一代数字技术的支柱，将对未来几十年的国际安全和经济产生影响。2019年4月，美国国防部国防创新委员会发布《5G生态系统：国防部的风险与机遇》，介绍了5G发展历程、目前全球竞争态势以及5G技术对国防部的影响与挑战，并在频谱政策、供应链和基础设施安全等方面提出了建议。2019年5月，美国联合全球30多个国家发布了非约束性政策建议“布拉格提案”。2020年3月，美国白宫发布了《美国5G安全国家战略》，正式制定了美国保护5G基础设施的框架，阐明了美国要与最紧密的合作伙伴和盟友共同领导全球安全可靠的5G通信基础设施的开发、部署和管理的愿景。2020年12月，美国国防部发布《5G技术实施方案》报告，从技术、安全、标准、政策以及应用合作等方面提供5G安全路线图，重点提到计划扩大在包括3GPP在内的标准制定组织中的活动力度；响应国防部方案，美国国家标准与技术研究院（NIST）设立了“5G安全演进”项目，并于2021年2月发布《5G网络安全实践指南》草案，旨在帮助使用5G网络的组织以及网络运营商和设备供应商提高安全能力。

3.1.2 欧盟

欧盟高度重视5G发展，并着力构建各成员国统一的安全框架。早在2015年，欧盟正式公布5G合作愿景（EU vision for 5G Communication），力求确保欧洲在下一代移动技术全球标准中的话语权。2017年的发布《网络与信息安全指令》和2018年发布的《欧洲电子通信守则》要求成员国针对5G网络和相关基础技术的安全保障尽快制定国家战略，明确战略执行机构、风险评估计划、应急处置措施和部门协作机制等。2019年3月，欧盟批准生效《网络安全法案》，赋予欧盟网络和信息安全局

（ENISA）一项重要任务，即推动建立欧盟首个统一的网络安全认证制度，该认证将适用于欧盟市场的所有信息通信设备、服务和流程（包含5G）。欧盟委员会还通过了《5G网络安全建议》，呼吁欧盟成员国完成国家风险评估并审查国家安全措施，并在整个欧盟层面共同开展统一风险评估工作，同时就一个通用的缓解措施工具箱进行商议。2019年10月，欧盟遵循ISO/IEC 27005《信息技术-安全技术-信息安全风险管理》中的风险评估方法，分析了5G网络的主要威胁和威胁实施者、受威胁的资产、各种脆弱点以及战略风险，发布了《欧盟5G网络安全风险评估报告》。2020年1月29日，欧委会通过欧盟5G安全工具箱，通过一系列战略和技术措施解决《欧盟5G网络安全风险评估报告》中所有已识别出的风险。

3.1.3 国内现状

在我国，党和政府高度重视 5G 网络技术的发展及应用。《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》指出“加快 5G 网络规模化部署，用户普及率提高到 56%，推广升级千兆光纤网络”，“构建基于 5G 的应用场景和产业生态，在智能交通、智慧物流、智慧能源、智慧医疗等重点领域开展试点示范”，体现了国家对于发展 5G 的决心。2019 年 6 月，工信部发放 5G 商用牌照，加速推动 5G 发展应用。2019 年 11 月，工信部印发《“5G + 工业互联网”512 工程推进方案》（工信厅信管〔2019〕78 号），明确到 2022 年实现一批面向工业互联网特定需求的 5G 关键技术突破，加快垂直领域“5G+工业互联网”的先导应用；2020 年 3 月，工信部印发《关于推动 5G 加快发展的通知》（工信部通信〔2020〕49 号），全力推进 5G 网络建设部署，加大 5G 技术研发力度与应用推广；2020 年 5 月，《政府工作报告》提出“加强新型基础设施建设，发展新一代信息网络，拓展 5G 应用”，再次就加快 5G 网络等新型基础设施建设做出战略部署。

在推动 5G 发展的同时，5G 网络安全也被提高到国家战略层面。相关法律法规、政策文件的要求对于加快建设 5G 安全保障体系，合理规划标准化体系等方面具有重要指导意义。在法律法规层面，《网络安全法》主要从网络安全责任制、关键信息基础设施保护、个人信息保护三个方面提出保障 5G 网络安全发展的要求。《中华人民共和国电信条例》规定，任何组织或者个人不得利用电信网络从事危害国家安全、社会公共利益或者他人合法权益的活动，不得有危害电信网络安全和信息安全的行为。《网络安全审查办法》要求“关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的”，应当通过“有关部门组织的国家安全审查”。已被全国人大列入立法计划的《数据安全法》《个人信息保护法》也对网络数据提出严格的管理要求。在政策方面，《关于推动 5G 加快发展的通知》要求加强 5G 网络基础设施安全保障、强化 5G 网络数据安全保护、培育 5G 网络安全产业生态，构建 5G 安全保障体系，并要求开展安全评估，积极防范安全风险。2021 年 3 月，工信部科技司在

《2021 年工业和信息化标准工作要点》中明确，将推动开展 5G 及下一代移动通信、网络和数据安全等标准的研究与制定。

3.2 5G 网络安全标准化现状

3.2.1 国外标准化情况

3.2.1.1 ISO/IEC JTC1

目前，国际标准化组织 ISO/IEC JTC1 SC27(信息安全、网络安全和隐私保护分技术委员会)已发布的与 5G 网络安全相关的标准主要集中在信息安全管理、供应链安全管理等方面，在研 5G 网络安全相关的标准主要聚焦网络虚拟化安全。ISO/IEC JTC1 在 5G 网络安全领域的重点标准包括：

- ISO 27000《信息技术 安全技术 信息安全管理系统》系列标准明确了在组织内部建立信息安全管理目标，以及完成这些目标所用方法的体系，其中 ISO/IEC 27005《信息技术 安全技术 信息安全风险管理》标准被欧盟用于开展 5G 网络安全风险评估。
- ISO/IEC 27036《信息技术 安全技术 供应商关系信息安全》围绕供应商关系信息安全展开研究，主要阐述了 ICT 供应链信息安全中面临的相关风险，实施信息安全的要求和 ICT 供应链信息安全的标准内容等。
- 在研标准 ISO/IEC 27033-7《信息技术 网络安全 第七部分：网络虚拟化安全指南》旨在分析网络虚拟化安全性的主要挑战和风险，提供网络虚拟化安全性的框架，并提出针对网络虚拟化设施、虚拟化网络功能、虚拟化控制和资源管理等的安全实施指南。

3.2.1.2 ITU-T

国际电信联盟电信标准化部门（ITU-T）已发布的标准聚焦在 IT 化网络设施安全领域，主要围绕基于 SDN 的业务链安全、SDN/NFV 网络中软件定义安全。此外，ITU 正在针对 5G 网络安全基础、IT 化网络设施安全、网络安全、数据安全和安全运营管控展开标准研究。ITU-T 在 5G 网络安全领域的重点标准包括：

- ITU-T X.1043《基于软件定义网络的服务功能链的安全框架和要求》和 ITU-T X.1046《软件定义网络/网络功能虚拟化网络中的软件定义安全框架》两项标准。其中 X.1043 对基于 SDN 的业务链安全、网元安全、接口安全、业务链策略管理及相关安全机制进行了规定，X.1046 提出了 SDN/NFV 网络的软件定义安全框架，并对框架中组件功能、接口功能以及流程等进行了

规定，同时提出了部署实践参考。

- ITU-T X.5Gsec-guide《基于 ITU-T X.805 的 5G 通信系统安全导则》主要针对基于 ITU-T X.805 的 5G 通信系统展开安全研究，通过结合该系统在运用边缘计算、网络虚拟化、网络切片等技术时所产生的特点，研究其在 3GPP 网络架构和非 3GPP 网络架构下的安全威胁和安全能力。
- ITU-T X.5Gsec-ecs《5G 边缘计算服务的安全框架》根据 5G 边缘计算的部署方式以及典型的应用场景，分析 5G 边缘计算的安全威胁、安全需求，提出 5G 边缘计算服务安全框架。
- ITU-T X.5Gsec-t《5G 生态系统中基于信任关系的安全框架》研究 5G 生态系统中的信任关系和安全边界，制定 5G 生态系统的安全框架。

3.2.1.3 3GPP

第三代合作伙伴计划标准化组织（3GPP）聚焦在 5G 基础共性、应用与服务安全和 IT 化网络设施安全等方面。3GPP 在 5G 网络安全领域重点标准包括：

- 在安全基础共性方面，发布了 3GPP TS 33.501《5G 系统的安全架构和流程》、3GPP TR 33.841《256 位算法对 5G 的支持研究》、3GPP TR 33.834《长期密钥更新程序（LTKUP）的研究》三项基础共性类标准，分别对 5G 系统的安全架构和流程、256 比特密钥长度和密码算法、长期密钥更新等进行了规定。
- 在 IT 化网络设施方面，3GPP TR 33.848《虚拟化对安全性的影响研究》分析了虚拟化对网络架构的影响，安全威胁和相应的安全需求。3GPP TR 33.818《适用于 3GPP 虚拟网络产品的安全保证方法（SECAM）和安全保证规范（SCAS）》针对虚拟化网络产品的安全保障方法展开研究和分析。
- 在应用与服务安全方面，发布了 3GPP TS 33.535《在 5G 中基于 3GPP 凭证的应用程序的身份验证和密钥管理》，该标准以 5G 物联网场景下的应用层接入认证和安全通道建立为切入点，研究了利用 5G 网络安全凭证为上层应用提供认证和会话密钥管理能力的解决方案。针对 5G 在物联网、垂直行业、位置服务、车联网、超可靠低时延特性等方面的安全威胁及需求，展开了研究制定并评估了对应的解决方案。
- 在通信网络方面，3GPP TR 33.813《网络切片增强的安全性研究》针对 5G 网络设备的安全保障、5G 网络引入服务化接口安全、5G 网络中伪基站安全、5G 切片安全等问题，研究了 5G 移动通信网网络切片的安全增强技术，包括网络切片安全特性、关键问题、安全需求及解决方案。

