ISC 2019 第七届互联网安全大会

5G网络安全标准及测试认证

魏亮

中国信息通信研究院安全所所长

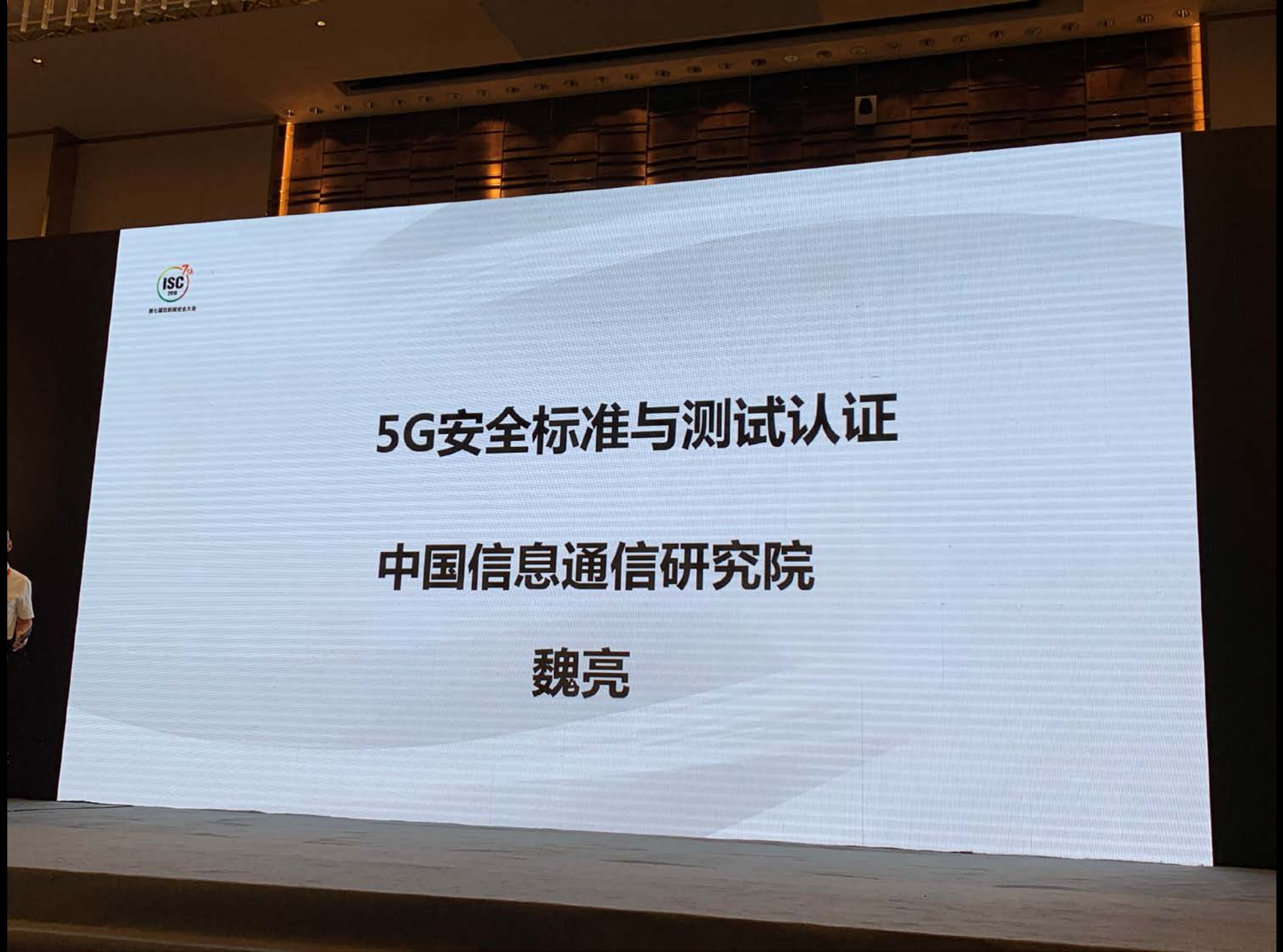
小鹅助理

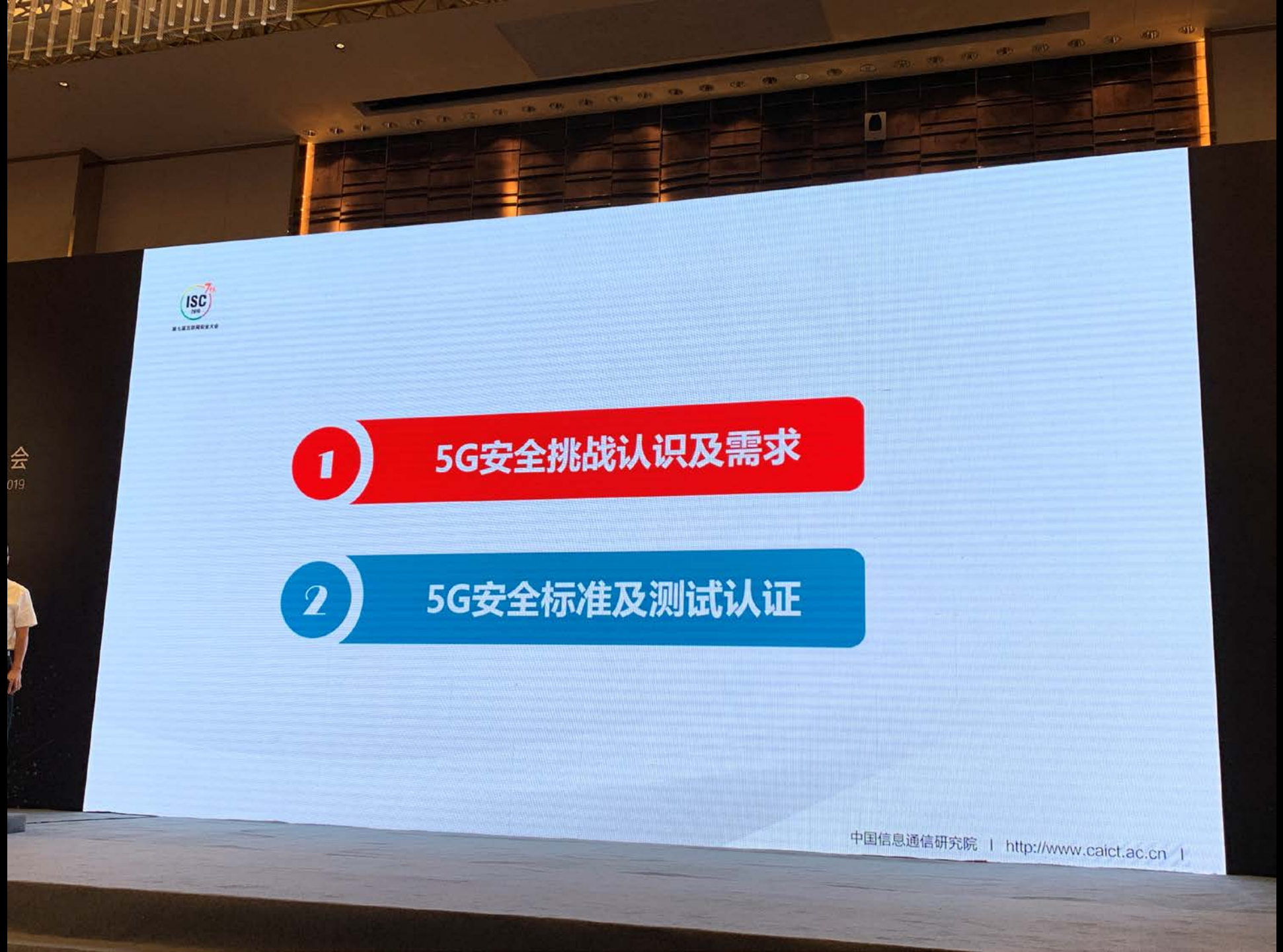
扫码添加小鹅助理，与数万科技圈人士

分享重量级活动PPT、干货培训课程、高端会议免费

门票


ISC
2019
第七届互联网安全大会
360互联网安全中心
Internet Security Conference 2019
魏亮
中国信息通信研究院安全所 所长


ISC
2018
第七届互联网安全大会
5G安全标准与测试认证
中国信息通信研究院
魏亮


ISC
1 5G安全挑战认识及需求
2 5G安全标准及测试认证
中国信息通信研究院 | http://www.caict.ac.cn |

5G时代已经来临

5G在业务需求和技术创新双驱动下，打通了“人”与”物”、”现实“与”虚拟“之间的联接，开启了全新的“万物互联”时代。

