全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

TC260-TR-002-2026

# 网络安全标准化技术研究报告
## ——6G 网络内生及边界安全技术与标准化研究

v1.0-202603

全国网络安全标准化技术委员会秘书处

全国网络安全标准化技术委员会通信安全标准工作组（WG6）

2026 年 3 月

本文档可从以下网址获得：
www.tc260.org.cn/

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

# 前　言

《网络安全标准化技术研究报告》（以下简称《技术报告》）是全国网络安全标准化技术委员会（以下简称“网安标委”）秘书处组织编制和发布的技术研究类文件。本文件立足新技术新应用领域网络安全前沿动态，通过系统的技术研究、产业调研、标准分析与综合研判，梳理关键领域网络安全风险与挑战，提出标准化发展趋势及相关工作实施建议，为网络安全国家标准制修订与网络安全保障实施提供前瞻性的技术参考与决策支撑。

# 声　明

本《技术报告》版权属于网安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译《技术报告》的任何部分。凡转载或引用本《技术报告》的观点、数据，请注明“来源：全国网络安全标准化技术委员会秘书处”。

# 技术支持单位

本《技术报告》得到中国移动通信集团有限公司网络与信息安全管理部、中国移动通信集团有限公司研究院、中国信息通信研究院、中兴通讯股份有限公司、国家互联网应急中心、中国科学院科技战略咨询研究院等单位的技术支持。

主要编写人员：邱勤、袁璐、赵刚、粟栗、杜海涛、刘畅、白杰、卢丹、马泽龙、王意军、卢帆、周继华、陈悦、肖冰、李加莲。

# 目 录

# 摘　要

随着全球数字化进程加快，第六代移动通信技术（6G）作为下一代通信系统的核心驱动力，正加速向“泛在连接、智能内生、空天地一体”的目标演进。与 5G 相比，6G 不仅将实现更高的传输速率、更低的时延和更广的连接密度，还将以全面 IT 化、服务柔性化和智能化为基础，推动网络架构从集中式、垂直化向多域协同、分布自治转变，构建真正意义上的“网络-计算-感知”一体化通信体系。在 6G 场景下，空地融合通信、边缘智能协同、算网融合能力将广泛部署，网络节点呈现出异构分布、功能柔性、状态动态的特点。这一趋势虽然极大拓展了 6G 的服务能力和业务空间，但也带来了前所未有的安全挑战。

首先，网络架构的深度开放使得传统“外围部署安全模块”式的防护理念难以适应 6G 网络的动态组网模式与多样化接入方式。网络暴露面显著扩大，攻击路径更加多样，网络功能模块的细粒度开放也导致安全边界逐渐模糊，形成大量潜在风险点。其次，6G 网络中的安全需求不再局限于数据加密与身份验证，还包括服务可信、策略透明、节点可控等多维度的安全保障能力，安全能力必须实现“从源头生长、与系统共构”，即构建具有“原生安全能力”的网络架构，即“内生安全”。

同时，在 6G 所构建的空天地一体、算网融合网络环境中，异构网络边界频繁切换，业务动态迁移，设备、平台、网络多样化协同运

行，身份认证、资源隔离、信任建立等问题面临重重挑战。传统集中化的访问控制和边界防护机制，难以满足多域、跨网、异构环境下的安全需求。建立智能动态、可信可控的边界防护体系，构建统一、灵活的分布式信任架构和访问控制机制，是保障 6G 网络安全稳定运行的关键。

为促进 6G 与相关产业的健康安全发展，切实发挥标准在网络安全中的基础性、规范性、引领性作用，有必要体系化推进面向 6G 的标准化研究。与 5G 以“外挂式”为主的安全模式不同，6G 安全正朝着“内生融合”与“智能协同”方向演进，安全能力将作为原生要素深度嵌入网络架构底层。在此背景下，本报告聚焦 6G 网络架构中“内生安全体系构建”与“异构网络边界防护”两大核心方向，重点分析从 5G 到 6G 演进过程中所面临的新型安全挑战。前者强调安全机制与网络功能的一体化设计，实现自我免疫与持续演进的安全内生能力；后者针对 6G 空天地海异构融合、边界动态模糊所带来的新型接入风险，构建跨域可信、弹性自适应的智能防护体系。报告系统分析了两类方向下的威胁形态、技术路径与标准需求，评估了国内外相关标准化进展与差距，并提出适用于 6G 场景的标准化实施建议，为我国构建自主可控、安全可信的 6G 网络基础设施提供技术支撑与标准依据。

# 一. 6G 网络发展现状

## （一）6G 网络架构

面向 6G 网络体系演进，全球产业界与标准组织围绕新型网络架构持续开展前瞻探索，形成了多种具有代表性的架构设计方案。这些方案普遍体现出“跨域融合、算网一体、智能内生、安全可信”的发展趋势，从资源组织方式、功能分层到能力开放路径等方面，为 6G 网络构建提供了系统性参考。

### 1. 中国移动提出“三体四层五面”6G 网络架构

中国移动在 2022 年提出“三体四层五面”的 6G 网络架构，认为 6G 网络将秉承兼容、跨域、分布、内生、至简、孪生六大设计理念进行架构设计，从空间、逻辑与功能组成三个角度呈现跨域、跨层、多维的 6G 网络。


图 1 中国移动提出的“三体四层五面”的 6G 网络架构

如图 1 所示，6G 网络在空间视图上包括网络本体、管理编排体、数字孪生体三大实体。网络本体是最重要的网络实体，实现网络功能和网络运行；管理编排体对网络进行实例化及变更操作，实现全生命

周期编排管理；数字孪生体构建了网络的数字空间，实现了虚实映射。6G 网络逻辑层次上自下而上包含资源与算力、路由与连接、服务化功能、开放使能“四层”，一方面突出了 6G 架构在分层要素和能力上的丰富，另一方面体现了跨域拉通、多域协同及融合发展的理念。6G 网络功能构成方面，增强传统控制面、用户面功能，并引入新的数据面、智能面、安全面，共同组成“五面”。

## 2. IMT-2030（6G）推进组提出的 6G 网络架构

如图 2 所示，IMT-2030（6G）推进组在 2023 年提出 6G 网络系统架构分为基础设施资源层、网络功能层、应用与开放层，以及贯穿各层级的安全可信和管理与编排功能，认为 6G 网络将成为一个开放创新和提供信息服务的平台，具备超越连接的服务能力。

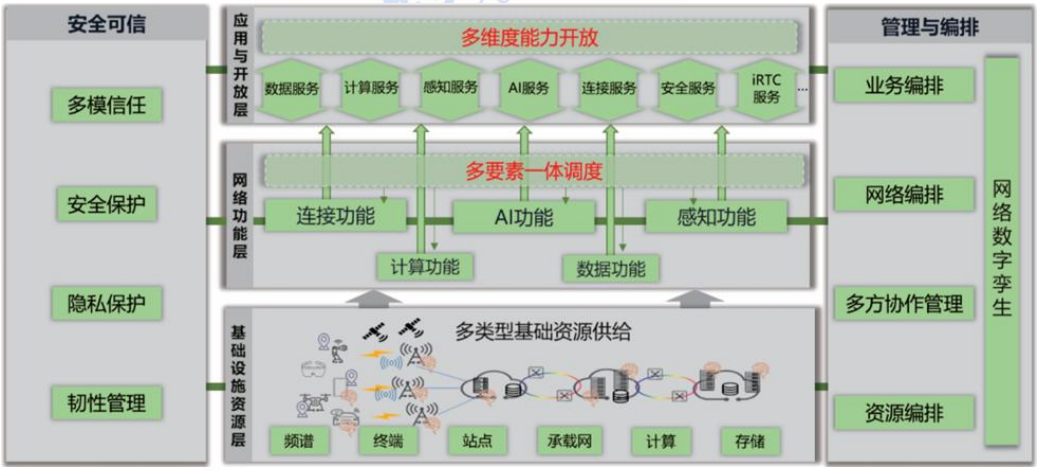



图 2 IMT-2030（6G）推进组提出的 6G 网络架构

基础设施资源层提供频谱、终端、站点、传输、计算以及存储等多类型的基础资源，涵盖空天地多种方式接入，端管网云融合的服务设施。网络功能层提供连接功能、AI 功能、感知功能、计算功能和数据功能，以满足 6G 新增业务在速率、带宽、时延、可靠性等关键

指标上的提升需求，并支撑 AI、沉浸式应用、通感一体等新型业务需求。应用使能与开放层构建于网络功能层之上，在传统能力开放的基础上扩展丰富内涵和外延，以聚合各种应用使能功能，同时提供更加灵活的、自动化的、实时的信息交互能力。安全可信方面，需充分考虑安全、隐私、韧性三方面，将可信内嵌在系统中，通过系统设计保障整个网络的可信能力。此外，面向业务的多样性、复杂性，网络资源的动态性、异构性，需要通过网络 AI 管理和编排技术进行统一、动态的编排调度，提高网络/计算的执行效率，提升用户体验。

### 3. 未来移动通信论坛（FuTURE 论坛）提出的 6G 网络架构

未来移动通信论坛在 2024 年提出 6G 网络架构，包括网络资源和基础设施层、网络功能层、服务与能力开放层、管理编排、内生赋能，如图 3 所示。

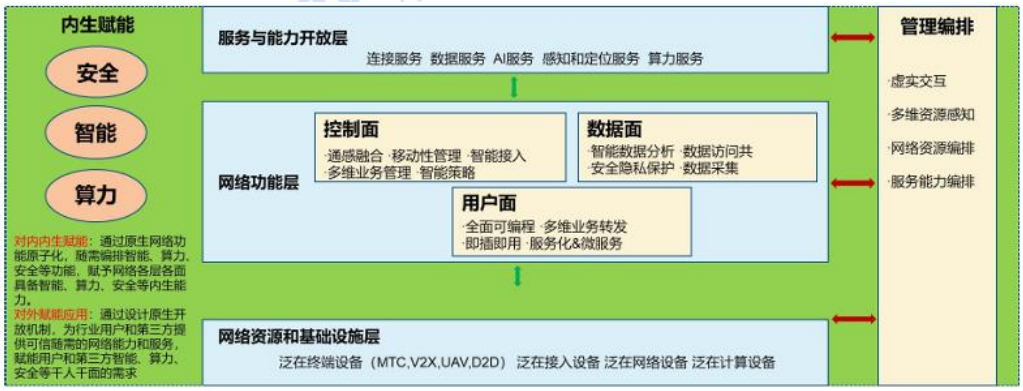



图 3 未来移动通信论坛（FuTURE 论坛）提出的 6G 网络架构

网络资源和基础设施层为网络功能层的功能生成提供相应基础设施和多维资源，涵盖泛在的无线、计算、存储、网络等多维资源，包括统一虚拟化的虚拟资源、可抽象的物理资源和专用的高性能硬件资源。网络功能层将动态分布式的资源互联，通过对多维资源的统一

协同调度，为服务与能力开放层提供通感算智数安等网络功能。服务与能力开放层对下层的网络功能进行提取、封装和组合，为网络内部业务或外部应用按需提供可以开放的能力或服务。编排管理通过对用户意图、业务需求的智能感知，实现跨多业务、多领域、全生命周期的智能协同编排和意图策略动态调度，实现异构环境下业务质量的闭环保证。内生赋能在网络内部实现内生能力全生命周期管理和内生能力多要素的按需调度，构建随需取用、灵活高效的内生能力资源池。

**（二）6G 网络应用场景**

6G 网络将在 5G 三大典型场景——增强移动宽带（eMBB）、海量物联网连接（mMTC）、超可靠低时延通信（URLLC）的基础上加以延续并进一步深化，以更高速率、更低时延、更广连接为核心目标，打造一个智能、泛在、可信的通信网络。同时，6G 还将深度融合人工智能、量子通信、卫星通信、感知技术等新兴技术，催生一系列前所未有的创新应用。

根据国际电信联盟（ITU）2023 年 11 月发布的《Framework and overall objectives of the future development of IMT for 2030 and beyond（IMT-2030）》，6G 网络规划了六大典型应用场景：沉浸式通信、极高可靠低时延通信、超大规模通信、泛在连接、通信感知一体化与通信智能一体化，以及适用于所有场景的四大设计原则，即：可持续性、泛在智能、安全/隐私/弹性、连接未连接的用户，如图 4 所示。