3.2.1.4 NIST

美国国家标准与技术研究院（NIST）提出了 NIST SP 800-37《信息系统和组织的风险管理框架》，定义了信息系统风险管理框架，可用于指导 5G 网络的安全部署应用。NIST SP 800-53《信息系统和组织的安全和隐私控制》、NIST SP 800-207《零信任架构》、NIST SP 800-82《工业控制系统安全指南》、NIST SP 800-160《网络安全工程技术指南》等分别针对控制措施和隐私保护、零信任架构、工业控制系统安全、安全工程技术等提供了与 5G 网络安全部署应用相关的安全实施指南。

此外,NIST 正在推进《5G 网络安全实践指南》的制定，目前已完成了相关草案的编制。该指南向 5G 网络运营商和用户提出减缓 5G 网络安全风险的方法，包括通过增强系统的体系结构组件、启用 5G 标准中引入的安全功能、提供基于云的安全支持基础架构等安全措施，以帮助使用 5G 网络的组织、网络运营商和设备供应商提高安全能力，并为电信和公共安全界提供参考。

3.2.2 国内标准化情况

3.2.2.1 强制性国家标准

国家标准化管理委员会于 2021 年 2 月发布了强制性国家标准 GB 40050-2021《网络关键设备安全通用要求》，该标准主要用于落实《网络安全法》中第二十三条中关于网络关键设备安全的要求，为 5G 网络设备的安全性提供了技术保障和依据。标准主要内容包括了网络关键设备的安全功能要求和安全保障要求。其中，安全功能要求聚焦于设备的技术安全能力，安全保障要求则对网络关键设备提供者在设备全生命周期的安全保障能力提出要求。

3.2.2.2 TC260 推荐性国家标准

在 5G 网络安全标准研究方面，全国信息安全标准化技术委员会（TC260）针对 5G 网络安全推动了《5G 网络安全标准体系》研究，涵盖了安全基础共性、终端安全、IT 化网络设施安全、应用与服务安全、数据安全和安全运营管理等方面，并持续完善相关配套标准。TC260 在 5G 网络安全领域相关的重点标准包括：

- 在基础共性方面，GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》，规定了第一级到第四级等级保护对象的安全保护的安全通用要求和安全扩展要求，用于指导网络运营者按照网络安全等级保护制度的要求，履行网络安全保护义务。
- 在终端安全方面，GB/T 30284-2020《信息安全技术 移动通信智能终端操

作系统安全技术要求》、GB/T 34975-2017《信息安全技术 移动智能终端应用软件 安全技术要求和测试评价方法》、GB/T 35278-2017《信息安全技术 移动终端安全保护技术要求》、GB/T 37093-2018《信息安全技术 物联网感知层接入通信网的安全要求》分别对通用固件和操作系统安全、移动智能终端安全、终端侧应用软件安全开展了研究。

- 在 IT 化网络设施安全方面，TC260 已发布标准主要聚焦于云平台安全，GB/T 31167-2014《信息安全技术 云计算服务安全指南》、GB/T 35279-2017《信息安全技术 云计算安全参考架构》、GB/T 34942-2017《信息安全技术 云计算服务安全能力评估方法》、GB/T 31168-2014《信息安全技术 云计算服务安全能力要求》，提出了针对云计算服务的安全指南、安全参考架构、安全能力评估方法和安全能力要求。
- 在网络安全方面，在研标准《信息安全技术 边缘计算安全技术要求》分析边缘计算系统因云边协同控制、计算存储托管、边缘能力开放等引入的安全风险，提出了边缘计算安全参考模型，并从应用安全、网络安全、数据安全、基础设施安全、物理环境安全、运维安全、安全管理等方面提出边缘计算的安全技术要求。该标准可用于指导边缘计算相关方提高边缘基础设施研发、测试、生产、运营过程中应对各种安全威胁的能力。
- 在应用与服务安全方面，GB/T 37971-2019《信息安全技术 智慧城市安全体系框架》、GB/Z 38649—2020《信息安全技术 智慧城市建设信息安全保障指南》从安全角色和安全要素的视角提出了智慧城市安全体系框架，为智慧城市建设全过程的信息安全保障机制与技术建设提供指导。此外，TC260 正在开展新业务应用领域安全标准研制，涉及的领域涵盖了物联网、工业互联网、车联网（智能网联汽车）等。
- 在数据安全方面，TC260 发布了 GB/T 37988—2019《信息安全技术 数据安全能力成熟度模型》、GB/T 35273-2020《信息安全技术 个人信息安全规范》、GB/T 34978-2017《信息安全技术 移动智能终端个人信息保护技术要求》等相关标准用于指导数据和个人信息的保护工作。
- 在安全运营管理方面，GB/T 25068.1-2012《信息技术 安全技术 IT 网络安全 第 1 部分：网络安全管理》、GB/Z 20985-2007《信息技术 安全技术 信息安全事件管理指南》、GB/T 36958-2018《信息安全技术 网络安全等级保护安全管理中心技术要求》、GB/T 38561-2020《信息安全技术 网络安全管理支撑系统技术要求》、GB/T 24363-2009《信息安全技术 信息安全

应急响应计划规范》、GB/T 36637-2018《信息安全技术 ICT 供应链安全风险管理指南》等标准提出了网络安全管理、信息安全事件管理、应急响应计划和 ICT 供应链安全风险管理等方面的要求。

3.2.2.3 TC485 推荐性国家标准

目前，全国通信标准化技术委员会（TC485）正在推进关于 5G 网络相关标准的研究，在研标准主要涵盖基础共性、通信网络安全等方面。

- TC485 在研标准《5G 移动通信网通信安全技术要求》主要围绕 5G 移动通信网中的通信安全总体技术要求展开研究，为运营商和监管机构在 5G 安全方面工作的开展提供技术参考。
- TC485 在研标准《5G 移动通信网络设备安全保障要求 核心网网络功能》、《5G 移动通信网络设备安全保障要求 基站设备》主要围绕 5G 设备安全，从核心网网络功能、基站设备等方面，对 5G 移动通信网络设备安全提出保障要求。

3.2.2.4 CCSA 行业标准

中国通信标准化协会(CCSA)已发布的 5G 网络安全相关行业标准主要聚焦在基础共性、终端安全、IT 化网络设施安全等方面。CCSA 在 5G 网络安全领域重点标准包括：

- 在基础共性方面，YD/T 3628-2019《5G 移动通信网 安全技术要求》明确了对 5G SA 网络和 NSA 网络的基本安全要求，包括 5G 网络安全架构、安全需求，安全功能实现等。在研标准《5G 网络中的 IPSec 需求和方案研究》主要围绕 5G 网络中的 IPSec 需求和方案开展研究。
- 在终端安全方面，CCSA 已发布的标准主要关注移动智能终端安全和特定行业专用终端安全，发布了 YD/T 2407-2013《移动智能终端安全能力技术要求》、YD/T 2408-2013《移动智能终端安全能力测试方法》、YD/T 2502-2013《手机支付 移动终端安全技术要求》。
- 在 IT 化网络设施安全方面，在研标准《网络功能虚拟化（NFV）安全技术要求》主要聚焦于网络功能虚拟化（NFV）安全技术要求。
- 在通信网络安全方面，在研标准涵盖了 5G 边缘计算安全、5G 移动通信网络设备安全、5G 网络组网安全等领域。
- 在应用与服务安全方面，在研标准《5G 业务安全通用防护要求》《互联网新技术新业务安全评估要求 基于 5G 场景的业务》分别提出 5G 业务安全通

用防护和互联网新技术新业务安全评估的要求。

- 在数据安全方面，在研标准《5G 数据安全总体技术要求》从 5G 业务应用、5G 终端设备、5G 无线接入、5G 核心网等方面规定了 5G 数据安全的总体技术要求。
- 在安全运营管控方面，在研标准《5G 移动通信网通信管制技术要求》主要关注 5G 移动通信网通信管制技术要求。

4 5G 网络安全风险

相较于2G、3G和4G网络，5G网络在性能指标、应用场景和安全能力方面更趋完善。随着5G网络相关技术的快速发展，工业互联网、车联网等融合应用的深入推进，5G网络的安全挑战依旧严峻。本章从5G特点出发，梳理分析了5G网络新技术新应用所带来的终端安全风险、IT化网络设施安全风险、通信网络安全风险、行业应用安全风险、数据安全风险和网络运维风险，为5G网络安全标准框架的构建提供参考。

4.1 终端安全风险

5G 网络接入终端的种类繁多、数量巨大，终端的计算能力和安全防护措施差异明显。伴随终端的大量接入，伪造的、被劫持的、包含病毒或恶意程序的、缺少基本安全防护能力的终端可能将终端安全风险通过 5G 网络进行传播和扩大。同时，随着 5G 网络在工业互联网、车联网等行业中广泛应用，各类行业终端使用的非通用协议的安全风险也被引入 5G 网络。

4.2 IT 化网络设施安全风险

5G 基于通用硬件使用虚拟化技术实现网络功能节点的软件化，通信网络由传统电信功能网元设备为主的系统演化成由网络功能虚拟化基础设施、业务通信及管理功能组成的系统。网络功能通过云计算服务部署，通信网络边界变得模糊，传统通过物理隔离部署的安全措施不再适用。同时，由于虚拟化技术的广泛使用，安全漏洞、虚拟机逃逸攻击、针对虚拟化平台的恶意攻击等安全风险也被引入 5G 网络。