2018.12.1	2018.12.1	2019.4.17	2019.5.30	2019.6.6
为企业用户提供5G服务	在12个城市正式开通5G服务	推出5G商用服务	在6个城市开通5G服务	正式发放5G商用牌照

中国信息通信研究院 | http://www.caict.ac.cn |

5G带来了巨大的变革

5G网络在技术、业务应用、终端等方面带来了巨大变化。

技术层面的变化

- 虚拟化技术广泛应用，如NFV、SDN等
- 灵活的组网架构，网络切片技术的应用
- 网络功能下沉，如C/U分离技术，MEC的应用
- 网络能力开放，如安全能力的开放
- 新的安全机制，如标识加密（SUCI）、256bit 密码算法

业务层面的变化

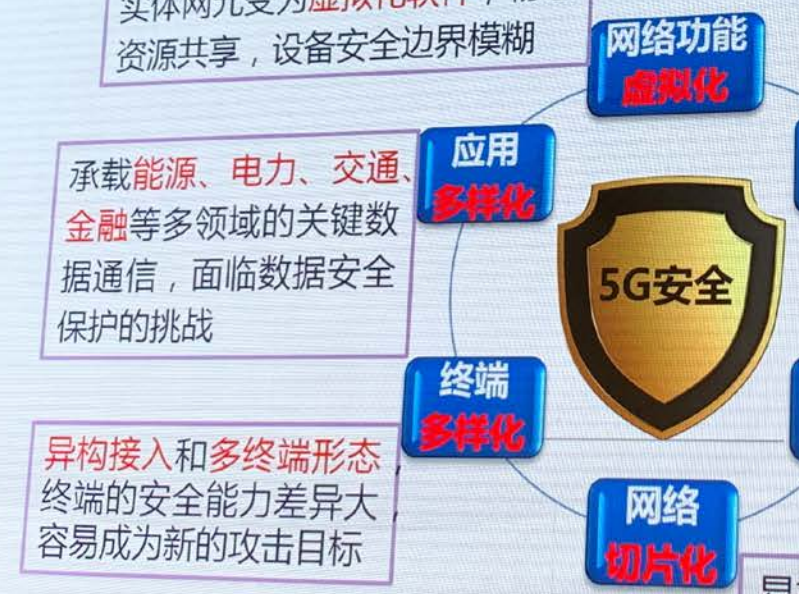
- 业务服务方，从以2C为主转到2C与2B并重
- 业务应用极大丰富，业务数据流量千倍增长，催生智慧生活、智慧生产和智慧城市等诸多场景。

