5G 网络安全

白皮书

2020

中通服設計
CICD INSTITUTE

中通服咨询设计研究院有限公司

前 言

5G 作为新一代移动通信技术体系，采用了很多新业务、新架构、新技术，将在提升移动互联网用户业务体验的基础上，进一步满足未来物联网应用的海量需求，与工业、医疗、交通、传媒等行业深度融合，实现真正的“万物互联”。是未来数字世界的使能者。

然而，任何一项新技术的出现往往都是“双刃剑”，5G 技术给人们带来诸多便利的同时也对网络安全和用户隐私保护等提出了新的挑战。5G 网络安全体系除了要满足基本通信安全保障要求之外，还需要为不同 5G 业务场景提供差异化安全服务，能够适应多种网络接入方式及新型网络架构，保护用户隐私，并提供开放的安全能力。

本白皮书分析了 5G 网络关键安全需求，明确了 5G 网络所面临的网络安全风险和挑战，在充分调研业内在 5G 网络安全方面所做的相关工作的基础上提出了 5G 网络安全治理的技术和监管方案建议。介绍了中通服设计院在 5G 安全方面所做的工作，愿同各方协作，共筑 5G 安全的美好未来。

编制单位：中通服咨询设计研究院有限公司

主编人员：王小鹏、邓萍萍

审核人员：乔爱峰、房树森、王强、唐怀坤

目 录

1. 5G 网络概述

“4G 改变生活，5G 改变世界”，5G 作为新一代移动通信技术，在核心技术、用户体验和应用场景等方面都将产生创新性的改变。2019 年是 5G 商用元年，6 月初，工信部向四大运营商正式发放了 5G 商用牌照，10 月末，中国电信、中国移动、中国联通三家运营商共同宣布启动 5G 商用。5G 网络将成为助力万物互联的新型基础设施，广泛应用于城市管理、工业制造、文化传媒、医疗卫生等各个方面，打开万亿级的 5G 应用市场空间，推动“数字中国”建设再上新台阶。

5G 技术的正式商用将在城市管理、工业制造、个人生活等多个领域产生重大变革，大量 5G 新应用新业务将不断涌现。5G 技术在带给人们更好的生活体验、更高的生产效率的同时也会带来诸多新的网络安全风险，需要业界高度重视、提前分析、积极应对，以更好地迎接丰富多彩的 5G 时代的到来。

1.1 5G 网络新特征

5G 需要具备比 4G 更高的性能，支持 0.1 至 1Gbps 的用户体验速率，每平方公里 100 万的连接数密度，毫秒级的端到端时延，每平方公里数十 Tbps 的流量密度，每小时 500 千米以上的移动性以及数十 Gbps 的峰值速率。其中，用户体验速率、连接数密度和时延是 5G 最基本的 3 个性能指标。同时，5G 还需要大幅提高网络部署和运营效率，与 4G 相比，其频谱效率提升 5 至 15 倍，能效和成本效率提升百倍以上。

5G 网络的优势可以概况为三个方面：一是容量增强，5G 将实现 1000 倍的网络容量提升、10-100 倍用户速率的提升，以实现人与物、物与物等之间的连接，使用网络技术将城市设施、家居生活、物流状态等融于一体；二是海量接入终端，每平方公里会有 1000K 连接数、需要延长 10 倍以上的电池寿命；三是超高可靠低时延；5G 网络可达到 1ms 时延、99.999%可靠性，下行速度最高可达每秒 10Gb，下载高清电影分秒之间即可完成，网络操作与实际操作紧密结合，在视频通话、娱乐、医疗、交通等领域将会占据举足轻重的地位。

1.2 5G 新的应用场景

5G 的三大场景，包括增强型移动宽带(enhanced mobile broad band，简称 eMBB)、海量物联网(massive machine type communications，简称 mMTC)以及高可靠低延时连接(ultra-reliable and low latency communications，简称 URLLC)。具体来说，三大应用场景的特点为：

图 1-1 5G 的三大应用场景

（1） eMBB(增强型移动宽带)，聚焦对带宽有极高需求的业务。 此类场景主要处理以人为中心的潜在需求，要求能提供 100Mbps 的用户体验速率。例如高清视频，VR(虚拟现实)/AR(增强现实)等，满足人们对数字化生活的需求。

（2） mMTC(海量物联网)，覆盖对于联接密度要求较高的场景。此类场景主要处理大规模智能设备的通信问题，要求能够支撑百万级低功耗物联网设备终端。例如智慧城市、智能农业、各种穿戴设备的连接服务等，能满足人们对于数字化社会的需求。

（3） uRLLC(高可靠低延时连接)，聚焦对时延极其敏感的业务。此类场景主要处理对可靠性要求极高、时延极其敏感的特殊应用场景，要求在保证超低于 1 毫秒时延的同时，提供超高的传输可靠性。例如自动驾驶/辅助驾驶、远程控制、工业自动化等，满足人们对于数字化工业的需求。

通过 3GPP 的三大场景定义我们可以看出，5G 的通信不仅仅是人的通信，而且是物联网、工业自动化、无人驾驶等业务被引入，通信从人与人之间通信，开始转向人与物的通信，直至机器与机器之间的通信。

总体来说，5G 技术将给人们带来更为丰富多彩的世界，VR、AR、车联网、无人驾驶、智能制造、远程医疗等应用将实现。，随着技术应用的广泛化、多样化，依托 5G 网络会给人们的生产、生活乃至整个国家的效率提升产生非常重要的影响，正因为如此，各个国家都非常重视 5G 网络的安全问题。

1.3 5G 引入的新技术

为提高通信系统的灵活性、可扩展性和部署速度，5G 网络架构将引入新的 IT 技术，他们在使能网络功能的灵活性、可扩展性和快速部署的基础上，也给 5G 安全带来了新的挑战。

（1） 软件定义网络（Software Defined Network，SDN），

SDN 是一种新型网络创新架构，是网络虚拟化的一种实现方式。通过将网络设备的控制面与数据面分离开来，从而实现了网络流量的灵活控制，使网络作为管道变得更加智能，为核心网络及应用的创新提供了良好的平台。

（2） 网络功能虚拟化(Network Function Virtualization， NFV)

NFV 通过使用通用性硬件以及虚拟化技术，来承载很多功能的软件处理。从而降低网络昂贵的设备成本。可以通过软硬件解耦及功能抽象，使网络设备功能不再依赖于专用硬件，资源可以充分灵活共享，实现新业务的快速开发和部署，并基于实际业务需求进行自动部署、弹性伸缩、故障隔离和自愈等。

（3）移动边缘计算(mobile edge computing，简称 MEC)

MEC 利用无线接入网络就近提供电信用户 IT 所需服务和云端计算功能，而创造出一个具备高性能、低延迟与高带宽的电信级服务环境，加速网络中各项内容、服务及应用的快速下载，让消费者享有不间断的高质量网络体验。

（4） 网络切片

5G 网络建立网络切片，为不同业务提供差异化的安全服务，根据业务需求针对切片定制其安全保护机制，实现客户化的安全分级服务。

（5） 网络能力开放

5G 网络的能力开放功能可以部署于网络控制功能之上，以便网络服务和管理功能向第三方开放。5G 网络能力开放在促进移动互联网基础业务能力与第三方服务深度合作的同时，能够将网络业务从个人通信服务扩展到交通、工业、电力、金融等国家命脉行业，使得数据和信息从封闭平台扩展到开放平台。

1.4 5G 安全的重要性

5G 网络与 4G 相比，通过技术革新进一步提升了网络服务能力，将成为全面构筑经济社会发展的关键信息基础设施。5G 技术将为我们构建万物互联的美好未来，网络安全风险也随之渗入到生产和生活的方方面面，一旦发生网络安全攻击，其影响范围及所带来的后果也日趋严重，5G 的安全性显得格外重要。5G 网络所涉及的用户隐私保护、敏感数据安全、网络可用性健壮性等安全问题已经成为业界关注的重点。“网络安全与信息化是一体之双翼”，没有网络安全的保障，就没有 5G 信息化的未来。

在 5G 时代，商业流程会实现从人的连接扩展到物的连接。5G 网络包括网络功能虚拟化、边缘计算、5G 网络能力开放、异构接入和终端形态多样化、网络切片等新技术，这些技术将面临新型安全挑战，成为勒索软件和僵尸网络等复杂安全威胁的攻击目标。同时，5G 网络自身的开放性和支撑多业务场景的特性，使得 5G 系统自身的安全问题和业务应用的安全问题相互交融，这将主要给我们带来四个方面的安全挑战。包括：5G 网络自身安全、5G 业务应用安全、5G 数据安全、信息内容安全等。我们将在下一章中作详细介绍。

2. 5G 网络安全挑战

5G 技术将为我们构建万物互联的美好未来，网络安全风险也随之渗入到生产和生活的方方面面，让各类网络安全威胁有了可乘之机。值得注意的是，5G 网络自身的开放性和支撑多业务场景的特性，使得 5G 系统自身的安全问题和业务应用的安全问题相互交融，网络安全问题将更为错综复杂，这将主要带来四个方面的安全挑战。

2.1 系统安全

5G 网络自身引入了许多全新技术，使得 5G 网络不再是一个封闭的专有的通信网络。

（1）对多无线接入来说，需要统一的认证框架来解决 3GPP 体制和非 3GPP 体制接入的问题。比如无线 Wi-Fi 接入需要统一认证，在多接入环境下提供安全的运营网络。

（2）SDN 和 NFV 这样的技术引入，可以构建逻辑隔离的安全切片，用来支持不同应用场景差异化的需求。但这些技术的引入也对安全造成带来了巨大的挑战，由于它使网络边界变得十分模糊，以前依赖物理边界防护的安全机制难以得到应用。所以，安全机制要适应虚拟化、云化的需要。

（3） 5G 新的网络架构，把原来 4G 的物理网元进行了重新的分解和组合，通过服务和服务编排的方式来提高网络的功能，通过服务总线实现网元之间的逻辑接口。服务总线的开放能力和可兼容性使得网络具有很大的灵活性和可扩展性，可以支持不同的业务。但这对我们的安全设计也会带来新的挑战，我们也要适应这样的服务化、虚拟化、软件定义的变化，也就是说我们要提供安全即服务、软件定义的安全等能力。

（4）5G 网络切片技术的应用，使得切片之间以及切片内部的安全隔离和防护成为新的挑战。

（5）边缘节点自身的安全防护、用户数据和应用的管控等。

2.2 业务安全

5G 网络不仅仅是速率变得更高，时延变得更低，它将渗透到万物互联的各个领域，与工业控制、智慧交通紧密结合在一起。所以，安全就变得尤其重要。

ITU 为 5G 定义了三大应用场景，而每类场景都存在一些新的网络安全挑战。

（1）对 eMBB(增强移动宽带)来说，它的安全挑战需要更高的安全处理性能，这时候用户体验速率已经达到 1G，配套的网络安全技术手段性能和功能能否相匹配；二是它需要支持外部网络二次认证，能更好地与业务结合在一起；三是需要解决目前发现的已知漏洞的问题。

