

第2研究组 第4号课题

帮助发展中国家落实一致性和互操作性项目以及打击假冒信息通信技术和盗窃移动设备的行为



ITU-D第4/2号课题输出成果报告

帮助发展中国家落实一致性和互操作性项目以及打击假冒信息通信技术和盗窃移动设备的行为

2018-2021年研究期



帮助发展中国家落实一致性和互操作性项目以及打击假冒信息通信技术和盗窃移动设备的行为：2018-2021年研究期ITU-D第4/2号课题输出成果报告

ISBN 978-92-61-34135-0 (PDF版)

ISBN 978-92-61-34145-9 (EPUB版)

ISBN 978-92-61-34155-8 (Mobi版)

© 国际电联 2021

国际电信联盟, Place des Nations, CH-1211 日内瓦, 瑞士

部分版权所有。该作品通过创作共享署名-非商业-共享3.0 IGO许可 (CC BY-NC-SA 3.0 IGO) 向公众授权。

根据本许可证的条款, 如果作品被适当引用, 您可以出于非商业目的复制、重新分发和改编作品。在使用该作品时, 不应建议国际电联认可任何具体的组织、产品或服务。不允许未经授权使用国际电联的名称或标志。如果您改编作品, 那么您必须在相同或等效的创作共享许可下使您的作品获得许可。如果您创作了这部作品的译文, 您应该加上下面的免责声明以及建议的引文: “这部译文不是由国际电信联盟 (ITU) 创作的。国际电联对本译文的内容或准确性不承担任何责任。英文原版须为具有约束力的权威版本”。欲了解更多信息, 请访问:

<https://creativecommons.org/licenses/by-nc-sa/3.0/igo/>

建议的引文。帮助发展中国家落实一致性和互操作性项目以及打击假冒信息通信技术和盗窃移动设备的行为：2018-2021年研究期ITU-D第4/2号课题输出成果报告。日内瓦：国际电信联盟，2021年。许可证：CC BY-NC-SA 3.0 IGO。

第三方材料。如果您希望重用本作品中属于第三方的材料, 如表格、图形或图像, 则您有责任确定是否需要该重用的许可, 并从版权所有者那里获得这一许可。因侵犯作品中任何第三方拥有的内容而导致索赔的风险需完全由用户承担。

一般免责声明。本出版物中使用的名称和材料的表述并不意味着国际电联或其秘书处对任何国家、领土、城市或地区或其当局的法律地位, 或对其边界或界线的划定表达任何意见。

提及特定公司或某些制造商的产品并不意味着国际电联认可或推荐这些公司或产品优先于未提及的其他类似性质的公司或产品。除了错误和遗漏之外, 专有产品的名称用大写字母区分。

国际电联已采取所有合理的预防措施来核实本出版物中包含的信息。然而, 资料的发行没有任何明确或隐含的担保。资料的解释和使用责任由读者自负。在任何情况下, 国际电联都不对因其使用而造成的损害负责。

封面图片鸣谢: Shutterstock

鸣谢

国际电联电信发展部门（ITU-D）研究组提供了一个中立性平台，来自世界各地的政府、业界、电信组织和学术界的专家可汇聚一起，制定解决发展问题的实用工具和资源。为此，ITU-D的两个研究组负责在成员所提出输入意见基础上制定报告、导则和建议。研究课题每四年在世界电信发展大会（WTDC）上决定。国际电联成员于2017年10月在布宜诺斯艾利斯举行的WTDC-17上商定，在2018-2021年期间，第2研究组将在“信息通信技术服务和应用促进可持续发展”的总体范围内处理七项课题。

本报告是针对**第4/2号课题 – 帮助发展中国家落实一致性和互操作性项目以及打击假冒信息通信技术设备和盗窃移动设备的行为** – 编写的。该研究组由主席Ahmad Reza Sharafat先生（伊朗伊斯兰共和国）领导，并得到以下副主席的支持：Nasser Al Marzouqi先生（阿拉伯联合酋长国）（2018年辞职）； Abdelaziz Alzarooni先生（阿拉伯联合酋长国）； Filipe Miguel Antunes Batista先生（葡萄牙）（2019年辞职）； Nora Abdalla Hassan Basher女士（苏丹）； Maria Bolshakova女士（俄罗斯联邦）； Celina Delgado Castellón女士（尼加拉瓜）； Yakov Gass先生（俄罗斯联邦）（2020年辞职）； Ananda Raj Khanal先生（尼泊尔共和国）； Roland Yaw Kudozia先生（加纳）； Tolibjon Oltinovich Mirzakulov先生（乌兹别克斯坦）； Alina Modan女士（罗马尼亚）； Henry Chukwudumeme Nkemadu先生（尼日利亚）； 王珂女士（中国）； 和Dominique Würges先生（法国）。

第4/2号课题报告人Cheikh Tidjani Oudaa先生（毛里塔尼亚）领导起草了本报告，以下副报告人参与了协作： Ahmadou Dit Adi Cisse先生（马里）； Amel Khier女士（阿尔及利亚）； Joseph Onaya先生（肯尼亚）； Brillant Harivony Rakotoratsimanjefy先生（马达加斯加）和Serigne Abdou Lahatt Sylla先生（塞内加尔）。

