5G 安全报告

中国信息通信研究院
IMT-2020(5G)推进组

2020年2月

前　言

当前，全球新一轮科技革命和产业变革加速发展，5G 作为新一代信息通信技术演进升级的重要方向，是实现万物互联的关键信息基础设施、经济社会数字化转型的重要驱动力量。加快 5G 发展，深化 5G 与经济社会各领域的融合应用，将对政治、经济、文化、社会等各领域发展带来全方位、深层次影响，将进一步重构全球创新版图、重塑全球经济结构。世界主要国家都把 5G 作为经济发展、技术创新的重点，将 5G 作为谋求竞争新优势的战略方向。根据全球移动供应商协会（GSA）统计，截至 2019 年底，全球 119 个国家或地区的 348 家电信运营商开展了 5G 投资，其中，61 家电信运营商已经推出 5G 商用服务。

“每个硬币都有两面”。5G 技术造福社会、造福人民的同时，也引发了新的网络安全风险。中国国家主席在第二届世界互联网大会上指出，维护网络安全是国际社会的共同责任。国际社会应该在相互尊重、相互信任的基础上，加强对话合作，共同构建和平、安全、开放、合作的网络空间。5G 安全是全球面临的共同问题，更需要倡导开放合作的网络安全理念，客观看待和应对 5G 安全风险，深化合作，增进互信，共同提高 5G 安全保障水平。

基于此，中国信息通信研究院和 IMT-2020(5G)推进组，作为国内 5G 领域专业研究机构，结合前期工作基础及近期调研情况联合编制

了本报告，系统梳理了关键技术、典型应用场景及产业生态的安全风险，提出了安全理念和应对思路措施，并对后续加强各方互信合作，更好地推动 5G 发展与安全进行了展望和倡议。

目 录

一、5G 发展重大意义

（一）5G 是全球信息技术发展最新成果。移动通信网络历经第一代（1G）到第四代（4G）的快速发展，已进入 5G 发展的关键阶段。5G 最重要的突破是将人与人之间的通信，拓展到人与物、物与物之间的通信，开启万物泛在互联、人机深度交互、智能引领变革的新时代。同时，5G 产业日渐成为各国共同参与、紧密相连的生态系统，来自不同国家和地区的技术、产品和服务高效流动，推动全球共享 5G 发展红利。全球产业界和学术界携手合作，于 2018 年 6 月发布了第一版 5G 标准（R15），成为 5G 发展进程中的重要里程碑，为推动形成全球统一 5G 产业生态奠定了良好基础，成果来之不易。

（二）5G 培育经济发展新动能。当前，以数字化、网络化、智能化为主要特征的第四次工业革命蓬勃兴起，与世界经济新旧动能转换形成历史性交汇。根据世界银行研究，宽带普及率每提升 10%，将带动 GDP 增长 1.38%。5G 作为实现万物互联的关键信息基础设施，应用场景从移动互联网拓展到工业互联网、车联网、物联网等更多领域，能够支撑更广范围、更深程度、更高水平的数字化转型，释放信息通信技术对经济发展的放大、叠加、倍增作用。国际咨询机构 IHS Markit 预测[1]，到 2035 年 5G 将在全球创造 13.2 万亿美元的经济产出，产生 2230 万个就业机会。

[1] IHS Markit:《5G 对全球经济的贡献》, 5G 经济 2019.11

（三）5G 创造智慧社会新模式。5G 与云计算、大数据、人工智能等技术融合应用，有助于形成以数据为驱动的科学决策机制，推进政府管理和社会治理模式创新。利用 5G 广覆盖、大容量、高速率、低时延等特点，推进以 5G 为核心的智能基础设施与城市治理深度融合，通过交通管理、环境监测等应用改善城市生活环境，促进感知智能化、管理精准化、服务便捷化的智慧城市运营，为人们打造健康、舒适、环保的城市生活空间。