终端层面的变化

- 终端内容采集、生产、展现能力全面提升
- 终端类型多样化，泛智能终端预计到2021年达千万级

新变化带来新挑战

技术、业务和终端等的新变化，给5G带来了新的安全风险和挑战。



实体网元变为虚拟化软件，物理资源共享，设备安全边界模糊

网络基础设施下沉分散，边缘不可靠的环境导致外部攻击和入侵更为容易

承载能源、电力、交通、金融等多领域的关键数据通信，面临数据安全保护的挑战

打破传统电信网络能力封闭的特点，开放端口成为数据泄露的脆弱点

异构接入和多终端形态终端的安全能力差异大，容易成为新的攻击目标

易被攻击，安全责任归属不好界定

5G安全是未来社会正常运作的根基

- 5G网络已从传统的个人移动通信服务，渗透到物联网、车联网和工业互联网等更广阔的领域，甚至是军网，**深入到生活、生产、军事等方方面面**。
- 5G网络的任何安全风险影响的不再仅仅是个人的通信，而是与之相连接的各种系统，包括关键部门的敏感系统，安全生产系统，甚至军队作战系统等等。 **5G网络对安全的需求超过以往任何一代网络。**

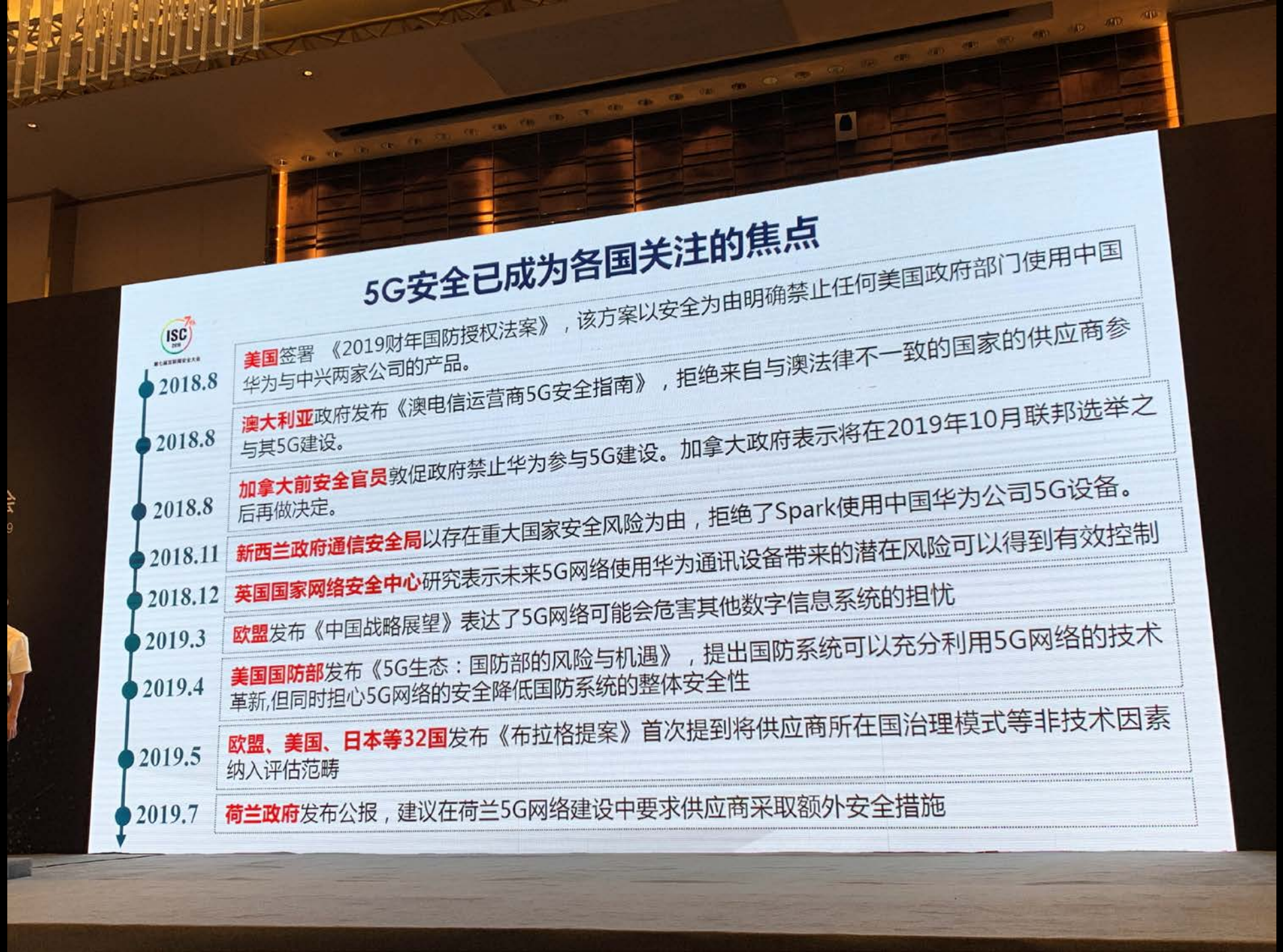

智慧生活


智慧城市



智慧生产

5G


5G安全已成为各国关注的焦点
2018.8
美国签署《2019财年国防授权法案》，该方案以安全为由明确禁止任何美国政府部门使用中国华为与中兴两家公司的产品。
2018.8
澳大利亚政府发布《澳电信运营商5G安全指南》，拒绝来自与澳法律不一致的国家的供应商参与其5G建设。
2018.8
加拿大前安全官员敦促政府禁止华为参与5G建设。加拿大政府表示将在2019年10月联邦选举之后再做决定。
2018.11