（2）对 mMTC (海量物联网)来说，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；需要通过群组认证机制，解决海量物联网设备认证时所带来的信令风暴的问题；需要抗 DDOS 攻击机制，应对由于设备安全能力不足被攻击者利用，而对网络基础设施发起攻击的危险。

（3）对 uRLLC(高可靠低延时连接)来说，需要提供低时延的安全算法和协议，要简化和优化原有安全上下文的交换、密钥管理等流程，支持边缘计算架构，支持隐私和关键数据的保护。

图 2-1 5G 业务场景安全

针对各个具体的 5G 应用场景，也有其特有的网络安全风险，如：车联网场景下，面临着车载操作系统安全、通信网络安全、信息服务平台安全、行驶数据安全等诸多关系交通安全的风险；工业互联网场景下，面临着细分场景多防护复杂、工控系统自身防护能力弱、互联互通导致网络攻击路径增多等可能引发关键工业设施瘫痪的风险；智能电网场景下，终端接入方式更加多样、网络结构更加复杂、边界更加模糊、数据聚合共享更加频繁，使得传统和新型安全风险聚集，存在引发大范围断电的风险；远程医疗场景下，智能医疗终端安全、网络信号的稳定性和可靠性、诊疗数据的安全保护等都蕴藏着跟患者生死攸关的安全风险。

2.3 数据安全

5G 是万物互联的时代，各类智慧城市、智慧家庭、个人辅助类的应用将使用海量的传感设备，室内室外、地上地下全方位的数据采集结合云计算和大数据技术，在给人们生活和城市管理带来便利的同时，也潜藏着巨大的数据安全和隐私保护挑战。万物互联之后个人隐私信息从封闭转为开放，接触状态从线下变为线上，用户的家电、生活用品等可能都会进入网络，会涉及到很多的用户隐私问题，数据泄露的风险也在加大。相比现有的相对封闭的移动通信系统来说，会面临更多的网络空间安全问题。比如 APT 攻击、DDOS、Worm 恶意软件攻击等，而且攻击会更加猛烈，规模更大，影响也会更大。

5G 网络不但需要解决前几代移动通信技术已有的如用户身份标识泄露等数据安全问题，而且需要满足 5G 时代各类应用场景下更高的用户隐私保护需求，各类 5G 应用也必须将数据安全作为一个非常重要的问题加以综合考虑。所以，"加大用户数据（在线数据及离线数据）的保护力度"是 5G 移动通信的迫切需求。我们需要严格控制主要数据的获取、传输、存储和处理等各个环节的可访问性，制定周全的隐私保护策略，以保护用户的身份、位置、接入服务等不被泄露。

2.4 内容安全

5G 的广泛应用，必将带来互联网生态的空前繁荣，从移动互联网向万物互联的物联网深入演化，信息内容的传播方式、传播速度都会有重大变化，给政府的信息安全管控带来挑战。

一方面，海量信息内容高速传播。5G 的高速率、低时延特性，使得串行方式信息安全管控技术手段难以为继；边缘计算和 D2D 终端直通技术的引入使得基于 IDC 为核心的内容源端管控手段成效甚微；视频、VR 等流媒体会逐步成为内容传播的重要途经，这一块完全做到同步监管难度较大，其监管技术复杂、成本高昂。

另一方面，新技术新业务层出不穷。5G 时代很多互联网业务没有确定的网站、移动应用，更多体现为随身穿戴的物品、智能家居、智能汽车、智慧校园、智慧城市、智慧工厂等等，隐藏在社会生活的每个角落；网络切片技术在增加了网络复杂度的同时也增加了监管的复杂度。因此业务形态的泛化带来互联网监管的困难。

因此，5G 网络内容安全管理在监测溯源的广度、难度和复杂度等方面都大幅提升。

（1）信息监测难度增加

新媒体的信息监测分析技术尚不成熟，对高码率音视频流量的实时监测、分析识别的难度加大；同时，终端在不同接入方式下切换，差异化的认证协议和安全机制加大了信息连续监测的难度；端到端加密通信的广泛应用也使得监测难度增大。

（2）信息源头治理难度增加

5G 网络环境下，发布信息的终端数量更多、形式更多样化、更隐蔽，给源头治理带来新的挑战；网络功能开给第三方，责任主体不明，也带来源头治理安全责任归属之争。

随着 5G 时代的到来，其高带宽、低时延、广连接的特性必将给我国互联网的治理和信息安全管控带来新的挑战，需要政府提前筹划、积极应对，避免“红旗法案”的出现。

3. 5G 网络安全架构

针对 5G 网络安全的挑战和风险进行深入的分析，我们需要研究相应的安全解决思路。5G 网络安全框架是将 5G 网络的安全需求分而治之的一种处理方式。

目前，4G 的安全框架无法完全地刻画 5G 的安全需求。首先，4G 的信任模型不适用于 5G，5G 引入新的利益相关者(如服务提供商和新型的设备)使得 4G 的信任模型不再完整；其次，虚拟化及其管理也并不存在于 4G 安全框架中，因而无法准确地展示新系统对虚拟化方面的安全需求；最后，垂直服务行业，尤其是涉及健康、交通、工业自动化控制等服务需要考虑新的安全威胁因素。

5G 安全框架涉及 5G 网络七个域的安全。在 4G 的安全框架的基础上，针对 5G 网络开放性与虚拟化的特点，引入了网络开放接口安全、切片与 VNF 安全；针对终端的高安全防护能力需求，引入了终端安全；针对移动边缘计算等新型移动服务方式，扩展了应用安全。

图 3-1 5G 网络安全架构图

表 3-1 5G 网络七个安全域

编号	安全域名称	安全域定义
1	接入安全	关注设备接入 5G 网络的安全性，主要目标是保证设备安全地接入网络以及用户数据在该段传输的安全性。

2	网络安全	保障网元之间信令和数据传输的安全性，包括接入网内部、核心网内部、接入网与核心网以及服务网络和归属环境(网络)之间的交互。
3	用户安全	关注终端设备与身份标识模块之间的双向认证安全，在用户接入网络之前确保设备以及用户身份标识模块的合法性以及用户身份的隐私安全等。
4	应用安全	保障用户设备上的应用与服务提供方之间通信的安全性。
5	可信安全	关注用户、移动网络运营商和基础设施提供商之间的信任问题，也包括用户根据不同的信任强度选择符合服务条款的安全措施(即安全机制可配置性的安全)和垂直服务将信任关系授权给第三方实体等。
6	终端安全	提升终端自身安全防护能力以及适配专用领域应用的安全
7	安全管理	在监测和分析的基础上为系统维护者提供全局的系统安全视角，包括安全上下文管理、密钥管理、内容安全和安全编排。

4. 5G 网络安全关键需求

随着 5G 网络架构的变化和应用场景的丰富，与传统通信网络相比，5G 所面临的安全问题和挑战也纷繁复杂，可根据上述 5G 安全框架归纳为以下几部分内容。

4.1 接入安全

接入控制在 5G 网络安全中扮演非常重要的角色，起到了保护频谱资源和通信资源的作用，也是为设备提供 5G 服务的前提。不同于 4G 同构的网络接入控制(即，通过统一的硬件 USIM 卡来实现网络接入认证)，5G 对各种异构接入技术和异构设备的支持使得 5G 的接入控制面临巨大的挑战。具体来说，5G 亟待解决的问题主要有：

4.1.1 构建统一的认证框架和层次化密钥

5G 时代要实现万物互联，5G 网络不仅用于人与人的通信，还用于人与物、物与物的通信，为此，5G 网络需要支持多样化的接入终端，多种接入类型和多种接入技术。

从终端类型看，分为有卡终端和无卡终端；从接入类型看，5G 网络需要支持 3GPP 接入，非 3GPP 接入，可信接入和非信任接入；从接入技术看，5G 网络除了支持 5G 新无线接入技术之外，还要兼容 3G 接入、LTE 接入、WLAN 和固定接入等技术。

因此 5G 网络是融合了多种类型的终端、接入类型和接入技术的异构型网络，而不同的终端，不同的接入类型和接入技术存在不同的安全需求，使用不同的认证协议和密钥协商机制，5G 网络需要研究构建统一的认证框架来融合不同的接入认证机制，满足具有不同安全能力的终端的安全接入需求，并建立统一的密钥体系。

4.1.2 满足不同应用场景的有效接入认证机制

未来 5G 网络需要支持三大类典型应用：增强移动宽带(eMBB)、海量机器类通信(mMTC)和超可靠低时延通信(uRLLC)。这三类应用场景根据各自的应用特性存在不同的接入安全需求。

(1) eMBB 应用的接入安全通过继承和扩展 LTE 的接入安全机制实现，主要针对 LTE 接入下用户首次接入时 IMSI 采用明文传送存在的安全风险，采取了 IMSI 加密传输的机制，再结

合 5G 网络架构，进一步增强了密钥派生机制来满足各接入层次安全传输的需要。

（2） mMTC 应用，需要研究包括简化认证机制，优化认证协议在内的满足 MTC 设备高效快速接入的轻量化安全接入方式。针对物联网传输的是小数据且是零星传送的数据特征，需要为小数据传送建立通道。如果小数据传送的无线网络缺少安全保护机制，攻击者就有可能通过访问小数据接口入侵网络，因此还需要研究针对小数据的空口传输安全保证机制。

（3）uRLLC 应用的接入安全，需要同时保证可靠性和低时延等业务性能，需要研究车联网通信时的身份认证、车辆身份信息的保护、数据传输安全等接入安全解决方案。

4.1.3 抗拒绝服务攻击

拒绝服务(denial-of-service，简称 DoS)攻击的目的是使网络资源被耗尽而无法提供正常的服务。在 5G 中，黑客如果利用海量物联网设备对网络发起分布式拒绝服务攻击，对网络造成的危害将比传统终端带来的危害更大。限制或阻止对资源的过度请求，可以一定程度避免 DoS 攻击；但另一方面，尽量减少每次请求对网络资源的消耗，也将是缓和 DoS 攻击的一种措施。如何避免 DoS 攻击，也将成为 5G 网络未来的一个重要研究内容。

4.2 网络安全

网络安全域最重要的问题就是网络切片安全。

网络切片体现了 5G 网络的灵活性，然而 5G 需要为网络切片提供持续的安全隔离机制，并能为用户或者基础设施运营商提供有效的隔离证明。因为一方面，由一个网络切片管理的敏感数据可能通过一些侧信道攻击被运行于另一个网络切片中的应用获得；另一方面，一个切片内部的错误和故障也会对其他切片产生影响。此外，网络功能在不同切片之间的共享，基础网络功能与第三方提供的网络功能在切片内的共存等都对安全提出了新的挑战。

网络切片需要提供不同切片实例之间的隔离机制，防止本切片内的资源被其他类型网络切片中网络节点非法访问。例如医疗切片网络中的病人，只希望被接入到本切片网络中的医生访问，而不希望被其他切片网络中的人访问。