（四）5G 拓展民生福祉新内涵。5G 是改善民生福祉的重要支撑，能够满足人们个性化、智能化的服务需求，改善人民生活方式，提升人民生活品质。5G 推动更优质、更丰富的信息通信服务惠及广大群众，创造更多适应消费升级的有效供给，降低全社会信息消费成本，有效弥合城乡数字鸿沟。5G 提供远程教育、智慧医疗公共事业等新模式，实现公共服务供给与需求之间的精准匹配和有效对接，提升公共服务效率，推动优质资源共享，增强人民群众的获得感、幸福感。

二、5G 网络概述

2015 年，国际电信联盟（ITU）发布了《IMT 愿景：5G 架构和总体目标》，定义了增强移动宽带（eMBB）、超高可靠低时延（uRLLC）、海量机器类型通信（mMTC）三大应用场景，以及峰值速率、流量密度等八大关键性能指标。与 4G 相比，5G 将提供至少十倍于 4G 的峰值速率、毫秒级的传输时延和每平方公里百万级的连接能力。

（一）5G 网络架构和关键技术

从网络架构来看，5G 网络整体延续 4G 特点，包括接入网、核心网和上层应用（如下图）。为满足 5G 移动互联和移动物联的多样化业务需求，5G 网络在核心网和接入网均采用了新的关键技术，实现了技术创新和网络变革。

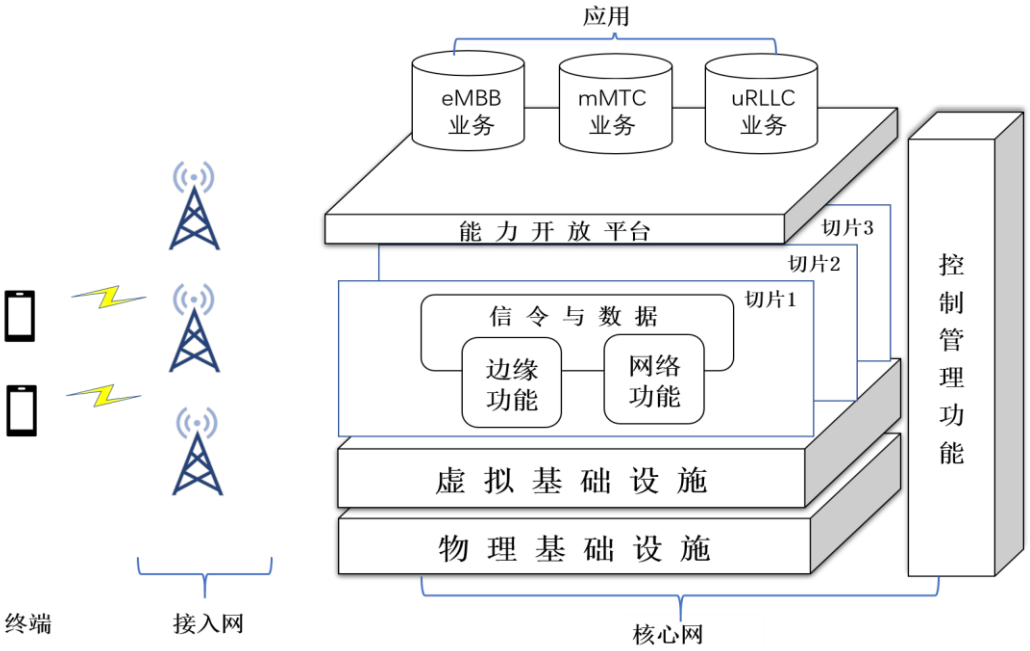

图 5G 网络架构

5G 采用的主要关键技术有:

·**服务化架构:** 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。5G 服务化架构是 5G 时代迅速满足垂直行业需求的重要手段。

·**网络功能虚拟化:** 采用虚拟化技术，将传统网络的专用网元进行

软硬件解耦，构造出基于统一虚拟设施的网络功能，实现资源的集中控制、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。

·**网络切片：**网络切片可在一个物理网络上切分出功能、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，可以提高网络资源利用率、隔离不同业务场景所需的网络资源。