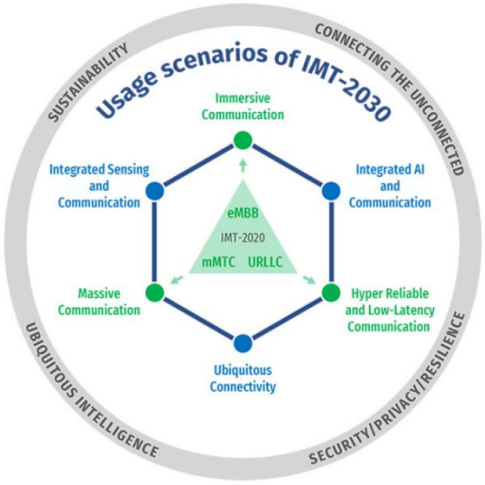



图 4 IMT-2030 六大场景和四大原则

1. 沉浸式通信

面向虚实融合交互需求，沉浸式通信以 XR、全息通信和多感官传输为代表，提供视觉、听觉乃至触觉等多维一体的交互体验。其核心依赖超高带宽、毫秒级低时延及算网协同能力，支撑远程教育、医疗、工业等场景，实现跨时空的“身临其境”通信体验。

2. 超大规模连接

在 5G mMTC 基础上进一步扩展，支撑海量异构终端接入与多样化业务需求，广泛应用于智慧城市、工业物联网等领域。该场景呈现设备数量巨大、业务差异显著、通信特征多样等特点，对网络的灵活调度、能效管理和智能感知能力提出更高要求。

3. 超高可靠低时延通信

面向工业控制、自动驾驶、远程医疗等关键业务，提供极低时延与极高可靠性的通信保障，并兼顾抖动控制与时间同步等确定性指标。支撑人机物深度协同与实时控制，推动生产系统由局域封闭向广域开放演进，提升系统安全性与运行效率。

4. 泛在连接

依托空天地海一体化网络，实现全域、全时、全场景的无缝连接能力，覆盖城市、海洋、空中及偏远区域。通过多层次接入方式，满足从低功耗物联设备到高带宽业务的差异化需求，为万物互联提供基础通信支撑。

5. 通信智能一体化

将通信与人工智能深度融合，为分布式学习与推理提供一体化支撑，同时赋能网络自身智能化运行。通过调度边缘与终端算力，实现高效模型训练与实时决策，广泛应用于数字孪生、智能制造等场景，提升系统整体效率与服务能力。

6. 通信感知一体化

融合通信与感知能力，实现定位、识别、成像与环境重构等功能一体化，支持高精度空间感知与智能决策。可广泛应用于车联网、工业监测等场景，同时通过感知信息反哺通信过程，提升网络资源利用效率与服务质量。

3GPP 于 2026 年发布的《6G 场景用例与业务需求》标准研究项目中根据 ITU 前期制定的框架，系统识别并分析了 212 个典型场景用例，定义了“AI 服务能力”、“数据服务能力”、“算力服务能力”三大重要服务。

## （三）6G 关键特性

### 1. 沉浸多感与极致通信

6G 面向沉浸式交互与智能协同需求，融合沉浸式通信与超高可靠低时延通信能力，构建沉浸多感网络，支撑云化 XR、全息通信及远程多感官交互等新型业务形态，实现视觉、听觉、触觉等多维信息的实时协同与三维呈现，广泛应用于医疗、教育、工业控制及人机交互等场景。该类业务对网络提出超高带宽、毫秒级时延、超高可靠性及高精度同步等综合性能要求。在安全方面，多模态感知数据的传输显著增加隐私泄露与行为反演风险，同时超低时延约束对传统加密机制形成挑战，需发展轻量化、低时延安全防护技术，并提升多维数据传输过程中的安全保障能力。

### 2. 泛在连接与空天地一体化网络

6G 以泛在连接为核心目标，依托空天地海一体化组网，实现地面、空中、海洋及偏远区域的全域覆盖，支撑人—机—物的无缝连接。同时，网络从 5G mMTC 向超大规模连接演进，连接对象呈现海量化与多样化特征，涵盖智慧城市、智能制造、数字孪生等场景，设备在速率、时延、功耗及通信频次等方面差异显著。该类融合网络在提升覆盖能力的同时，也带来显著安全挑战：一方面，多接入链路使网络边界进一步模糊，攻击路径更加多样，节点伪装、链路劫持等风险上升；另一方面，跨域异构网络间信任体系不统一，易形成安全薄弱环节。此外，卫星及空基节点资源受限，传统安全机制适配困难，需构建统

一高效的跨域安全防护体系。

### 3. 通信感知一体化

6G 推动通信与感知深度融合，使网络从“连接能力”向“感知与认知能力”演进，通过复用频谱与硬件资源，实现高精度定位、环境重构、目标识别等能力，广泛应用于车联网、智能工厂及数字孪生等场景。同时，超大规模连接为物理世界实时映射提供数据基础，支撑虚实融合与智能决策。在安全方面，通感融合带来的高精度感知能力，使用户位置、行为及环境信息面临更高的隐私泄露与推理攻击风险。同时，多类型节点协同参与感知与计算，现有信任机制难以支撑跨域、多主体环境下的统一信任管理与动态验证，亟需完善跨层级安全与隐私保护机制。

### 4. 通信智能一体化

6G 以通信智能一体化为关键特征，推动网络具备自感知、自决策、自优化能力，通过融合连接、算力与数据资源，支撑分布式智能训练与推理，广泛应用于智能制造、自动驾驶及智慧城市等场景，同时实现网络运行效率与服务能力的整体提升。在安全方面，网络智能化显著扩大攻击面，开放接口与数据流增加潜在入侵路径，攻击者可利用智能决策链路实施深度渗透。同时，网络运行形态动态变化，传统静态防护机制难以适应，亟需提升安全态势感知、动态防护及协同响应能力。需要说明的是，AI 模型本身的安全问题属于人工智能安全范畴，不在本报告的研究范围内。

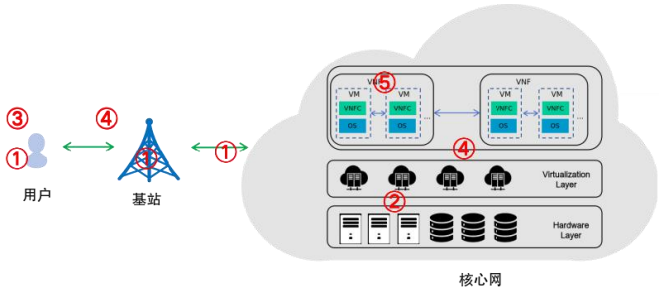
## （四）6G 网络内生及边界安全关键技术

### 1. 6G 网络内生安全

随着 6G 网络与人工智能的深度融合，网络安全正从传统以边界防护和被动响应为主的模式，向主动感知、自主决策和智能响应方向演进。6G 网络具备对网络运行数据、用户行为、业务特征以及安全威胁信息的持续感知和智能学习能力，为实现更高层次的通信安全保障提供了技术基础。6G 网络安全建设亟需从依赖外部防护的传统模式，向“内生安全”理念转型。

内生安全的目标，是将安全根植于 6G 网络并与网络共生，使网络在运行过程中具备自我保护、自我修复和自我适应能力，系统性提升 6G 网络的整体安全性和可靠性。内生安全作为基础能力嵌入于 6G 网络各层级与关键功能单元之中，贯穿终端侧、接入网、传输网、核心网以及算力与数据平面等关键环节，并与网络功能模块深度耦合，形成“默认安全”的体系化能力布局。

6G 内生安全将围绕抗量子安全、可信计算、无线空口安全增强、隐私保护增强以及虚拟化安全等关键技术方向展开，如图 5 所示。这些技术具有显著的“原生性”和“融合性”，属于网络设计与生俱来的安全基因，能够推动安全能力由静态配置向动态免疫演进，实现安全与网络业务的“同生共长”，体现“安全融于架构、安全嵌入流程、安全贯穿全生命周期”的设计理念，是 6G 内生安全体系的核心支撑。




① 抗量子安全 ② 可信计算 ③ 无线空口安全增强 ④ 隐私保护增强 ⑤ 虚拟化安全

图 5 6G 网络内生安全覆盖范围及关键技术方向

(1) 抗量子安全

抗量子安全是指采用不依赖大整数分解、离散对数等传统数学难题的密码体系，以应对量子计算对现有加密机制的破解能力。5G 网络主要依赖 RSA、椭圆曲线密码（ECC）等非对称算法，其安全性在量子计算条件下将被削弱甚至失效，且现有标准缺乏系统性抗量子设计与密钥演进机制，存在体系性风险。面向 6G，需在架构设计阶段引入抗量子公钥密码（PQC），实现认证、密钥交换与签名体系的全面升级；同时增强对称加密强度与密钥协商能力。在高安全场景下，可结合量子密钥分发（QKD）等物理层技术，构建“算法安全+物理安全”协同的多层防护体系，保障未来网络长期安全性。

(2) 可信计算技术

可信计算通过构建硬件信任根和完整性度量机制，实现从系统启动到运行过程的可信验证，确保设备与软件行为可控可溯。5G 阶段主要在核心网与设备侧开展应用，依赖 TPM/TPCM 等实现单节点可信，但存在性能开销较大、接口标准不统一、跨域协同能力不足等问题，整体仍停留在“单点可信”。面向 6G 网络云-边-端深度融合与动态

协同的特征，可信计算需向体系化演进，构建统一可信框架，支持多级信任根、远程度量与动态验证机制，实现跨平台、跨域信任协同。

(3) 无线空口安全增强技术

无线空口安全通过利用无线信道的随机性与空间特性，在物理层与链路层实现轻量化安全防护，是对传统加密机制的重要补充。5G 安全主要集中在 PDCP 等高层协议，物理层及控制信令保护相对不足，仍存在伪基站、信令劫持等风险。面向 6G，需构建跨层安全防护体系，在物理层引入信道特征建模与动态密钥生成机制，实现低时延密钥保护；结合射频指纹、信道指纹等实现终端快速认证；在 MAC 层加强控制信令的机密性与完整性保护。通过“物理安全+协议安全”协同，提升在高频段、大规模天线及高动态场景下的空口安全能力。

(4) 隐私保护增强技术

隐私保护技术旨在防止用户身份、行为轨迹及数据内容在通信与计算过程中的泄露。5G 通过加密 IMSI 提升了空口隐私保护，但临时标识符之间仍存在关联性，易被跟踪分析，且缺乏跨层、跨域的系统性隐私保护机制。在 AI 应用场景中，数据与模型亦面临推理攻击与信息泄露风险。在 6G 网络中，隐私保护将从“单点匿名”向“全生命周期保护”演进，覆盖数据生成、传输、存储与使用全过程。核心技术包括安全多方计算（MPC）与同态加密（HE），实现“数据可用不可见”；同时引入分级隐私凭证与动态授权机制，结合分布式身份管理，支撑跨域环境下的可控共享与可追溯访问，提升隐私保护能力。

(5) 虚拟化安全技术

虚拟化安全通过隔离与访问控制机制保障多租户环境下的资源与业务安全。5G 及传统网络主要依赖 VLAN、VXLAN 等实现逻辑隔离，但在动态拓扑与高密度部署场景下，静态划分难以及时适配，易产生横向渗透风险。6G 网络的虚拟化程度将进一步提升，需引入基于身份与上下文的动态安全策略，实现细粒度访问控制与按需通信管理，核心理念为“默认拒绝、按需放行”，并与身份与访问管理（IAM）深度融合，构建“以身份为边界”的安全模型，支撑网络切片与跨域服务的安全隔离与可信互通。

**2. 异构网络边界安全**

在 6G 时代，空天地一体化网络融合地面、卫星及空中节点，形成高度异构、动态自组织的通信体系，在实现全球无缝连接的同时，使传统“固定边界”安全模式难以适用。随着跨域协同增强与链路开放，网络边界由清晰走向模糊，暴露面显著扩大，易引发身份伪装、信号劫持及跨域滥用等风险，且在天基与边缘环境中进一步放大，亟需构建适配动态、多域环境的新型边界安全体系。

如图 6 所示，6G 异构网络边界安全，是指面向多网络、多接入及多场景融合环境，基于内生安全理念，通过跨域协同与动态防护机制，构建覆盖物理与逻辑边界的系统性防护体系，实现对接入、传输及业务交互全过程的可信管控。边界安全主要部署于不同网络域之间及关键交互接口位置，包括空天地一体化接入边界、异构网络融合边

界、运营商间互联互通边界，以及网络与算力平台、数据中心和外部业务系统之间的接口边界等关键节点，围绕跨域连接与资源交互过程，承担访问控制、流量检测、异常识别与策略执行等安全职责。