相同业务类型的网络切片之间也存在隔离的需求，例如不同的企业的在使用相同业务类型的切片网络时，并不希望本企业内的服务资源被其他企业的网络切片节点访问。

服务、资源和数据在网络切片中被隔离保护的效果要达到接近于传统私有网一样用户感受，

这样才能使得用户能放心的将原本存放在私有网络中的应用数据存放到在云端，用户在享有随时随地可访问私有资源的同时不需要担忧这些资源的安全问题，这样才能促进各种垂直业务的健康快速发展。

当运营商根据业务的不同将网功能分割成不同的网络切片时，需要考虑是否进行切片内的认证和授权，以及如何进行切片内的认证和授权。当切片管理的某些功能开放给第三方时，还需要考虑哪些认证和授权功能可以开放给第三方，以及由运营商控制的主认证和授权与由第三方控制的二次认证和授权的融合机制。

4.3 用户安全

用户身份认证安全和用户隐私保护是用户安全域最重要的问题。

4.3.1 认证安全

认证/鉴别与授权主要包括以下方面的需求：

（1） 广泛网络实体的身份标识支持

在 5G 网络服务背景和物联网应用需求下，用户、机构、网络设备和资源、网络服务等不同种类的网络实体将大量接入，需要 5G 网络对不同类型的实体标识进行广泛的支持。需要定义网络实体的身份标识，以及制定相应的身份标识注册和查询机制。

（2） 海量网络实体接入的凭证支持

5G 网络服务需要为物联网提供海量实体身份凭证的支持，高效地进行凭证的生成和验证，并针对网络实体不同的安全能力与安全需求等级提供可靠的多级别凭证服务。

（3） 统一的网络实体身份鉴别

5G 网络中需要接入网络用户、网络设备及网络服务等多类网络实体，网络应用需要对各类实体进行有效身份鉴别。由于网络实体身份凭证的提供方、网络身份凭证类型和鉴别机制都不尽相同，为确保网络应用对于网络实体身份的高效、正确鉴别，5G 网络中需研究并提供统一的身份鉴别机制或服务，使得网络实体可以互通互认，同时在鉴别过程中有效保护网络用户隐私信息。

（4）多元实体间的安全资源授权管理

5G 网络中，网络实体的广泛接入，将引发网络应用、网络资源的大规模扩张，各类网络

应用互通协作也将越来越多，这将带来网络资源跨应用共享的迫切需求。需要通过有效的授权管理来保证网络应用可控、安全地访问特定网络用户网络资源，建立网络身份提供方和网络资源提供方等众多网络实体间的多元信任。

4.3.2 用户隐私保护

5G 网络需要为不同业务场景提供差异化安全服务，能够适应多种网络接入方式及新型网络架构。这些新场景、新架构和新技术都让 5G 网络有了更高的隐私保护需求。另外，5G 网络针对垂直行业用户会产生大量的敏感信息。迫切需要在 5G 开放网络环境之上，采取措施保证行业用户的隐私安全。

uRLLC 作为 5G 网络典型应用场景广泛应用于车联网自动驾驶及远程工业控制领域。在自动驾驶过程中，车辆的身份信息、位置信息存在被暴露和跟踪的风险，这些隐私信息一旦被泄露，产生的后果是非常严重。mMTC 和 eMBB 场景使得 5G 网络中的业务信息会以几何级别增长。这些信息包含针对某个网络实体的不同测度的描述。通过对这些海量数据的分析，网络用户的隐私信息可能会被泄漏。例如，黑客可能获取某用户的部分移动电话数据、运动手环数据、部分 APP 的消费数据、位置信息数据等等多方面的信息之后，通过对这些数据的分析获取某人特定的隐私信息。在 5G 场景下，如何实现对隐私数据的分级，提高抵抗大数据攻击的隐私保护的能力将会成为一个亟待解决的问题。

5G 网络作为一个复杂的生态系统，存在基础设施提供商、移动通信网络运营商、虚拟运营商等多种类型参与方，用户数据在这个由多种接入技术、多层网络、多种设备和多个参与方交互的复杂网络中存储、传输和处理，面临着诸多隐私泄露的风险。另外，5G 网络中大量引入虚拟化技术，在带来灵活性的同时也使得网络安全边界更加的模糊，在多租户共享计算资源的情况下，用户的隐私数据更容易受到攻击和泄露。相比传统网络而言，这种情况所产生的隐私泄露影响范围更广、危害更大。因此，对 5G 网络的隐私保护提出了更高的挑战。

当前 4G 网络中，系统已经使用临时签约标识符来增强用户的隐私，降低签约数据通过偷听无线链路的方式被识别和跟踪的可能性。但现有 4G 网络也暴露了一些隐私问题需要解决，比如用户的长期身份标识(International Mobile Subscriber Identification，简称 IMSI)泄露问题以及位置信息的泄露问题。IMSI 的泄露会直接导致用户身份信息的泄露。因此，在 5G 网络设计之初，需要充分考虑现有 4G 网络中的隐私漏洞，增加适合 5G 网络的安全措施和协议来

弥补之前网络的隐私漏洞，保护用户的身份信息和位置信息。

4.4 应用安全

与前几代移动通信网络不同，5G 支持海量物联网设备连接，但物联网设备通常频繁地发送小数据包，这势必造成接入网与核心网之间信令的频繁交互，从而消耗网络带宽，造成传输效率下降。5G 需要确保小数据的通信安全，针对机器类终端进行高效的连接设计，在满足小数据信令和数据包传输需求的基础上，确保信令和数据传输的安全性，如隐私保护和完整性保护。

4.4.1 移动边缘计算(Mobile Edge Computing，MEC)

MEC 技术，是在移动网边缘提供 IT 服务环境和云计算能力的技术。MEC 技术的核心思想是：将对带宽和时延要求严格的业务数据的计算、处理和存储推向无线侧，以减少网络操作和服务交付的时延消耗，提高用户的使用体验。解决现阶段 MEC 技术引入带来的安全部署问题，可实现从 4G 到 5G 的平滑过渡。具体安全需求如下：

（1） 物理设施保护

MEC 按需临近部署的特点在客观上缩短了攻击者与 MEC 物理设施之间的距离，使得攻击者更有可能接触 MEC 物理设施，造成 MEC 物理设备毁坏、服务中断、用户隐私和数据泄露等严重后果。另一方面，广泛部署的 MEC 边缘计算节点同样面临着各种自然灾害 (如台风、冰雹) 和工业灾难的威胁。以上因素都可能直接破坏 MEC 硬件基础设施，造成服务的突然中断以及数据的意外丢失。因此需要在考虑性能和成本的基础上最大限度为 MEC 节点配备相应的物理设施保护措施。

（2）安全能力受限下的 MEC 节点安全防护

由于性能、成本、部署灵活性要求等多种因素制约，单个 MEC 节点的安全防护能力受到限制。因此需要针对 MEC 节点应用特征及终端特征，有的放矢地部署相应的安全防护措施；充分利用 MEC 节点的高可协作特性，通过例如基于智能协同的安全防护等技术，借助周边节点的空闲安全防护资源，提升单个节点能抵御的攻击强度上限。

（3）扩展信任模型构建

MEC 系统与移动通信系统共生融合的部署方式，扩充了以往的“用户分别跟网络和服务进

行认证”的二元信任关系构建模型。需要构建用户、MEC 系统、MEC 应用、移动通信网络两两之间，以及 MEC 系统内部的信任关系。

（4） 隐私及数据保

MEC 在提供便利的同时，也让 MEC 应用不可避免的接触到大量移动用户与设备的隐私和数据信息，如用户身份、位置、移动轨迹等。因此，在 MEC 隐私及数据保护中，需要配备相应的隐私泄漏防护措施，严控第三方 MEC 应用的行为；需要通过动态身份标识和匿名等技术削弱 MEC 计算节点标识和地理位置的映射关系；需要确保数据在边缘的安全存储；需要向用户提供隐私及数据管理服务，确保隐私策略用户可适配。

4.4.2 数据完整性和机密性

在 5G 网络中无线空中接口仍然存在窃听、篡改等安全威胁。在接入网存在的安全问题主要来自无线的空中接口。空中接口的信息是在无线信道上传输的，入侵者容易捕获手机终端或基站的无线信号，从而非法取得或篡改用户和网络发送的信息。

4.5 可信安全

作为普适性的全连接网络，5G 将比上一代网络更加开放，而网络能力开放需要相应安全保障。更进一步，可以将安全能力（同网络能力一样），通过 API 接口，开放给垂直行业使用。第三方业务，可以直接安全的部署业务，从而降低了业务门槛，并缩短了部署时间。运营商可以充分利用网络安全基础设施，丰富业务经验，与垂直行业一起共同创造和分享价值。

5G 网络为了优化用户体验、提供新型商业模式，将向大量第三方应用开放网络，借此实现网络和第三方应用的互动，并优化网络资源配置。首先,5G 将提供一些网络功能如移动性、会话、QoS 和计费等功能的接口，方便第三方应用独立完成网络基本功能。此外，5G 还将开放 MANO(管理和编排)，让第三方服务提供者可以独立实现网络部署、更新和扩容等网络编排能力，最终实现动态地定制网络。以上面向第三方开放的能力都是 5G 网络的基本功能，如果在开放授权过程中出现信任问题，则恶意第三方将通过获得的网络操控能力对整个 5G 网络发起攻击。此外。随着用户(设备)种类增多、网络虚拟化技术的引入，用户、移动网络运营商和基础设施提供商之间的信任问题也比以前的网络更加复杂。

4.6 终端安全

从 3G 网络引入到 4G LTE 盛行，移动终端日益成为黑客攻击的主要目标。由于缺乏有效的安全设计，终端安全只能完全依靠终端厂家自行维护，移动终端安全技术发展缓慢，很快就成为用户隐私泄露的重灾区。

5G 网络的安全体系需要由移动终端侧和网络侧配合共同完成，无论是控制面还是用户面都少不了移动终端的安全配合。从信息流向来看，移动终端既是用户信息和隐私数据的源头也是其归宿；从网络切片来看，移动终端是网络安全切片的实现起点也是实现终点；从垂直行业来看，5G 网络的一大特征就是对垂直行业的深度支持，垂直行业存在着多样化的安全要求，其安全能力更是需要移动终端的支持。因此，移动终端安全是 5G 网络安全体系中不可缺少的一环。它涉及到硬件层、操作系统层以及应用层等多个层面的问题，威胁因素主要来自外部网络。

解决终端安全问题，首先要从多个层面提升终端自身抵御攻击的免疫能力，同时也要对外部网络如网络接入、应用服务等进行安全增强，引入基于云的安全增强机制来为终端安全提供辅助支撑。5G 移动终端安全的需要主要从以下两个方面进行阐述：