·**边缘计算：**边缘计算是在网络边缘、靠近用户的位置，提供计算和数据处理能力，以提升网络数据处理效率，满足垂直行业对网络低时延、大流量以及安全等方面的需求。

·**网络能力开放：**5G 网络可以通过能力开放接口将网络能力开放给第三方应用，以便第三方按照各自的需求设计定制化的网络服务。

·**接入网关键技术：** 5G 在接入网采用灵活的系统设计来支持多业务、多场景，采用新型信道编码方案和大规模天线技术等以支持高速率传输和更优覆盖。

此外，第三代移动通信伙伴计划（3GPP）标准在接入网和核心网之间明确定义了接口，两者功能不同，边界清晰，业界专家认为[2]，即使 5G 核心网的部分功能部署在网络边缘，功能上的界限依然是很明确的。同时，还可以通过在核心网（包括边缘计算）与接入网之间部署安全网关等来增强安全性。因此，运营商可选取多元化的供应商提

[2] 2019 年 6 月，英国议会下院科学与技术委员会“英国电信基础设施”公开听证会，3GPP SA3 副主席 Alf Zugenmaier 教授, Munich University 等业界专家的观点。
https://www.parliamentlive.tv/Event/Index/65f2ce0c-2994-46b2-bd9b-3b10dc38ca6f

供接入网和核心网产品，提高网络韧性。

（二）5G 安全框架

5G 安全既包括由终端和网络组成的 5G 网络本身通信安全，也包括 5G 网络承载的上层应用安全。移动通信网络标准在设计之初，就充分考虑了网络的可靠性和安全性，经过全球通信行业几十年的共同努力，移动通信网络安全架构日臻完善。

5G 继承了 4G 网络分层分域的安全架构，在 3GPP 5G 安全标准《5G 系统安全架构和流程》[3]中规定：在安全分层方面，5G 与 4G 完全一样，分为传送层、归属层/服务层和应用层，各层间相互隔离；在安全分域方面，5G 安全框架分为接入域安全、网络域安全、用户域安全、应用域安全、服务域安全、安全可视化和配置安全六个域，与 4G 网络安全架构相比，增加了服务域安全。

5G 提供了比 4G 更强的安全能力，包括：

·服务域安全。针对 5G 全新服务化架构带来的安全风险，5G 采用完善的服务注册、发现、授权安全机制及安全协议来保障服务域安全。

·增强的用户隐私保护。5G 网络使用加密方式传送用户身份标识，以防范攻击者利用空中接口明文传送用户身份标识来非法追踪用户的位置和信息。

·增强的完整性保护。在 4G 空中接口用户面数据加密保护的基础

[3] 3GPP TS 33.501, 《5G 系统安全架构和流程》。

上，5G 网络进一步支持用户面数据的完整性保护，以防范用户面数据被篡改。

·增强的网间漫游安全。5G 网络提供了网络运营商网间信令的端到端保护，防范以中间人攻击方式获取运营商网间的敏感数据。

·统一认证框架。4G 网络不同接入技术采用不同的认证方式和流程，难以保障异构网络切换时认证流程的连续性。5G 采用统一认证框架，能够融合不同制式的多种接入认证方式。

综上，5G 针对服务化架构、隐私保护、认证授权等安全方面的增强需求，提供了标准化的解决方案和更强的安全保障机制。

三、5G 安全理念

5G 作为关键信息基础设施和数字化转型的重要基石，在开启万物互联新局面的同时，也带来了新的安全挑战和风险，成为全球面临的共同问题，需要坚持开放合作的网络安全理念，全面客观看待和应对 5G 安全风险。

（一）以发展理念看待 5G 安全。5G是信息技术发展的最新成果，反映了全球信息化发展的历史潮流和趋势，不能因为 5G 有安全风险，就放慢或迟滞 5G 发展。要坚持用发展的视角看待安全风险，正确处理发展和安全的关系，坚持安全与发展同步推进。就 5G 自身来看，其设计了更灵活的安全保护机制，可提供比 4G 更强大的通信安全能力，并将建立“风险-应对-新风险-新应对”的良性循环，3GPP 将针对