边界安全的研究重点包括分布式信任、统一身份与访问控制，以及多协议环境下的边界防护与策略执行能力，核心解决“边界界定、接入控制与动态防护”问题。

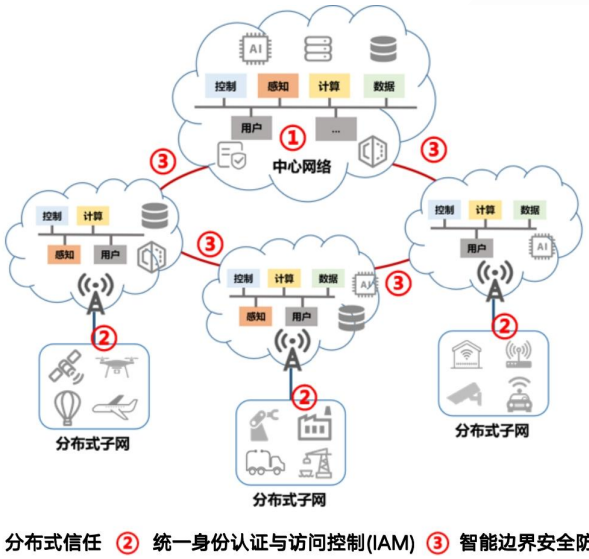



图 6 6G 异构网络边界安全覆盖范围及关键技术方向

(1) 分布式信任技术

分布式信任技术以区块链为核心，通过去中心化账本与密码机制，实现数据不可篡改与可追溯，支撑多主体间的可信协同。5G 阶段主要依赖中心化 CA 及层级信任体系，存在单点失效、跨域扩展性差等问题，难以适应 6G 空天地一体化及多域协同场景。面向 6G，需引入区块链等分布式机制，结合 P2P 网络、共识算法及智能合约，构建跨域可信基础；同时发展分布式公钥基础设施（DPKI），替代集中式证书体系，实现多方协同认证。在用户与设备侧，引入去中心化身

份（DID）等机制，实现身份自主管理与可信验证，支撑跨网络、跨域环境下的统一信任协同。

(2)统一身份认证与访问控制（IAM）

IAM通过身份识别与权限管理,实现对网络资源访问的安全控制。5G主要采用运营商集中认证与基于边界的访问策略，难以适应6G多主体、多接入及动态拓扑环境，存在跨域访问不一致与身份碎片化问题。面向6G，IAM需向零信任架构演进，构建“持续认证、动态授权”的访问控制体系。通过融合多因素认证、行为感知访问控制及策略驱动模型，基于设备、位置、行为等上下文信息进行实时风险评估与权限调整。同时，引入DID与可验证凭证（VC）增强身份自主性与隐私保护，支撑跨域、跨平台的统一身份管理与精细化访问控制。

(3)智能边界安全防护

智能边界安全防护通过对网络边界流量与行为的实时分析与策略控制，实现对跨域访问与攻击行为的动态防御。5G阶段安全主要集中于核心网与高层协议，物理层及边界防护能力不足，难以应对跨域攻击与横向渗透。面向6G，随着网络边界动态化与分布式演进，需构建智能化边界防护体系。以新一代防火墙（NGFW）和安全网关为核心，融合身份识别、应用解析及加密流量检测能力，实现细粒度策略控制；结合入侵检测/防御（IDS/IPS）技术，对流量进行实时监测与威胁识别，提升对DDoS、恶意信令等攻击的防护能力，支撑空天地融合及边缘场景下的高效安全保障。

# 二. 6G 网络安全相关政策与标准分析

## （一）6G 网络安全法规和政策

### 1. 国外法规和政策

新型网络安全问题成为 6G 发展的核心挑战，各国纷纷出台政策和标准规划以应对未来的安全需求。

(1) 美国

美国系统布局 6G 内生安全与边界防护技术，并通过国际合作争夺 6G 安全主导权。2022 年 1 月，美国电信行业解决方案联盟(ATIS)组建的 Next G 联盟发布了其首份 6G 报告，即《6G 路线图：构建北美 6G 领导力基础》。报告从 AI 原生安全、物理层加密、分布式架构、动态拓扑防护、通信和传感（JCS）安全及零信任机制等维度，阐述了 6G 内生安全与边界防护的技术路径。2022 年 6 月，美国国家科学基金会等启动“弹性和智能下一代系统项目”（RINGS），计划投资 4000 万美元支持网络边缘防护等 6G 关键领域基础研究。2024 年 1 月，美国 ATIS 与欧盟智能网络联合发布“超越 5G 和 6G 路线图”，强调 6G 网络应提供最高级别的可信度、安全性和弹性。2024 年 2 月，美国与澳大利亚、加拿大、捷克、芬兰、法国、日本、韩国、瑞典和英国等十国联合发布《6G 原则联合声明》，强调 6G 发展应基于“安全、有弹性、保护隐私”的原则，推动全球行业主导的包容性标准制定和国际合作。

(2) 欧盟

欧盟通过旗舰研究项目与产业协同，推动 6G 安全架构设计与关键技术验证。2021 年 1 月，欧盟启动 6G 安全旗舰项目 Hexa-X，提出“可信赖性”核心目标，研究 AI 驱动的安全架构和隐私计算技术，为 6G 内生安全奠定基础。2021 年 2 月，欧盟联合私营企业资助设立“智能网络和服务联合伙伴”项目，计划投资约 131 亿元人民币用于构建 6G 系统总体架构和验证平台，为 6G 标准化提供基础。2023 年 1 月，在 Hexa-X 的基础上，Hexa-X-II 项目于 2023 年启动，重点验证分布式身份认证、跨域信任链等边界防护技术，覆盖从芯片到服务的全栈安全。2025 年 1 月，欧盟“智能网络和服务联合伙伴”资助的 6G 安全研究关键项目 XTRUST-6G 启动，进一步强化零信任（ZT）架构，开发动态微隔离、持续认证等工具，应对空天地一体化网络的边界安全挑战。

(3) 日本

日本紧跟国际趋势，积极开展 6G 安全技术研发与合作。2020 年 6 月，日本总务省正式发布《Beyond 5G（即 6G）推进战略》，提出将在 2025 年逐渐完成基础技术研发、5G 必要专利全球占比达 10%以上、在 2030 年创造 44 万亿日元附加价值的战略目标。2022 年 3 月，日本 Beyond 5G 推进联盟发布自皮书《Message to the 2030s》，内容包括:流量趋势、电信行业的市场趋势、其他行业趋势、B5G 所需的能力和 KPI、B5G 技术趋势等。该白皮书指出，为了应对 B5G 用户

的多样化需求，不仅需要在功能和性能的技术创新方面取得进展，还需要提供一个所有利益相关方都可以安全使用(Safely and Securely)的可信赖网络基础设施，其中可信赖技术应该包括安全、隐私和网络空间弹性等三个方面。此外，日本还积极与美国、荷兰开展 6G 技术联合研发，Beyond 5G 推进联盟分别与北美 Next G 联盟和欧盟 6G 旗舰项目 Hexa-X 签署合作协议。

(4) 韩国

韩国政府高度重视 6G 技术的发展，将其列为 12 项国家战略目标技术之一，并发布多项战略推动 6G 商业化进程。2021 年 6 月，韩国公布“6G 研究开发实行计划”，包括 6G 核心自主技术研发、抢占专利和国际标准话语权、构建研发和产业基础三方面内容。其中，最重要的是推动 6G 安全技术等 10 项核心技术自主研发。2023 年 3 月，韩国启动 K-Network2030 计划。针对该计划，韩国推进一项约合 32.9 亿元人民币的 6G 研发项目，重点布局基础材料、关键器件、低轨卫星等产业基础攻关。2023 年 11 月，韩国发布 6G 研发推进战略，重点推进中高频段技术、扩大覆盖范围技术、以软件为中心的网络等关键技术领域。在技术研发方面，韩国的三星电子等企业在 6G 关键技术研究上投入了大量资源，在新型天线技术、通信芯片研发等方面取得了一定的成果，为韩国 6G 技术的发展提供了技术支持。

## 2. 国内法规和政策

近年来，我国通过顶层设计和专项政策，系统性推进 6G 技术研

发，并将网络内生安全和边界安全作为核心方向。相关政策不仅强调技术储备和国际合作，更明确要求构建自主可控的安全架构，强化与量子信息、AI 安全的协同。

2021 年 3 月，《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》中提出前瞻布局 6G 网络技术储备，要求核心技术研发需统筹安全与发展，为后续内生安全设计奠定基础。

2021 年 11 月，工业和信息化部印发《“十四五”信息通信行业发展规划》，深化 5G、6G、人工智能、物联网等领域标准、研发、投资和治理规则的国际交流合作。

2022 年 1 月国务院发布《“十四五”数字经济发展规划的通知》，强调加快建设信息网络基础设施，前瞻布局第六代移动通信（6G）网络技术储备，加大 6G 技术研发支持力度，积极参与推动 6G 国际标准化工作，明确 6G 需支持“空天地一体化”组网，并推动通感一体化场景下的信号级安全防护。

2023 年 6 月，工业和信息化部发布新版《中华人民共和国无线电频率划分规定》，将 6425MHz—7125MHz 共 700MHz 频谱全部或者部分划分用于 IMT（国际移动通信，含 5G-A/6G）应用。同时，工业和信息化部发布《关于微波通信系统频率使用规划调整及无线电管理有关事项的通知》，优化微波通信系统安全要求，为我国未来 6G 发展提供频谱资源保障。

2024 年 1 月，工信部等七部门印发《关于推动未来产业创新发展的实施意见》，提出 5G/6G、工业互联网、物联网、车联网等领域的数据安全需求分析，推动专用数据安全技术产品创新研发、融合应用。提出 6G 需结合数字孪生和 AI 驱动的主动防御技术，构建“动态防护、内生安全”框架，并推动数据可信流通。

2024 年 12 月，国家发展改革委、国家数据局、工业和信息化部发布《国家数据基础设施建设指引》要求 6G 网络与数据基础设施深度融合，通过 AI 编排技术实现安全策略的动态部署，构建高效弹性的数据传输网络。

2025 年 3 月，全国《政府工作报告》首次将 6G 技术纳入未来产业培育核心框架，明确其与生物制造、量子科技等并列的战略地位。3 月 12 日，工业和信息化部召开干部大会，强调要持续推动信息通信业高质量发展，扩大 5G 规模化应用，加快 6G 研发进程。

2025 年 10 月，中国共产党第二十届中央委员会第四次全体会议审议通过的《中共中央关于制定国民经济和社会发展第十五个五年规划的建议》中明确提出前瞻布局未来产业，推动量子科技、生物制造、氢能和核聚变能、脑机接口、具身智能、第六代移动通信等成为新的经济增长点。

## （二）6G 网络安全标准化现状

### 1. 国外标准化现状

在全球发展态势上，中国、美国、欧盟以及其他国家都在积极布

局 6G，通过战略规划、资金投入、技术研发等多种方式，力求在全球 6G 竞争中占据有利地位。国际标准制定工作也在有序推进，如图 7 所示，国际电信联盟（ITU）和第三代合作伙伴计划（3GPP）等国际组织发挥着关键作用，为 6G 技术的全球推广和产业发展奠定基础。

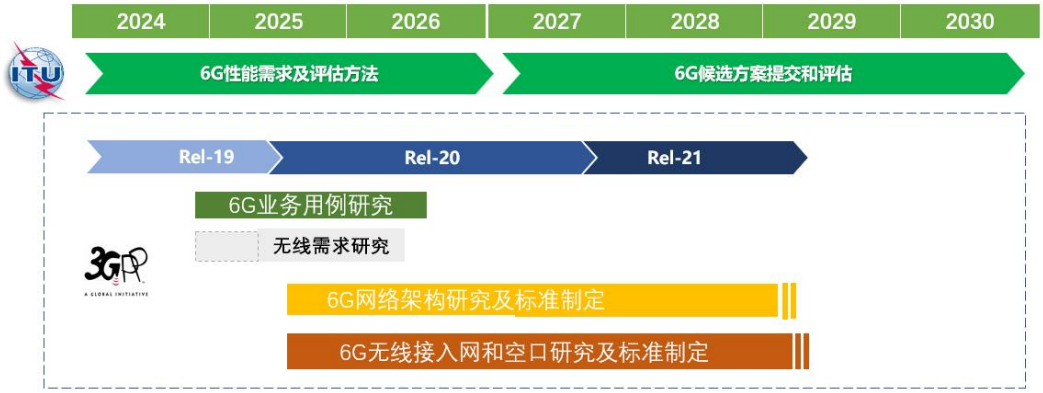



图 7 6G 标准化研究内容推进时间表

中国已成为 6G 安全国际标准化的重要引领力量。国内电信运营商、设备制造商以及高校与科研机构深度参与 ITU、3GPP、NGMN、GSMA 等主要国际标准组织，在 6G 安全架构、关键技术与治理机制等方面持续输出系统性主张。我国牵头或主导的技术提案已覆盖后量子密码、通感一体安全、AI 赋能安全、空口底层安全、认证授权、数据隐私与跨域信任等基础性与前沿领域，展现出从总体理念到关键机制的全链条技术布局能力，逐步形成在 6G 安全国际标准制定中的核心影响力。