4.6.1 行业用户共性的安全需求

5G 网络引入了垂直行业作为新的利益相关方，因此 5G 终端安全需要考虑针对不同行业用户群体的安全需求。包括：可信执行环境、统一的安全体系、标准化的安全接口。

4.6.2 三种电信应用场景的安全需求

5G 网络明确了三种典型应用场景，带来 eMBB、mMTC、uRLLC 三种典型终端，因此 5G 终端安全需要考虑针对不同应用终端的安全需求。

（1） eMBB 终端安全需求

eMBB 终端的典型安全需求主要有三个方面，一是要具备与 5G 网络速率相适配的高速率加密能力，同时还具备较低的功耗要求；二是对普通用户具备对个人信息或标识以及地址信息等等隐私信息的保护能力，对行业用户具高等级的认证、端到端加密、信息完整性保护等能力；三是具备异构接入的统一认证和安全上下文管理能力，提高异构接入安全上下文切换效率。

（2） mMTC 终端安全需求

mMTC 终端的典型安全需求包括：一是轻量级的密码算法和协议，满足 mMTC 终端的低功耗、低带宽要求；二是安全可靠的网络接入模式，如 5G 网络提供为物联终端提供去中心化的身份管理和接入认证模式，包括缩短认证链条、快速安全接入、网络与业务融合分层身份管理等，降低管理复杂度；三是低成本的设备认证和身份管理实现，满足物联终端低成本要求。

（3）uRLLC 终端安全需求

uRLLC 终端的典型安全需求包括：一是高安全等级的保护强度，具备高等级的认证、端到端加密、信息完整性保护等能力；二是超高可靠和超低时延的能力，在不降低安全保护强度的前提下，支持认证节点下移，简化认证框架与协议，提高移动性安全上下文迁移和密钥重建机制效率，采用高效密码算法，减少加解密处理时间。

4.7 安全管理

4.7.1 安全上下文

安全上下文(security context)是网络为设备建立的临时状态信息，其中包括密钥信息和数据承载信息，目的是减少设备在不同状态之间切换时与网络进行相互认证的资源消耗，方便设备快速从空闲状态安全切换到连接状态并安全通信。5G 中，设备移动、设备在不同接入网之间切换均需要考虑安全上下文的迁移和管理，迁移过程中，不同的网络对密码算法的支持情况也不同，涉及算法的重协商、上下文的标识和存储安全。此外，小数据通信模式下，安全上下文受限于设备的计算能力，也需要全新的处理方式。

4.7.2 安全编排

编排是通过一个中心控制节点来协同业务流程中的各种事件/活动，以达到控制总体的作用。编排的特点是服务可以连接服务，即一个服务的输出可作为另一个服务的输入，因此能实现服务组合，创造出新的业务模型，最终满足不断变化的市场和用户需求。5G 在关键技术 SDN 和网络切片中大量使用编排来灵活地提供服务。管理和编排过程复杂，最基本的安全需求是保证各服务之间共享资源的关联性和一致性。此外，编排决定了网络/特定服务的拓扑结构，编排本身将决定在何处部署安全机制和安全策略。5G 系统需要在编排过程中提供足够的安全保证。

4.7.3 证书管理

5G 将引入公钥基础设施(public key infrastructure，简称 PKI)来加强用户身份的机密性保护以及网络各节点之间的相互认证。PKI 的引入使得系统必须维护庞大的 CA 系统，一方面对 CA 容量要求高;另一方面，将面临一系列证书管理的开销，如大量并发的证书申请、证书更新、证书撤销等操作。因此，5G 必须加快促进 CA 技术的发展，并将其高效地部署在 5G 系统中。此外，5G 也面临着 PKI 升级换代所带来的安全挑战和影响。

4.7.4 内容安全

5G 的广泛应用，必然带来互联网生态的空前繁荣，从移动互联网向万物互联的物联网深入演进，信息内容的传播方式、传播速度都会有重大变化，必将给我国互联网的治理和信息安全管控带来新的挑战，需要政府提前筹划、积极应对，避免“红旗法案”的出现。

5. 5G 安全技术保障

5.1 统一安全认证框架

5G 网络支持多种应用场景，不同的应用场景使用不同类型的终端，采用不同的接入技术。为了使用户可以在不同接入网间实现无缝切换，5G 网络需要一个统一的认证框架，实现灵活并且高效地支持多种接入方式和接入凭证，从而保证终端的合法接入，为终端和网络提供接入安全。

可扩展认证协议(Extensible Authentication Protocol，简称 EAP)认证框架，是能满足 5G 统一认证需求的备选方案之一。框架适用于任何类型的订阅者以任何一种 3GPP 定义的接入技术(包括 3G,4G)和非 3GPP 定义的接入技术(包括 WiFi、WiMAX)进行接入网认证。

EAP 认证框架，是一种支持多种认证方法的三方认证框架，框架本身不提供任何安全性，只规定了消息的封装格式，具体的安全目标依赖于使用的认证方法。目前，EAP 支持的认证方法有 EAP-MD5、EAP-OTP、EAP-GTC、EAP-TLS、EAP-SIM 和 EAP-AKA，还包括一些厂商提供的方法和新的建议。在 5G 中，具体的 EAP 协议运行于 UE，AUSF(相当于后端服务器)和 SEAF(相当于前端认证器)之间。

在 5G 统一认证框架里，各种接入方式均可在 EAP 框架下接入 5G 核心网：用户通过 WLAN 接入时可使用 EAP-AKA' 认证，有线接入时可采用 IEEE 802.1x 认证，5G 新空口接入时可使用 EAP-AKA 认证。不同的接入网使用在逻辑功能上统一的 AMF 和 AUSF/ARPF 提供认证服务，基于此，用户在不同接入网间进行无缝切换成为可能。5G 网络的安全架构明显有别于以前移动网络的安全架构。统一认证框架的引入不仅能降低运营商的投资和运营成本，也为将来 5G 网络提供新业务时对用户的认证打下坚实的基础。

5.2 满足海量终端设备接入的认证方案

物联网中存在大量的终端需要接入网络，这些终端通常为低功耗资源受限设备，如果采用传统接入认证机制接受海量物联网终端并发接入网络，则极容易产生信令风暴，造成网络拥塞。针对该问题，研究对传统认证机制进行局部优化来满足海量终端接入网络的要求。

（1）采用聚合认证方式优化网络信令开销

该方案通过在近用户端部署消息聚合设备，例如信令聚合设备部署于无线接入网络域，配合认证设备（接入认证点、认证服务器）完成对 MTC 终端接入网络的接入认证。

消息聚合设备接收海量 MTC 终端发送的消息，对每个终端的信令消息进行解析，并按照一定的策略进行消息聚合处理，例如将同为接入请求的消息进行解析，提取必要用户信息后，合并为一条接入请求消息。聚合设备将聚合消息发送给接入认证点和认证服务器。认证服务器根据接收的消息，完成对消息中包含的所有用户的认证批处理，例如向签约信息服务器获取对应用户的聚合认证向量。认证服务器将认证结果返回给聚合设备，聚合设备进行消息解析，并将认证结果返回给每个 MTC 终端。聚合认证方式大大降低了信令开销，从而减轻认证设备的处理负担以及网络中的传输流量。

（2）采用群组认证方式优化网络信令开销

该方案对海量 MTC 终端进行分组，为每组用户设立群组网关负责组内 MTC 终端的接入认证。群组用户接入网络的前提是群组网关首先接入网络。群组网关接入网络发起认证时，签约信息服务器接收到群组网关的接入认证参数请求，此时根据组签约信息，签约信息服务器需要为群组网关接入产生认证向量，同时还要为组内所有用户产生认证向量，并将群组认证向量（包含网关认证向量和组用户认证向量）返回给认证服务器。在群组网关接入认证成功之后，认证服务器将对应的组用户认证向量发送给群组网关保存。后续当组内用户接入网络发起认证时，由群组网关作为认证代理，完成对组用户的接入认证。MTC 终端的认证直接和群组网关交互完成，而不需要另外和接入认证点、认证服务器、签约信息服务器等进行信令交互。

5.3 基于标识的切片安全隔离

网络切片是 5G 的重要组件，它使得运营商可以根据不同的市场情景和丰富的需求定制网络，以提供最优的服务。一个网络切片是一系列为特定场景提供通信服务的网络功能的逻辑组合。网络切片本身是一种网络虚拟化技术，因此，不同切片的隔离是切片网络的基本要求。

切片的隔离最先要考虑的是在切片的生成阶段。一个切片可以横跨多个子域:如终端、接入网、核心网、承载网等，各个子域的隔离都需要考虑，并进行资源的统筹安排，以达到一致的、端到端的隔离要求。其次，在实际业务运行时，终端与切片网络的网元交互、安全协议、流程，都需要考虑到相应的隔离

为了实现切片隔离，每个切片被预先配置一个切片 ID，同时，符合网络规范条件的切片安全规则被存放于切片安全服务器(Slice Security Server，简称 SSS)中，用户设备(User Equipment，简称 UE)在附着网络时需要提供切片 ID，附着请求到达归属服务器(Home Subscriber Serve，简称 HSS)时，由 HSS 根据 SSS 中对应切片的安全配置采取与该切片 ID 对应的安全措施，并选择对应的安全算法，再据此创建 UE 的认证矢量，该认证矢量的计算将绑定切片 ID。通过以上步骤，来实现切片之间的安全隔离。网络切片本身是一个复杂的系统，切片之间由于共享基础设施或共同协作实现更高级别的功能，使得切片之间的通信安全也至关重要。目前对这个问题的研究仍然处于初级阶段，随着 5G 网络架构的不断完善，这个问题在未来的研究中必将得到合理的解决。

5G 网络可以通过网络切片实现不同安全等级的网络，实现按需组网，安全分级，即通过按需组网、安全分级的网络切片安全关键技术，根据业务场景和业务需求实现切片的安全隔离，采用不同的安全机制实现不同的安全等级，实现终端的接入认证和鉴权和切片间的通信安全，实现 5G 网络的按需组网和安全分级。

5.4 差异化的隐私保护机制

5G 网络上面承载着很多用户的隐私和敏感信息，不同用户、不同业务场景对隐私保护的需求不尽相同，因此需要针对不同的用户和业务场景采用不同技术措施解决 5G 网络的隐私保护问题。另外，根据隐私数据在 5G 网络中的实际使用情况，从数据采集传输、数据脱敏、数据加密、安全基线建立、数据发布保护等方面采用不同技术措施保证数据的隐私安全。5G 网络中隐私保护所采用的主要技术措施有：

（1）数据加密技术

数据加密是 5G 网络中保证数据隐私安全的最有效手段之一，也是最常见技术手段之一。按照实现思路，可以将其划分为静态加密技术和动态加密技术。从实现的层次上，可以分为存储加密、链路层加密、网络层加密、传输层加密等。采用加密技术可以有效保证 5G 网络隐私数据的机密性、完整性和可用性。针对 5G 网络虚拟化和云化的新特点，可以引入一些新的加密技术来保证数据的隐私安全。比如同态加密技术，该技术提供了一种对加密数据进行处理的功能。同态加密技术对加密的数据处理得到输出，将这一输出进行解密，其结果与用同一方法处理未加密的原始数据得到的结果相同。