特别感谢该章协调人的奉献、支持和专业知识。

本报告是在电信发展局研究组联系人、编辑以及出版物制作团队和ITU-D研究组秘书处的支持下编写的。

目录

鸣谢	iii
表和图目录	vii
内容提要	viii
第1章 – 有助于实现可持续发展目标的信息通信技术产品	1
1.1 ICT产品对社会的相关性	1
1.2 ICT设备：作为社会经济中坚力量的替代	1
1.3 通过与公认标准保持一致性，实现ICT用户和网络的互连互通并进行保护	2
1.4 新冠病毒大流行对型号核准程序的影响	3
第2章 – 一致性和互操作性	4
2.1 引言	4
2.2 审查国家和区域的关键事项/优先事项	4
2.3 技术要求和标准	6
2.4 一致性评定的相互认可安排/协议	7
2.4.1 什么是相互认可安排/协议？	7
2.4.2 MRA在C&I机制中的作用	8
2.5 虚拟基础架构	8
2.5.1 虚拟测试	8
2.5.2 远程互操作性测试	8
2.5.3 远程设备选型测试	10
2.6 市场监督	10
2.6.1 主要利益攸关方	11
2.6.2 关于市场监督情报和经验的咨询	11
2.7 新技术的一致性评估	11
2.7.1 新技术挑战	11
2.7.2 预一致性测试	12
2.7.3 预期影响	12
第3章 – 打击假冒、残次和破坏设备行为	13
3.1 难题和问题	13
3.2 定义	14
3.3 导则	15
3.4 国家经验（案例研究）	16
3.4.1 马达加斯加	16
3.4.2 几内亚	17

3.4.3 塞内加尔.....	17
3.4.4 卢旺达.....	18
3.4.5 津巴布韦.....	18
3.4.6 加纳.....	18
3.4.7 巴基斯坦.....	19
3.4.8 GSM协会.....	20
3.4.9 巴西.....	20
3.4.10 阿曼.....	21
3.4.11 国际标准和建议书.....	21
第4章 – 盗窃的移动设备	22
4.1 简介	22
4.2 难题和问题	22
4.2.1 设备犯罪和诈骗.....	23
4.2.2 利益攸关方的角色和责任.....	24
4.2.3 打击盗窃设备行为的基本工具	24
4.3 导则	25
4.4 国家经验（案例研究）.....	26
4.4.1 中非共和国.....	26
4.4.2 墨西哥.....	26
4.4.3 伊朗科技大学.....	27
第5章 – 物联网与一致性和互操作性（C&I）.....	28
5.1 介绍	28
5.2 物联网对C&I和ICT准备的影响.....	29
5.2.1 物联网的挑战.....	29
5.2.2 物联网受到的制约.....	30
5.2.3 示例：罗德与施瓦茨（Rohde & Schwarz）物联网测试.....	31
5.2.4 标准制定组织.....	32
5.3 物联网和ICT的法规和政策.....	33
5.3.1 协作监管概述.....	33
5.3.2 物联网监管.....	34
5.4 结论	35
第6章 – 信息、知识技能和知识的转让.....	36
6.1 C&I学习需求和教育机会.....	36
6.2 响应知识获取/保留的相关需求	36
6.3 结论	38
Annexes	39
Annex 1: Conformance and interoperability frameworks: Country data.....	39

Annex 2: Counterfeiting – a survey of national frameworks and practices	41
Annex 3: Initiatives in the fight against equipment counterfeiting and mobile terminal theft in Burundi	43
A3.1 Introduction.....	43
A3.2 Impact of the proliferation and use of counterfeit mobile terminals.....	43
A3.3 National initiatives in the fight against mobile terminal theft and equipment counterfeiting	43
A3.4 Conclusion	44
Annex 4: Illustrations for chapters of the Output Report on Question 4/2	45
Annex 5: Ideas for the future of the Question	48
Annex 6: List of contributions and liaison statements received on Question 4/2	49

表和图目录

表目录

Table 1A: Summary of ITU World Telecommunication/ICT Regulatory Survey (edition 2019): Survey on regulatory practices related to the distribution and use of counterfeit ICTs	41
---	----

图目录

图1: 一致性评定活动.....	6
图2: 远程互操作性测试.....	9
图3: 远程设备选型测试.....	10
图4: 假冒智能手机导致的销售损失: 欧盟和全球	13
图5: 打击假冒的责任.....	15
图6: 型号批准进程.....	19
图7: 设备识别、注册和阻止系统 (DIRBS)	20
图8: CEMI工作流程	21
图9: 全球常用设备连接数.....	28
图10: 物联网无线技术.....	29
图11: 知名物联网平台数量.....	30
图12: 物联网标准制定组织和联盟概况 (垂直和水平域)	31
图13: 适合的认证方案需求.....	31
图14: OTA测量	32
图15: 各代ICT监管 – 概念框架.....	33
图16: 协作监管.....	34
图17: CIP培训模块 (OM是必修模块, EM是合格模块)	37
Figure 1A: C&I legal frameworks from 114 countries that provided information	40
Figure 2A: Regional distribution of responses from survey – Question 1	42
Figure 3A: Regional distribution of responses from survey – Question 2	42
Figure 4A: Regional distribution of responses from survey – Question 3	42
Figure 5A: Illustration for Chapter 2 – What is conformance and interoperability (C&I)	45
Figure 6A: Illustration for Chapter 2 – C&I frameworks	46
Figure 7A: Illustration for Chapter 3 – Combating the proliferation of counterfeit, substandard and tampered devices	46
Figure 8A: Illustration for Chapter 5 – The Internet of Things and C&I	47

内容提要

全世界对ICT设备的依赖和信任

信息通信技术（ICT）设备是进入数字世界的大门。为了保障网络互操作性，实现用户和机器互连，世界各国协调和遵守相关标准至关重要。

在推行一致性和互操作性（C&I）计划，采取先进技术打击假冒ICT设备扩散和移动设备盗窃行为方面，世界各国均取得相应进展，部分国家进展显著。

国际电联电信发展部门（ITU-D）持续帮助成员国评估ICT设备一致性和互操作性有关的技术和经济问题，重点是援助、能力建设和国际电联成员国最佳做法的共享。在这些问题上，ITU-D与国际电联无线电通信部门（ITU-R）和国际电联电信标准化部门（ITU-T）密切合作，推动上述工作取得协同效应，发挥更大作用。