4.3 通信网络安全风险

5G 网络的服务化架构使网络功能以通用接口对外呈现，可以实现灵活的网络部署和管理，伴随接口开放，通用接口在身份认证、访问控制、通信加密等方面都面临潜在的风险，安全方案设计的缺陷会导致泛洪攻击、资源滥用等风险。

此外，边缘计算节点的安全机制缺失或策略错误配置可能导致非授权的边缘计

算网关接入、边缘节点过载、边界开放 API 接口滥用等风险；网络切片技术的使用可能面临非授权用户接入网络切片等安全风险。

4.4 行业应用安全风险

5G 技术在行业应用融合，涉及端到端安全、通信网络安全、应用安全、终端安全等问题，导致相关方安全责任界定困难；5G 网络面临的 IT 化网络设施安全风险、通信网络安全风险会影响行业应用的稳定运行；同时，行业应用由于安全漏洞、错误安全配置等原因可能将应用自身安全风险向 5G 网络传导。

4.5 数据安全风险

随着 5G 网络的大规模推广应用，数据安全风险不断多样化。边缘计算造成网络及用户数据下沉至网络边缘，数据安全管理责任界定、网络边缘数据隔离与保护的挑战明显；虚拟化技术带来的网络边界模糊增加了数据保护的难度；网络切片技术对数据的安全隔离与保护提出更高要求；接入设备数量的快速增长和防护措施能力的差异导致数据泄漏风险点增多、违法有害信息管控难度增大。

4.6 网络运维安全风险

5G 网络架构的演进带来安全运维的问题，包括：网络功能安全缺陷定位难度增大，安全缺陷可能来源于硬件、虚拟化技术、网络功能软件及编排器（MANO）；5G 网络的集中化部署增加了运维复杂性，安全事件、系统故障的影响范围更大，网络功能失效可能导致多个地区通信业务异常或中断；运维人员对网络功能虚拟化、软件定义网络等知识、技能和运维经验的缺乏可能导致安全风险难以及时有效处置。此外，光模块、射频模组等重要元器件的安全性可通过供应链直接影响 5G 网络安全。

5 5G 网络安全标准框架

5.1 总体原则

为有效应对 5G 网络安全风险，在梳理分析 5G 网络相关网络安全国家、行业标准的基础上，依据三项原则，提出了 5G 网络安全标准框架，给出了重点急需标准的研制建议。

兼顾全面，突出重点。5G 网络安全标准架构应在现有信息安全国家标准体系基础上，综合考虑 5G 网络安全面临的安全风险。同时，应聚焦 5G 网络安全风险与 2G、3G 和 4G 网络相关风险的主要差异，重点关注 5G 网络在 IT 化网络设施、服务化网络架构、边缘化计算资源，以及行业融合应用等方面特有的安全风险，全面梳理分析提炼安全标准化需求。

聚焦问题，持续完善。随着 5G 网络基站的部署和应用的推广，5G 网络安全风险目前主要集中在网络虚拟化安全、软件定义网络安全、网络切片安全、网络服务开放安全、终端安全、边缘计算安全等方面。针对现阶段 5G 网络的主要安全问题，应细化标准化需求，加快推动重点急需标准研制。由于 5G 网络技术和应用仍在快速发展阶段，技术演进和 5G 融合应用的深入推进将带来新的安全风险和挑战，应紧密跟踪 5G 技术和应用发展趋势，坚持问题导向，不断完善 5G 网络安全标准架构。

协调一致，开放引领。ISO/IEC JTC1、ITU-T、3GPP、NIST 等国外标准化组织，TC260、TC485、CCSA 等国内标准化组织均在 5G 网络安全领域开展了相关标准化研究工作，5G 网络安全标准架构应充分参考借鉴国外标准化组织的先进经验，协调一致 5G 网络技术和网络安全标准化工作成果，充分发挥我国在 5G 网络领域的技术优势，为 5G 网络的安全部署、应用和运维提供标准化支撑。

5.2 5G 网络安全标准化需求

针对 5G 新技术新应用带来的安全风险和挑战，结合 5G 关键技术发展现状，提出以下七个方面的安全标准化需求。

（1）基础共性类需求

目前，国际上已开展 5G 系统安全架构、流程相关标准的研制，国内可参考开展 5G 网络安全参考模型、通用技术相关标准研究，进一步明晰 5G 生态中各角色及其之间安全职责，指导 5G 网络规模化安全建设部署，安全开展 5G 应用活动。

（2）终端安全类需求

随着 5G 网络部署和行业融合应用的不断推进，5G 终端连接数量持续快速增长，针对 5G 终端面临的新型安全风险，应完善移动智能终端安全标准，加强物联网终端安全、专用终端安全等相关标准研究，提出安全防护措施。

（3）IT 化网络设施安全类需求

5G 的 IT 化网络设施指 5G 网络基础设施中通过 IT 技术实现的部分，是构建 5G 核心网络的重要基础。目前，国际上已针对网络虚拟化技术、软件定义网络等关键技术及应用开展相关安全标准的研制，我国的网络安全标准化工作尚未完全覆盖相关领域，急需面向网络虚拟化安全、软件定义网络安全等重点问题开展标准研制。

（4）通信网络安全类需求

5G 通信网络提出了全新网络架构及安全需求，在网络架构层面涉及无线接入网、核心网、边缘网络、网络切片及网络设备等方面。相对于传统的无线通信安全、核心网安全、互联互通安全、传输交换安全、网络设备安全等需求，边缘计算安全和网络切片安全是具有 5G 特性的安全需求，急需面向边缘计算安全、网络切片安全等重点问题开展标准研制。

（5）5G 业务与应用安全类标准

5G 业务与应用发展应考虑通用应用场景和 5G 融合应用场景的安全标准化需求，主要包括 eMBB、uRLLC、mMTC 三大 5G 场景下新业态特有的安全要求，以及工业互联网、车联网等 5G 融合应用重点领域中的安全要求。目前，急需推动 5G 网络能力开放应用与服务安全相关标准的研制，为 5G 融合应用的安全发展提供标准支撑。

（6）数据应用安全类需求

国内在个人信息保护、数据处理活动、重要数据安全、应用与服务数据安全等领域已开展了大量的学术研究和标准研制工作，为保障 5G 网络领域的数据安全应用，可从安全技术和安全管理两个维度充分参考借鉴现有个人信息保护和数据安全标准化成果，研究终端个人信息采集与保护、融合应用领域数据交换共享相关标准，支撑 5G 网络、融合应用领域数据保护工作开展。

（7）网络安全运营类需求

国内在网络安全管理方面已建立相对完善的标准体系，但缺乏专门针对 5G 网络的安全运营标准，可根据 5G 网络全生命周期的安全管理运维、安全应急响应、供应链安全需求，加强相关标准研究，强化现有网络安全管理标准在 5G 应用场景下的落地实施，支撑 5G 网络安全“三同步”工作有序开展。

5.3 5G 网络安全标准框架

结合对 5G 网络安全的需求分析，5G 网络安全标准框架包括基础共性、终端安全、IT 化网络设施安全、通信网络安全、应用与服务安全、数据安全、安全运营管理七大类标准研制方向。本白皮书明确了每一类研制方面的重点标准项目，为后续具体标准研制提供指导。