新西兰政府通信安全局以存在重大国家安全风险为由，拒绝了Spark使用中国华为公司5G设备。
2018.12
英国国家网络安全中心研究表示未来5G网络使用华为通讯设备带来的潜在风险可以得到有效控制
2019.3
欧盟发布《中国战略展望》表达了5G网络可能会危害其他数字信息系统的担忧
2019.4
美国国防部发布《5G生态：国防部的风险与机遇》，提出国防系统可以充分利用5G网络的技术革新,但同时担心5G网络的安全降低国防系统的整体安全性
2019.5
欧盟、美国、日本等32国发布《布拉格提案》首次提到将供应商所在国治理模式等非技术因素纳入评估范畴
2019.7
荷兰政府发布公报，建议在荷兰5G网络建设中要求供应商采取额外安全措施

国外对5G安全的主要观点(一)

观点1：5G安全意义重大

- 5G网络的安全性对于**国家安全、经济安全**和其他**国家利益**以及**全球稳定性**至关重要。

—欧盟、美国、日本等32国《布拉格提案》

- 5G网络中的任何安全风险都可能会危害所连接系统，包括关键部门的敏感系统，造成重大破坏性影响。5G网络应纳入**关键网络信息系统安全管理体系**。

—欧盟《欧盟-中国战略展望》

- 5G网络将能够彻底革新现有的国防系统，提升信息共享、作战协作、武器装备等能力，5G网络是保障国家安全的**重要基础设施**。

—美国国防部《5G：国防部的风险与机遇》

观点2：5G引发新的安全风险

- 5G网络将为海量、多样化终端提供服务，数据流量大幅度提升，**使得网络潜在的“攻击面”增加**，恶意流量检测难度加大，这些安全问题的攻击门槛降低、防御难度更大。
- 5G核心基础设施还存在一些额外的问题，比如**网络“切片”功能**，它会将网络暴露给非运营商，**增加核心网络的攻击面**。