此外，在这个通过ICT设备实现了越来越密切的互联互通的社会中，使用C&I框架仍然是开发商、制造商、进口商、运营商和用户广泛讨论的重要问题。监管机构在这方面发挥作用，对于平衡所需的安全和控制级别至关重要。

最后，对C&I未来发展十分重要的一个问题是物联网（IoT）驱动下各行各业不断涌现的新技术，以及发展中国家在实施或修订C&I框架时要考虑的标准。

基于以上情况，本报告讨论了实现最佳解决方案的最佳做法。

C&I领域的背景工作

国际电联在之前的研究期重点关注为发展中国家的一致性和互操作性提供帮助这一重要问题。这一阶段产生了一些重要成果，这些重要成果与ITU-D第4/2号课题开展的工作有关。第4/2号课题的前一份报告可参考<https://www.itu.int/pub/D-STG-SG02.04.1-2017>，ITU-D部门支持发展中国家的其他活动，如国家和区域性C&I框架数据库、区域评估和能力建设活动可参考https://itu.int/go/CI_Development。

第1章 – 有助于实现可持续发展目标的信息通信技术产品

1.1 ICT产品对社会的相关性

数字化转型正在给每个行业以及我们生活的方方面面带来快速变化。移动性、宽带和云这三大基本ICT力量正在重塑价值链，推动商业模式数字化，克服距离带来的问题。例如，在一些地区人们开始越来越多地共享商品与服务，而非购买和拥有商品与服务，可以说，一种新型的服务经济正在兴起，而这都是数字时代释放创新的新商业模式和改变生活的实例。¹

ICT的主要益处是帮助个人、社区和经济体提升获取能力、连接能力和效率：²

- 获取信息和服务：通过ICT设备基础设施，使用包括移动电话、蜂窝电信网络（如3G和LTE）、互联网和宽带等技术，ICT能够改善全球农村和城市地区个人对信息和服务的普遍接入。
- 个人与组织之间的互连互通：增强个人、组织和网络之间即时或近即时连通性，能够提高多个行业和社区的生产力和创新能力，并且提供快速扩大关键业务规模所需的实时通信。
- 生产力和资源效率提高推动效率提升。
- 通过开展一致性工作采用绿色标准，有效减少气候变化。
- ICT能够通过提升个人对信息和通信的获取能力释放和利用生产力增幅（例如减少浪费在差旅、人工数据收集上的资源），还能够提供收集和分析大量数据（如大数据）的基础设施。

1.2 ICT设备：作为社会经济中坚力量的替代

为奉行统一政策和加强基于ICT的发展举措，政策制定者需要一个战略框架。必须将ICT纳入公共政策和经济活动的方方面面。为实现这点，必须克服许多障碍：

- 制定有利于充分利用ICT的公共政策和规定；
- 迅速扩展和升级ICT基础设施；
- 增进公私合作伙伴关系来孵化那些愿意提供合适的本地服务的新的ICT初创企业；

¹ 正如爱立信总裁兼首席执行官Hans Vestberg为[ICT与SDG – 最终报告：信息通信技术如何加速实现可持续发展目标的行动](#)写的前言，哥伦比亚大学地球研究所和爱立信。

² 华为。[2017年ICT可持续发展目标基准](#)。华为，2017年。

- 解决ICT互操作性问题；
- 开展管理ICT系统的能力建设；
- 确保政策和监管必须与ICT的快速创新和部署保持同步。

1.3 通过与公认标准保持一致性，实现ICT用户和网络的互连互通并进行保护

基础设施和创新方面的投资是经济增长和发展的关键驱动力。技术进步亦是应对经济和环境挑战找到永久性解决方案的关键，如创造新工作岗位和提高能源效率。推动可持续发展的产业，投资科学研究和创新都是促进可持续发展的重要方式。³

可持续发展目标9：建造具备抵御灾害能力的基础设施，促进具有包容性的可持续工业化，推动创新标准。

具体目标：

9.1 – 发展优质、可靠、可持续和有抵御灾害能力的基础设施，包括区域和跨境基础设施，以支持经济发展和提升人类福祉，重点是人人可负担得起并公平利用上述基础设施。

9.a – 向非洲国家、最不发达国家、内陆发展中国家和小岛屿发展中国家提供更多的财政、技术和技能支持，以促进其开发有抵御灾害能力的可持续基础设施。

9.b – 支持发展中国家的国内技术开发、研究与创新，包括提供有利的政策环境，还包括实现工业多样化，增加商品附加值。

9.c – 大幅提升信息通信技术的普及度，力争到2020年使最不发达国家能够以低廉的价格普遍接入互联网。

为保护ICT用户和网络，聚焦于以下方面十分重要：

- 质量
- 安全
- 互操作性
- 无干扰频谱环境
- 国家规定
- 可持续性
- 可靠性
- 抵御干扰的能力

³ 联合国开发计划署（UNDP）。可持续发展目标。[可持续发展目标9：工业创新和基础设施](#)。

- 价格可承受（通过一致性和互操作性（C&I）实现的规模经济）。

为此，必须考虑与ICT设备和系统有关的问题，包括：

- 技术要求和标准
- 一致性评估
- 设备控制
- 后市场监督
- 推广相互认可协议。

为此，应确立评估一致性和互操作性的**创新方法**，应包括：

- 新开展或共享实验室测试
- 虚拟实验室服务
- 反映本地和区域性需求与限制的相互认可协议（MRA）
- 上市后监督
- 智能测试解决方案
- 标准的协调统一。