（2）基于限制发布的隐私保护技术

限制发布技术即是有选择地发布原始数据、不发布或者发布精度较低的敏感数据，以实现隐私保护。当前此类技术的研究集中于数据匿名化：即在隐私披露风险和数据精度间进行折中，有选择地发布敏感数据及可能披露敏感数据的信息，但保证对敏感数据及隐私的披露风险在可容忍范围内。目前，比较成熟的匿名化技术有 k-anonymity（k-匿名化）,l-diversity（l-多样化）,t-closeness（t-贴近性）技术等。

（3）访问控制技术

访问控制技术也是 5G 网络隐私保护采用的最常用技术手段之一。访问控制可以通过策略和技术手段保证隐私数据不被非法使用和窃取。传统的访问控制技术包括用户口令、数字证书、USB KEY、生物识别技术等。这些技术同样可以应用到 5G 网络之中。另外，针对 5G 网络功能实体的协议交互流程处理中的隐私安全，可采用基于规则、流程的访问控制技术，使得攻击者无法通过假冒合法用户访问用户数据库的方式窃取用户隐私信息。

（4）虚拟存储和传输保护技术

为保证隐私信息在 5G 虚拟化网络存储过程中的隐私安全，可采用用户数据库的动态迁移和随机化存储技术。动态迁移技术可以在保证虚拟机上服务正常运行的同时，将一个虚拟机的数据从一个物理主机迁移到另一个物理主机的过程。这使得攻击者即使成功入侵用户数据库也无法锁定要窃取的用户数据。隐私信息在 5G 网络传递过程中的隐私安全，可以根据 5G 网络传输协议交互流程，采用相关信息的动态关联和协同重组技术，使得攻击者无法通过数据挖掘技术从散布的用户数据中分析出有价值的用户隐私信息。

（5）5G 网络隐私增强技术

目前，5G 网络隐私增强技术研究的重点主要集中在使用非对称密钥加密的方法来加密 5G 网络的永久标识符（IMSI），或是使用伪 IMSI 的方法来隐藏用户的永久标识符。这两种方法都可以有效的防止用户签约身份信息的泄露。同时，由于有效保护了用户的身份隐私，所以即使攻击者得到了用户的位置信息，也不知道对应于这个位置的身份是谁，通过这样保护用户身份的方法间接地也保护了用户的位置隐私。

5.5 移动边缘计算安全机制

针对 MEC 系统的特殊安全需求，在传统安全机制的基础上，设计了 MEC 边缘节点硬件设施保护、MEC 系统隐私泄露防护、MEC 三元认证与鉴权方案。其中 MEC 边缘节点硬件设施保护方案针对物理设施防护的安全需求，旨在消除边缘节点暴露的硬件基础设施带来的安全威胁；MEC 系统隐私泄露防护方案针对隐私与数据保护的安全需求，通过管控运行于 MEC 系统中的第三方应用阻止隐私信息流出；而 MEC 三元认证与鉴权方案针对认证、鉴权与权限管理的安全需求，主要解决服务下沉至网络边缘带来的实体间互认证和权限分配问题。

（1）MEC 边缘节点硬件设施保护

MEC 硬件设施保护方案的基本策略为“尽力保护，按需备份”。“尽力保护”指采取一切可行的措施降低 MEC 边缘节点硬件基础设施被破坏的可能。由于 MEC 服务被下沉至网络边缘客观上缩短了其与攻击者之间的物理距离，“尽力保护”的首要目标在于减小攻击者接触到 MEC 边缘节点硬件基础设施的机会。另一目标在于降低恶劣环境破坏 MEC 边缘节点硬件基础设施的风险。为此必须强化边缘节点硬件基础设施的防火、防水、防尘、防辐射能力，采用耐高温、防水的线缆、材料和防护外壳制作高尘密水密等级的 MEC 边缘节点服务器设备。

（2）MEC 系统隐私泄露防护

为了向用户提供精准服务，MEC 系统将不可避免的接触到大量移动用户与设备的隐私信息，如用户身份、位置、移动轨迹等。因此，MEC 隐私保护的关键在于保证用户隐私信息不通过 MEC 系统任意泄露。

第三方 MEC 应用获得用户隐私信息途径有两种：直接通过终端客户端获取、通过 MEC 基础平台的 5G 标准开放服务获取。为了应对第三方 MEC 应用泄露、滥用用户隐私信息的问题，MEC 节点与 MEC 控制器应协同工作增强 MEC 系统的隐私保护，其特点在于：

- 隐私保护策略可适配

用于限制 MEC 应用行为的隐私保护策略可由用户制定或由 MEC 系统适配。隐私保护策略需同时满足隐私信息的安全需求与应用的基本服务要求。

- MEC 节点监控应用行为

考虑到 MEC 低时延的特性，服务提供方提前根据可能的安全策略构造应用并提供给 MEC 系统。接收到用户发布或自主生成的安全策略后，MEC 系统检索与之匹配的应用，同时在 MEC

节点配置相应的虚拟环境。符合安全策略的应用在 MEC 节点的专用虚拟环境中实例化。MEC 节点通过多种措施监控 MEC 应用的行为。

- MEC 控制器管控应用与第三方通信

MEC 应用与外界的通信将由 MEC 控制器进行统一的代理与监管。MEC 控制器代理服务提供方或连接应用的请求，使服务提供方无法直接连接到运行于边缘节点上应用。同时，MEC 控制器负责监管应用发往外界的全部通信，过滤所有数据流中的隐私信息，阻止其流向非法第三方。

（3）MEC 三元认证与鉴权

为保障基本的安全和服务，MEC 系统必须为各实体分配身份，并实现所有实体间的互认证。MEC 通用场景中的相关实体包括隶属于运营商的 MEC 系统（以下称 MEC 系统），第三方提供的 MEC 应用（以下称应用），以及 MEC 用户使用的用户设备（以下称用户），三者构成了 MEC 基本的三元信任模型。其中信任闭环建立的关键在于用户与应用、MEC 系统与应用间的互认证。除此之外，在三元信任模型内部，MEC 系统由 MEC 控制器与 MEC 节点组成，为防止“伪节点”的出现，需由 MEC 控制器对每个新加入的节点进行认证。而在三元模型外部，5G 网络也要对 MEC 系统进行认证。

同时，在资源配置的过程中，移动边缘协调器分别 MEC 节点和用户进行鉴权，面向不同权限的节点和用户选择性地开放部分服务。MEC 节点进一步对运行于其上的 MEC 应用进行鉴权，开放相应的服务给每个不同的应用。

5.6 数据完整性和机密性安全机制

为了应对网络面临的窃听、篡改等安全威胁，5G 网络在移动终端和网络设备之间提供数据完整性和机密性保护，为用户提供 5G 网络安全保障。

5G 网络数据保护体现为用户面和数据面的数据完整性和机密性保护。目前 5G 网络用户面数据保护终结点为基站，即提供移动终端到基站之间的用户面数据完整性和机密性保护。5G 网络信令面数据保护终结点为基站和核心网，即同时提供移动终端到基站之间的信令面数据完整性和机密性保护、移动终端到核心网之间的信令面数据完整性和机密性保护。

为了应对 5G 网络域内和不同网络域之间的信息安全问题，5G 网络域内和不同网络域之间一般采用 IPSec 对传输的数据进行完整性和机密性保护。对于边界保护采用划分安全域的方式，

在安全域的边界进行保护。

为了进一步保证行业的业务应用安全性，也可在终端的应用层增加端到端的数据保护，对传输的数据进行完整性和机密性保护。

5.7 开放的安全能力

将移动网络的强大的安全功能开放给垂直行业，有利于满足垂直行业的网络及业务的安全需求。当然，需要以受控的方式进行网络安全能力开放，这样才不会危及运营商， 确保运营商网络自身的运营能力。

业务开放带来安全挑战的同时，也给运营商安全业务带来了更广泛的机会。作为 5G 连接基础设施平台的提供者和运营者， 电信运营商是业务提供商的最佳使能者，是行业客户可信任的商业伙伴。

垂直行业可以直接使用运营商开放的安全能力，降低了一些新型垂直行业的业务门槛和成本，并缩短上市时间。通过安全 能力开放，运营商可以盘活网络资产和基础设施，开创新的利益增长点;可以打破管道化运营和封闭网络模式，以电信网络为中心构建安全生态系统;提升差异化竞争力，并形成运营商、垂直行业、安全厂商、个人用户的生态链，合作共赢共创商业价值。

安全能力开放要求 5G 网络内的安全功能以模块化的方式部署，并能够通过相应接口方便调用。通过组合不同的安全功能， 可以快速提供安全能力以满足多种业务的端到端安全需求。通过安全能力开放，垂直行业可以直接安全地部署业务，从而 降低了业务门槛并缩短部署时间。运营商则可以充分利用网络安全基础设施，丰富业务体验，与垂直行业一起共同创造和 分享价值。这里安全功能或能力可以包括用户身份管理、认证鉴权，密钥管理及安全上下文的管理等等。

5.8 终端安全体系结构

在终端安全体系中，密码是其核心支撑技术。密码技术与终端的不同结合方式，带来两种不同的安全体系结构，这两种体系结构各有其鲜明的特点。

（1）物理门卫式体系结构

红黑隔离的物理门卫式安全体系架构，是在终端内部的信息通路上物理地串接密码处理部件，形成物理流过式的密码安全处理，实现安全数据所在的“红区”与非安全数据所在的“黑

区”隔离的安全架构。该架构具有以下三个特点：一是可确保在“红区”没有任何来自“黑区”的非安全数据；二是可为“红区”阻拦来自“黑区”的所有已知和未知网络攻击，包括零日漏洞攻击等；三是该架构的安全性易于证明，能够适用民用安全、商用安全、特殊安全等多种使用场景。

（2）逻辑门卫式体系结构

逻辑门卫式体系结构，是指在终端内部的信息处理通路上，通过系统软件调用安全模块的方式，实现对信息的保护和执行环境的保护。从执行环境的安全启动、操作系统加固、运行时动态度量到信息的传输加密、存储加密、应用安全、输入/输出控制等功能，采用分层、组合的方式调用安全模块，达到逻辑门卫式的安全防护效果。逻辑门卫式体系结构可根据行业安全需求或业务类型安全需求，按需部署相应的安全保护机制，为不同行业或业务提供差异化安全服务。

5.9 丰富的密钥层级架构

5G 的密钥层次考虑的是如何利用一个根密钥为不同层面，不同类型的消息流提供多个相互独立的密钥的问题。因此，在 5G 的密钥层次中，需要考虑：不同的接入方式、移动性管理与会话管理的分离、核心网与接入网的分离、加密与完整性、由移动性引入的密钥更新与隔离、密钥之间的相互独立性。

此外，未来 5G 需要考虑大规模物联网终端接入、超低时延超高可靠性等场景，以及并可能出现用户凭证使用非对称密钥的情况。未来 5G 的密钥体系也可能随着这些场景与用户凭证的变化而发生变化。

通过丰富的密钥层级架构，5G 系统可以提供核心网控制面（即非接入层）的机密性、完整性密钥，还可以提供无线网（即接入层）控制面的机密性、完整性密钥，用户面的机密性和可选的完整性密钥，以及用来支持不同需求的密钥。