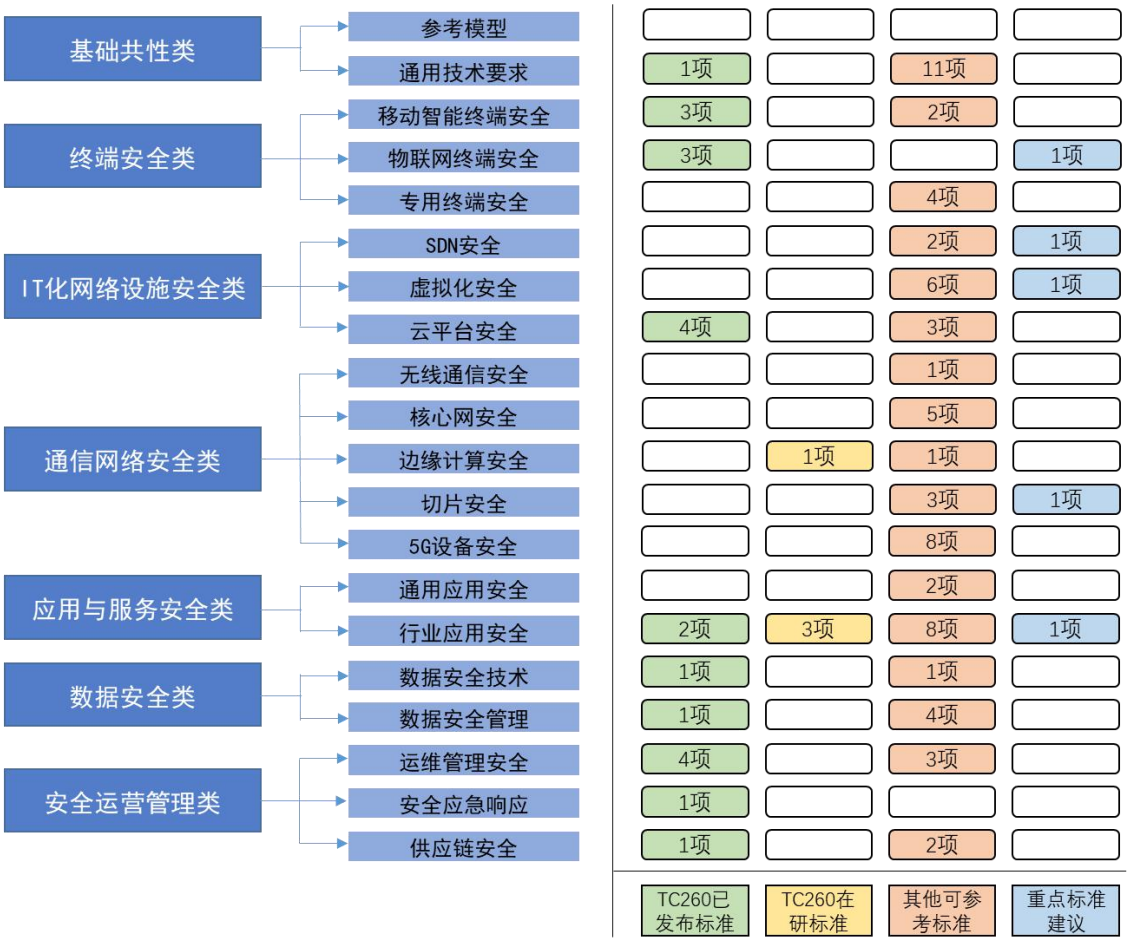


图 3 5G 网络安全标准架构

5.3.1 基础共性类标准

基础共性类标准提供 5G 网络安全标准的基础技术支撑，主要包括参考模型、通用技术要求等标准。目前，已发布和在研国家标准基本能够支撑 5G 网络的通用安全需求。

参考模型类标准用于规范 5G 网络安全参考模型等相关标准。对于 5G 网络安全参考模型，可参考 3GPP TS 33.501《5G 系统的安全架构和流程》。

通用技术要求类标准用于提出 5G 网络安全通用要求等相关标准。GB/T 22239-2020 《信息安全技术 网络安全等级保护基本要求》、YD/T 3628-2019《5G

移动通信网 安全技术要求》，以及 TC485 在研标准《5G 移动通信网通信安全技术要求》提出了相关要求，可作为后续标准化工作基础。

5.3.2 终端安全类标准

终端安全类标准主要针对连接 5G 网络的终端提出安全要求，包括移动智能终端安全、物联网终端安全、专用终端安全等。目前，已发布和在研国家标准覆盖了移动智能终端、物联网终端相关安全要求，但在轻量级终端和专用终端方面缺少相关标准，建议尽快开展研制工作。

移动智能终端安全标准应覆盖移动智能终端操作系统、应用软件安全模型和防护机制、安全开发和生命周期管理等方面的安全要求。TC260 已发布 GB/T 35278-2017《信息安全技术 移动终端安全保护技术要求》、GB/T 34975-2017《信息安全技术 移动智能终端应用软件 安全技术要求和测试评价方法》等多项相关标准，建议在后续标准制修订中增加移动智能终端的 5G 网络相关安全要求。

物联网终端安全标准主要关注终端接入和管理的安全要求，以保障各类安全防护能力差异明显的物联网终端可管可控。TC260 现有标准对物联网感知层终端安全网关、安全接入、安全应用提出了要求，已发布 GB/T 37093-2018《信息安全技术 物联网感知层接入通信网的安全要求》、GB/T 37024—2018《信息安全技术 物联网感知层网关安全技术要求》、GB/T 36951—2018《信息安全技术 物联网感知终端应用安全技术要求》等相关标准，建议后续重点开展海量、轻量级终端的安全防护要求研究，推动物联网终端网络安全相关标准研制。

专用终端安全标准主要面向高安全级别或有特殊安全要求的行业，主要涉及特定行业的安全资产定义和威胁分析、安全体系结构、行业特色安全要求、安全功能和保障、安全评测等。目前，手机支付终端、警用终端等相关行业标准正在研制，可参考使用。

5.3.3 IT 化网络设施安全类标准

IT 化网络设施安全类标准主要针对 5G 通过 IT 技术实现的基础设施提出要求，包括 SDN 安全、虚拟化安全、云平台安全等。目前，已发布和在研国家标准覆盖了云平台相关安全要求，但在网络虚拟化、软件定义网络等方面缺少相关标准，建议尽快开展研制工作。

SDN 安全类标准应重点关注 SDN 控制器、转控分离接口等方面的安全要求。目前，ITU 已发布的 X.1043《基于软件定义网络的服务功能链的安全框架和要求》和 X.1046《软件定义网络/网络功能虚拟化网络中的软件定义安全框架》两项标准可供

参考，国内相关研究仍在起步阶段，建议加快开展软件定义网络应用安全相关标准研制。

虚拟化安全标准应重点关注 NFV 基础设施安全、NFV 安全功能实现等方面的安全要求。目前我国主导的 ISO/IEC 27033-7《信息技术-网络安全-第七部分：网络虚拟化安全指南》正在研制，为网络虚拟化设施、虚拟化网络功能、虚拟化控制和资源管理等提供安全实施指南，建议参考在研国际标准，加快网络虚拟化技术安全相关国家标准的研制工作。

云平台安全标准应重点关注云基础设施的安全，建议在 GB/T 31167-2014《信息安全技术 云计算服务安全指南》、GB/T 31168-2014《信息安全技术 云计算服务安全能力要求》基础上，细化组件安全、网元隔离、东西向流量监控等安全要求。

5.3.4 通信网络安全类标准

通信网络安全类标准包括无线通信安全、核心网安全、切片安全、边缘计算安全和 5G 设备安全。目前，已发布和在研国家标准覆盖了无线通信、核心网和边缘计算、5G 设备安全相关安全要求，在网络切片方面缺少相关标准，建议尽快开展研制工作。

无线通信安全标准应重点关注终端接入鉴权、空中接口协议、通讯接口、通讯协议及参数、通信数据安全、通讯密钥管理、双向认证、日志审计等方面的安全要求。

核心网安全标准应重点关注核心网网元间的通信安全，包括 SBA 架构下网元直接通信和间接通信、SEPP 安全等方面的安全要求。

边缘计算安全标准应覆盖 MEC 平台、MEC 编排管理系统、UPF 以及 APP 安全等。目前，TC260 在研国家标准《信息安全技术 边缘计算安全技术要求》可指导相关工作。

切片安全标准应重点关注终端与切片安全隔离、切片安全认证、切片管理等。目前，已发布的 3GPP TS 33.501《5G 系统的安全架构和流程》、YD/T 3628-2019《5G 移动通信网 安全技术要求》，以及 TC485 在研的《5G 移动通信网通信安全技术要求》覆盖了无线安全、核心网安全、网络接片管理安全相关要求，在网络建设运维中可直接参考。建议进一步研制网络切片安全管理相关标准，保障网络切片安全使用。

5G 网络设备安全标准应覆盖网络设备的通讯协议安全和网络设备的自身安全以及安全功能要求。已发布的 3GPP TS 33.511-33.519 网络设备安全保障要求系列标准可参考，我国已发布强制性国家标准 GB 40050-2021《网络关键设备安全通用

要求》对 5G 网络相关设备提出了应满足的最基本安全要求。

5.3.5 应用与服务安全类标准

应用与服务安全类标准用于指导重要行业和领域的 5G 网络安全规划和建设，包括基于 5G 网络的通用安全应用和行业应用安全等标准。5G 网络应用仍在起步阶段，建议优先推动网络能力开放安全相关标准研制工作，并同步推进行业应用的标准化研究。

通用应用安全标准针对 5G 网络的应用提出安全要求，包括 5G 应用安全框架，以及 eMBB、mMTC、uRLLC 三大应用场景下安全风险防范要求等，可参考 3GPP TS 33.501《5G 系统的安全架构和流程》关于安全能力开放的相关接口定义，制定网络能力开放安全技术要求，为网络层、应用层间职责划分、安全交互提供规范指导。

行业应用安全标准针对工业互联网、智慧城市、车联网、智能家居、智能安防、智慧医疗、公共服务等行业领域，指导各行业安全开展 5G 网络应用和服务。相关安全标准包括 GB / Z 38649-2020《信息安全技术 智慧城市建设信息安全保障指南》。目前，TC260 已经开展《信息安全技术 汽车电子系统网络安全指南》《信息安全技术 工业互联网平台安全要求及评估规范》可为相关领域 5G 网络的安全应用提供指导。

5.3.6 数据安全类标准

数据安全类标准应重点覆盖 5G 网络相关技术在数据安全管理和安全技术等方面的要求。5G 网络的数据安全问题是由边缘计算、网络切片、虚拟化等新技术的应用所引入，在具体技术要求和管理要求方面，目前已发布和在研国家标准基本能够覆盖。可参考 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》、GB/T 37973—2019《信息安全技术 大数据安全管理指南》，针对边缘节点数据采集、传输、存储、处理、交换、销毁等全生命周期环节提出安全要求。

5.3.7 安全运营管理类标准

安全运营管理类标准应重点覆盖 5G 网络运维管理、应急响应、供应链安全等方面的要求。目前，已发布和在研国家标准基本能够覆盖相关安全要求。可参考 GB/T 36626—2018《信息安全技术 信息系统安全运维管理指南》、GB/T 24363—2009《信息安全技术 信息安全应急响应计划规范》、GB/T 36637-2018《信息安全技术 ICT 供应链安全风险管理指南》的技术要求，针对 5G 的服务化网络架构、IT 化网络设施等特点，完善网络安全运营管理要求，提升应急相应能力，强化 5G 全生命周期的

供应链安全。

5.4 5G 网络安全重点标准研制建议

结合 5G 网络安全标准化需求，以及已发布和在研相关标准现状，梳理得出目前在终端安全、IT 化网络设施安全、通信网络安全、应用与服务安全等领域存在待制定标准需求。为保障 5G 技术应用安全与产业发展急需，下一步应重点加强轻量级终端安全防护、网络虚拟化技术安全、软件定义网络安全、网络切片安全、网络能力开放安全等相关标准的研制。表 5-1 中给出了建议近两年加快研制的 5G 网络安全标准，包括标准名称、状态、标准拟解决的问题和对应类别等内容，为我国 5G 网络安全标准制修订工作提供参考。