任务包括：

- 提高认识
- 面向ITU-D成员的C&I网络平台
- 促进对课题囊括的若干事项的协作、研究和经验分享
- 确保ITU-D成员对其他C&I相关论坛的参与（如ISO/CASCO STAR小组会议）
- 制作问卷调查表，以收集国家报告和跟踪在C&I方面取得的进展
- 编制导则
- 发布建议。

1.4 新冠病毒大流行对型号核准程序的影响

新冠病毒大流行已经并将继续影响国际贸易和包括ICT设备在内的产品合格评定。由于边界关闭和设施使用方面存在的困难（如物理测试实验室和现场专业人员难以到位），型号核准活动受到了严重影响。这就需要寻找创新的方法认证产品一致性和质量。监管机构、制造商和运营商一直在开发临时解决方案，用于维持业务运营，避免贸易链中断。是时候利用数字技术的潜力来提供合格评定的解决方案了。

第2章 – 一致性和互操作性

2.1 引言

一致性评估可确保ICT设备符合技术规范和标准。合规性可帮助供应商和用户评估设备与其他设备集成到网络中提供网络服务时的性能。互操作性测试用于衡量两个或多个产品是否正确实行了必要的技术规范，确保成功集成以支持特定通信协议。

设备在ICT网络中可能不符合公认的行业标准，进而可能会影响提供的网络服务质量，开展C&I测试以识别出设备的上述特性十分重要。商用先进高品质产品有助于网络技术和相关网络服务的广泛部署。

2.2 审查国家和区域的关键事项/优先事项

C&I的问题源于多方面的忧虑和难题，包括但不限于：⁴

- 在更换移动网设备、信令时传统智能网信令（互操作性问题）的服务行为（如接入、核心、SMS）；
- 不同厂商之间的设备缺乏一致性和互操作性；
- 由于采用非标准化接口或协议，不同制造商的设备存在差异；
- 来自一家制造商的设备经过不同软件修订导致客户端协议（SIP）不兼容；
- 不同互联网协议电视（IPTV）中间件制造商制造的机顶盒（STB）设备的一致性；
- 带宽：即当用户对现有网络增加负载时，网络的语音、数据和视频传输容量；
- 通过整合网络和设备，应对网络复杂性，从而实现互操作性；
- 一些提供商启动的服务未提供与其它运营商实现互操作性的基础设施和支撑团队；
- 定义采用标准的方法；
- 用于计费的CDR管理；
- 在所有平台上实施新功能和他务；
- 收费模式五花八门；
- 新技术无法与传统设备实现互操作性；

⁴ ITU-D第2研究组2014-2017年研究期第4/2号课题最后报告：[帮助发展中国家落实一致性和互操作性项目](#)，国际电联，2017年。

- 缺少测试中心和设施；
- 缺少完成C&I工作的训练有素人员；
- ISDN支持问题；
- 不同系统的用户终端问题；
- 客户使用的服务和终端设备的互操作性问题；
- 厂商的专有和非标准化接口；
- 成本；
- 人力和培训机遇匮乏；
- 制度薄弱；
- 缺乏对标准化的认识；
- 互操作性挑战。

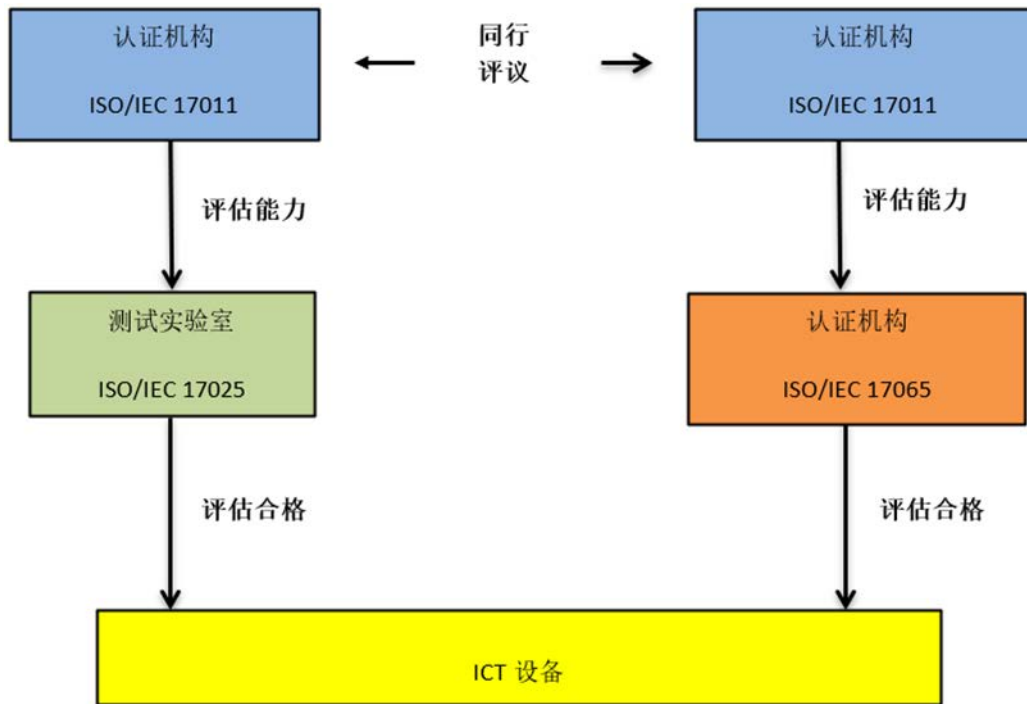
一致性评定活动

一致性评定活动包括：

- 认证机构的任命/认可
- 认证机构的指定/认可
- 测试实验室的指定/认可
- 注册/认证。

一致性评定活动如图1所示。

图1：一致性评定活动



2.3 技术要求和标准

服务提供商和运营商规定了用于向客户提供服务的设备和系统的标准和要求。国家监管机构制定适用于境内部署的设备和系统的法规、标准和规范。用户、服务提供商和国家监管机构要求提供证据和证明，证明设备和系统符合适当的标准和规范，能够按照规定实现交互操作。⁵