（1）支持新空口

目前，5G 将空口安全的终结点放在接入网内，而针对切片的安全留待将来解决，因此目前的核心网与接入网的密钥主要考虑面向 MM 移动性管理的安全密钥衍生。

（2）支持非 3GPP 无线接入网

考虑到其他接入方式，还引入了 3GPP 之外的其他接入网的密钥：因此，密钥层次中针对

现有 3GPP 无线网络和 non-3GPP 无线网络均产生独立的密钥。

（3）适应网络切片

每个切片中必须有一个 SMF 会话管理服务尚未成为共识，因为一直以来核心网都被认为是可信的，而核心网切片之间通过虚拟化技术实现了资源的隔离；到各个切片的信令，由可信的 AMF 来进行转发，且 AMF 和 SMF 之间是安全链路，所以可认为是 AMF 与各个切片的 SMF 之间是安全的，所以在虚拟化技术做好切片间隔离的前提下，并不需要单独的 SM 密钥来保护 NAS SM。

（4）向后兼容 SEAE/LTE

目前 5G 密钥衍生是基于有共享 K 的前提，以 LTE 的密钥层次作为基础，考虑了 5G 会引入多种认证机制，考虑所有密钥是否需要以及密钥如何衍生。接入层密钥可以直接由 SEAF 进行推衍而非接入层机密性与完整性保护密钥不能像 4G 那样直接由 SEAF 进行推衍。

（5）隔离接入层与非接入层

此外，针对攻击者通过核心网攻击获取接入层的密钥参数的情况，有一些隔离接入层与非接入层的密钥体系被提出。其设计思想是：通过与无线链路相关的、不需要分发的物理层密钥，使得终端和接入点能够不依赖核心网，独立产生并更新与无线链路、节点强相关性的加密和完整性保护密钥作为接入层密钥；而终端和核心网协商使用与身份信息强相关的加密和完整性保护密钥作为非接入层密钥；接入层密钥的更新过程与非接入层密钥的更新过程完全独立；接入层密钥根据无线通信信道特征的变化随时更新。

6. 5G 安全综合管理策略

6.1 构建 5G 安全保障体系

5G 网络安全保障体系设计的总体思路，是针对 5G 网络防护对象，通过 5G 网络安全治理组织体系的建立，逐步实现 5G 风险识别能力、安全防御能力、安全检测能力、安全响应能力与安全恢复能力，最终实现风险可见化，防御主动化，运行自动化的安全目标，保障 5G 网络的安全。

5G 网络安全保障体系框架的设计，这里我们参考了 NIST Cybersecurity Framework 的 IPDRR 模型。该模型包括风险识别（Identify）、安全防御（Protect）、安全检测（Detect）、安全响应（Response）和安全恢复（Recovery）五大能力。IPDRR 的模型框架实现了“事前、事中、事后”的全过程覆盖，从原来以防护能力为核心的模型，转向以检测能力为核心的模型，支撑识别、预防、发现、响应等，变被动为主动，直至自适应（Adaptive）的安全能力。

图 6-1 5G 网络安全保障体系框架

（1）识别防护体系

识别防护体系包含：风险识别和安全防御，即识别 5G 相关的系统、资产、数据的网络安全风险，并制度和实施适当的安全措施，以确保 5G 的稳定运行。

（2）监测处置体系

监测处置体系包含：安全检测和安全响应。，即制度并实施适当的活动，来识别 5G 网络安

全事件的发生，并对检测到的 5G 网络安全事件采取行动。

（3）灾备恢复体系

灾备恢复体系指制定并实施适当的活动，以保持计划的弹性，并恢复由于 5G 网络安全事件而受损的任何功能或服务。

6.2 5G 网络安全三道防线

在 5G 网络安全保障组织架构方面，我们建议采用三道防线治理架构，从多角度保障 5G 网络的安全性。建立基于三道防线的组织架构来推进 5G 网络安全治理工作，一方面从组织机制上解决利益冲突问题，避免一线设备厂商为了 5G 产品和服务的市场进度，而牺牲安全要求的风险；另一方面遵循风险控制的原则，通过 5G 设备厂商的自我检查、基础电信运营企业和业务应用企业的独立安全监测、行业主管部门的安全审计，从多个角度和多个层次保障产品的安全性。

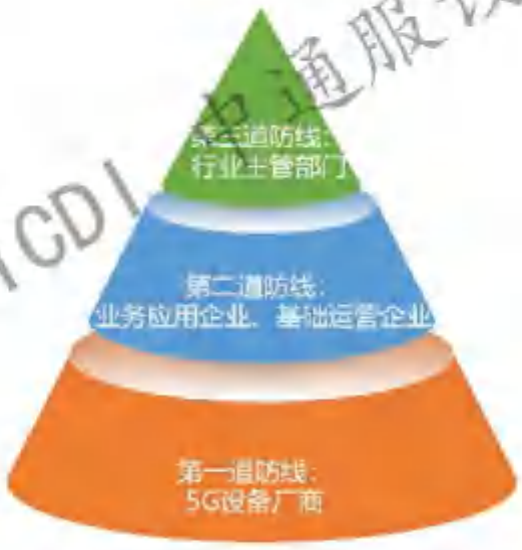

图 6-2 5G 网络安全治理组织架构图

（1）5G 设备厂商，作为第一道防线实现 5G 设备安全性的自我管控。

各 5G 设备厂商通过设备侧异常状态数据接口，对各类 5G 设备吞吐量、会话数、系统负荷等实时运行状态数据进行监测与分析，建立 5G 网络设备安全的自我规划、自我执行、自我检测和自我改进，做好 5G 网络自身的安全保障，并把 5G 安全的相关标准、合规性做好，实现 5G 安全的自我管控

（2）基础电信运营企业和业务应用企业，作为第二道防线实施独立的安全监测。

业务应用企业，对自身运营的业务进行实时安全监测，加强安全审计；基础电信运营企业和业务应用企业通过大网侧网络质量感知能力（含企业侧的主动感知、用户侧的被动感知），对 5G 网络时延、掉话率等网络性能参数进行监测与预警，实现网络侧的异常感知。从多个角度审核 5G 网络的安全性。通过监督与制约机制进一步降低安全风险，对发现的问题 实施闭环管理跟踪，直到问题解决，实现网络安全治理的持续改进。

（3）行业主管部门，作为第三道防线评估与审计第一、第二道防线运作的有效性

行业主管部门通过建设 5G 网络安全综合监测管理平台，汇聚、联动、综合分析第一、第二条监测渠道的业务数据，结合 5G 终端用户、垂直行业、外部第三方独立机构等 5G 网络威胁/异常数据源，实时监测掌握 5G 网络整体安全态势并及时处置。审计第一道防线和第二道防线的工作，包括流程执行的符合性检查和 5G 网络安全检测和审计。同时接受 5G 用户、垂直行业和外部第三方独立机构的安全审计。

6.3 贯彻落实网络安全三同步

网络安全三同步是《网络安全法》对于关键信息基础设施建设的明确要求，5G 网络作为我国非常重要的关键信息基础设施，在 5G 网络的规划、建设和使用中需要持续贯彻落实该要求，以保障 5G 网络及其应用的安全运行。

（1）同步规划

在 5G 网络及应用的规划设计阶段同步考虑网络安全保障需求，同步规划网络安全设施建设，包括 5G 网络及应用的安全技术保障能力和安全管理平台等的建设；

（2）同步建设

在项目建设阶段，需要落实 5G 网络及应用建设方的网络安全责任，确保 5G 网络及应用的网络安全设施严格按照规划设计要求进行同步建设。保证项目上线时，网络安全设施的验收和主体工程验收同步进行，确保只有符合网络安全要求和通过安全风险评估的系统和业务才能上线；

（3）同步使用

5G 网络和应用的日常运营维护中，应当保持 5G 网络安全设施处于正常工作状态，确保网络安全识别、监测、处置的各项流程贯通，具备高效的安全事件处置和应急响应能力。

6.4 促进 5G 安全标准的体系化建设和完善

5G 新技术、新架构给 5G 网络带来了新的安全风险，为了应对 5G 网络在系统安全、业务安全和数据安全等方面面临的安全风险和挑战，保障 5G 网络在建设、运行、应用各个环节的安全可靠，我们需要构建完善的 5G 安全标准体系。

目前，国内外 5G 安全标准化工作情况如下：

（1）3GPP 制定了 5G 安全架构和流程（3GPP TS 33.501）以及 5G 安全保障系列标准（TS33.511、TS33.512、TS33.513、TS33.514、TS33.515、TS33.516、TS33.517、TS33.518、TS33.519），但没有监管相关标准

（2）国内 5G 安全标准涉及国家标准和通信行业标准两大层面。目前，已提交立项建设的国家标准包括《5G 安全总体技术要求》、《5G 移动通信网通信安全技术要求》、《5G 移动通信网络设备安全保障要求 核心网网络功能》等；通信行业标准约十余项，主要为 5G 移动通信网、网络功能虚拟化、5G 网络及设备安全保障要求、网络日志留存要求等。

总体来看，国内外对于 5G 网络安全标准主要都以推进 5G 网络和业务安全发展为主，研究工作主要集中于 5G 网络新技术安全、网络架构安全等方向，网络安全监管标准相对零散，5G 安全监管需求和标准研究并不完全同步，尚未形成体系化、系统化的 5G 网络安全监管标准体系。

因此，未来需要从联盟标准、行业标准、国家标准多个层面来共同推进 5G 安全的标准化工作，全面覆盖 5G 安全涉及的各个领域，统筹考虑 5G 安全技术要求和监管要求。使得 5G 数据安全、业务安全、应用安全等各个场景能够得到有效的保护。可以从以下几个方面考虑：

（1）开展 5G 安全技术研究。开展 5G 网元安全保障，5G 网络在安全隔离、用户认证、运行维护等方面的安全机制研究等；

（2）研发 5G 安全系列标准。制定和完善 5G 安全防护类标准。现有固定/移动网络类安全防护标准大多针对固定通信场景，移动通信场景标准较少，且网络和系统单元类别未涵盖 5G 网络切片、虚拟化网络单元等。因此需补充 5G 网络和系统单元类安全防护标准；制定 5G 专用设备等基线配置类标准；制定 5G 业务和应用上线前的安全评估相关标准；

（3）标准先行，强化指导。制定和完善 5G 应用场景安全防护标准和管理规范制定。例如 5G 物联网平台及终端、AR/VR、智慧城市、工业控制、远程医疗系统等业务场景的安全防护标准；完善现有车联网平台防护标准及工业互联网防护标准，补充 5G 网络引入的安全风险及应

对策略。

7. 5G 网络安全监测管控

随着 5G 时代的到来，安全的环境正在发生剧烈的变化，外部的威胁变得更加突出，自动化攻击与黑色产业链日臻完善，我们既要保护 5G 平台本身的安全，又要提供方法和机制来保护那些建立在 5G 平台之上的服务。因此，原来以策略和网络防护为核心的理念已无法适应新的环境。因此，新一代 5G 网络安全保障体系建设的目标至少包含如下三点：