表 5-1 建议制定的 5G 网络安全标准

序号	标准名称	状态	标准拟解决的问题	对应类别
1	**轻量级终端安全防护技术要求**	建议研制	本标准是在海量轻量级终端接入的背景下，为解决由于设备资源受限等情况，终端缺乏相应的安全保护机制与措施，极易引发安全风险并在 5G 网络空间泛化传播等问题，提出轻量级终端应具备的安全防护要求。	终端安全类
2	**网络虚拟化技术安全指南**	建议研制	本标准为解决由于 5G 网络虚拟化技术应用引入的新的安全风险，包括在物理资源层、虚拟资源层、应用层等层面面临的网络安全风险和威胁，提出 5G 网络虚拟化技术应用方面的安全框架及实施准则。 目前，**ISO/IEC 27033-7 标准《信息技术-网络安全-第七部分：网络虚拟化安全指南》正在研制**，旨在分析网络虚拟化安全性的主要挑战和风险，提供网络虚拟化安全性的框架并提出实施准则。	IT 化网络设施安全类
3	**软件定义网络应用安全要求**	建议研制	本标准为解决软件定义网络技术在对底层网络进行软件编程及管理过程中，缺乏规范的安全要求而提出的标准化解决方案。如针对网络控制平面与用户数据平面分离操作及跨网路层级、跨域地部署软件定义网络时存在的安全风险提出安全防护技术	IT 化网络设施安全类

序号	标准名称	状态	标准拟解决的问题	对应类别
			与管理要求，为通信运营商及网络服务提供商提供端到端的软件编程能力服务提供参考。	
4	**网络切片安全技术要求**	建议研制	为解决网络切片技术面向垂直行业应用提供切片服务所面临的安全风险，本标准规定网络切片按需定制和安全隔离的核心能力，给出包含网络切片安全接入、安全认证、安全隔离的安全防护架构，根据行业应用的特定安全需求，划分网络切片服务安全保障等级，以满足网络切片隔离在行业应用的安全需求。	通信网络安全类
5	**网络能力开放安全技术要求**	建议研制	为解决 5G 网络能力开放架构面临的安全风险，本标准基于 5G 网络能力及安全能力开放关键技术与定制化需求，给出网络能力与安全能力开放接口、调用及平台等方面的安全要求，促进 5G 与各行业的融合应用，保障行业应用和运营商网络之间安全可靠地传递能力开放信息。	应用与服务安全类

6 5G 网络安全标准化工作推进建议

6.1 加快推进 5G 网络安全标准体系建设与重点标准研制

《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》提出要构建新型基础设施标准体系，为发挥网络安全标准在保障5G产业发展中的基础性、规范性和引领性作用，推动5G网络安全保障与5G网络架构演进、网络部署同步实施，应规划建设5G网络安全标准体系，根据5G技术应用与产业发展急需，加快重点领域标准研制。

- 聚焦 5G 关键核心技术与典型业务与应用场景的安全需求，围绕基础共性、关键技术安全、终端安全、网络与通信安全、数据安全、应用与服务安全、安全运营与管理等方面，构建 5G 网络安全标准体系；
- 做好 5G 网络安全标准体系与网络安全国家标准体系的科学衔接，同时注重与物联网安全、工业互联网安全、车联网安全、智慧城市安全、大数据安全等新兴领域标准体系的设计融合以及与现有网络安全基础通用标准的关联应用；
- 围绕 5G 终端安全、IT 化网络设施安全、通信网络安全、应用与服务安全等重点急需领域，开展网络虚拟化安全、软件定义网络安全、轻量级终端安全、网络切片安全、网络能力开放安全等相关标准的研制，在边缘计算安全，以及工业互联网、车联网等与 5G 紧密相关的行业应用安全标准研制过程中充分考虑 5G 安全特性，为 5G 网络与行业融合应用安全发展提供标准支撑。

6.2 提前布局 5G 融合应用安全风险与保障研究

“十三五”期间，我国已建成全球规模最大的光纤和4G网络，5G网络部署与产业整体实力迈入全球前列。目前，5G网络建设仍在持续推进，5G商用还未全面铺开，推动5G融合应用发展已成为助力数字经济发展与产业模式创新的必然趋势，5G将面向个人、企业、行业等多端用户和市场同时发力，在为行业数字化转型发展带来机遇的同时，5G融合应用也面临着诸多挑战，尤其是更加复杂的网络环境下所面临的安全风险挑战。为明确5G网络安全需求并指引相关标准化工作方向，应提前布局5G融合应用等领域的安全风险和保障措施的研究。

- 推进 5G 与各行业融合应用安全风险研究，在提升 5G 自身网络安全防护能力的同时，注重面向各行业应用开展差异化网络安全需求分析，推动 5G 网络安全能力向开放化、定制化方向演进；
- 打造升级版 5G 网络安全防御理念，构建产业协同安全生态，探索推进人工智能、区块链、量子信息等新兴技术在 5G 网络安全防护中的应用，突破传统通信网络边界防护模式，加强与工业互联网、物联网、车联网、智慧城市等行业的安全互动和协同防护，构建积极主动的综合防御体系；
- 提升 5G 融合应用安全方面的监管能力，持续跟踪 5G 与各行业融合发展时在供应链安全、数据安全等方面的安全态势变化，及时研制 5G 网络安全监管所需配套标准，以标准支撑建立贯穿 5G 网络设计、规模部署、商业应用、跨领域垂直融合等全方位的安全保障体系，规范引导 5G 与各行业产业安全健康发展。

6.3 大力开展 5G 网络安全标准验证与实施

5G网络安全标准将为5G电信运营商、网络与通信设备厂商、应用与服务提供商、安全厂商等开展5G相关业务提供安全技术要求和参考规范，应不断完善网络安全标准化的运行机制，以5G网络部署与安全防护协同发展为契机，确保5G网络安全标准在通信网络部署与运行中的有效实施与应用。

- 充分借鉴现有网络安全国家标准体系中的基础通用性标准，重点围绕网络安全风险管理、应急处置、供应链安全等相关标准开展验证，提高对已发布网络安全国家标准的利用率，对存在不适用条款的基础通用性标准适时开展修订工作；
- 聚焦边缘计算等新兴技术及 5G 供应链安全等领域开展标准验证应用。截至目前，TC260 已开展了《信息安全技术 边缘计算安全技术要求》等国家标准研制和《边缘计算密码应用基本要求研究》《5G 边缘计算安全体系及技术研究》《5G 供应链安全评估指南》等相关标准研究，通过开展 5G 网络安全标准应用试点等工作，验证评估相关标准研究成果，遴选出一批应用效果好的标准项目适时进行标准成果转化和推广应用。

6.4 深度参与 5G 网络安全国际标准化工作

网络安全问题已成为全球性的挑战，应坚持开放合作的理念推进网络安全国际标准化工作，在5G等新兴技术领域更多贡献中国方案。目前，在国际标准化层面，

5G技术性国际标准数量众多且体系相对完善，5G网络安全国际标准主要聚焦在安全架构设计与核心技术安全领域，以ISO、ITU、3GPP、ETSI等为代表的国外标准化组织积极推进5G网络安全标准研究。在国际标准化工作方面应做好以下几项工作：

- 充分借鉴、消化、吸收国际国外已有的 5G 网络安全国际标准化工作成果，结合我国 5G 技术发展优势与安全需求，探索具有我国特色的 5G 网络安全标准化工作思路，推进国内 5G 网络安全标准与国际标准的互联互通，促进标准化成果交流共享，共同构建安全、开放、互信的 5G 生态；
- 持续深入研究国际国外 5G 网络安全政策法规，研究跟进国际标准研制进展，引进实施国际标准组织先进的 5G 网络安全相关标准，进一步补充完善 5G 网络安全标准体系；
- 梳理国际国外 5G 网络部署与安全防护工作脉络与先进经验，优化提升我国 5G 网络安全工作发展模式，充分发挥我国国际标准化交流与合作机制，积极支持我国单位和专家参与 5G 国际标准研制，推动国内先进的 5G 网络安全标准在国际标准组织的立项，提升我国在国际上的话语权与影响力。

7 参考文献

[1] ITU-R M.2083-0. IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond [S]. ITU-R, 2015
[2] 朱莉欣，李康．网络安全视野下的 5G 政策与法律[J]．中国信息安全,2019,117(09):96-98.
[3] 工业和信息化部.《工业和信息化部关于推动 5G 加快发展的通知》[R]. 北京.2020 年 3 月 24 日
[4] YD/T 3628-2019. 5G 移动通信网 安全技术要求[S]. CCSA, 2019
[5] TS 33.501. Security architecture and procedures for 5G System [S]. 3GPP, 2018
[6] TR 33.841. Study on the support of 256-bit algorithms for 5G [S]. 3GPP, 2018
[7] TR 33.834. Study on Long Term Key Update Procedures (LTKUP) [S]. 3GPP, 2018
[8] ITU-T X.5Gsec-q. Security guidelines for applying quantum-safe algorithms in 5G systems [S]. ITU-T, 2020
[9] ITU-T X.5Gsec-t. Security framework based on trust relationship for 5G ecosystem [S]. ITU-T, 2020
[10] ITU-T X.5Gsec-guide. Security guideline for 5G communication system based on ITU-T X.805 [S]. ITU-T, 2019
[11] ITU-T X.ssc. Security Service Chain Architecture and its Application [S]. ITU-T, 2019
[12] 5G Security Trust Model [S]. GSMA, in press.
[13] GB/T 30284-2020. 移动通信智能终端操作系统安全技术要求[S]. TC260, 2020
[14] GB/T 35278-2017. 信息安全技术 移动终端安全保护技术要求[S]. TC260, 2017
[15] GB/T 37093-2018. 信息安全技术 物联网感知层接入通信网的安全要求[S].TC260,2018
[16] YD/T 2407-2013. 移动智能终端安全能力技术要求[S]. CCSA, 2013
[17] YD/T 2408-2013. 移动智能终端安全能力测试方法[S]. CCSA, 2013
[18] ITU-T X.1043. Security framework and requirements of Service Function Chain based onsoftware defined networking [S]. ITU-T, 2019
[19] ITU-T X.1046. Framework of software-defined security in software-defined networks/network functions virtualization networks [S]. ITU-T, 2020
[20] ITU-T X.srnv. Security Requirements of Network Virtualization [S]. ITU-T, 2019
[21] ITU-T X.SRIaaS. Security Requirements of Public Infrastructure as a Service (IaaS) in Cloud Computing [S]. ITU-T, 2020