为了促进国际标准、指南和建议的发展，世界贸易组织（WTO）的技术壁垒和贸易委员会（TBT）确立了六项原则：⁶

- 透明
- 开放
- 公正与共识
- 相关性和有效性
- 连贯性
- 发展维度。

⁵ 国际电联，[建立一致性和互操作性的制度：完整导则](#)，2015年2月。

⁶ 世贸组织。贸易技术壁垒委员会。第G/TBT/9号文件，2000年11月。

标准的重要性

与技术标准保持一致：

- 对设备和网络的互操作性至关重要；
- 降低被锁定到特定技术或供应商的风险；
- 确保满足合法目标，包括与安全和无干扰相关的目标；
- 促进区域一体化；
- 促进市场整合、提高竞争力和发展贸易。

新程序

新程序包括下列组合：

- 制造商的合规性声明、商业测试机构的合规测试以及市场监督；
- 国家之间或国家组群之间在标准和批准方面的全球标准和MRA。

2.4 一致性评定的相互认可安排/协议

2.4.1 什么是相互认可安排/协议？

一致性评定的相互认可安排/协议（以下称MRA）是各方（私人或公共实体）之间认可一致性评定结果的自愿性安排/协议（关于程序和过程）。

相互认可协议是当事方承认电信设备一致性评定结果的正式法律承诺。它本身涉及法规要求，以下称为“监管MRA”。此类协议通常是由两个或多个政府在双边、区域或多边基础上达成的。

相互认可安排是各方之间的自愿安排，承认电信设备的一致性评定结果。它本身涉及非监管要求，以下称为“监管MRA”。相互认可安排的一个例子是认可机构做出的承诺，即相互认可来自公认的一致性评定机构的一致性评定结果。

为了互惠互利，MRA各方有义务制定实施MRA的流程和程序。这同样适用于监管性和非监管性的MRA。

MRA不会损害协议/安排双方管辖范围内监管机构的权威。MRA应指定参与实施过程中的各个团体：

- 当事人：已同意参与MRA的实体；
- 指定权威机构：由当事方指定的政府机构或认可的主管机构，目的是指定一个一致性评定机构来评估MRA的一致性；
- 认可机构：负责根据国际标准评估和认定测试实验室和/或认证机构特定能力的机构；

- 一致性评定机构：根据MRA标准评估是否符合另一方电信要求的指定机构（可以是第三方或供应商的测试实验室或认证机构）；
- 联合委员会：由双方共同组建的委员会，目的是管理MRA的起草和实施，适时开展必要的调整，并处理与MRA的平稳运行有关的，包括今后变更和调整的其他事项；
- 监管机构：负责电信事务的法定主管实体。

2.4.2 MRA在C&I机制中的作用

MRA用于：

- 对第三方有能力执行国家监管/型号核准程序进行认可；
- 避免重复测试成本并提高透明度；
- 为进入国外市场提供便利；
- 缩短上市时间和生产成本；
- 解决掠夺性做法和进入市场的障碍；
- 简化程序和方法，从而大大降低生产者在多个市场销售产品的成本。