新出现的攻击手段和安全威胁不断进行安全增强[4]，实现 5G 安全与发展的协同推进。

（二）以系统理念看待 5G 安全。信息技术变化越来越快，过去分散独立的网络变得高度关联，相互依赖。5G 技术向各领域融合渗透，安全风险与多主体紧密相关，需要用全面系统的理念看待和应对。5G 技术发展以及应用场景具有广泛性、开放性、挑战性和多元性，既需要明确网络运营商、设备供应商、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，又需要加强各主体之间的协同合作，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，明晰各方安全责任，打造多方参与的 5G 安全治理体系。

（三）以客观理念看待 5G 安全。任何网络技术都存在安全风险和漏洞，5G 网络也不例外，应坚持用客观理念来分析和看待 5G 安全风险。特别是由于 5G 与物联网、人工智能等新技术新应用融合，会带来更加复杂的安全问题，需要从客观、中立的技术角度对 5G 安全风险进行全面评估，在现有成熟机制和已有的技术应对手段基础上，通过产业创新和技术研发逐步解决。将技术层面的安全问题扩大化、复杂化，甚至政治化，对不同的企业区别标签或采取非市场的手段对待，无助于 5G 安全问题的有效解决。

[4] 3GPP：5G 将对抗重放攻击、抗安全降级攻击、抗中间人攻击等其他安全威胁以及运营商间安全问题进行重新评估，进一步实现安全增强。https://www.3gpp.org/news-events/1975-sec_5g

（四）以合作理念看待 5G 安全。世界各国虽然国情不同、网络发展阶段不同、面对的现实挑战不同，但推动数字经济发展的愿景相同，应对安全风险挑战的立场相同、加强网络安全空间治理的诉求相同，国际社会日益成为“你中有我、我中有你”的命运共同体。5G 安全是全球性挑战，没有谁可以独善其身。从之前的全球多个标准到 5G 时代的全球统一标准，5G 进程正是各方创新合作的生动写照，在安全方面也应携手努力，加强创新合作，共同构建和平、安全、开放、合作的网络空间。

四、5G 安全分析

5G 不仅是技术变革，更是新生态体系的构建，认识 5G 安全问题，既需要从技术、场景等角度进行客观分析，也需要从产业生态维度进行综合评估。

（一）5G 关键技术安全分析

1. 网络功能虚拟化

安全风险：一是虚拟环境下，管理控制功能高度集中，一旦其功能失效或被非法控制，将影响整个系统的安全稳定运行；二是多个虚拟网络功能（VNF）共享下层基础资源，若某个虚拟网络功能被攻击将会波及其他功能；三是由于网络虚拟化大量采用开源和第三方软件，引入安全漏洞的可能性加大[5]。

[5] 欧洲网络与信息安全局（ENISA），《5G 网络安全图谱》，2019.11

技术应对措施：可借鉴现有在 4G 核心网和 IT 行业应用中使用的云化安全解决方案，并参考欧洲电信标准化协会（ETSI）制定的多个网络虚拟化安全标准[6]。一是进行系统安全加固，对管理控制操作进行安全跟踪和审计，提升防攻击能力。二是提供端到端、多层次资源的安全隔离措施，对关键数据进行加密和备份。三是加强开源第三方软件安全管理。

2. 网络切片

安全风险：网络切片基于虚拟化技术，在共享的资源上实现逻辑隔离，如果没有采取适当的安全隔离机制和措施，当某个低防护能力的网络切片受到攻击，攻击者可以此为跳板攻击其他切片[7]，进而影响其正常运行。

技术应对措施：针对上述安全风险，可使用云化、虚拟化隔离措施，如物理隔离，虚机（VM）资源隔离、虚拟防火墙等，实现精准、灵活的切片隔离，保证不同切片使用者之间资源的有效隔离，同时要做好网络切片运维和运营安全的管理，确保相应的技术措施得到落实。

3. 边缘计算

安全风险：一是边缘计算节点下沉到核心网边缘，在部署到相对不安全的物理环境时，受到物理攻击的可能性更大。二是在边缘计算平台上可部署多个应用，共享相关资源，一旦某个应用防护较弱被攻