[22] ITU-T X.SRNaaS. Security Requirements of Network as a Service (NaaS) in Cloud Computing [S]. ITU-T, 2020
[23] ITU-T X.SRCaaS. Security requirements for communication as a service (CaaS) application environments [S]. ITU-T, 2020
[24] TR 33.848. Study on security impacts of virtualization [S]. 3GPP, 2018
[25] TR 33.818. Security Assurance Methodology (SECAM) and Security Assurance Specification (SCAS) for 3GPP virtualized network products [S]. 3GPP, 2018
[26] NFV threat analysis [S]. GSMA, in press.
[27] ISO/IEC 27033-7. Information Technology-Network Security-Part 7: Guidelines for network virtualization security [S]. ISO, 2021
[28] NG.113. 5G roaming Guideline [S]. GSMA, 2020
[29] NG.116. Generic Network Slice Template [S]. GSMA, 2019
[30] IR.77. Interoperator IP backbone security Req. For Service and Inter operator IP backbone Providers [S]. GSMA, 2010
[31] TS 33.511-33.519. Security Assurance Specification (SCAS) [S]. 3GPP, 2018
[32] TR 33.855. Study on security aspects of the 5G Service Based Architecture (SBA) [S]. 3GPP, 2018
[33] TR 33.809. Study on 5G security enhancements against false base stations [S]. 3GPP, 2018
[34] TR 33.813. Study on security aspects of network slicing enhancement [S]. 3GPP, 2018
[35] ITU-T X.5Gsec-ecs. Security Framework for 5G Edge Computing Services [S]. ITU-T, 2019
[36] Network Slice Isolation [S]. GSMA, in press.
[37] TS 33.535. Authentication and Key Management for Applications based on 3GPP credential in 5G [S]. 3GPP, 2019
[38] TR 33.819. Study on security enhancements of 5GS for vertical and Local Area Network (LAN) services [S]. 3GPP, 2018
[39] TR 33.814. Study on the security of the enhancement to the 5GC Location Services (LCS) [S]. 3GPP, 2018
[40] TR 33.836. Study on security aspects of 3GPP support for advanced V2X services [S]. 3GPP, 2019
[41] TR 33.807. Study on the security of the wireless and wireline convergence for the 5G system architecture [S]. 3GPP, 2018
[42] TR 33.861. Study on evolution of cellular IoT security for the 5G System [S]. 3GPP, 2018
[43] TR 33.825. Study on the security of Ultra-Reliable Low-Latency Communication (URLLC) for 5GS [S]. 3GPP, 2018
[44] GB/T 35273-2020. 信息安全技术 个人信息安全规范[S]. TC260, 2020

[45] GB/T 34978-2017. 信息安全技术 移动智能终端个人信息保护技术要求[S]. TC260,2017
[46] ITU-T X.sgtBD. Security guidelines of lifecycle management for telecom Big Data [S]. ITU-T, 2020
[47] ITU-T X.1052-rev. Organization information security management guideline [S]. ITU-T, 2020
[48] ITU-T X.1054-rev. Governance of information security [S]. ITU-T, 2020
[49] ITU-T X.Framcdc. Framework for the creation and operation of a cyber defense center [S]. ITU-T, 2018
[50] ITU-T X.Ciag. Cyber insurance acquisition guideline for Information and Communication Technologies (ICT) services provider [S]. ITU-T, 2021
[51] ISO 28000:2007. Specification for security management systems for the supply chain [S]. ISO, 2007
[52] ISO/IEC 27036-2:2014. Information technology - Security techniques - Information security for supplier relationships [S]. ISO, 2014

附录 A 国内外已发布及在研相关标准

A.1 国内已发布相关安全标准

主题及分类		标准名称	归口单位	标准编号
基础共性类	通用技术要求	《5G 移动通信网 安全技术要求》	CCSA	YD/T 3628-2019
		《信息安全技术 网络安全等级保护基本要求》	TC260	GB/T 22239-2019
终端安全类	移动智能终端安全	《信息安全技术 移动通信智能终端操作系统安全技术要求》	TC260	GB/T 30284-2020
		《信息安全技术 移动智能终端应用软件 安全技术要求和测试评价方法》	TC260	GB/T 34975-2017
		《信息安全技术 移动终端安全保护技术要求》	TC260	GB/T 35278-2017
		《移动智能终端安全能力技术要求》	CCSA	YD/T 2407-2013
		《移动智能终端安全能力测试方法》	CCSA	YD/T 2408-2013
	物联网终端安全	《信息安全技术 物联网感知层接入通信网的安全要求》	TC260	GB/T 37093-2018
		《信息安全技术 物联网感知层网关安全技术要求》	TC260	GB/T 37024—2018
		《信息安全技术 物联网感知终端应用安全技术要求》	TC260	GB/T 36951—2018
	专用终端安全	《手机支付 移动终端安全技术要求》	CCSA	YD/T 2502-2013
通信网络安全类	5G 设备安全	《网络关键设备安全通用要求》	工信部	GB 40050-2021
IT 化网络设施安全类	云平台安全	《信息安全技术 云计算服务安全指南》	TC260	GB/T 31167-2014
		《信息安全技术 云计算安全参考架构》	TC260	GB/T 35279-2017
		《信息安全技术 云计算服务安全能力评估方法》	TC260	GB/T 34942-2017
		《信息安全技术 云计算服务安全能力要求》	TC260	GB/T 31168-2014
应用	行业应用安全	《信息安全技术 智慧城市安全体	TC260	GB/T 37971-2019

与服务安全		系框架》		
		《信息安全技术 智慧城市建设信息安全保障指南》	TC260	GB/Z 38649—2020
数据安全类	数据安全管理	《信息安全技术 个人信息安全规范》	TC260	GB/T 35273-2020
	数据安全技术	《信息安全技术 移动智能终端个人信息保护技术要求》	TC260	GB/T 34978-2017
安全运营管理	运维管理安全	《信息技术 安全技术 IT 网络安全 第 1 部分：网络安全管理》	TC260	GB/T 25068.1-2012
		《信息技术 安全技术 信息安全事件管理指南》	TC260	GB/Z 20985-2007
		《信息安全技术 网络安全等级保护安全管理中心技术要求》	TC260	GB/T 36958-2018
		《信息安全技术 网络安全管理支撑系统技术要求》	TC260	GB/T 38561-2020
	安全应急响应	《信息安全技术 信息安全应急响应计划规范》	TC260	GB/T 24363-2009
	供应链安全	《信息安全技术 ICT 供应链安全风险管理指南》	TC260	GB/T 36637-2018

A.2 国内在研相关安全标准

主题及分类		标准名称	归口单位
基础共性类	通用技术要求	《5G 移动通信网通信安全技术要求》	TC485
		《5G 网络中的 IPSec 需求和方案研究》	CCSA
IT 化网络设施安全类	虚拟化安全	《网络功能虚拟化（NFV）安全技术要求》	CCSA
终端安全类	专用终端安全	《行业终端安全技术要求》	CCSA
		《增强宽带终端安全技术要求》	CCSA
		《工业互联网设备安全防护要求》	CCSA
通信网络安全类	5G 设备安全	《5G 移动通信网络设备安全保障要求 核心网网络功能》	TC485
		《5G 移动通信网络设备安全保障要求 基站设备》	TC485
		《5G 移动通信网络设备安全保障要求 核心网网络功能》	CCSA
		《5G 移动通信网络设备安全保障要求 基站设备》	CCSA
		《移动通信网络设备安全保障通用要求》	CCSA
	核心网安全	《5G 网络独立组网（SA）日志留存技术要求》	CCSA
		《5G 网络非独立组网（NSA）日志留存技术要求》	CCSA
	边缘计算安全	《信息安全技术 边缘计算安全技术要求》	TC260
应用与服务安全	通用应用安全	《5G 业务安全通用防护要求》	CCSA
		《互联网新技术新业务安全评估要求 基于 5G 场景的业务》	CCSA
	行业应用安全	《信息安全技术 工业互联网数据安全防护指南》	TC260
		《信息安全技术 工业互联网平台安全要求及评估规范》	TC260
		《信息安全技术 车载网络设备信息安全技术要求》	TC260
数据安全	数据安全管理	《5G数据安全总体技术要求》	CCSA
	数据安全技术	《工业互联网数据安全分类分级指南》	CCSA
安全运营管理	运维管理安全	《5G 移动通信网通信管制技术要求》	CCSA