最终目标：“一次测试，全球公认”。

2.5 虚拟基础架构

2.5.1 虚拟测试⁷

在ICT行业，通过互联网提供虚拟服务已是一种趋势，这一新趋势也体现在日益凸显的经IP网络的ICT设备连接的评估机制方面，因此，十分符合新的融合网络的要求。

虚拟实验室可以为自身缺乏测试能力的发展中国家提供及时、价格低廉的可持续测试服务。

以下介绍虚拟测试的两种解决方案：远程互操作性测试和远程设备选型测试。

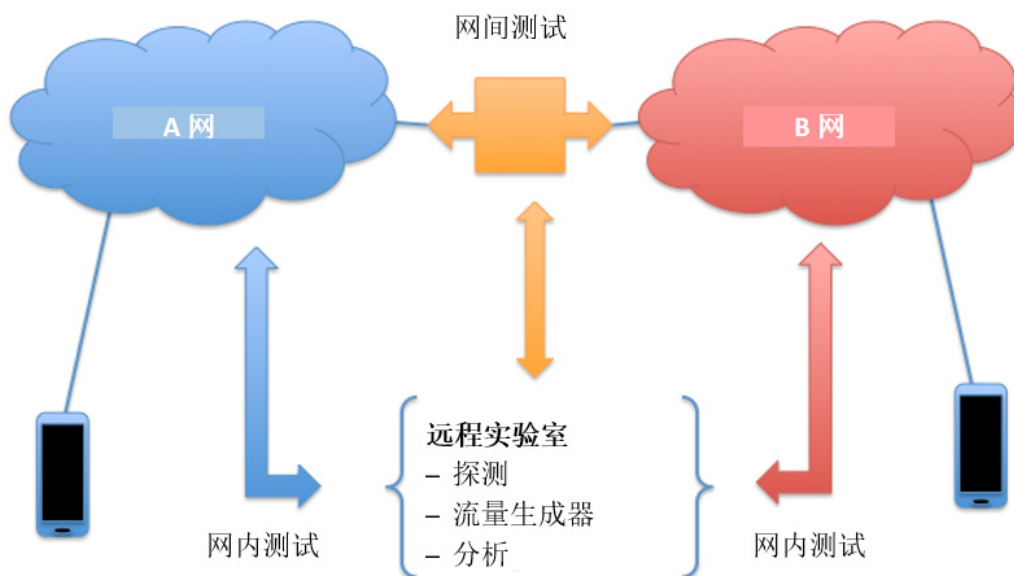
2.5.2 远程互操作性测试

目标：评估不同国家/区域运营商网络的互操作性。

世界各地的经验表明，由于信息通信技术（ICT）在工作时为用户和运营商带来诸多问题，因此，各方对这类产品和系统的测试和标准化认证程序具有共同需求。

⁷ ITU-D第2研究组2014-2017年研究期第4/2号课题最后报告。见前文。

图2：远程互操作性测试



缺乏互操作性可能导致许多问题，包括：

- 通信速率降下降；
- 通信可靠性差；
- 装置和设备的有效寿命缩短；
- 耗能高；
- 业务间相互干扰（特别是无线系统之间）；
- 设备不合规规格，导致无法演进，无法与新技术和协议兼容；
- 设备缺乏与其它设备的互操作性，造成通信瓶颈（且常常难以诊断）；
- 由于缺乏监测设备和软件电话的程序，网络性能起伏不定；
- 不同制造商生产设备和不同国家网络之间互连困难。

远程测试具体目标包括：产品开发、监管机构认证、ICT产品前一致性和互操作性预测试、移动装置和IP协议的合规性评估、现场服务。

目标受众：电信运营商、设备制造商和用户（客户、运营商、协会组织、监管机构等不同需求）。

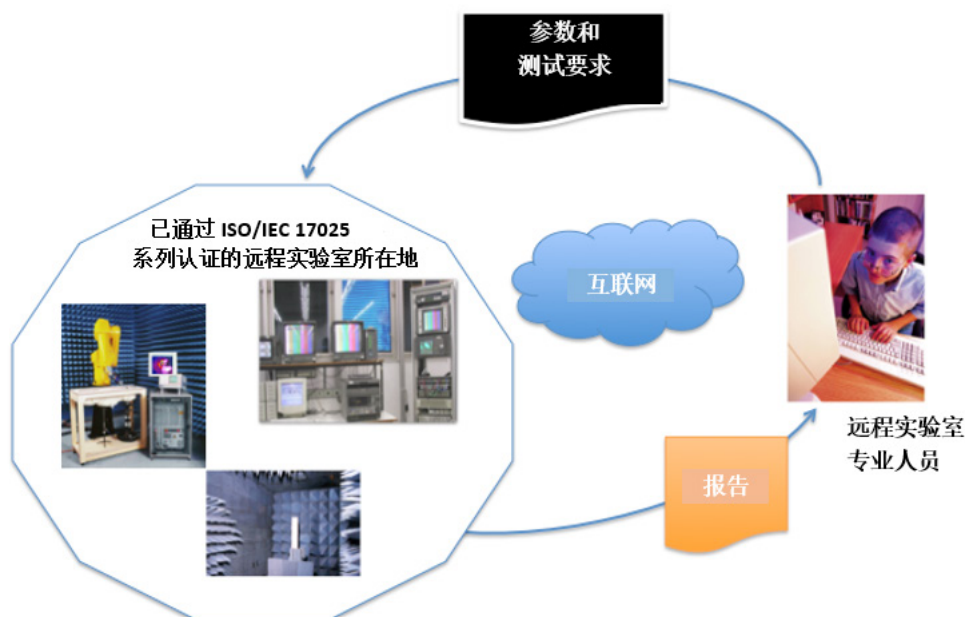
应与测试和测量系统主要制造商建立密切和强有力的伙伴关系，以保证基础设施得以快速更新。

2.5.3 远程设备选型测试

目标：提供远距离访问物理测试基础设施的机会用于设备选型。

在远程设备选型测试时，实验室可以使用其他实验室的基础设施，利用远程或虚拟模式，对ICT产品样品进行实验室开发、前一致性预测试以及一致性和互操作性测试。样品将由实体（所涉方面）提供。

图3：远程设备选型测试



可以通过几个阶段来调试实验室服务水平：

- 阶段1：远程培训。
- 阶段2：对样品进行测试，对每个步骤进行视频传输，并传送数据以构成报告。
- 阶段3：本地实验室越来越多地参与测试特定类型的产品，特别是核心网络产品（在满足核心基础设施需求方面实现益处最大化）。
- 阶段4：提供供远程测试的基础设施（为适合的测试和测量基础设施投资）。
- 阶段5：为提供本地测试基础设施开展咨询和培训（如有要求）。

要求：适用标准、测试、筛查等。

2.6 市场监督

对已部署电信设备实施市场监督的目标是确保投放市场的产品不会造成电磁干扰，危害公共电信网络，或给公众的健康、安全或任何其他方面造成危害。事实上，市场监督包括采取一切必要行动（禁止、撤回、召回）阻止不符合相关法律和规定要求的产品在市场上流通，保证产品合规并采取制裁措施。市场监督对电信市场的顺利运作至关重要。