[6] 欧洲电信标准化协会（ETSI），网络功能虚拟化安全系列标准，https://www.etsi.org/deliver/etsi_gs/NFV-SEC/

[7] 欧盟网络信息安全合作组（NISCG），《欧盟 5G 网络安全风险评估报告》，2019.10

破，将会影响在边缘计算平台上其他应用的安全运行。

技术应对措施：一是对边缘计算设施加强物理保护和网络防护，充分利用已有的安全技术进行平台加固并增强边缘设施自身的防盗防破坏措施。二是加强应用的安全防护，完善应用层接入到边缘计算节点的安全认证与授权机制，在部署第三方应用时，要根据部署模式明确各方安全责任划分并协作落实。

4. 网络能力开放

安全风险：一是网络能力开放将用户个人信息、网络数据和业务数据等从网络运营商内部的封闭平台中开放出来，网络运营商对数据的管理控制能力减弱，可能会带来数据泄露的风险。二是网络能力开放接口采用互联网通用协议，会进一步将互联网已有的安全风险引入到 5G 网络。

技术应对措施：一是加强 5G 网络数据保护，强化安全威胁监测与处置。二是加强网络开放接口安全防护能力，防止攻击者从开放接口渗透进入运营商网络。

从整体看，尽管 5G 网络引入的网络功能虚拟化、网络切片、边缘计算、网络能力开放等关键技术，一定程度上带来了新的安全威胁和风险，对数据保护、安全防护和运营部署等方面提出了更高要求，但这些技术的引入也是逐步推进和不断迭代的，其伴生而来的安全风险，既可通过强化事前风险评估，也可在事中事后环节采取相应的技术解决方案和安全保障措施，予以缓解和应对。

（二）5G 典型场景安全分析

5G 应用场景因技术本身以及应用场景自身特点面临新的安全风险，成为影响 5G 融合业务发展的关键要素。目前 5G 典型场景以增强移动宽带业务为主，并逐步拓展到各垂直行业。3GPP 已经完成 eMBB 场景相关安全标准制定工作， uRLLC 及 mMTC 场景标准正在制定中。

增强移动宽带（eMBB）场景：主要应用包括 4K/8K 超高清移动视频、沉浸式的 AR（增强现实）/VR（虚拟现实）业务。主要风险是：增强移动宽带场景下的超大流量对于现有网络安全防护手段形成挑战。由于 5G 数据速率较 4G 增长 10 倍以上，网络边缘数据流量将大幅提升，现有网络中部署的防火墙、入侵检测系统等安全设备在流量检测、链路覆盖、数据存储等方面将难以满足超大流量下的安全防护需求，面临较大挑战。

超高可靠低时延（uRLLC）场景：典型应用包括工业互联网、车联网自动驾驶等。uRLLC 能够提供高可靠、低时延的服务质量保障，其主要安全风险是：低时延需求造成复杂安全机制部署受限。安全机制的部署，例如接入认证、数据传输安全保护、终端移动过程中切换、数据加解密等均会增加时延，过于复杂的安全机制不能满足低时延业务的要求。

海量机器类通信（mMTC）场景：应用覆盖领域广，接入设备多、应用地域和设备供应商标准分散、业务种类多。主要安全风险是：泛

在连接场景下的海量多样化终端易被攻击利用，对网络运行安全造成威胁。5G 时代将有海量物联网终端接入，预计到 2025 年全球物联网设备联网数量将达到 252 亿[8]。其中大量功耗低、计算和存储资源有限的终端难以部署复杂的安全策略，一旦被攻击容易形成僵尸网络，将会成为攻击源，进而引发对用户应用和后台系统等的网络攻击，带来网络中断、系统瘫痪等安全风险[9]。

针对 5G 典型应用场景安全风险，可采取如下应对措施：一是加强安全防护技术和设备的演进升级，有效适应和应对超大流量对现有防护手段带来的冲击。二是建立面向低时延需求的安全机制，统筹优化业务接入认证、数据加解密等环节带来的时延，尽力提升低时延条件下安全防护能力。三是构建基于大规模机器类通信场景的安全模型，建立智能动态防御体系应对网络攻击，防止网络安全威胁横向扩散。