(1) ITU

在 ITU 标准组织中，中国已成为 6G 安全国际标准化的重要牵头力量和规则塑造者。以中国移动为代表的国内运营商，联合设备商、高校与科研机构，持续在 6G 安全总体框架、关键技术路线和标准路

线图等方面发挥主导作用，推动 6G 安全从理念提出向体系化标准建设迈进。

2023 年 11 月，ITU-R（国际电信联盟无线电通讯部门）发布《IMT 面向 2030 及未来发展的框架和总体目标建议书》，将“安全、隐私、弹性”作为 6G 的设计原则和重要能力，并明确要求 6G 网络需具备原生 AI 防御、分布式信任机制和动态弹性架构等内生安全关键特性。此外，该文件特别指出，6G 需应对“边界模糊化”挑战，通过通感一体化信号加密和空天地跨域认证强化边界防护。

2024 年 9 月，中国移动成功主导完成 ITU-T（国际电信联盟标准化部门）首个 6G 安全研究项目《IMT-2030（6G）网络的安全考虑/Security Consideration for IMT-2030 Networks》立项，提出“主动免疫、弹性自治”的内生安全目标，并指出可通过 AI 驱动的威胁自愈和硬件级可信执行环境（TEE）实现网络原生防护。

2025 年 4 月，在 ITU-T SG17 全会上中国移动进一步主导完成了《面向 IMT-2030 的固定、移动、卫星网络融合安全》等 4 个国际标准/项目立项，面向 6G 场景中固定网络、移动网络和卫星网络融合场景的安全技术开展研究，为构建面向下一代移动通信网的天地一体化网络奠定安全基础。同期，中国移动专家成功担任新研究周期 Q6 网络业务安全组联合报告人、Q2 网络安全组副报告人职位，负责牵头制定《6G 安全标准路线图》。这是继 2024 年牵头 ITU 第一个 6G 安全研究项目之后，中国对 6G 安全标准布局的进一步深化，将引领通、

感、智、算、安等 6G 要素的安全标准体系建设。

围绕 6G“通、感、智、算、安”等关键要素，我国在 ITU 内分别牵头推进通感一体安全、智能体安全、物联网数据安全可验证技术、服务访问过程安全编排等项目，在跨域信任、网络能力与安全能力融合编排等方面形成一系列具有前瞻性的标准成果，持续推动 6G 安全关键议题形成国际共识。

(2) NGMN

在 NGMN（下一代移动网络联盟），我国运营商，特别是中国移动，在 6G 安全研究中发挥了核心牵头和共识凝聚作用。作为全球运营商主导的产业组织，NGMN 更强调从网络运营和产业协同视角对 6G 安全进行顶层思考，我国运营商在该组织中的持续主导，有效提升了我国在 6G 安全理念层面的国际影响力。

2023 年，NGMN 发布《6G 信任考虑》（6G Trustworthiness Considerations）白皮书。该白皮书由中国移动牵头完成，系统分析了 6G 在安全、隐私、韧性、可靠性以及公共安全等方面的核心需求与挑战，提出分布式信任基础设施、动态信任模型、智能安全协同、解耦式安全服务和客观信任评估等关键安全原则，为 6G 安全技术研究和标准化提供了重要参考框架。

2025 年，NGMN 发布《6G 网络架构演进》（Network Architecture Evolution towards 6G）白皮书，进一步将内生安全明确为 6G 网络架构设计的关键原则之一。我国运营商在该报告中持续推动将安全能

力作为网络原生属性纳入架构演进路径，强化了内生安全在全球运营商共识中的基础性地位。

(3) 3GPP

在 3GPP 体系内，我国运营商、设备商和研究机构长期保持高强度参与，是 6G 安全标准化的重要推动力量。3GPP 更侧重具体技术规范制定，我国企业在安全需求、技术方案和实现路径等方面的持续贡献，为 6G 安全从理念走向可落地规范提供了关键支撑。

2024 年 3 月，3GPP 在 CT、SA 和 RAN 的第 103 次全体会议上决定了 6G 标准化的时间表，如图 8 所示。

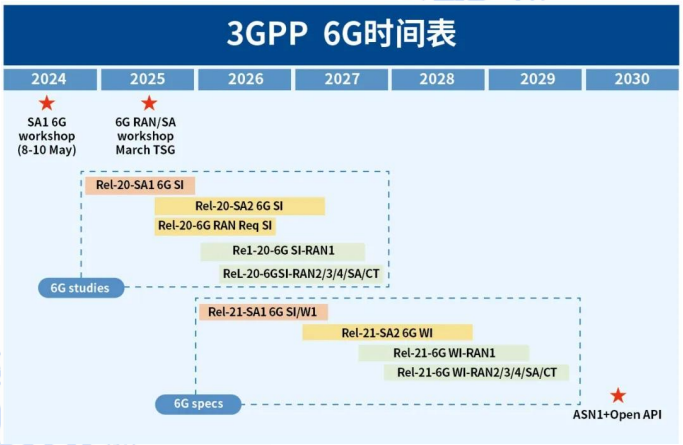



图 8 3GPP 6G 时间表

目前，3GPP 已于 2024 年启动《6G 场景用例与需求》等 6G 标准项目，逐步推进 6G 安全标准化工作。3GPP SA1 工作组已经开始了部分 6G 安全需求的讨论，并初步形成了抗量子、分布式信任、数字身份、隐私保护等相关需求。这是 6G 标准化进程中的一个重要里程碑，为后续的工作奠定了基础。

2025 年 3 月，3GPP 召开了 6G 专题研讨会（6G Workshop），来

自全球的通信企业与研究机构在会上介绍了各自对 6G 发展的愿景与技术规划。需要说明的是，当前 3GPP 的安全技术研究更多基于 5G-A（5G-Advanced）的技术分析和实践验证，尚未完全达到 6G 技术实现阶段，但这些研究成果体现了 6G 安全技术的演进趋势和发展方向。整体来看，6G 系统的安全设计从"被动防御"走向"主动内建"，聚焦于内生安全、异构网络边界防护安全等核心领域。

在内生安全与异构网络边界防护安全方向，3GPP 重点关注以下技术领域。

一是抗量子安全能力，面对未来量子计算的加密威胁，提出将抗量子加密算法（PQC）和量子密钥分发技术（QKD）嵌入 6G 体系架构，作为网络长期安全性保障的重要组成部分。

二是网络功能安全，保障 6G 网络中软件与硬件功能模块的完整性和可信性，随着网络功能的虚拟化和分布式部署，需构建从启动到运行的全流程验证机制，防止篡改、伪造与恶意植入，确保关键功能可信执行。

三是 MAC 层信令安全，加强物理层之上的控制信令保护，重点关注对 MAC 控制元素的认证与加密，防止未经授权的消息篡改。

四是隐私保护技术，使用隐私增强技术（PETs），引入数据最小化、同态加密、差分隐私等新技术手段，降低用户数据在传输、存储与处理过程中的泄露风险，建立跨域通用的统一用户同意框架，适用于感知、定位、AIML 等业务场景，明确用户数据的收集、使用、共

享与撤回流程。

五是安全能力的服务化与编排，强调将身份认证、防火墙、策略下发等安全能力通过安全即服务（SECaaS）方式按需提供，构建可编排、可演化的网络安全能力池，增强系统的内生免疫能力。

六是信任机制增强，提升网络内部与跨域之间的信任水平，尤其是在移动核心网（CN）与多云、边缘计算平台、漫游网络之间建立一致可信的身份和策略模型，实现不同运营商之间的动态互信。

七是零信任架构演进，6G 不再依赖固定边界上的信任，而是构建"身份即安全"的模型，通过持续验证、细粒度权限与动态策略控制，实现真正意义上的零信任防护。

八是接口安全，确保 6G 架构中包括大量异构系统之间的通信接口在内的所有接口具备完整性和保密性，防止信息在传输过程中的中间人攻击与篡改。

此外，3GPP 也关注 AI 安全与自主防御能力的研究。在 6G 系统中，AI 被用于资源调度、安全检测与行为识别，如何保障 AI 模型的完整性、防止训练数据被攻击，是确保安全自动化与智能化的前提。但如前所述，AI 技术本身的安全风险及其防护机制属于人工智能安全领域的专门研究方向，已有较为成熟的标准体系和研究框架，不在本报告的深入研究范围内。

在具体技术研究层面，我国企业积极参与抗量子安全、网络功能安全、MAC 层信令安全、隐私增强技术、安全能力服务化与编排、跨

域信任增强、零信任架构演进以及接口安全等方向的讨论，并推动相关研究成果逐步纳入 3GPP 安全研究框架。

电信运营商方面，中国移动在 3GPP 推进多项安全需求和技术方案详细设计，积极参与 3GPP SA1《6G 场景用例与需求研究》中已经采纳的七类 17 项安全需求讨论；中国电信和中国联通聚焦“固定、移动和卫星融合”安全，积极推进相应安全方案，中国联通关注算网安全，立项算网融合的安全需求和指引。

设备商方面，华为牵头后量子密码迁移研究课题，并在分布式信任及 AI 安全等重点方向持续深化投入；中兴着力推动无线空口 MAC 层控制单元（MAC CE）的安全增强研究；中信科则聚焦于数据面安全与空天地一体化安全等领域的技术布局与标准推进。

高校与科研机构方面，北京邮电大学、西安电子科技大学、紫金山实验室等也在积极关注 6G 安全标准化进程，结合自身研究优势开展 6G 安全关键技术攻关，为 6G 安全发展贡献中国方案。

2025 年 5 月份，3GPP SA3#122 次会议上，讨论了第一个 6G 安全相关的立项：《New SID on supporting AEAD algorithms》。未来，第一个 3GPP 6G 规范预计于 2028 年底在 Release 21 中完成。这意味着在大约四年的时间内，3GPP 将完成 6G 的核心规范制定工作，为 6G 技术的商用化铺平道路。

### 2. 国内标准化现状

中国主要电信运营商、设备商以及高校与科研机构等，依托

IMT-2030（6G）推进组等组织，积极参与 6G 安全体系架构及关键技术的研究，推进 6G 安全标准化进程。

（1）TC260

全国网络安全标准化技术委员会（TC260）归口管理了多项网络安全国家标准，这些标准为 6G 网络安全提供了基础的规范和技术支撑。例如，2025 年发布的 6 项国家标准，聚焦于数据安全、生成式人工智能安全等关键领域，为国家数据安全和人工智能安全的管理工作及产业发展提供标准支撑。由于 6G 网络涉及大量的数据处理和人工智能技术的应用，这些领域与 6G 网络安全密切相关。后续随着 6G 网络技术的逐渐成熟和应用场景的明确，TC260 将组织制定 6G 网络安全相关的国家标准，规范 6G 网络中的数据安全、设备安全、通信安全等方面的技术要求和管理规范，推动 6G 网络安全技术在产业中的应用，促进 6G 产业安全健康发展。

（2）CCSA

中国通信标准化协会（CCSA）当前已经开展 5G-A 安全、云化电信网内生安全架构及关键技术等研究，扎实地做好 5G 商用和 5G-Advanced 演进的同时，前瞻布局 6G 各项研究工作，为 6G 网络安全研究提供参考。

（3）IMT-2030（6G）推进组

IMT-2030（6G）推进组是中国为推动第六代移动通信技术（6G）的研究、标准化和产业化而成立的重要组织，由中国工业和信息化部

于 2019 年 6 月主导设立。该工作组汇聚了中国主要的运营商、设备制造商、高校和研究机构，旨在整合产学研用资源，加速 6G 关键技术研发，并参与全球 6G 标准制定和国际合作。

2021 年 9 月，中国移动牵头发布《6G 网络安全愿景技术研究报告》，提出了“主动免疫、弹性自治、虚拟共生、泛在协同”的 6G 网络安全愿景，并深入探讨了 6G 网络安全的关键技术和研究方向。

2023 年 12 月，IMT-2030（6G）推进组发布《6G 可信内生安全架构研究报告》，在 6G 安全愿景的基础上，向技术架构进一步深化，提出融合“信任+安全”的设计理念，从安全能力、安全控制和安全决策三个层次构建 6G 可信内生安全架构，并对支撑 6G 可信内生安全架构的无线物理层安全技术、泛在可信技术、区块链技术、数字孪生安全技术等关键技术进行了深入阐述。

2024 年 11 月，IMT-2030（6G）推进组发布《6G 天地一体化网络安全技术研究报告》，中国移动牵头编写，明确星间链路加密、动态拓扑防护等 12 项核心技术攻关方向。11 月还发布《6G 通信感知一体化安全需求与技术研究报告》，系统梳理了通感融合场景下的安全挑战与关键技术。