要。这对于保护消费者和工人免受不符合要求的产品带来的风险至关重要。此外，市场监督有助于保护负责任的企业免受无视规则或偷工减料的无良经营者的不公平竞争。世界各地的许多监管机构对市场监督组织有具体的法律要求。法规给市场监督机构明确规定了义务，规定它们必须拥有正确履行职能所需的必要权力、资源和知识。要求建立程序，以跟踪投诉、监测事故、核实是否已采取纠正措施并收集有关安全问题的科学技术知识。

2.6.1 主要利益攸关方

主要利益攸关方包括：

- 政府/监管机构
- 认证机构（AB）
- 一致性评定机构（CAB）
- 制造商、进口商、供应商和服务提供商。

2.6.2 关于市场监督情报和经验的咨询

活动包括：

- 与已建立市场监督和执法计划的其他国家共享信息并向其咨询，尤其是本区域内使用同种语言，甚至开展类似频谱管理、获得类似业务频率指配的国家。
- 针对特定国家或地区早期部署的技术和产品的一致性问题的，向合作伙伴发送通知或预先警告，当产品或技术被更广泛地部署时提醒合作伙伴注意潜在的一致性问题，使检查和审核工作更有针对性。

2.7 新技术的一致性评估

随着ICT服务和应用深入人类生活的方方面面，新技术（物联网、5G等）的普及成为现实，发展中国家若不及时做好准备，将面临一致性和互操作性方面的严重问题。

对未来万物互联的预期为C&I需求提供了驱动力。发展中国家试图以创新的方式应对层出不穷的各种问题，包括：

- 确定统一的技术要求；
- 在国际层面确认主要的技术参考（标准）；
- 制订有力的C&I框架政策，推动在各个利益攸关方在ICT环境中开展协作（如通过制定包括接受供货方声明和双边认可协定在内的机制）。

2.7.1 新技术挑战

挑战包括：

- 互操作性问题对扩展工作的影响：
 - 监管机构层面的意识
 - 认为监管是进入障碍的认知
- 开发人员对C&I的认识和看法：
 - 货币成本
 - 安全和人工成本
- 有限的项目/产品资金和资源：
 - 认证费用
 - 仍处于起步阶段的市场。

2.7.2 预一致性测试

预一致性测试要求如下：

- 具备C&I意识：
 - 与特定产品设计有关
 - 在产品进入市场的每个阶段开展测试
- 了解C&I的影响：
 - 理解初创企业的成本（金钱、时间、技术）
 - 规则是有益的而不是一种障碍。

2.7.3 预期影响⁸

C&I可以通过以下方式提升成功前景：

- 有助于形成智能产品组合；
- 从一开始就纳入C&I；
- 知晓什么时候需要哪些人和资源。

可以通过以下方式帮助监管机构促进新兴产品和业务的发展：

- 倡导跨领域MRA；
- 促进企业家的知情参与。

⁸ 国际电联，[第4/2号课题的专题会议](#)2019年10月16日。

第3章 – 打击假冒、残次和破坏设备行为

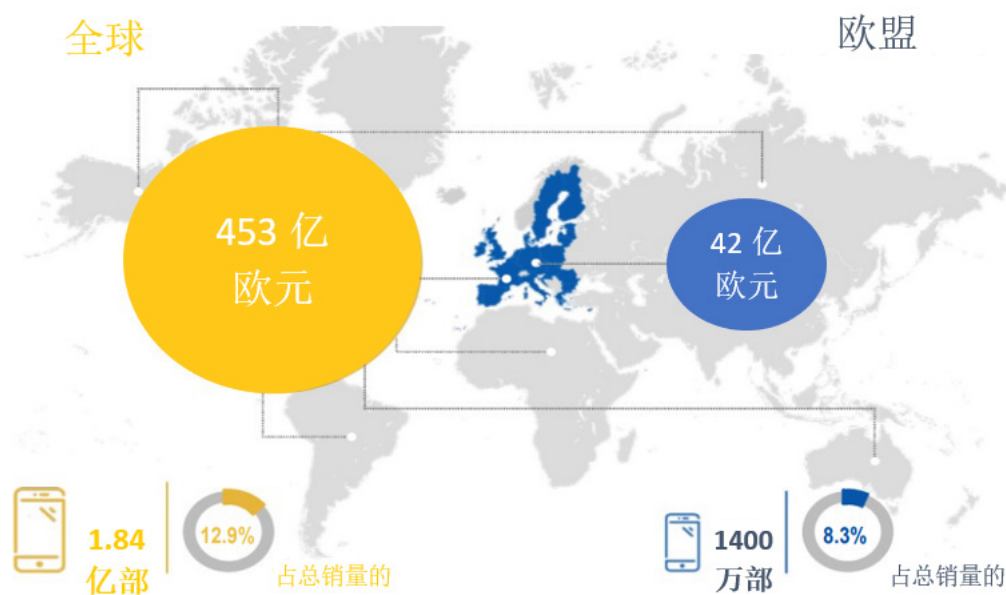
如今，ICT市场的假冒产品和假冒移动设备的交易已成为一个全球性社会经济问题，对创新、投资、经济增长、健康和就业都造成负面影响。此外，还存在资源被用于有组织犯罪的危险。

2017年世界电信发展大会（WTDC-17）在修订后的第79号决议（2017年，布宜诺斯艾利斯，修订版）中，将打击假冒设备装置扩散确定为第4/2号课题的重点事项。本章介绍了假冒电信/ICT设备造成的问题，并提供了识别和打击假冒设备使用的导则。

3.1 难题和问题

假冒电信/ICT设备，特别是移动电话，对用户、制造商和政府以及创新、投资和经济增长都构成全球性挑战。欧盟知识产权局（EUIPO）估算，2015年由于假货，全球智能手机销售收入损失高达453亿欧元。⁹