（三）5G 产业生态安全分析

5G 产业生态主要包括网络运营商、设备供应商、行业应用服务提供商等，其安全基础技术及产业支撑能力的持续创新性和全球协同性，对 5G 安全构成重要影响。

1. 网络部署运营安全分析。5G 网络的安全管理贯穿于部署运营的整个生命周期，网络运营商应采取措施管理安全风险，保障这些网

[8] GSMA 研究报告，《物联网：下一波连接和服务》
https://www.gsmaintelligence.com/research/2018/04/iot-the-next-wave-of-connectivity-and-services/665/

[9] 欧盟网络信息安全合作组（NISCG），《欧盟 5G 网络安全风险评估报告》，2019.10

络提供服务的连续性：一是在 5G 安全设计方面，由于 5G 网络的开放性和复杂性，对权限管理、安全域划分隔离、内部风险评估控制、应急处置等方面提出更高要求。二是在 5G 网络部署方面，网元分布式部署可能面临系统配置不合理、物理环境防护不足等问题；三是在 5G 运行维护方面，5G 具有运维粒度细和运营角色多的特点，细粒度的运维要求和运维角色的多样化意味着运维配置错误的风险提升，错误的安全配置可能导致 5G 网络遭受不必要的安全攻击。此外，5G 运营维护要求高，对从业人员操作规范性、业务素养等带来挑战，也会影响 5G 网络的安全性。

2. 垂直行业应用安全分析。5G 与垂直行业深度融合，行业应用服务提供商与网络运营商、设备供应商一起，成为 5G 产业生态安全的重要组成部分。一是 5G 网络安全、应用安全、终端安全问题相互交织，互相影响，行业应用服务提供商由于直接面对用户提供服务，在确保应用安全和终端安全方面承担主体责任，需要与网络运营商明确安全责任边界，强化协同配合，从整体上解决安全问题。二是不同垂直行业应用存在较大差别，安全诉求存在差异，安全能力水平不一，难以采用单一化、通用化的安全解决方案来确保各垂直行业安全应用。

3. 产业链供应安全分析。5G 技术门槛高、产业链长，应用领域广泛，产业链涵盖系统设备、芯片、终端、应用软件、操作系统等，其安全基础技术及产业支撑能力的持续创新性和全球协同性，对 5G 及其应用构成重大影响。如果不能在基础性、通用性和前瞻性安全技

术方面加强创新，产业链各环节同步更新完善 5G 网络安全产品和解决方案，不断提供更为安全可靠的 5G 技术产品，将增加网络基础设施的脆弱性，影响 5G 安全体系的完善。

根据 5G 网络生态中不同的角色划分，5G 网络生态的安全应充分考虑各主体不同层次的安全责任和要求，既需要从网络运营商、设备供应商的角度考虑安全措施与保障，也需要垂直行业如能源、金融、医疗、交通、工业等行业应用服务提供商采取恰当的安全措施。

五、5G 安全思路和措施

应对和解决 5G安全问题，可以基于现有 4G 安全管理框架和技术保障措施，针对新的安全风险和不确定性，采取有针对性的完善措施。

（一）坚持发展与安全同步部署。坚持发展与安全并重、鼓励与规范并举的理念，在加快 5G 网络部署、深度推进 5G 与各领域融合应用的同时，持续开展 5G 安全能力建设，统筹做好 5G 网络设施安全、应用安全、数据安全等工作。密切跟踪 5G 安全风险，动态开展 5G 技术安全评估，明确 5G 安全保障重点。

（二）构建多元协同、清晰明确的安全责任体系。明确产业生态各方责任，不断完善个人信息保护、关键信息基础设施保护、网络信息治理等相关法律法规和政策要求，确保网络运营商、设备供应商、行业服务提供商等主体各司其职、各负其责。加强各行业之间的协同，