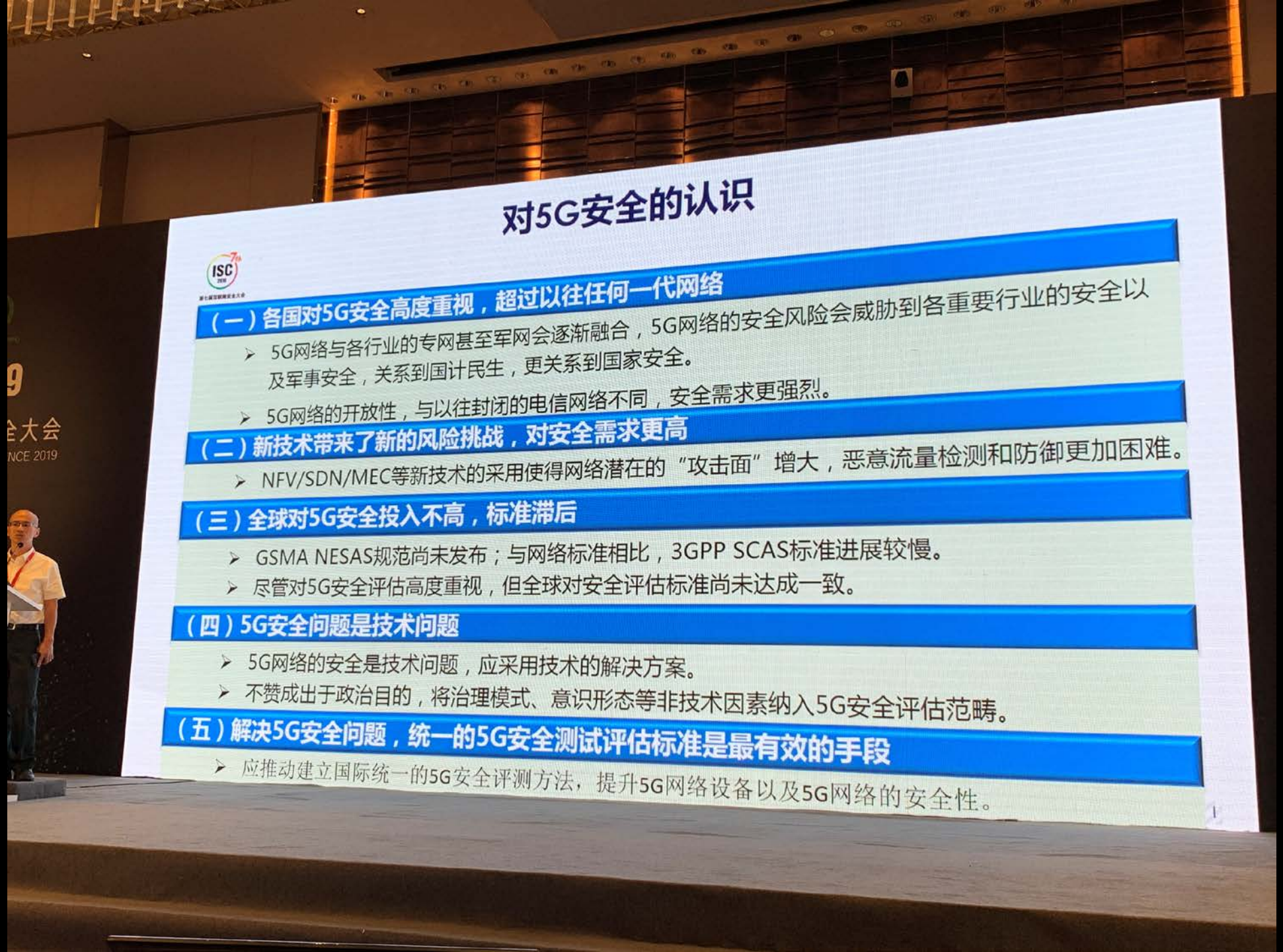
—美国国防部《5G：国防部的风险与机遇》

- 利益相关方应考虑5G网络部署带来的技术变革，例如**边缘计算和软件定义网络（SDN）/网络功能虚拟化（NFV）的使用**，以及对通信渠道整体安全性的影响。

—欧盟、美国、日本等32国《布拉格提案》

- 5G将**模糊网络的“边缘”部分与“核心”**部分，将带来安全风险。

—澳大利亚政府《澳电信运营商5G安全指南》


对5G安全的认识
（一）各国对5G安全高度重视，超过以往任何一代网络
5G网络与各行业的专网甚至军网会逐渐融合，5G网络的安全风险会威胁到各重要行业的安全以及军事安全，关系到国计民生，更关系到国家安全。
5G网络的开放性，与以往封闭的电信网络不同，安全需求更强烈。
（二）新技术带来了新的风险挑战，对安全需求更高
NFV/SDN/MEC等新技术的采用使得网络潜在的“攻击面”增大，恶意流量检测和防御更加困难。
（三）全球对5G安全投入不高，标准滞后
GSMA NESAS规范尚未发布；与网络标准相比，3GPP SCAS标准进展较慢。
尽管对5G安全评估高度重视，但全球对安全评估标准尚未达成一致。
（四）5G安全问题是技术问题
5G网络的安全是技术问题，应采用技术的解决方案。
不赞成出于政治目的，将治理模式、意识形态等非技术因素纳入5G安全评估范畴。
（五）解决5G安全问题，统一的5G安全测试评估标准是最有效的手段
应推动建立国际统一的5G安全评测方法，提升5G网络设备以及5G网络的安全性。

5G安全整体需求

5G安全需求来自于新业务场景和新型技术的应用

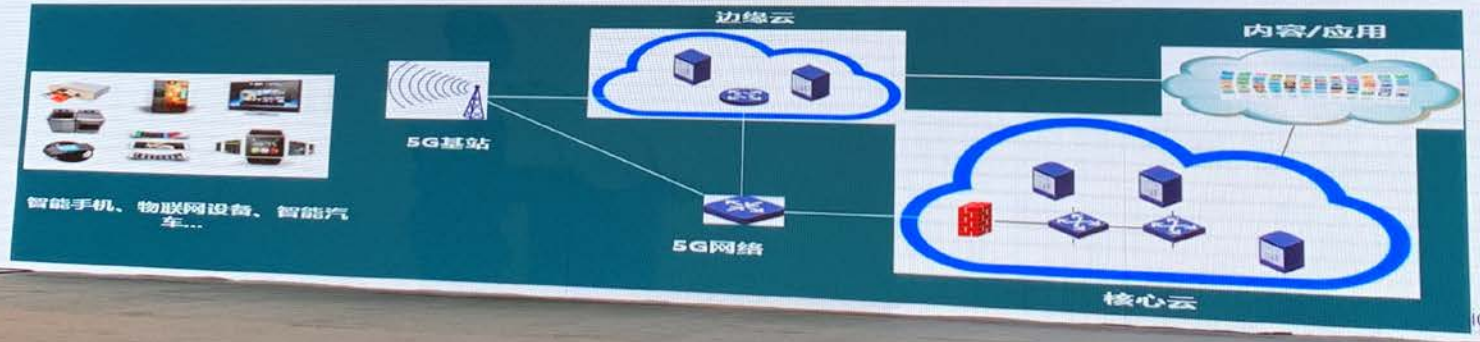
4G安全增强 + 多样化业务场景 + 新型技术（NFV/SDN等） = 5G安全需求