A.3 国外已发布相关安全标准

主题及分类		标准名称	归口单位	标准编号
基础共性类	通用技术要求	Security architecture and procedures for 5G System	3GPP	3GPP TS 33.501
		Study on the support of 256-bit algorithms for 5G;	3GPP	3GPP TR 33.841
		Study on Long Term Key Update Procedures (LTKUP)	3GPP	3GPP TR 33.834
IT 化网络设施安全类	SDN 安全	Security guideline of Service Function Chain based on software defined networking	ITU	ITU-T X.1043
		Framework of software-defined security in software-defined networks/network functions virtualization networks	ITU	ITU-T X.1046
通信网络安全类	5G 设备安全	Security Assurance Specification (SCAS)	3GPP	3GPP TS 33.511-33.519
		NESAS 设备安全保证框架系列标准	GSMA	GSMA FS.13-FS.16
	切片安全	Generic Network Slice Template	GSMA	GSMA NR.116
	核心网安全	Study on security aspects of the 5G Service Based Architecture (SBA)	3GPP	3GPP TR 33.855
		Interoperator IP backbone security requirements	GSMA	GSMA IR.77
		5G roaming Guideline	GSMA	GSMA NR.113
应用与服务安全	行业应用安全	Authentication and Key Management for Applications based on 3GPP credential in 5G	3GPP	3GPP TS 33.535
安全运营管控	供应链安全	Specification for security management systems for the supply chain	ISO	ISO 28000:2007
		Information technology - Security techniques - Information security for supplier relationships	ISO	ISO/IEC 27036

A.4 国外在研相关安全标准

主题及分类		标准名称	归口单位
基础共性类	通用技术要求	Security framework based on trust relationship in 5G ecosystem	ITU-T
		Security guideline for 5G communication system based on ITU-T X.805	ITU-T
		Security Service Chain Architecture and its Application	ITU-T
		5G Security Trust Model	GSMA
		Security guidelines for applying quantum-safe algorithms in 5G systems	ITU-T
IT化网络设施安全类	虚拟化安全	Study on security impacts of virtualisation	3GPP
		Security Assurance Methodology (SECAM) and Security Assurance Specification (SCAS) for 3GPP virtualized network products	3GPP
		Security Requirements of Network Virtualization	ITU-T
		NFV threat analysis	GSMA
		Information Technology —Network Security—Part 7: Guidelines for network virtualization security	ISO
	云平台安全	Security Requirements of Public Infrastructure as a Service (IaaS) in Cloud Computing	ITU-T
		Security Requirements of Network as a Service (NaaS) in Cloud Computing	ITU-T
		Security requirements for communication as a service (CaaS) application environments	ITU-T
通信网络安全类	无线安全	Study on 5G security enhancements against false base stations	3GPP
	边缘计算安全	Security Framework for 5G Edge Computing Services	ITU-T
	切片安全	Study on security aspects of network slicing enhancement	3GPP
		Network Slice Isolation	GSMA
应用与服务安全	行业应用安全	Common Implementation Guide to Using the SIM as a ‘Root of Trust’ to secure IoT Application	GSMA
		Study on security enhancements of 5GS for vertical and Local Area Network (LAN) services	3GPP
		Study on the security of the enhancement to the 5GC Location Services (LCS)	3GPP
		Study on security aspects of 3GPP support for advanced V2X services	3GPP

		Study on the security of the wireless and wireline convergence for the 5G system architecture	3GPP
		Study on evolution of cellular IoT security for the 5G System	3GPP
		Study on the security of Ultra-Reliable Low-Latency Communication (URLLC) for 5GS	3GPP
数据安全	数据安全管理	Security guidelines of lifecycle management for telecom Big Data	ITU-T
		Organization information security management guideline	ITU-T
		Governance of information security	ITU-T
安全运营管理	运维管理安全	Cyber insurance acquisition guideline for Information and Communication Technologies (ICT) services provider	ITU-T
		Framework for the creation and operation of a cyber defense center	ITU-T

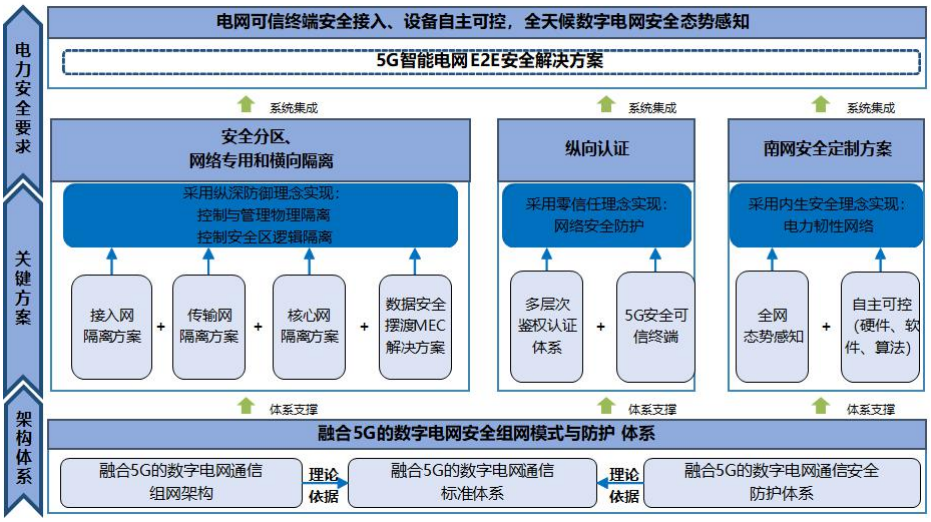
附件 B 5G 网络安全标准应用实践案例

B.1 5G 智能电网安全标准应用实践

1、安全实践介绍

2020年3月，工信部与国家发改委印发《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》，明确提出了重点支持面向智能电网等七大领域的5G创新应用。在国家政策指引下，中国移动加快与电力行业开展5G合作的步伐，进行了一系列5G赋能电力行业的实践，针对电网公司电力监控系统安全防护要求，打造了一套多维度安全防护体系。

根据国家能源局《关于印发电力监控系统安全防护总体方案等安全防护方案和评估规范的通知》（国能安全〔2015〕36号）关于电力监控系统的隔离要求，设计3个电力业务网络切片，并利用多种切片隔离技术满足电网不同的业务需求。接入网层面，采用RB资源预留来满足不同物理切片之间的隔离，在单个切片内采用5QI优先级调度技术满足不同电力业务之间的隔离。传输网层面，基于SPN特性，采用FlexE/MTN来满足物理切片的接口隔离，在单个切片内采用VPN+QoS逻辑隔离技术满足不同电力业务之间的隔离。核心网层面，计划建设独占专项的MEC和核心网元来满足与其他行业专网的隔离。在电力业务数据保护方面，考虑了MEC容器加固，以及部署虚拟防火墙等举措。在感知预警方面，3个电力业务网络切片计划接入南方电网的网络安全态势感知系统，在用户侧安全设备内置安全探针，支持安全设备信息上报以及策略下发。通过数据挖掘、机器学习等技术分析电力切片业务流与网络不安全结果之间的关系，构建面向切片业务流数据在内的新网络安全态势感知方案。



图B.1 5G智能电网立体防护体系

2、安全标准应用情况

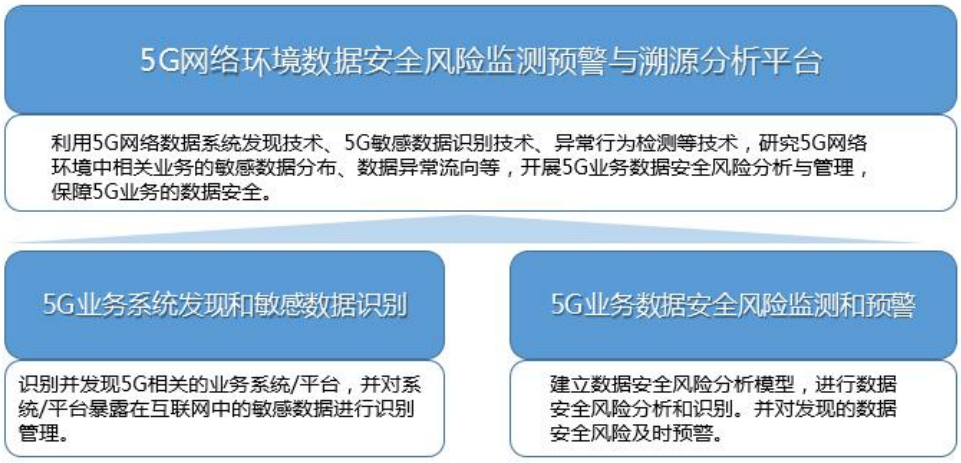
在该解决方案设计过程中，中国移动会同电力企业、设备制造商等，按照YD/T 2020-0147《5G数据安全总体技术要求》、国家标准《信息安全技术 关键信息基础设施网络安全保护基本要求(报批稿)》《信息安全技术 关键信息基础设施安全检查评估指南（报批稿）》等标准要求，进一步量化安全技术指标和架构设计，包括5G 网络切片安全性、业务隔离等，以提供满足电力行业多场景差异化的解决方案，并进行技术验证和示范。

B.2 5G 数据安全标准应用实践

1、安全实践介绍

5G 为信息处理方式带来了全新的挑战。目前由于传输速率与时延的原因，移动智能终端设备通过硬盘、芯片去存储与运算数据。伴随着 5G 带来传输速率的提升，海量的数据和计算向云端迁移，移动智能终端可以仅作为接收设备。5G 应用场景下，相关数据安全问题较多发生在 IDC/云计算/边缘计算等场景下，具体表现为数据安全防控措施不到位，对海量数据的安全处置不及时，容易造成数据非受控使用。

中国移动针对 5G 网络场景开展数据安全监测和分析，基于 IDC/云计算等数据，建立 5G 网络环境数据安全风险监测预警与溯源分析平台（以下简称“5G 业务数据安全分析平台”），利用 5G 网络数据系统发现技术、5G 敏感数据识别技术、异常行为检测等技术，研究 5G 网络环境中相关业务的敏感数据分布、数据异常流向等，开展 5G 业务数据安全风险分析与管理，保障 5G 业务的数据安全，提升 5G 业务的管理能力。