发挥行业组织作用，建立健全5G网络与垂直行业安全服务保障准则和信用体系，共同应对5G垂直领域融合应用安全问题。

（三）持续推进5G安全创新发展。加强5G安全技术与标准研究，加快建立5G安全检测体系，大力推进5G安全技术攻关，推动资产识别、漏洞挖掘、入侵防御、数据保护、追踪溯源等网络安全产品的演进升级，持续构建完备、多元、可靠的5G安全产品供应和服务体系。加速5G安全技术创新成果转化和试点验证，加大在车联网、工业互联网等垂直领域的安全服务和解决方案推广力度。

（四）强化5G应用安全风险动态评估。5G在各类垂直行业中的融合应用将在网络规模部署后不断涌现，其特点与垂直领域高度相关，安全风险也呈现持续动态变化的特点，需结合5G垂直领域各自特点，开展行业应用安全相关标准研究，持续开展安全风险跨行业、跨领域评估，强化评估结果运用和转化，及时提出安全应对和处置措施，防范安全风险。

（五）构建5G网络安全一体化防护机制。积极推动5G网络基础设施安全保障手段建设，建立健全5G网络威胁信息共享联动机制，实现威胁信息共享、共治。加快构建5G网络威胁监测、全局感知、预警防护、联动处置一体化网络安全防御体系，形成覆盖全生命周期的网络安全防护能力。

（六）加强5G综合人才培养和培训。统筹推进5G跨学科专业人才培育，建立完善产教融合、校企合作的人才培养体系，加大人才

培养支持力度，持续深化 5G 安全培训教育，丰富 5G 安全人才发掘机制，建立多层次安全从业人员选拔渠道。

六、展望和倡议

在 5G 发展中各方既有共同关切，也有不同诉求，应当在尊重彼此核心利益的前提下，谋求共同福祉，应对共同挑战，让 5G 技术更好地造福世界。我们倡导各方秉持合作互信的理念，加快 5G 安全国际标准制定，建立互信互认的评测认证体系，加强产业上下游合作，提升全球 5G 安全发展信心。

（一）加强开放合作互信，共同应对 5G 安全风险。秉持开放包容、平等互利、合作共赢的理念和原则，推动建立增强互信的双边或多边框架，充分重视各方对 5G 安全问题的正当关切，积极在联合国国际电信联盟等多边组织框架下探讨 5G 安全相关国际政策和规则；增进各方战略互信，进一步完善对话协商机制，加强 5G 网络威胁信息的共享，有效协调处置重大网络安全事件。探索最佳实践，共同分享应对 5G 安全风险的先进经验和做法。

（二）加快推进 5G 安全国际标准，凝聚全球统一共识。在 ITU、3GPP 等 5G 国际标准框架下，聚焦网络功能虚拟化、网络切片等 5G 网络新引入或增强的关键技术，共同推进 5G 增强技术及安全机制后续国际标准研制，加快形成针对覆盖多种应用场景的 5G 安全解决方案。加强产品和服务安全体系建设，在 5G 产品设计、研发、运维等

全生命周期严格遵循国际安全标准规范。

（三）建立 5G 安全国际评测认证体系，推动实现互信互认。加强交流合作，推进形成全球共识的 5G 安全评测认证体系，构建 5G 产品研发设计、生产制造和运行维护全流程的安全审计和技术安全检测机制，加快形成全球范围内公开透明、广泛可接受的 5G 安全信任基线和安全测评等级，促进测评结果的双边或多边互认，共同保障 5G 全球产业链的健康发展。

（四）加强产业链上下游合作，提振 5G 安全信心。加强全球移动通信产业链协同和创新，积极搭建全球产业应用合作和创新平台，加大在关键元器件、核心算法等方面的全球创新研究合作，促进多元化应用在 5G 网络上示范合作和实践经验分享。鼓励多元化全球采购策略，促进形成高效合理的产业链全球配置和分工，推动移动通信供应链条互联互通，逐步连通全球各区域上下游供应链的各类生产要素。为 5G 产业全球化发展营造开放、公平、透明、非歧视的市场环境。

中国信息通信研究院

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62300155

传真：010-62304980

网址：www.caict.ac.cn

IMT-2020(5G)推进组

联系电话：010-62300164

邮箱：imt2020@catr.ac.cn

网址：http://www.imt2020.org.cn