（1）风险可视化：未知攻，焉知防，只有看得见风险才能做好风险的防范工作；

（2）防御主动化：进行主动防御、纵深防御；

（3）运行自动化：保证全天候自动化的安全运营，以保障安全体系的落实。

在严峻的 5G 网络空间安全威胁的形势下，必须结合当前移动互联网威胁监测机制，适应 5G 网络高带宽、低延时、广连接的特性，引入更加智能的态势感知技术，建立更完善、更合理的安全监测管控平台，以便为 5G 网络的安全监测预警与应急处置提供强有力的支撑。

7.1 沿用当前互联网威胁监测机制

（1）基于信令面数据

针对网络数据流量大、范围广的特点，采用分布式流量监测方式，分析速率、接通率、掉话率等多个性能指标参数，预警网络异常情况。

（2）基于用户面数据

利用设置业务网关/代理/平台的方式，在移动互联网网络边界构建网络用户 UNI，规范用户对网络侧系统和设备的访问行为。

（3）基于 DFI（动态流检测）数据

对常用端口、流量峰值、重点 IP 吞吐量等网络测量数据，关联用户身份，细分流量与业务，提升网络感知能力，实现网络流量异常的分析；同时利用智能管道技术，实现高精度流量控制，对重点业务和用户的网络情况进行重点监测。

（4）基于 DPI（深度包检测）数据

根据网络传输中的 IP 地址、HTTP 会话连接以及移动终端中的 IMSI 号等进行网络溯源，还原移动应用流量，实现对网络应用异常的检测。

在关键安全域内部署入侵检测和防御系统，监测记录网络内相关操作，判别非法进入网络

和破坏系统的恶意行为，发现违规、越权等恶意操作。

7.2 适应 5G 网络特性的安全检测技术

在移动互联网（3、4G）较为成熟的网络安全监测预警机制基础上，结合 5G 的业务与技术特点，通过将 5G 系统中多维度、多种类的安全业务数据进行融合，健全 5G 网络安全事中监测技术体系。

（1）结合 5G 网络的海量终端通信的特点，对海量物联网终端发起的多来源、多粒度的信令和多种用户类型上报的数据等进行收集，通过大数据平台技术实现海量数据的分析，进而精确定位网络异常；

（2）结合 5G 网络高带宽、低成本、攻击成本低的特点，利用多源数据采集技术对 5G 网络的系统日志、资产数据、网络流量等数据进行实时在线监测、自动采集和预处理，发现原始数据中的异常信息并及时告警，提升安全监控响应速度，以对抗大规模网络攻击；

（3）结合 5G 网络业务场景多样化的特点，通过用户行为分析（UEBA），对已收集的 5G 网络多样化的异构数据和威胁情报，利用人工智能、数据挖掘、精量化威胁分析等手段对数据进行多维度智能分析、对安全事件追踪溯源，快速聚合有效高危告警。

7.3 建立智能化的监测与管控平台

5G 是个开放的网络，海量物联网设备暴露在户外、硬件资源受限、无人值守，易受黑客攻击和控制，因此网络将会面临大量的网络攻击。如果采用现有的人工防御机制，不仅响应速度慢，还将导致防御成本急剧增加，所以需要考虑采用智能化的手段防御海量物联网设备的安全威胁。此外，网络攻击日趋自动化，0day 攻击的可能性越来越大，5G 中需要考虑被动变主动的安全防御机制。

5G 网络的复杂性和开放性、海量物联网设备的接入、行业用户安全需求的多样性使得安全管理的复杂度和工作量大增。依赖人工进行安全管理可能会导致响应慢、成本高等问题。因此，5G 网络需要考虑引入基于智能化的主动防御技术，结合 IT 网络防御机制，形成一个基于统一情报威胁分析的，支持 ICT 联动的智能化的监测预警与管控平台。

图 7-1 5G 监测与管控平台流程图

7.3.1 安全监测与数据采集

5G 网络的复杂性和开放性使得安全威胁的种类大大增加，我们需要对 5G 网络安全状态进行全面监测，并汇集各渠道、各类型的公共网络安全的基础数据，包括但不限于有害程序事件、网络攻击事件、信息泄露事件、安全隐患等。

可以通过 5G 网络中不同位置的安全感知工具监测管理网络系统设施，如服务器、网络设备或软件等，根据地址信息，引入人工智能、数据聚合来分析大量数据，根据分析结果捕捉整个系统状态，建立捕捉系统状态模型，进行可视化、共享、查询和分析，识别以前或正在进行的威胁，检测未知攻击、复杂攻击。

可以依靠设备状态监控实现 5G 网络的状态监控，通过定义切片内部网络设备、安全设备、服务器、终端等设备的状态管理、故障管理和安全通告管理接口，实现基于策略的应急响应处置和业务跟踪功能，包括预警信息库、漏洞库、处理预案库等。

可以基于威胁分析与决策治理技术实现攻击的监测，分析攻击步骤之间及攻击步骤与告警信息间的关系，并通过提取各个攻击步骤阶段相应的攻击意图后，计算预测未来持续的攻击步骤和有效修复建议，实现对网络防御能力的动态调整，同时结合大数据技术，研究安全风险特征，实现安全预警和防御。最后通过与网络切片内虚拟网元、防火墙之类安全设备的安全策略联动，实现威胁处置。

7.3.2 态势感知与分析

通过对虚拟化安全设备及物理环境基础设施安全设备进行广泛采集，将各类告警数据和运行状态数据进行统计分析、关联分析、预测分析和影响性分析等处理，用以有效识别 APT 攻击、DDoS 攻击等安全威胁。安全态势分析包括静态特征检测、动态行为分析、异常行为挖掘、事件关联分析和综合态势分析五个方面。

最终从宏观方面分析整个 5G 网络总体安全状况，包括对所监测的网络安全威胁和网络安

全事件进行态势分析和展示，提供网络安全总体态势的展示和呈现。

7.3.3 安全预警与通报

针对监测到的各种安全数据（包括网络性能异常、状态异常、攻击异常数据等）、安全事件（包括突发网络安全事件、有害程序事件、网络攻击事件、信息泄露事件、重大网络安全隐患等）自动生成符合模板的预警通报；并定期生成综合性通报。

7.3.4 安全联动与处置

为了快速应对安全威胁，行业主管部门、运营商、设备厂商、行业用户之间通过监测管控平台进行联动，实时交换安全情报，实现安全协同的自动化、智能化。平台业务流可实现调查任务下发与处置响应的返回。例如，行业主管部门在运营商网络检测到异常终端时，可以在平台将终端异常状态及时通知运营商和行业用户，行业用户来打补丁或清除恶意代码；运营商和行业用户之间通过平台人工智能技术直接交换异常信息，联合分析异常，定位攻击，可以提高效率，减少人工介入操作带来的响应时延。

7.3.5 安全运维管理

对 5G 网络的安全管控，建立自动化防御，在网络的各层各域部署漏洞扫描、安全加固、防火墙、恶意代码检测、流量异常检测等多种安全功能。引入人工智能，提高从安全监控，到安全检测分析、攻击阻止、攻击隔离、攻击预防等各环节的自动化程度，实现敏捷的安全管理。

当管理员通过安全态势感知和分析对当前 5G 网络的安全态势形成一定了解并认为有必要进行安全策略调整的时候，可以将调整目标进行分解，拆分/形成一系列的对应到不同虚拟化设备中的安全策略，通过统一的接口将这些策略下发到各个虚拟化设备中予以执行，同时收集这些策略的执行结果，跟踪网络的安全态势更新，验证安全策略调整的有效性。

8. 中通服设计院 5G 安全能力

8.1 行业地位

中通服设计院是“江苏省 5G 产业联盟”的副理事长单位,旨在构建开发的信息共享与合作创新，形成优势互补；推动 5G 产业核心技术、关键设备、行业应用及产业人才的培育与健康发展。

图 8-1 江苏省 5G 产业联盟

公司是中国电信的“5G 白皮书项目组”的成员单位。联合中国电信共同发布《中国电信 5G 技术白皮书》。这是全球运营商首次发布全面阐述 5G 技术观点和总体策略的白皮书。

公司是中国通服网络安全业务四大能力中心之一（安全咨询和评估能力中心）及八大区域中心之一，是中国电信集团长期的网络安全风险感知和漏洞发掘竞赛工作技术支撑单位，江苏省互联网应急中心 JSCERT 网络安全信息通报单位，拥有贯穿信息通信系统全生命周期的包括安全咨询、安全评估、安全设计、安全集成、安全运营、安全培训在内的一体化安全服务能力。具有完备的安全服务资质，可为包括智慧城市、工业互联网在内的众多 5G 网络及应用提供全方位的安全保障。

公司所属中国通信服务股份有限公司在 2019“中国软件业百强企业”中名列第 5，在“安全牛”2019 中国网络安全 100 强企业中位列领导者企业象限。

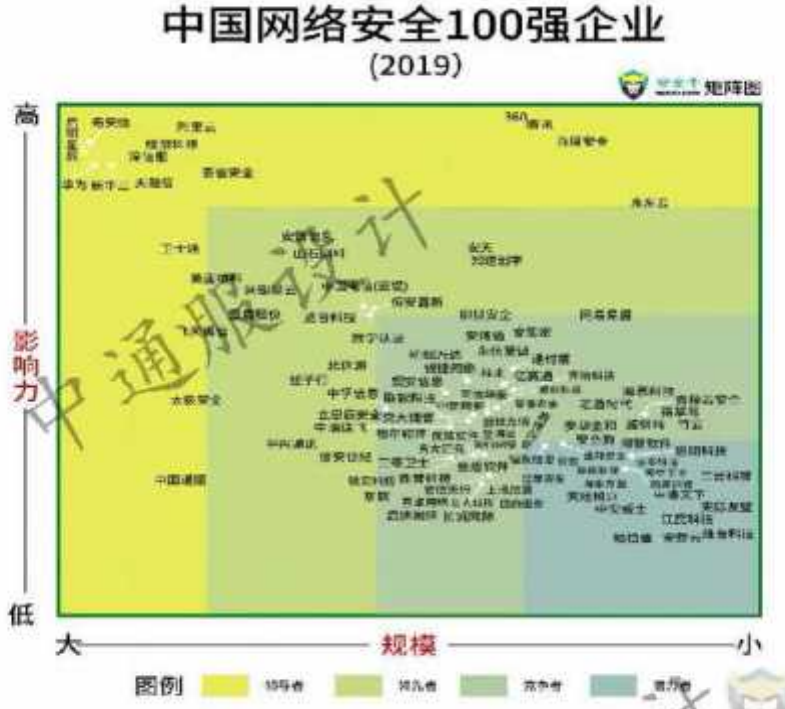

图 8-2 中国网络安全百强企业

8.2 5G 研究成果

中通服设计院在 5G 方向开展了一系列的研究，并获得了显著的成果。包括：

（1）出版了多本 5G 方向的专著，包括《5G-2020 后的移动通信》等；

图 8-3《5G-2020 后的移动通信》

(2) 申请了数十项发明专利，包括《一种 5G 物联网电力数据采集终端接入控制方法》、《4G 和 5G 无线通信系统中数字喷泉码的参数优选方法》等；

(3) 发布了业界多份 5G 白皮书，包括《技术发展及网络建设白皮书》等；

(4) 主编多项工程建设标准，包括《数字蜂窝移动通信网 5G 核心网工程技术规范》、《数字蜂窝移动通信网 5G 无线网工程技术规范》等；

(5) 参编多项 CCSA 课题，包括《5G 基站供电和制冷技术研究》等；

(6) 发表了数百篇 5G 相关论文和技术期刊，包括《人民邮电报》技术专题文章《5G 改变世界，安全守护未来》等。

8.3 5G 技术奖项

中通服设计院近年来获得多项 5G 相关的奖项，包括：

(1) 与客户联合研发、申报 5G 示范应用，荣获工信部“绽放杯” 奖项。

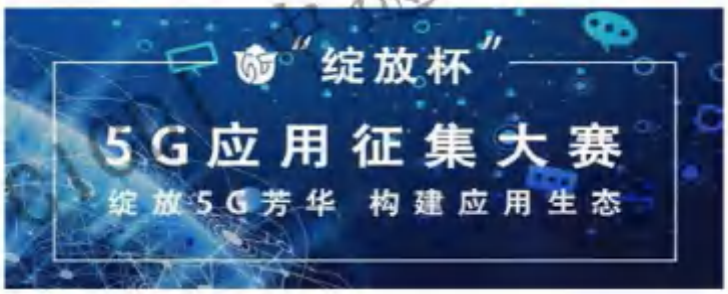

图 8-4 工信部“绽放杯”