图B.2 5G业务数据安全分析平台逻辑架构

5G 业务系统发现及敏感数据识别：识别并发现 5G 相关的业务系统/平台。例如，5G 微站监控云平台、5G 车辆智能监控平台、5G 智慧燃气云、5G + 生产监控平台等 5G 业务处理相关平台等，并对系统/平台暴露在互联网中的敏感数据进行识别管理。

5G 业务数据安全风险监测和预警：建立数据安全风险分析模型，对 5G 业务系统/平台在数据采集、传输、存储、使用、开放共享等操作过程汇总的数据安全风险进行分析和识别，并对发现的数据安全风险及时预警。

2、安全标准应用情况

在该平台的使用和建设过程中，参考了 GB/T 35273-2020《信息安全技术 个人信息安全规范》、YD/T 2020-0147《5G 数据安全总体技术要求》、YD/T 3865-2021《工业互联网数据安全保护要求》、TC260 在研国家标准《信息安全技术 数据出境安全评估指南（送审稿）》等。通过 5G 数据安全控制措施的落地，在 5G 业务数据识别、风险分析、监测预警方面取得了相应成果。依托平台实践应用推动孵化了行业标准，相关平台也入围了 2020 年工信部试点示范项目。

B.3 5G 边缘计算安全标准应用实践

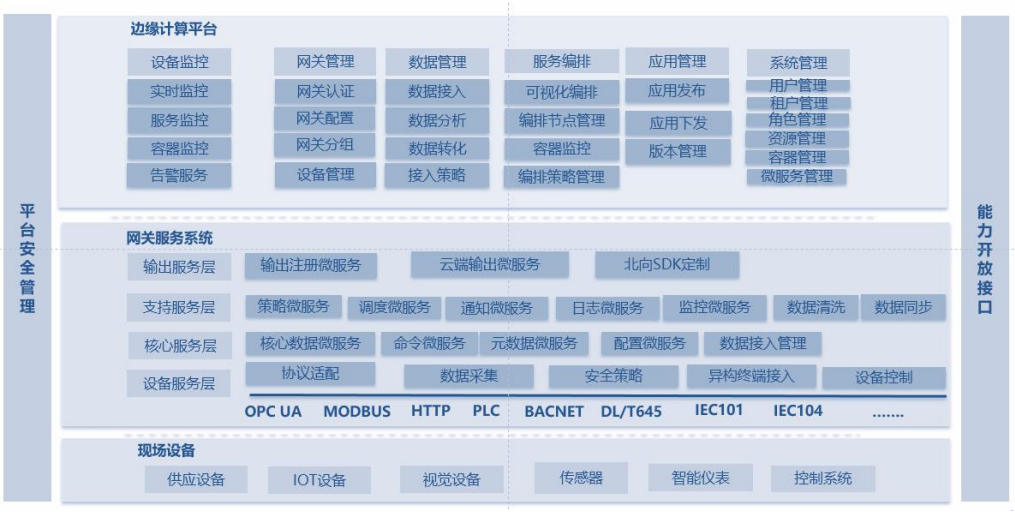
1、安全实践介绍

5G 边缘计算架构通过将云计算能力和 IT 服务环境下沉到移动通信网络边缘，就近向用户提供服务，从而构建一个具备高性能、低时延与高带宽的电信级服务环境。综合不同业务对时延、成本和企业数据安全性的考量，下沉到汇聚机房和园区是最常见的部署方案，主要部署场景可分为广域 MEC 和局域 MEC 两大类。

(1) 广域 MEC：对于低时延业务，由于百公里传输引入的双向时延低于 1ms，基于广域 MEC 的 5G 公网已经能够为各类垂直行业提供 5G 网络服务。权衡应用对接、运维复杂度、设备和工程成本等多种因素，MEC 部署在汇聚机房是当前运营商广域 MEC 的常见方案。

(2) 局域MEC：对于安全与隐私保护高敏感的行业，可以选择将MEC部署在园区，以满足数据不出园的要求。港口龙门吊的远程操控，钢铁厂的天车远程操控，以及大部分的制造、石化、教育、医疗等园区/厂区都是局域MEC的典型场景。局域MEC部署场景下，MEC将满足uRLLC超低时延业务；同时支持企业业务数据本地流量卸载，为园区客户提供本地网络管道。

在工业领域，数据采集基础系统能够帮助解决工业制造大融合下的分工，即OT和CT的融合；在智慧城市/交通/医疗等领域，数据采集基础系统解决了边缘层异构模型融合，实现了各类高效边缘智能化应用；在消费领域，数据采集基础系统通过网络、安全、边缘智能等手段渗入生产消费各个环节，将市场消费体系带入了新零售阶段。



图B.3 5G边缘计算逻辑

5G边缘计算融合了多方面的安全体系或架构，包括5G网络安全、虚拟化平台安全、容器安全、外部通信安全、内部服务调用安全、系统或组件级的原生安全、高可用架构和安全运营与监控等等。

2、安全标准应用情况

5G边缘计算可参考的安全标准包括3GPP TS 33.501《5G系统的安全架构和流程》、TS 33.117《通用安全保障要求目录》、TS 33.513《5G安全保障规范（SCAS）：用户平面功能（UPF）》等。通过安全标准的应用，构建安全边缘计算平台，为用户提供边缘计算服务。

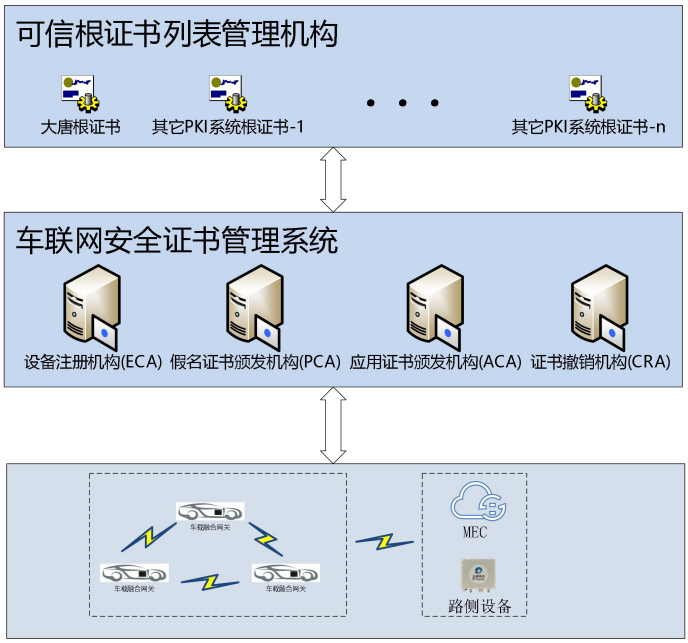
B.4 C-V2X 车联网安全标准应用实践

1、安全实践介绍

车联网产业是汽车、电子、信息通信、道路交通运输等行业深度融合的新型产业形态，已成为我国战略性新兴产业的重要发展方向。我国车联网产业化进程逐步加快，车联网的功能安全、网络安全、隐私和数据安全是构建车联网应用的关键环节。

C-V2X技术是基于5G移动通信网络的新技术，通过Uu接口(蜂窝通信接口)和PC5接口(直连通信接口)的协同应用，可极大提高汽车与外界交互的可靠性。C-V2X车联网应用作为5G重要的应用之一，通过车-车、车-路、车-网通信等通信方式实现低时延和高可靠的车联网通信，对于无人驾驶技术的具体应用有着至关重要的作用。C-V2X车联网安全包括通信安全和应用安全，通信安全采用了蜂窝移动通信的安全架构和安全机制，C-V2X系统使用基于公钥证书的PKI机制确保终端间的安全认证和安全通信，通过采用数字签名和加密等技术手段实现车联网终端之间消息的安全通信。

因此需要车联网安全管理系统来实现证书颁发、证书撤销、终端安全信息收集、数据管理、异常分析等一系列与安全相关的功能，确保车联网应用安全。



图B.4 车联网安全架构

2、安全标准应用情况

C-V2X车联网安全架构参考了多项国际标准和行标，针对C-V2X通信安全，主要参考3GPP TS 33.536 《3GPP支持先进V2X服务的安全方面》和TS 33.185 《V2X服务LTE支持的安全方面》；针对应用层安全，主要参考了IEEE1609.2《IEEE 车载环境（WAVE）无线接入-面向应用和管理消息的安全业务》，ETSI TS 102 731《智能交通系统（ITS）：安全业务和架构》，ETSI TS 102 940《智能交通系统：安全：ITS通信安全架构和安全管理》，ETSI TS 102 941《智能交通系统（ITS）：安全：可信和隐私管理》，YD/T 3594-2019《基于LTE网络的车联网通信安全总体技术要求》等标准。C-V2X车联网安全借鉴了国际标准的内容并结合我国车联网安全需求提出了安全证书管理标准。

附录 C 术语定义

1、5G

第五代移动通信技术。

2、NFV

网络功能虚拟化。

3、SDN

软件定义网络。

4、边缘计算

将数据和任务在靠近数据源头的网络边缘侧进行计算和执行的一种新型服务模型。

5、供应链

通过多个资源和过程联系在一起的一系列组织，根据由服务协议或其他采购协议建立连续的供应关系，每个组织充当一个需求方、提供方或双重角色。

6、固件

存储在加密边界硬件中的加密模块的可执行代码，在不可修改或受限操作环境中运行时，不能被动态写入或修改。

7、设备

具有特定用途的机械、电气或电子装置。

8、网络切片

提供特定网络功能和网络特性的逻辑网络。

9、移动智能终端

能够接入移动通信网，提供应用软件开发接口，并能够安装和运行应用软件的移动终端。

10、应急响应

组织为了应对突发/重大信息安全事件的发生所做的准备，以及在事件发生后所采取的措施。

11、应急预案

一种关于备份、应急响应和灾后恢复的计划。

12、云计算平台

云服务商提供的云计算基础设施及其上的服务软件的集合。