2025 年 11 月，中国移动牵头在 IMT-2030（6G）推进组发布《6G 安全面技术研究报告》，提出 6G 安全设计需打破传统模式，聚焦系统性、高交互、低耦合三大目标，通过分层协同的“能力-编排-决策”安全防护能力框架实现安全能力整体提升，同时实现与 AI、数字孪

生、数据功能等关键网络功能的高效交互与能力协同。

除依托 IMT-2030（6G）推进组、CCSA 和 TC260 等三大组织开展系统性研究与标准布局外，我国电信运营商、设备制造商以及高校与科研机构还通过发布技术白皮书、研究报告等方式，围绕 6G 安全愿景、体系架构和关键技术持续开展前瞻性研究，逐步形成多层次、多视角的 6G 安全研究成果，为后续标准化工作提供了重要的技术储备和思想基础。

在电信运营商方面，中国移动在 FuTURE 论坛牵头发布《6G 安全潜在关键技术白皮书》，系统梳理 6G 网络面临的主要安全挑战与关键技术方向，为业界开展 6G 安全研究提供总体参考。中国电信在《6G 愿景与技术白皮书》中提出，6G 安全应具备安全原生、可扩展架构以及差异化、动态自适应和智能协同等能力。中国联通在《6G 网络体系架构白皮书》中强调，6G 安全应采用自底向上、端到端构建的内生安全可编排架构，从安全启动、通信建立和多方信任等方面实现覆盖网络全生命周期的安全防护。

在设备商方面，华为在《6G 网络内生安全架构及技术白皮书》中提出面向 6G 的内生安全架构，通过可信引擎和可信使能单元承载安全能力，支持安全能力的持续演进与灵活编排，实现安全与网络架构的深度融合。中兴通讯在《2030+网络内生安全愿景白皮书》中提出统一的网络内生安全定义，并规划由基础建设向自适应和自塑阶段演进的发展路径。中信科在《全域覆盖 场景智联——6G 场景、能力

与技术引擎白皮书》中指出，6G 网络需应对更高的隐私保护、动态认证授权和智能化安全管理需求，并提出通过分布式信任、可信计算和量子安全等技术增强网络安全能力。

在高校与科研机构方面，北京邮电大学提出 6G 安全应贯穿网络各层次，通过统一信任框架融合区块链、人工智能等关键技术，构建动态可信机制。西安电子科技大学认为 6G 安全新需求集中在隐私保护和内生安全方向，关键技术包括物理层安全和后量子密码学。紫金山实验室从体系角度提出 6G 内生安全可信体系，应跨层构建通信安全、网络弹性和隐私保护等能力，实现安全属性的可感知、可度量和可演进。

# 三. 6G 网络安全风险与标准化需求

## （一）内生安全

### 1. 安全风险

随着 6G 网络向高度云化、智能化、泛在化演进，网络架构、运行模式和服务形态均发生根本变化，传统以外挂式安全为主的防护体系面临适应性瓶颈，安全能力需从网络“外围附加”向“内核内生”转变。

- 攻击暴露面显著扩大：相较 5G 仅仅实现核心网服务化，6G 实现全网 IT 化与微服务化，服务能力向接入网、边缘及终端延伸，形成跨域开放接口体系。攻击路径由“点状突破”演变为“网状扩散”，攻击者可利用服务调用链实现横向渗透与深度控制。同时，5G 对物理层与控制信令保护不足，6G 引入太赫兹、智能反射面等技术后，伪基站、波束劫持等攻击更隐蔽，传统上层防护难以应对。
- 抗量子能力不足：5G 依赖 RSA、ECC 等传统公钥算法，在量子计算条件下将被快速破解，核心安全机制面临失效风险，并存在“收割后解密”威胁。当前体系缺乏抗量子设计与密钥演进机制。6G 需提前引入抗量子密码体系与快速密钥更新能力，但现阶段整体防护基础仍较薄弱。
- 可信计算适配不足与动态信任支撑能力缺失：5G 可信计算主要基于 TPM/TPCM 实现单节点静态可信，适用于集中部署环境。6G

面向空天地一体化与泛在计算，节点异构、动态变化，现有机制在功耗、性能及灵活性上难以适配边缘与终端场景，且缺乏对动态接入与业务迁移的实时信任支撑，难以满足端-边-云协同需求。

- 隐私泄露与推理攻击风险上升：5G 虽对 IMSI 加密，但标识符关联与跨层隐私保护不足。6G 中，通感融合与 AI 原生架构使高精度位置、行为及生物特征数据广泛流动，隐私暴露面显著扩大。攻击者可通过模型推理、数据关联等方式还原用户信息，而现有机制难以实现数据“可用不可见”与用途可控。
- 虚拟化资源滥用与隔离风险增强：5G 虚拟化主要基于虚拟机与静态隔离，应用范围有限。6G 全面云原生化，容器与微服务大规模部署，资源调度与网络切片高度动态，传统隔离机制难以适配。容器共享内核带来更高逃逸风险，多租户混合部署下，一旦被突破，易引发横向扩散与系统性失控。

**2. 标准化需求**

内生安全架构标准：制定“信任-安全融合”的一体化安全架构标准，将身份认证、信任根验证、访问控制、行为监测等机制深度嵌入网络基础设施与协议层，推动安全能力由“外挂式”向“内生式”演进。

- 抗量子安全标准：面向 6G 空天地一体化组网、海量异构终端接入等场景，构建量子安全能力与 6G 网络架构深度融合的标准体系。完善空天地一体化场景下的抗量子算法选型与适配标准，明

确不同节点的算法适配规则。

- 可信计算技术标准：面向 6G 的泛在智能接入、边缘协同和动态组网需求，构建统一的可信计算框架标准体系。补充适配边缘节点虚拟化、轻量终端、异构设备的可信根定义与远程度量机制，强化设备侧原生安全能力，支撑端-边-云间多主体可信协同，构建统一可信执行体系。
- 无线空口安全增强标准：面向 6G 高速率、低时延与空天地一体化通信场景，完善无线物理层安全相关标准。规范物理层密钥生成与信道特征建模机制，完善太赫兹通信与智能反射面（RIS）环境下的物理层认证与抗干扰技术标准，补充 MAC 层控制信令的机密性、完整性与重放保护要求。
- 隐私保护增强标准：补充安全多方计算（MPC）、同态加密（HE）等隐私计算接口规范与性能要求，明确跨域协同计算、隐私凭证管理及分级隐私授权机制。完善多层次隐私保护框架，定义数据生成、传输、共享、销毁环节的安全控制指标，推动用户身份与数据使用权限的自主可控，形成“可用不可见、可信可验证”的隐私计算标准体系。
- 虚拟化安全标准：补充虚拟机与容器的可信隔离机制、动态微隔离策略与上下文感知安全控制要求，定义虚拟化资源度量接口与可信执行环境（TEE）集成规范。推动基于身份与策略的访问控制模型，实现资源层与通信层的联合防护，构建按需可编排可验

证的虚拟化安全防御框架，支撑 6G 云原生网络的安全弹性运行。

## （二）异构网络边界防护安全

### 1. 安全风险

6G 将构建空天地一体、泛在连接的异构网络生态，传统依赖固定边界划分与集中式管理的安全防护体系面临根本性挑战。相比 5G 在单一运营商域内的相对封闭环境，6G 网络涉及地面蜂窝、低轨卫星、高空平台等多类型节点的跨域动态协同，边界日趋模糊，业务频繁迁移，接入方式多样化。在此背景下，异构网络边界防护面临以下三大核心挑战：

- 跨域节点信任传递断裂：5G 网络依赖集中式 CA 和层级 PKI，在单一运营商域内建立信任。6G 空天地一体化网络涵盖地面基站、低轨卫星、高空平台、边缘节点等多类型实体，分属不同运营主体，部署动态拓扑。传统集中式 CA 面临单点失效、证书更新延迟和跨域路径过长等问题，各域缺乏统一分布式信任锚点，节点信任状态难实时同步，易导致身份伪造、证书吊销失效及跨域信任传递失败。
- 身份认证碎片化与访问控制静态化：5G 身份认证依赖单一运营商数据库，访问控制基于静态角色。6G 多域接入中，用户和设备需在地面网、卫星网、边缘云及第三方平台频繁切换，跨域认证复杂。传统模式导致身份管理碎片化，认证状态难同步，静态访问控制无法感知动态上下文，如位置、设备安全或行为模式，

增加身份仿冒、会话劫持、越权访问等风险。

● 边界消失与渗透路径增加：5G 安全依赖核心网边界防火墙和接入网安全网关。6G 空天地一体化网络中，卫星链路可直连核心网，用户面功能下沉至边缘，多接入技术并存，传统物理边界防护失效。攻击者可通过卫星链路、无人机中继或临时接入点绕过地面防护，网络暴露面从固定边界扩展为动态多维边界，渗透路径大幅增加。

**2. 标准化需求**

● 分布式信任架构标准：推动基于区块链和去中心化身份（DID）的分布式信任框架标准，建设面向多域协同的 CA+DPKI 信任基石，构建去中心化身份锚点与可信凭证机制，实现跨域身份认证、授权与资源可信调用，提升 6G 异构环境下的信任支撑能力。

● 统一身份认证与访问控制标准：结合异构环境特性，制定支持多策略融合（属性/角色/上下文等）的身份认证与访问控制标准，实现终端身份、设备属性与使用场景间的统一身份认证和访问控制策略灵活匹配，提升资源调度过程中的精细化防控能力。

● 智能边界安全防护标准：规范下一代边界防护设备（如 NGFW、微隔离控制器）功能及接口标准，实现应用层可视、动态感知、策略自动化的安全联动能力，支撑 6G 服务快速编排与解耦部署。

● 除上述风险外，还需考虑 AI 驱动网络架构的新型攻击面、第三方服务链注入风险、供应链污染、量子计算与人工智能融合带

来的新型安全挑战等更深层次的系统性安全挑战。

## 四. 6G 网络内生与边界安全防护体系标准框架

结合对 6G 网络内生安全与异构网络边界安全需求的系统分析，面向 6G 网络的新架构、新能力和新场景，构建覆盖网络全生命周期的内生与边界安全防护标准体系已成为标准化研究的重要方向。如图 9 所示，6G 网络内生与边界安全防护标准体系可划分为若干类重点标准研制方向，涵盖安全体系架构、关键内生安全能力、异构网络边界防护机制等方面。本文围绕上述各类研制方向，进一步明确了每一类标准研制的重点内容和代表性标准项目，为后续 6G 网络内生与边界安全相关标准的立项、研制和协同推进提供系统性指导。

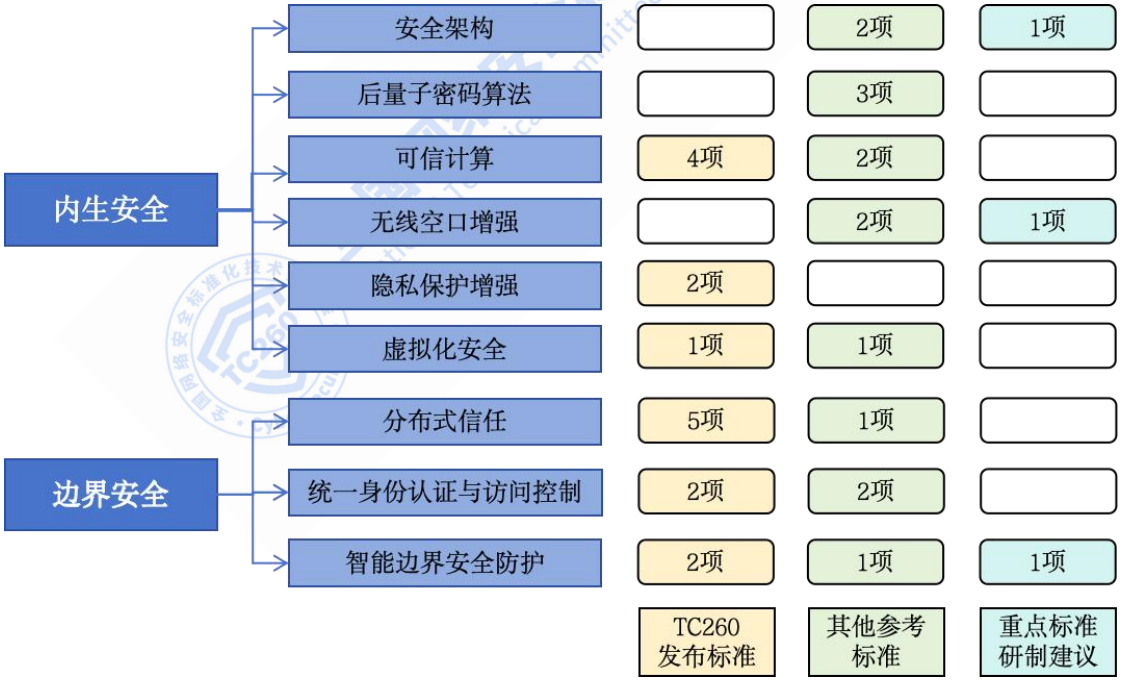



图 9 6G 网络内生及边界安全防护体系标准化框架

### （一）内生安全标准化分析与建议

#### 1. 内生安全架构标准

当前，尚无面向 6G 内生安全架构的一体化国家标准，相关能力多分散在可信计算、访问控制、网络架构设计等领域的已有标准中，缺乏融合性强、体系化构建的安全架构规范。

目前已有若干国际与国家标准对相关架构做出初步定义。如 ITU-T X.1031《Security architecture for digital ecosystem》提出了面向数字生态的整体安全架构框架，涉及可信根、安全域划分、信任链管理等内容。这些内容在理念层面可为 6G 网络内生安全架构提供支撑，但尚未针对 6G 网络特有的多域动态接入、边缘智能协同等新场景进行技术适配。GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》中提出关于安全域、访问控制、系统可信等原则，初步构建内生安全体系框架。但该标准偏向于传统 IT 系统安全，需在标准中补充对虚拟化架构、边缘智能、通信协议内嵌安全机制等 6G 场景的适配内容。GB/T 43696-2024《网络安全技术 零信任参考体系架构》，其提出了动态访问控制、持续认证、最小权限等理念，这些零信任思想可以作为 6G 网络动态防护机制的重要构件。此外，ISO/IEC 30141:2018《Information technology - Internet of Things (IoT) - Reference architecture》也提供了物联网环境下的安全组件嵌入方法，但对 6G 中“边-端-云”分布式协同、可信通信链构建等方面尚无支持。