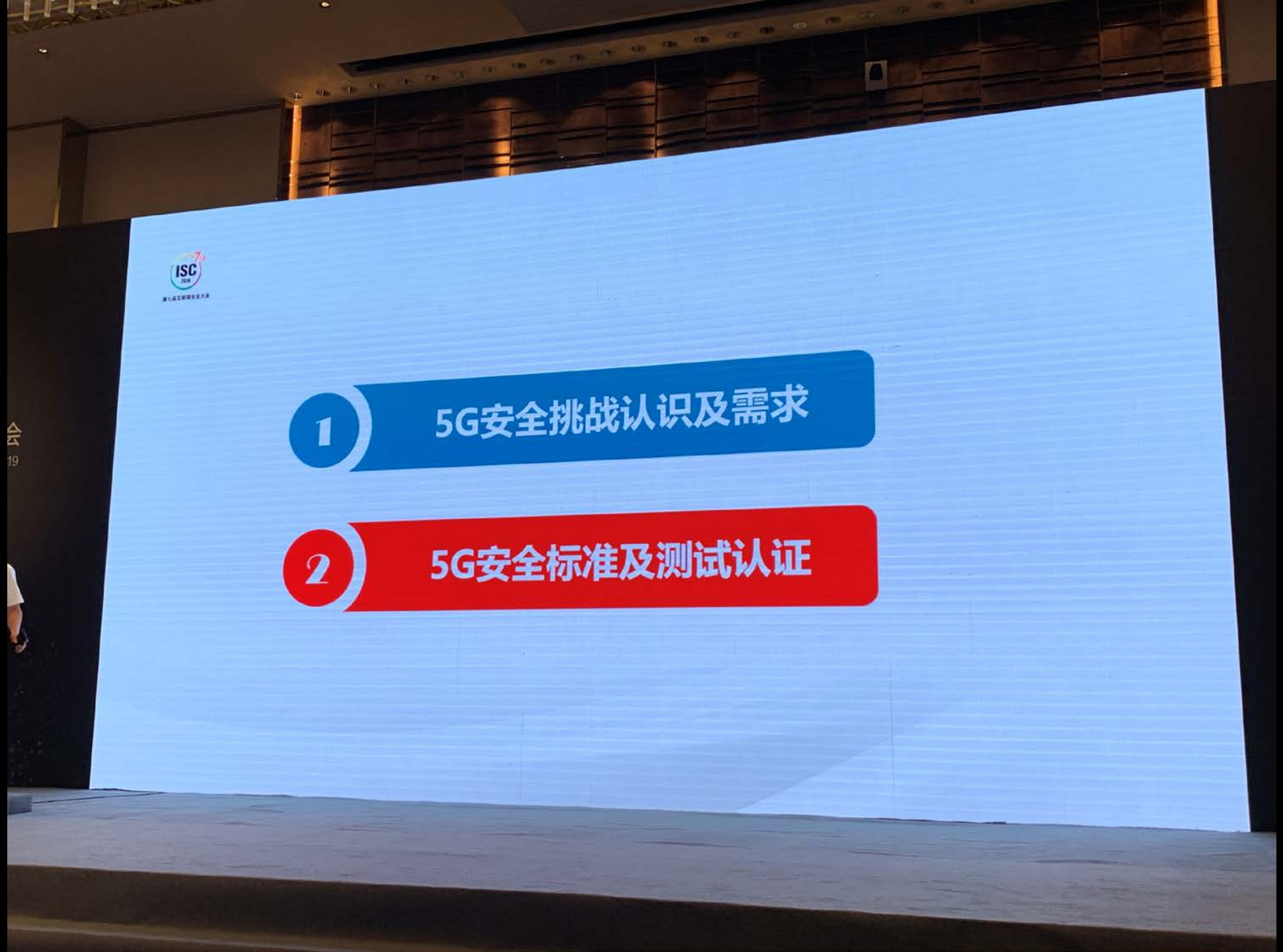
- 统一的认证鉴权
- 密钥管理
- 用户标识和凭证管理
- 增强的用户隐私

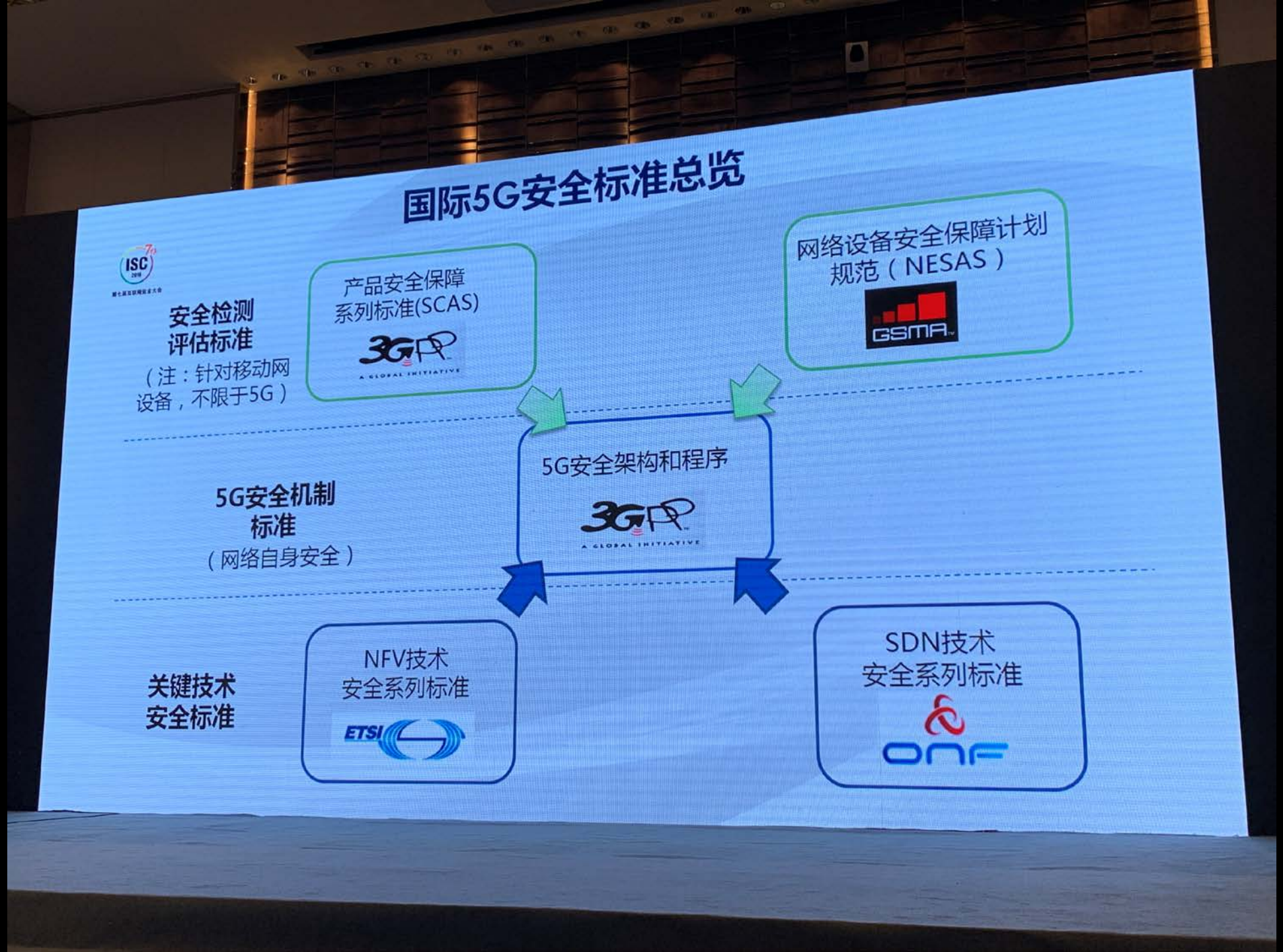
- 空口传输安全
- 加密算法
- 物理层安全

- NFV/SDN安全
- 核心云/边缘云安全
- 网络切片安全

- 第三方服务应用的接入授权



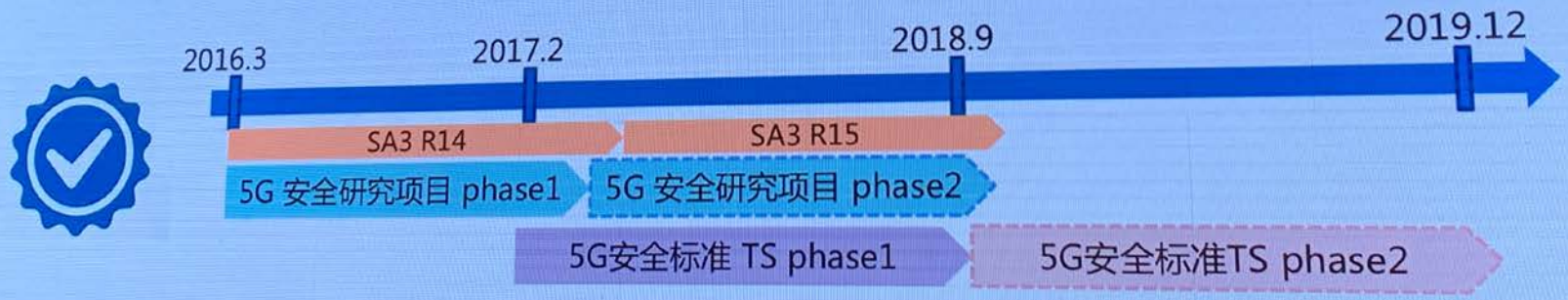

ISC
1 5G安全挑战认识及需求
2 5G安全标准及测试认证


国际5G安全标准总览
安全检测
评估标准
（注：针对移动网
设备，不限于5G）
产品安全保障
系列标准(SCAS)
3GPP
A GLOBAL INITIATIVE
网络设备安全保障计划
规范（NESAS）
GSMA
5G安全机制
标准
（网络自身安全）
5G安全架构和程序
3GPP
A GLOBAL INITIATIVE
关键技术
安全标准
NFV技术
安全系列标准
ETSI
SDN技术
安全系列标准
ONF