(2) 联合设计、自行开发、独立运营的 SDNO（IP 网络 SDN 编排器）荣获 2017 年中国电信集团科技进步一等奖 。

图 8-5 2017 年中国电信集团科技进步一等奖

8.4 5G 网络安全态势感知平台

作为 5G 网络建设的领军者，中通服设计院不但参与了多项 5G 网络建设工作，同时也针对 5G 网络安全监测管控的需求面向通信运营商和政府监管部门等推出了自主研发的 5G 网络安全态势感知平台。

在适应 5G 非独立组网（NSA）与独立组网（SA）两种网络结构条件下，聚焦于 5G 各类典型应用场景下网络与信息安全风险的自动化监测和研判工作，通过将海量数据采集分析、人工漏洞发掘、业务场景威胁建模、安全风险评估等与基于大数据发掘分析的人工智能技术相协同，能够快速识别主流 5G 应用所潜在的网络与信息安全风险、精准研判其影响范围及发展态势、为政府和企业的网信安全管理提供高效决策支持和应急处置建议，也可为运营商开展 5G 网络及相关应用的安全运营提供支撑。

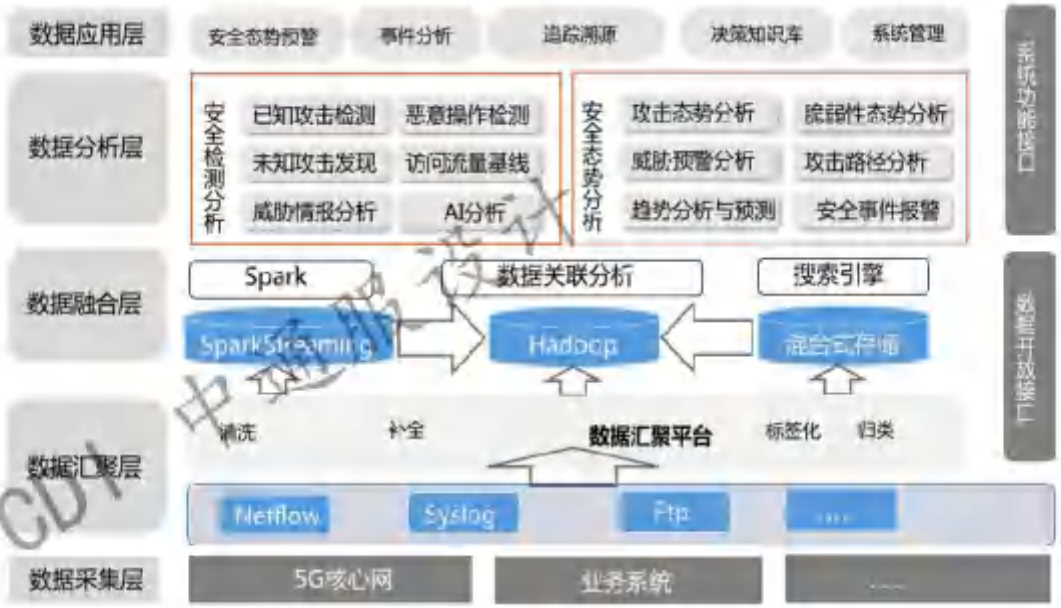

图 8-6 5G 网络安全态势感知平台体系架构

该 5G 网络安全态势感知平台具有如下特点：

（1）与运营商 5G 现网环境紧密结合

针对运营商 5G 业务进行安全监测分析能力的覆盖和验证，对 5G 商用的现网真实数据流量进行在线深度检测、协议识别、关联分析、规则匹配、建模比对和实时处置，输出预期结果，满足 5G 业务的现网安全需求。

（2）实现匿名通信流量的识别和分析

综合利用渗透攻击和流量分析方法，从隐藏桥节点和流量模式两个层面进行匿名流量的识别，并提取网络流突发段长度、报文间隔时间等特征建立典型匿名通信应用的流量模型。在此基础上，部署基于 Flink 的实时流量处理框架，有机结合传统机器学习和深度学习算法，实现匿名通信流量的在线识别和分析。

（3）完善的 5G 网络安全决策知识库

基于 5G 应用网络安全态势要素分类与提取技术，通过多粒度视角识别安全事件特征构建网络安全态势要素知识库模型，并通过案例持续更新与反馈机制，形成一个可实现态势信息表达、共享、复用、溯源和推理的决策知识库。协助网络安全运营和监管单位准确定位风险、精准处置风险。

（4）多类型网络安全威胁与多元事件关联分析

从攻击破坏性、环境、成功率、统计、关联和效果六个维度对网络安全威胁数据统计建模；面向流量、报文和恶意代码的多层次异常行为，突破基于智能学习方法（如深度神经网络等）的未知网络攻击发现技术；构建多源异域空间行为关联模式，建立基于用户行为大数据驱动的电信网络安全行为/事件分析与发现模型。基于所形成的已知和未知威胁检测技术理论及事件评估方法搭建全自动分析引擎，实现威胁的全过程检测。

（5）通过多维度数据关联精准计算 5G网络应用安全风险

将安全威胁感知、安全漏洞探测、安全事件感知、安全情报收集、网络资产属性等多维度的数据纳入到网络 5G 应用安全风险评估模型中进行统一的计算分析，其中安全漏洞探测和安全情报收集可借助安全众测和安全应急响应中心的人工安全信息收集功能，实现系统自动化收集数据和人工提供数据相结合。通过全新的网络安全风险评估模型对所分析的结果通过人工智能技术进行综合研判，从而实现网络安全预警的客观化和智能化，根据不同的风险等级采取相应的预警方式。

8.5 通服众测平台

通服众测平台是中通服设计院自主研发并运营的一个基于互联网的开放式网络安全测试暨竞赛平台，通过“互联网众包”的模式为广大运营商、政府和企事业单位提供按实际效果计费的可信赖的网络安全测试服务及漏洞发掘竞赛服务，为 5G 网络与应用提供 7*24 小时不间断的网络安全风险监测服务。

图 8-7 通服众测平台

通服众测目前已经拥有实名认证的安全测试白帽子人员四千多人，遍及全国 31 个省市，已累计收集各类系统安全漏洞 3 万多个，其中高危漏洞 7 千多个，帮助客户及时规避了数千万的经济损失和商誉的影响。目前日均 100 多个的安全漏洞收集量也成为全国规模领先的安全众测平台。

平台获得多项国家级的荣誉和表彰，包括：

（1）获中华全国总工会及国家应急管理部全国“安康杯”竞赛优胜班组联合表彰；

（2）中国电信集团 2018 年科技进步奖（第一完成单位）；

图 8-8 获中华全国总工会及国家应急管理部联合表彰

（3）工业和信息化部 2019 年网络安全技术应用试点示范项目；

（4）江苏省通信学会科技进步奖。

9. 总结和展望

5G 作为新一代移动通信网络基础设施，面向未来更加多样化的业务场景、多种接入方式、多种设备形态、新的商业模式、更高的隐私保护需求以及新型网络架构的安全需求，安全成为支撑其健康发展的关键要素。网络安全与信息化是一体之两翼、驱动之双轮，如何有效管控各类网络安全风险直接关系到 5G 应用的成败。

5G 技术向各领域融合渗透，相伴生的安全风险与多方责任主体紧密相关，需要用全面系统的理念看待和应对。首先，需要做好 5G 安全统筹规划。建议各单位在开展 5G 网络及应用建设和运营时，应尽早明确 5G 网络安全的关键需求和对应的解决方案，提前做好 5G 网络安全规划设计，采取多种措施从提升 5G 技术安全保障和加强 5G 安全综合管理两个方面来积极应对和管控相关安全风险。

此外，需要明确 5G 安全责任担当。需要明确 5G 设备供应商、网络运营商、行业应用服务提供商等产业链各环节不同主体的责任和义务，不过分关注或放大单一环节责任。同时要加强各责任主体之间的沟通协作，倡导各方秉持合作互信的理念，积极搭建 5G 安全合作平台，建立 5G 安全三道治理防线，从多个角度和多个层次保障 5G 网络及应用的安全性。

最后，需要加强 5G 安全协同互助。 充分发挥政府部门、 标准化组织、企业、研究机构和用户等各方的能动性，打造多方参与的 5G 安全治理体系。贯彻落实 5G 网络安全的三同步要求、促进 5G 安全标准体系的建立和完善，提升 5G 发展的信心。建立智能化的 5G 安全监测管控平台，为 5G 网络的安全监测预警与应急处置提供强有力的支撑，为构建 5G 时代的网络安全作出贡献。

中通服设计院作为新一代综合智慧服务商中国通服旗下咨询及总包服务领军企业，积极全面参与 5G 网络的建设和网络安全保障工作。愿充分发挥在 5G 安全领域的技术积累和产品研发实施及运营能力，与各方协作共同打造 5G 网络安全生态，为创建开放、合作、共赢的 5G 美好未来保驾护航。

创泽智能机器人集团主要产品

智能服务机器人

智能陪护机器人

安防巡检机器人

消毒机器人

智能党建机器人

智能教育机器人

智能导诊机器人

银行智能机器人

室外智能消毒机器人

多功能消毒机器人

全自动智能消毒杀菌机器人

智能医用消毒机器人

了解更多登录官网

www.chuangze.cn

中通服咨询设计研究院有限公司

地　址：江苏省南京市建邺区楠溪江东街 58 号

联系人：王小鹏

电　话：15366136781

网　址：http:/www.cicdi.com