然而，当前标准在“原生可信”能力的定义、“动态信任演化”机制设计、以及端边协同中安全能力的嵌入等方面仍存在缺失。尤其

是在边缘节点资源受限、连接频繁切换的场景下，传统安全机制难以胜任。建议研究明确内生安全定义及内生能力的统一架构，保障泛在异构网络中安全策略的原生嵌入与动态演化。国际标准化方面，建议定义一套可集成到 6G 网络协议栈各层、且能实现安全自演进、与网络功能协同的通用安全功能与接口规范，明确“安全能力内生于网络功能、服务、数据流”的核心原则。

**2. 抗量子安全标准**

当前，量子计算的快速发展对密码算法构成实质性威胁，6G 网络的密码解决方案应具备抗量子攻击能力，确保未来网络具备长期可持续的安全保障。

我国在量子安全领域已开展研究，发布 GB/T 42829-2023《量子保密通信应用基本要求》，规定了 QKD 技术在安全性、互操作性、可管理性等方面的基本要求，是目前最接近“抗量子安全应用基线”的国家标准。YD/T 4301- 2023《量子保密通信 网络架构》规范了基于 QKD 的量子保密通信网络的功能架构模型、各类网元及其功能模块、网络参考点、配置模型以及基础业务流程等。另外，2024 年，美国国家标准与技术研究院（NIST）正式发布 CRYSTALS-Kyber、CRYSTALS-Dilithium 和 SPHINCS+三种后量子密码算法标准，为全球抗量子密码应用提供技术基准。

尽管现有标准为 QKD 的应用奠定了基础，但面向 6G 网络空天地全域覆盖、万物智联的愿景，现有标准难以适配其高性能、广覆盖、

多场景的特性，亟需补充完善标准化体系。建议加快制定我国国产后量子密码算法标准，推动国产量子密码算法在 6G 网络中的标准应用。国际标准化方面，建议为 6G 制定平滑的后量子密码算法迁移路径和协议增强标准，制定分阶段迁移路线图，并关注对物联网等受限设备的适配。

### 3. 可信计算技术标准

随着 6G 终端边界泛化、服务协同深入，网络各节点必须具备内生可信能力。以可信计算为核心，提供从设备启动、运行到通信过程的全生命周期可信保障。

我国已形成较为完备的可信计算标准体系，主要覆盖体系架构、控制模块、密码支撑平台、可信执行环境等方面。例如，GB/T 38638-2020《信息安全技术 可信计算体系结构》定义了可信计算体系框架、完整性度量方式与可信计算节点类型，是可信体系总体构建的基础；GB/T 40650-2021《信息安全技术 可信计算规范 可信平台控制模块》规定了可信平台控制模块的功能组成、功能接口、安全防护、运行维护要求和证实方法；GB/T 29829-2022《信息安全技术 可信计算密码支撑平台功能与接口规范》定义密码模块接口与验证方法，为加密功能可信性提供支撑；GB/T 41388-2022《信息安全技术 可信执行环境 基本安全规范》则进一步提出对可信操作系统、虚拟化环境及可信应用的控制机制；ISO/IEC 27070:2021《信息技术 安全技术 虚拟信任根建立要求》解决云计算环境中信任建立的核心问题，

增强云基础设施的安全性；ISO/IEC 27071:2023《网络安全设备与服务建立可信连接的安全建议》为设备与服务之间建立可信连接提供一个安全框架和具体建议，规定了构建这种可信连接所需的关键安全组件及其要求。这些标准内容成熟，可直接引用构建 6G 可信基础能力框架。

但这些标准多基于传统 IT 或 IoT 环境设定，在 6G 计算场景下存在一定适配性不足。建议研究面向 6G 动态场景下的信任根管理、节点可信生命周期等能力指标，建立异构平台统一可信接口标准，规范不同硬件平台的可信根映射关系和功能等价性验证方法，补充适配边缘节点的可信根定义与远程度量机制标准。国际标准化方面，建议为 6G 云化、边缘化的网络功能及数据制定统一的数据保护框架与远程认证机制，支持容器化网元、AI 模型完整性度量。

**4. 无线空口安全标准**

随着 6G 终端边界泛化、网络服务协同深入，空口链路安全对全网可信能力提出了更高要求。无线空口在 6G 中不仅承担传统通信功能，还面向多接入、多频段、低轨卫星、无人机中继等复杂异构场景，其安全性直接关系到数据完整性、通信保密性与网络连续性。

我国在无线空口安全领域已制定了一些国家标准，主要覆盖空口安全协议、认证机制、密钥管理及无线接入防护等方面。如 GB/T 38636-2020《信息安全技术 传输层密码协议（TLCP）》规定了传输层密码协议，包括记录层协议、握手协议族和密钥计算。GB/T

35286-2017《信息安全技术 低速无线个域网空口安全测试规范》为低速无线个域网设备的空口安全测试提供了标准化的方法和依据。

然而，现有标准主要针对静态拓扑与单一频段设计，难以适应6G空天地一体化、频谱动态分配及多节点跨域协作的复杂环境。建议面向6G高速率、低时延与空天地一体化通信场景，规范物理层密钥生成与信道特征建模机制以及MAC层控制信令的机密性、完整性与重放保护要求。国际标准化方面，建议为支持超大带宽、通感一体等新特性的6G新空口制定增强物理层安全、轻量化认证等机制规范。

**5. 隐私保护技术标准**

随着6G网络中终端数量大幅增长、边缘计算广泛部署及跨域服务深入，隐私保护需求从“单点匿名”向“全生命周期自主可控”转变。6G分布式智能网络架构要求隐私保护覆盖数据生成、存储、传输、共享与使用全过程，形成端到端、多层次的防护体系。

我国在隐私保护领域已有的标准有GB/T 35273-2020《信息安全技术 个人信息安全规范》规范个人信息全生命周期管理，包括最小化原则、访问控制及风险评估方法，为用户数据管理提供技术依据。GB/T 43506-2023《电信和互联网服务 用户个人信息保护技术要求》界定了相关术语，并规定了保护范围、信息分类、分级对象、分级方法以及具体的保护要求。

现有标准基于静态数据环境设计，难以适应6G中终端泛在、边缘节点动态部署、多租户协作及高速数据流动场景。建议研究跨域数

据关联分析防护、全生命周期隐私管理及 AI 训练数据隔离能力指标。明确安全多方计算（MPC）、同态加密（HE）及分级隐私凭证在标准化中的接口、使用要求和验证方法，支持边云协同、跨域隐私计算与可验证共享。国际标准化方面，建议针对 6G 通感一体采集的环境数据、AI 训练数据、用户身份等，制定跨域、分级的数据最小化收集与处理标准。

### 6. 虚拟化安全标准

随着 6G 网络向云原生、多租户和高密度虚拟化方向发展，虚拟化安全成为保障网络隔离性、计算完整性和服务连续性的关键技术。虚拟化安全涉及虚拟机、容器、微服务及虚拟化资源管理层的安全策略、隔离机制及可信度量。

我国已有虚拟化安全相关标准体系，主要涵盖虚拟化环境安全要求、可信执行环境、虚拟化管理接口等。如 GB/T 41388-2022《信息安全技术 可信执行环境 基本安全规范》提出可信操作系统、虚拟化环境及可信应用控制机制，为虚拟化安全提供基础保障。GA/T 1541-2018《信息安全技术 虚拟化安全防护产品安全技术要求和测试评价方法》涵盖虚拟机监控（VMM）安全加固、资源隔离、访问控制与日志审计等核心虚拟化安全能力。GB/T 25068.7-2025《信息技术 安全技术 网络安全 第 7 部分：网络虚拟化安全》基于网络虚拟化安全威胁提出安全建议、安全控制、安全设计和考虑等，可为组织构建安全的虚拟化环境提供指引。

现有标准多基于传统数据中心或企业私有云场景，缺乏对 6G 边缘节点、高密度微服务及动态迁移场景的适配。建议研究边缘节点、轻量容器及高频动态迁移场景的虚拟化安全能力指标，推动跨域虚拟化安全策略协同标准化，实现策略可下发、可验证及跨平台互操作。国际标准化方面，建议面向全云化、服务化的 6G 核心网，制定网络功能的全生命周期安全标准，包括镜像安全、微服务隔离、自动化编排与修复等。

**（二）边界安全标准化分析与建议**

**1. 分布式信任架构标准**

6G 网络面临多域接入、跨系统协同、身份自治等信任挑战，传统中心化 CA 信任体系难以支撑大规模动态协作，需引入基于区块链的分布式公钥基础设施（DPKI）实现跨域身份认证、透明审计与动态信任管理。利用区块链的公开透明、多方共识、不可篡改的特性构建分布式信任基础设施，实现基于区块链的证书和身份管理、透明审计和跨域验证。

目前，分布式信任标准体系主要集中在区块链、分布式账本、数字身份认证等核心领域。例如，GB/T 42752-2023《区块链和分布式记账技术 参考架构》明确了区块链系统的功能视图与用户视图，提供了总体参考框架；GB/T 42570-2023《信息安全技术 区块链技术安全框架》对区块链安全功能组件、密码支撑与安全职责进行了系统规范，具有较强的基础性与可复用性；GB/T 43580-2023《区块链和分

布式记账技术 存证通用服务指南》构建了基于区块链的存证服务流程与信任模型，可支撑多场景的身份存证需求；GB/T 19713-2025《网络安全技术 公钥基础设施 在线证书状态协议》明确了公钥基础设施（PKI）中用于检验数字证书是否有效（如是否被撤销）的关键机制；GB/T 26855-2011《证书策略与认证业务声明框架》关注 PKI 体系的策略管理和信任评估，为 PKI 的运营者和使用者提供了一套通用的“说明书”撰写模板；此外，YD/T 4055-2022《电信网和互联网区块链基础设施安全防护要求》则对区块链基础设施的安全等级保护提出防护要求。这些标准可作为分布式信任架构构建的底层能力支撑。

但现有标准尚未针对 6G 网络的高动态性、多域交互特征进行适配，缺乏对分布式身份标识、跨域认证机制、轻量级共识机制等关键内容的专项定义。建议在已有认证标准的修订中考虑分布式信任技术方案，以适配通信网络分布式认证方式。国际标准化方面，建议制定适应“空天地一体、多域融合”网络、脱离单一中心化信任根、支持动态信任传递的通用框架与协议，解决多运营商、多安全域的网元互信问题，并适配物联网终端、卫星终端等资源受限设备。

**2. 统一身份认证与访问控制标准**

在 6G 异构网络环境下，用户、设备、场景均高度动态，基于固定角色或静态策略的传统访问控制机制难以应对灵活多变的资源调度与协同需求。

当前零信任架构已提出以“持续认证、最小权限、动态策略”为

核心的访问控制理念。国家标准 GB/T 43696-2024《网络安全技术 零信任参考体系架构》详细定义了零信任架构的核心组件、身份验证机制、安全策略引擎与审计机制等，提供了多维访问控制的架构参考。此外，GB/T 42573-2023《信息安全技术 网络身份服务安全技术要求》为各类网络应用中的用户身份认证服务建立统一的安全基线；GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》也在访问控制、身份认证、安全审计方面提出了基础要求，可作为最低保障基线。ISO/IEC 29146:2024《Information technology — Security techniques — A framework for access management》提供了访问管理的整体框架模型。