主要标准介绍—5G安全机制标准

- 3GPP TS 33.501《5G系统安全架构和程序》。
- 是5G安全的核心标准，规定了5G安全的总体技术要求。

- 2018年3月已发布5G第1阶段（R15）安全标准
  - •包括安全架构、认证安全、用户隐私、密码算法、凭证管理
- 2019年12月将发布5G第2阶段（R16）安全标准
  - •包括切片安全、小数据安全、海量UE接入认证、用户面数据保护、256bit密码算法等



主要标准介绍—3GPP SCAS 系列标准

- 为进一步提升移动网络产品的安全，3GPP立足于通用和可测试的安全评测方法，制定了产品安全保障标准 ，即**SCAS**。
- 已发布**3本**通用类标准，**9本**5G网元标准

SCAS标准内容

- **安全技术基线要求**：数据保护、可用性和完整性、认证和授权、用户会话保护、登录访问等
- **操作系统安全**：可用性和完整性、认证和授权、系统账号管理等
- **Web服务安全**：HTTPS、Web登录等

类别		标准号
通用类	通用安全保障需求	TS 33.117
	5G安全威胁与关键资产	TR 33.926
	3GPP虚拟化网元	TR 33.818
5G网元SCAS	gNB	TS. 33.511
	AMF	TS 33.512
	UPF	TS 33.513
	UDM	TS 33.514
	SMF	TS 33.515
	AUSF	TS 33.516
	SEPP	TS 33.517
	NRF	TS 33.518
	NEF	TS 33.519

主要标准介绍— GSMA NESAS规范

NESAS
（网络设备安全保障计划）

- **目的**：促进产业相关方**对网络设备的安全性达成共识**，确保网络设备**制造与运营安全良性发展。**
- **目标**：通过**业界认可的**安全保障评估方法，确保产品和运营的基准安全。

NESAS系列规范

- FS.13--总体概述
- FS.14--安全检测实验室认可需求和程序
- FS.15--产品开发与生命周期管理需求和认可程序
- FS.16--冲突解决程序

NESAS安全评估活动

产品
安全评估

产品管理流程安全审计 ＋ 产品安全检测

GSMA NESAS规范	•侧重于网络设备安全评估活动的管理和程序要求
3GPP SCAS标准	•制定网络设备安全技术要求及检测方法

检测依据

我国5G安全标准进展情况

中国通信标准化协会
China Communications Standards Association

TC5 WG5工作组：无线安全和加密

5G移动通信网 安全技术要求

- 参考3GPP标准R15 TS 33.501编写。
- 主要规定了5G安全架构，认证框架、接入、移动性及会话管理安全 、用户隐私、密码算法、凭证管理等
- 目前为征求意见稿阶段

5G移动通信网 设备安全保障系列标准

- 参考3GPP SCAS系列标准编写。
- 规定5G网络设备安全检测的通用基线要求。
- 已立项1个通用安全要求、9个5G网络设备安全保障要求

注：国内尚无与NESAS规范相对应的标准

5G安全评估评测已开展工作

GSMA NESAS	• **标准规范尚未完备**，NESAS管理规范尚未正式发布；所依据的3GPP SCAS标准也尚未完成。 • **国际认可度还有待提高**，NESAS起步较晚，已完成评估的产品寥寥无几，国际认可度不高。 • **审计机构及检测实验室匮乏**，目前审计机构仅有ATSEC和NCC Group，检测实验室仅有西班牙的Epoche一家。
国际CC安全认证	• CC是IT产品或技术领域的权威安全认证。 • 证书在成员国内是可以互认，但中国不是其成员国。 • **CC缺少针对移动通信设备特性的安全要求。**
国家级安全评估	• 一些发达国家设立自己的安全评估机制，如**英国的CSEC认证**，对产品设计、开发、生命周期管理等评估。 • 由于检测依据不公开,**难以形成能被国际认可的认证体系。**
国内评估工作	• **缺乏5G安全评估标准，**相关标准还在制定中。 • **我国目前尚未开展5G安全评估评测相关工作。**

无疑，**国际认可的权威的认证体系**有助于消除国际社会对5G设备安全性的担忧，但目前尚无成熟的体系可用，相关工作还有很长的路要走。

5G安全测试评估工作的初步设想

实施路径

- **近期**：借鉴NESAS工作机制，**推动我国5G安全认证体系的建立**；
- **未来**：**推进NESAS体系成熟**，推动国内5G安全认证和评估检测报告的**国际互认**。

加大投入，促进5G安全产业发展

- 加大5G设备、安全产品、服务和解决方案研发，强化供应链安全管理
- 加强5G安全威胁信息共享
- 强化5G安全运维管理

加快安全评测标准研究

- 联合国内厂商与运营商，共同推动3GPP SCAS标准和我国CCSA相应的**安全检测标准的研究和成熟**。
- 参考NESAS规范，制定我国**安全认证管理流程**相关标准。

构建我国5G安全认证体系

- 借鉴NESAS工作机制，构建我国5G安全认证体系的建立
- 覆盖产品研发、生命周期管理的安全审计，以及产品安全检测

推动国际互认

- 推进GSMA NESAS认证体系成熟
- 对接NESAS认证体系，推进认证结果的国际互认

小鹅助理

谢谢！

扫码添加小鹅助理，与数万科技圈人士

分享重量级活动PPT、干货培训课程、高端会议免费门票