然而，现有标准仍以传统 IT 系统为主，缺乏对 6G 异构场景中如基于场景上下文、基于策略自学习、跨域策略协同等能力的支持。建议推动 6G 网络统一身份认证与访问控制技术应用，支持多因素认证（MFA）、行为感知访问控制（BAC）与策略驱动访问模型（PBAC）融合，构建自适应授权体系。同时，开展边缘访问控制部署等关键技术研究。国际标准化方面，建议针对跨运营商、跨域的 6G 服务化架构，制定基于分布式身份的统一认证与细粒度访问控制规范，支持用户、设备、网元等多类型实体的身份管理，解决身份碎片化问题。

### 3. 智能边界安全防护标准

6G 网络边界呈现出动态化、虚拟化、多维化趋势，安全边界的传统静态划分与策略配置难以适应网络高弹性特征。下一代边界防护

设备需具备应用层深度可视、威胁动态感知、策略自动化编排等智能联动能力，以支撑 6G 服务的快速编排与解耦部署。

目前我国 GB/T 20281-2020《信息安全技术 防火墙安全技术要求和测试评价方法》对传统防火墙的技术要求进行了规范，但主要面向基于包过滤和状态检测的静态防护。GB/T 20275-2021《信息安全技术 网络入侵检测系统技术要求和测试评价方法》适用于网络入侵检测系统的设计、开发与测评。YD/T 4336-2023《基于 SDN/NFV 的电信网软件定义安全框架》提出了 SDN 控制层、转发层与安全功能之间的协同机制，定义了功能组件、接口流程及典型应用场景。该标准可用于指导 6G 边界控制器与安全策略协调调度机制。

然而，现有标准主要面向传统网络环境，对 6G 场景下的智能边界防护能力支持不足。建议明确智能边界安全的基本概念、体系结构与功能组成，规范基于软件定义与安全能力编排的边界防护技术。在国际标准化方面，应针对动态化、软件化的 6G 网络制定可编程、可编排的智能安全防护规范，实现边界实时监测、动态发现和快速拓扑更新，增强跨边界攻击防护与数据泄露防范能力，同时保障威胁响应与策略调整的自动化与智能化。

### （三）重点标准研制建议

结合 6G 网络内生与边界安全需求，以及现有国内外研究与标准化进展，梳理发现，在内生安全架构、无线空口安全、智能边界防护等领域仍存在标准空白和待完善需求。为支撑 6G 关键技术应用安全

与产业发展，应重点推进内生安全架构、6G 无线空口安全、智能边界安全防护等相关标准研制。表 1 为建议在未来两年加快推进的 6G 内生与边界安全标准，包括标准名称、研制状态、拟解决的核心问题及对应类别，为我国 6G 网络安全标准制修订与体系建设提供参考。

表 1 建议重点研制的标准

| 序号 | 标准名称 | 状态 | 标准拟解决的问题 | 对应类别 |
|---|---|---|---|---|
| 1 | 内生安全体系架构技术要求 | 建议研制 | 本标准是在 6G 网络向分布自治、智能内生和泛在异构方向演进的背景下制定，旨在解决现有安全体系中内生安全定义不统一、能力架构分散、安全策略难以协同演进等问题，明确内生安全定义，信任计算、动态认证、策略协同等内生能力的统一架构。 | 内生安全 |
| 2 | 6G 无线空口安全技术要求 | 建议研制 | 本标准是在 6G 高速率、低时延与空天地一体化通信背景下，规范物理层密钥生成与信道特征建模机制，完善太赫兹通信与智能反射面（RIS）环境下的物理层认证与抗干扰技术标准，MAC 层控制信令的机密性、完整性与重放保护要求。 | 内生安全 |
| 3 | 智能边界安全防护技术要求 | 建议研制 | 本标准明确智能边界安全的基本概念、体系结构与功能组成，规范基于软件定义与安全能力编排的边界防护技术，为统一建设与协同部署提供总体指导。 | 边界安全 |

## 五. 6G 网络安全标准化工作建议

6G 具有深度融合通感算智、天地一体全域覆盖等特点，网络架构、应用场景等较 5G 将有较大调整，未知安全风险更加突出，需做好提前布局和前瞻应对。我们应按照“基础框架构建、重点技术突破、普适能力研发”的总体思路，系统布局推进 6G 安全标准化工作，构建与 6G 发展相适应的安全保障体系。

### （一）坚持安全与网络同步设计，推动内生安全标准化

在 6G 架构设计初期，应将安全需求纳入标准化体系，提前谋划内生、弹性、智能的网络安全框架，确保安全能力与网络功能同步规划、同步部署、同步演进。

- 聚焦 6G 网络关键技术体系和典型应用场景的内生安全需求，围绕端、边、网、云协同架构，明确安全能力在不同网络层级和功能域中的内生部署方式，推动相关标准制定，明确内生安全定义及内生能力统一架构，保障泛在异构网络中安全策略的原生嵌入与动态演化。
- 注重 6G 内生安全相关标准与国家网络安全标准体系的衔接协同，同时加强与人工智能安全、数据安全、卫星安全等相关领域标准体系的融合设计，推动内生安全能力在不同网络形态和应用场景中的一致实现与协同应用，避免安全机制割裂和重复建设。
- 围绕 6G 网络内生安全的重点方向和迫切需求，重点推进分布式可信计算、无线空口安全增强、网络虚拟化与云原生安全、抗

量子安全等关键技术标准研制，并在边缘智能、通感一体和行业融合应用等相关安全标准研究中充分体现 6G 内生安全特性，为 6G 网络长期演进和融合应用提供系统化、可持续的安全标准支撑。

**（二）强化跨域协同与动态防护，推动 6G 边界安全标准化**

传统基于静态划界的防护模式难以适应异构接入和跨域协同需求，应在 6G 相关技术研究和标准化工作中系统推进边界安全能力建设，通过标准化方式明确边界识别、跨域信任和安全协同的基本原则与能力要求，为复杂融合场景下的安全防护提供统一支撑。

- 聚焦 6G 网络关键技术体系和典型应用场景下的边界安全需求，围绕多网络融合和跨域协同运行特征，系统梳理不同场景下异构网络之间的边界形态，推动相关标准制定，明确动态边界识别、跨域信任建立和安全责任划分的统一原则，保障异构融合网络环境下边界防护能力的有效实施与协同运行。
- 注重 6G 边界安全相关标准与国家网络安全标准体系的衔接协同，同时加强与卫星通信安全、物联网安全、工业互联网安全、车联网安全等相关领域标准体系的融合设计，推动边界安全要求在不同网络形态和应用场景中的一致落实，避免跨网络、跨行业融合过程中边界防护机制割裂和防护能力不均衡。
- 围绕 6G 网络边界安全的重点方向，推进分布式信任、跨域身份认证与访问控制、动态边界防护等关键技术标准研制，并在空天地一体、边缘计算、通感一体和行业融合应用等相关安全标准

研究中充分体现边界安全要求，为 6G 网络复杂融合场景下的安全运行提供系统化、可持续的标准支撑。

**（三）完善协同推进机制，推动 6G 安全标准验证与落地应用**

6G 网络安全技术涉及通信、安全、计算和人工智能等多个技术领域，标准研制周期长、技术不确定性高，单一主体难以完成系统性研究和有效验证。应围绕 6G 内生安全和边界安全的关键问题，完善产学研用协同推进机制，形成从技术研究、标准研制到验证应用的闭环路径。

- 依托现有标准组织和技术平台，推动运营商、设备厂商、安全企业、高校和科研机构围绕关键技术方向协同开展标准研究，统一技术理解和能力边界，减少重复研究和方向分散。
- 结合 6G 试验网络和典型融合应用场景，系统开展标准验证和能力评估工作，通过测试验证、试点示范等方式，提升安全标准的可操作性和可实施性，推动标准成果在网络规划、建设和运行阶段的实际应用。

**（四）前瞻布局国际标准，提升 6G 网络安全的全球协同水平**

6G 网络具有全球协同发展的技术和产业特征，安全标准的国际参与深度将直接影响技术路线选择和产业生态构建。3GPP SA3 首批确立的三项基础安全领域，与 AI 安全、数据面安全等新兴议题相互交织，初步勾勒出 6G 安全的技术图谱轮廓。对于中国产业界而言，这场技术与标准的角逐，既是严峻挑战，更是战略机遇。应在 6G 研

究和标准化早期阶段同步推进国际标准布局，增强我国在 6G 网络安全领域的规则参与和影响能力。

目前我国已积极参与 ITU、3GPP、ISO 等多个国际标准组织研究，面向 6G 场景中固定网络、移动网络和卫星网络融合场景的安全技术开展研究。下一阶段中国企业主要的挑战在于如何将庞大的技术贡献与市场影响力，有效转化为在基础性、支柱性安全领域的标准定义权与生态号召力。在国际标准化工作方面应做好以下几项工作:

- 立足 6G 网络仍处于全球协同研究和技术共识形成阶段的现实，系统跟踪和研判国际 6G 网络安全研究进展，在充分吸收国际前沿研究成果的基础上，结合我国在移动通信、网络安全和融合应用领域的技术积累，持续提出具有体系性和前瞻性的 6G 网络安全技术主张，推动国内 6G 安全研究成果与国际研究框架的有效对接，逐步形成可被国际采纳的技术思路和标准方向。
- 持续加强对国际 6G 网络安全研究动向、政策导向和标准化进程的跟踪分析，重点关注 6G 安全架构、内生安全机制和边界安全关键问题的研究进展，积极参与国际研究项目和技术讨论，推动我国研究成果在国际标准研究阶段的应用和验证，为后续标准制定奠定基础，完善我国 6G 网络安全标准体系的国际衔接能力。
- 在现有国际合作和交流机制基础上，把握住我国在移动通信领域的技术沉淀和市场发展优势，积极支持国内单位和专家以牵头或联合牵头方式参与 6G 国际标准研究与制定，推动内生安全、动

态边界防护等关键技术方向在国际标准组织中的立项和讨论，逐步提升我国在 6G 网络安全国际规则制定中的参与深度和影响力。

# 附录 A 相关政策法规清单（国际/国内）

| 序号 | 国家 | 政策法规名称 | 发布部门/组织 | 发布时间 |
|---|---|---|---|---|
| 1 | 美国 | 《6G 路线图：构建北美 6G 领导力基础》 | Next G 联盟 | 2022.01 |
| 2 | 美国与澳大利亚、加拿大、捷克、芬兰、法国、日本、韩国、瑞典和英国等十国 | 《6G 原则联合声明》 | / | 2024.02 |
| 3 | 日本 | 《Beyond 5G（即 6G）推进战略》 | 总务省 | 2020.06 |
| 4 | 日本 | 《Message to the 2030s》 | 日本 Beyond 5G 推进联盟 | 2022.03 |
| 5 | 中国 | 《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》 | 全国人大 | 2021.03 |
| 6 | 中国 | 《“十四五”信息通信行业发展规划》 | 工业和信息化部 | 2021.11 |
| 7 | 中国 | 《“十四五”数字经济发展规划》 | 国务院 | 2022.01 |
| 8 | 中国 | 《中华人民共和国无线电频率划分规定》 | 工业和信息化部 | 2023.06 |
| 9 | 中国 | 《关于微波通信系统频率使用规划调整及无线电管理有关事项的通知》 | 工业和信息化部 | 2023.06 |
| 10 | 中国 | 《关于推动未来产业创新发展的实施意见》 | 工业和信息化部等七部门 | 2024.01 |
| 11 | 中国 | 《国家数据基础设施建设指引》 | 国家发展改革委、国家数据局、工业和信息化部 | 2024.12 |

# 附录　B 相关标准列表（国际/国内）

| 序号 | 标准名称 | 标准组织 | 标准编号 | 牵头单位 | 时间 |
|---|---|---|---|---|---|
| 1 | Security Consideration for IMT-2030 Networks | ITU-T | TR.IMT2030-sec-con | 中国移动 | 2024.09 |
| 2 | Security architecture for digital ecosystem | ITU-T | ITU-T X.1031 | - | 2008.03 |
| 3 | Overview of trust provisioning in information and communication technology infrastructures and services | ITU-T | ITU-T Y.3052 | - | 2017.03 |
| 4 | Information technology - Internet of Things (IoT) - Reference architecture | ISO | ISO/IEC 30141:2018 | 无锡物联网产业研究院 | 2018.08 |
| 5 | Information technology — Security techniques — A framework for access management | ISO | ISO/IEC 29146:2024 | - | 2024.01 |
| 6 | Information technology — Security techniques — Requirements for establishing virtualized roots of trust | ISO | ISO/IEC 27070:2021 | - | 2021.12 |
| 7 | Cybersecurity — Security recommendations for establishing trusted connections between devices and services | ISO | ISO/IEC 27071:2023 | 中国电子技术标准化研究院 | 2023.07 |
| 8 | 电信网和互联网区块链基础设施安全防护要求 | CCSA | YD/T 4055-2022 | 中国信息通信研究院 | 2022.04 |
| 9 | 基于 SDN/NFV 的电信网软件定义安全框架 | CCSA | YD/T 4336-2023 | 中国移动 | 2023.07 |

| | | | | | |
|---|---|---|---|---|---|
| | 量子保密通信 网络架构 | CCSA | YD/T 4301 - 2023 | 国科量子通信网络有限公司 | 2023.05 |
| 10 | 信息安全技术 网络安全等级保护基本要求 | TC260 | GB/T 22239-2019 | 公安部第三研究所 | 2019.05 |
| 11 | 网络安全技术 生成式人工智能服务安全基本要求 | TC260 | GB/T 45654-2025 | 中国电子技术标准化研究院 | 2025.04 |
| 12 | 信息安全技术 个人信息安全规范 | TC260 | GB/T 35273 - 2020 | 中国电子技术标准化研究院 | 2020.03 |
| 13 | 数据安全技术 数据安全风险评估方法 | TC260 | GB/T 45577 - 2025 | 中国电子技术标准化研究院 | 2025.04 |
| 14 | 信息安全技术 边缘计算安全技术要求 | TC260 | GB/T 42564- 2023 | 中国移动 | 2023.05 |
| 15 | 信息安全技术 个人信息处理中告知和同意的实施指南 | TC260 | GB/T 42574 - 2023 | 中国电子技术标准化研究院 | 2023.05 |
| 16 | 网络安全技术 零信任参考体系架构 | TC260 | GB/T 43696-2024 | 奇安信 | 2024.04 |
| 17 | 信息安全技术 移动终端安全保护技术要求 | TC260 | GB/T 35278- 2017 | 中国信息通信研究院 | 2017.12 |
| 18 | 信息安全技术 网络安全等级保护基本要求 | TC260 | GB/T 22239-2019 | 公安部第三研究所 | 2019.05 |
| 19 | 信息安全技术 数据安全能力成熟度模型 | TC260 | GB/T 37988-2019 | 阿里巴巴 | 2019.08 |
| 20 | 信息安全技术 网络安全等级保护测评要求 | TC260 | GB/T 28448-2019 | 公安部第三研究所 | 2019.05 |
| 21 | 信息技术 数字孪生 第1部分：通用要求 | TC260 | GB/T 43441.1-2023 | 中国电子技术标准化研究院 | 2023.11 |
| 22 | 信息技术 装备数字孪生系统 通用要求 | TC260 | GB/T 45626-2025 | 中国电子技术标准化研究院 | 2025.04 |
| 23 | 区块链和分布式记账技术 参考架构 | TC260 | GB/T 42752-2023 | 中国电子技术标准化研究院 | 2023 |

| | | | | | |
|---|---|---|---|---|---|
| 24 | 信息安全技术 区块链技术安全框架 | TC260 | GB/T 42570-2023 | 清华大学 | 2023 |
| 25 | 区块链和分布式记账技术 存证通用服务指南 | TC260 | GB/T 43580-2023 | 厦门安妮股份有限公司 | 2023.12 |
| 26 | 信息安全技术 可信计算规范 可信平台控制模块 | TC260 | GB/T 40650-2021 | 华大半导体有限公司 | 2021.10 |
| 27 | 信息安全技术 可信计算密码支撑平台功能与接口规范 | TC260 | GB/T 29829-2022 | 联想 | 2022.04 |
| 28 | 信息安全技术 可信执行环境 基本安全规范 | TC260 | GB/T 41388-2022 | 中国银联 | 2022.04 |
| 29 | 综合能源系统的数字孪生技术规范 | 中国国际科技促进会 CIAPST | T/CI 203-2023 | 国家电投集团综合智慧能源科技有限公司 | 2023.11 |
| 30 | 信息安全技术 传输层密码协议（TLCP） | TC260 | GB/T 38636-2020 | 山东得安信息技术有限公司 | 2020.04 |
| 31 | 信息安全技术 低速无线个域网空口安全测试规范 | TC260 | GB/T 35286-2017 | 无线网络安全技术国家工程实验室 | 2017.12 |
| 32 | 信息安全技术 个人信息安全规范 | TC260 | GB/T 35273-2020 | 中国电子技术标准化研究院 | 2020.03 |
| 33 | 信息安全技术 虚拟化安全防护产品安全技术要求和测试评价方法 | TC260 | GA/T 1541-2018 | 国家计算机病毒应急处理中心 | 2018.12 |
| 34 | 量子保密通信应用基本要求 | TC485 | GB/T 42829-2023 | 国科量子通信网络有限公司 | 2023.08 |
| 35 | 网络安全技术 公钥基础设施 在线证书状态协议 | TC260 | GB/T 19713-2025 | 普华诚信信息技术有限公司 | 2025.02 |
| 36 | 信息安全技术 数字证书代理认证路径构造和代理验证规范 | TC260 | GB/T 29243-2012 | 中国科学院数据与通信保护研究教育中心 | 2012.12 |
| 37 | 信息安全技术 公钥基础设施 证书策略与认证业务声明框架 | TC260 | GB/T 26855-2011 | 国家信息中心 | 2011.07 |

| | | | | | |
|---|---|---|---|---|---|
| 38 | 信息安全技术 网络身份服务安全技术要求 | TC260 | GB/T 42573-2023 | 北京数字认证股份有限公司 | 2023.05 |
| 39 | 信息安全技术 防火墙安全技术要求和测试评价方法 | TC260 | GB/T 20281-2020 | 公安部第三研究所 | 2020.04 |
| 40 | 信息安全技术 网络入侵检测系统技术要求和测试评价方法 | TC260 | GB/T 20275-2021 | 公安部第三研究所 | 2021.10 |
| 41 | 电信和互联网服务 用户个人信息保护技术要求 | TC543 | GB/T 43506-2023 | 中国信息通信研究院 | 2023.12 |
| 42 | 信息技术 安全技术 网络安全 第7部分：网络虚拟化安全 | TC260 | GB/T 25068.7-2025 | 中国移动通信集团有限公司 | 2025.12 |

# 附录　C 未来安全技术

## （一）数字孪生网络安全推演技术

ITU-R 发布的《IMT 面向 2030 及未来发展的框架和总体目标建议书》中，提出数字孪生是面向 2030 及未来 6G 系统的九大用户应用发展趋势，将实现人、机、物的连接，实现物理世界和虚拟世界的实时同步。数字孪生网络是一个具有物理网络实体及虚拟孪生体，且二者可进行实时交互映射的网络系统。基于虚拟孪生体对网络进行分析、诊断、仿真和控制，可以实现低成本试错、智能化决策、高效率创新和预测性维护。

数字孪生技术可帮助安全领域寻求超越物理网络的解决方案，数字孪生技术可能应用于以下安全场景：与安全推演相结合，可以为网络安全提供接近真实网络的数字化验证环境，实现低成本试错、智能化决策和预测性维护，能够确保物理网络的安全性和可靠性；与攻击欺骗相结合，数字孪生网络提供更真实的诱捕环境以及实时网络的监控系统，并且可以根据攻击者的行为动态调整的诱捕方案；与安全运维相结合，实现对通信网络状态的评估、对现有问题的诊断和对未来趋势的预测，通过模拟各种攻击的可能性，提供更全面的、优化的安全策略。同时，其自主构建和扩展的能力可以实现新业务的需求探索与效果验证，为垂直行业提供精准安全服务。

目前标准方面，GB/T 43441.1-2023《信息技术 数字孪生 第 1 部分：通用要求》为数字孪生系统提供了参考架构、功能要求和安全

属性定义，具备较强通用性。GB/T 45626-2025《信息技术 装备数字孪生系统 通用要求》则进一步聚焦于设备身份认证、实时数据加密和抗攻击仿真，为数字孪生系统的安全属性提供具体条目。T/CI 203-2023《综合能源系统的数字孪生技术规范》则为特定行业的数据脱敏与攻击防御提供规范。

**（二）拟态防御构造技术**

拟态防御构造技术以动态异构冗余（DHR）为核心理念，通过构造具有多样性和动态变化能力的系统结构，实现对攻击路径的迷惑与干扰，有效增强网络在遭受攻击时的生存性和稳定性。拟态防御强调“结构决定安全”，不仅关注传统的信息安全与隐私保护，更面向人机物三元融合环境下的功能安全与系统可用性。

拟态防御构造技术可集成在 6G 系统的内生安全框架中，安全控制层承载拟态控制器能力，结构化策略控制模块集成拟态防御策略，其根据决策层安全部署请求，将面向用户的安全服务转为动态调度、随机迁移、冗余管理策略，如网络、软件参数的动态调整，等价功能异构体的管理、轮换策略等，然后把任务下发到编排器中；编排器负责新建一个拟态域网络切片，并在虚拟资源上生成若干 NFs（包括 VNF 的异构副本，网络功能级的拟态裁决器），在 SDN 控制器的协助下，根据安全要求完成这些 NFs 链路连接、路由规则下发及自动化部署等，然后把网络切片已生成的信息反馈给拟态控制器，完成一个拟态网络切片的生成。拟态网络切片会定时对网元执行体副本进行轮换，

以迷惑攻击者。同时，当拟态裁决器感知到执行体遭到攻击时，会通知拟态控制器，从而对受攻击执行体进行清洗与轮换，即使单个执行体被攻破，也能通过冗余机制避免因单点故障而造成业务停滞。

# 附录 D 缩略语列表

| 缩略语 | 全称 | 释义 |
|---|---|---|
| 6G | Sixth Generation | 第六代移动通信技术 |
| AI | Artificial Intelligence | 人工智能 |
| ML | Machine Learning | 机器学习 |
| eMBB | enhanced Mobile BroadBand | 增强移动宽带 |
| mMTC | massive Machine-Type Communications | 海量物联网连接 |
| URLLC | Ultra-Reliable and Low Latency Communications | 超可靠低时延通信 |
| XR | Extended Reality | 扩展现实 |
| VR | Virtual Reality | 虚拟现实 |
| AR | Augmented Reality | 增强现实 |
| MR | Mixed Reality | 混合现实 |
| RIS | Reconfigurable Intelligent Surface | 智能超表面 |
| ZT | Zero Trust | 零信任 |
| DHR | Dynamic Heterogeneous Redundancy | 动态异构冗余 |
| DPKI | Decentralized Public - Key Infrastructure | 分布式公钥基础设施 |
| DID | Decentralized Identifier | 去中心化身份 |
| SDSec | Software - Defined Security | 软件定义安全 |
| IAM | Identity and Access Management | 统一身份认证与访问控制 |
| VC | Verifiable Credentials | 可验证凭证 |
| MFA | Multi - Factor Authentication | 多因素认证 |
| BAC | Behavior - Aware Access Control | 行为感知访问控制 |
| PBAC | Policy - Based Access Control | 策略驱动的访问模型 |
| NGFW | Next - Generation Firewall | 下一代防火墙 |
| IDS/IPS | Intrusion Detection System / Intrusion Prevention System | 入侵检测与防御系统 |
| TIP | Threat Intelligence Platform | 威胁情报平台 |
| SOAR | Security Orchestration, Automation and Response | 安全编排自动化响应 |
| JCS | Joint Communication and Sensing | 通信和传感 |
| RINGS | Resilient and Intelligent Next - Generation Systems Project | 弹性和智能下一代系统项目 |
| TEE | Trusted Execution Environment | 可信执行环境 |
| CN | Core Network | 移动核心网 |
| PETs | Privacy - Enhancing Technologies | 隐私增强技术 |
| PQC | Post - Quantum Cryptography | 抗量子加密算法 |
| QKD | Quantum Key Distribution | 量子密钥分发技术 |

| | | |
|---|---|---|
| SECaaS | Security as a Service | 安全即服务 |
| ECC | Elliptic Curve Cryptography | 椭圆曲线密码 |
| MPC | Secure Multi-Party Computation | 安全多方计算 |
| HE | Homomorphic Encryption | 同态加密 |
| TPCM | Trusted Platform Control Module | 可信平台控制模块 |
| TSB | Trusted Software Base | 可信软件基 |
| PDCP | Packet Data Convergence Protocol | 分组数据汇聚协议 |