图4：假冒智能手机导致的销售损失：欧盟和全球



就用户而言，推动假冒终端快速扩散的原因包括：

- 伪造和被篡改的设备可能比正版设备更便宜，并且可以上网。
- 此类设备可为用户提供包括多SIM卡、电视、调频收音机和多种实用移动互联网服务（聊天、视频通话、网页浏览、转账等）在内的各种便利功能，而且价格低廉。

⁹ EUIPO。假冒智能手机研究，2018年10月。

（包括但不限于以下的）若干因素导致假冒终端对人体健康、网络和服务质量以及财务状况产生负面影响：

- 由于含有危险物质（如铅或镉）、比吸收率（SAR）较高、电池有爆炸危险，假冒设备并不可靠，会对人们的健康和环境造成威胁；
- 服务质量(QoS)降级，如语音接入问题、掉话、移动性问题（切换）和速度降低；
- 给正品终端制造商带来经济损失（销售损失以及对价格造成负面影响）；
- 财政损失（关税和税收）；
- 侵犯版权和商标权，不正当竞争；
- 保修和技术支持方面的损失；
- 由于功率不可控等原因扰乱电信网络性能。

关于网络性能问题，高通（Qualcomm）¹⁰的一份报告显示，假冒设备会影响网络性能：

- 降低网络容量：长期演进（LTE）数据容量减少23%、高速分组接入（HSPA）数据容量降低6%、全球移动通信系统（UMTS）声音容量降低27%。
- 缺乏LTE最新功能的支持，如运营商级集合（LTE-CA）、多入和多出（MIMO）4x4和256正交调幅（QAM），这都会对整体用户体验造成负面影响。
- 加大与资本和运营支出有关的网络站址数量方面的要求，将对移动运营商业务带来负面影响。

使用无效国际移动设备识别码（IMEI）的假冒设备带来的问题包括：

- 因为很多假冒移动设备拥有外观合法的IMEI码，因此不容易被确认和封堵。假冒者惯于在其产品上使用与合法设备制造商的号码相对应的IMEI号码范围，因此很难区分合法和假冒产品。
- 对公共安全的威胁。此类装置可能为犯罪活动和恐怖主义活动提供便利。
- 常常是用户受到已售出假冒设备网络被封堵而断网的影响，而不是那些进行假货交易的人。

3.2 定义

- **终端**：连接到一个电信网上以便提供接入一个或多个特定业务的设备（ITU-R V.662-3建议书）。¹¹

¹⁰ 高通公司。打击假冒和盗窃移动设备,2018年10月。

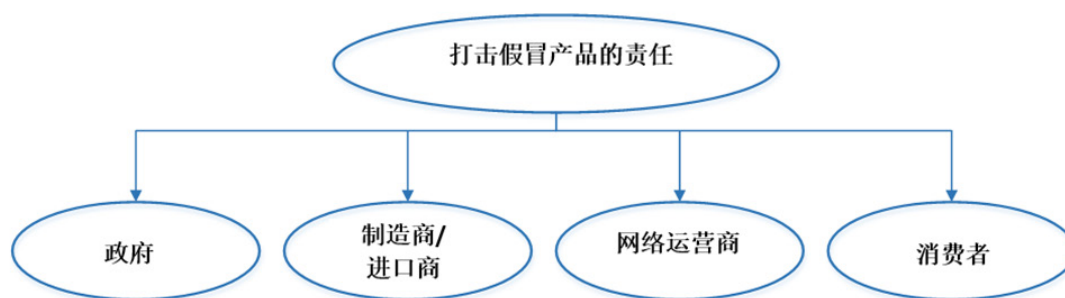
¹¹ 国际电联无线电通信部门（ITU-R）。ITU-R V.662-3 (05/2000)号建议书。术语和定义。

- **国际移动设备识别码（IMEI）**：制造商分配给每个IMT-2000移动终端的唯一代码，用于识别网络中的IMT-2000终端，以进行终端设备验证或类似任务。
- **设备标识寄存器（EIR）**：出于记录目的，将用户设备标识分配给一台寄存器。这些信息的性质、目的和使用是需要进一步研究的领域。
- **白名单**：授权可以在某个国家使用的设备（包括合法进口到该国或在该国制造的设备）登记表。
- **黑名单**：电信网络上拒绝为其服务的设备登记表。

3.3 导则

重要的是需要所有利益攸关方（即政府、制造商、网络运营商和消费者）携手努力，打击假冒电信/ICT设备的扩散。

图5：打击假冒的责任



协作对于制定打击假冒产品扩散的监管和技术框架至关重要，为此：

- 政府和监管机构应制定监管框架，实施标准程序，部署技术平台来实施监管；负责开展提高认识的活动，特别是用户使用假冒设备面临的风险，如健康风险和服务质量差的风险；加强市场监管，防范黑市设备交易。
- 政府应考虑降低合法进口设备的税费，从而降低使用成本。
- 在国家层面，监管机构可与设备制造商和网络运营商合作，确定假冒设备在本国市场的使用范围。
- 政府应给与海关和安全服务部门必要手段，打击非法贩运，并在其进口站点查验设备标识号的合法性。
- 制造商和进口商必须登记所有进口或本地制造设备，并遵守监管机构确立的审批程序。
- 制造商应遵守IMEI安全部署方面的技术设计原则，参与GSM协会（GSMA）报告和堵住IMEI安全漏洞的程序，以强化IMEI安全性。

- 运营商在打击假冒设备扩散中的责任包括：为监管机构和政府相关方面提供设备网络数据；设立EIR数据库，支持IMEI黑名单和白名单，从而阻断假冒设备接入；必要时通过短信（SMS）告知用户其设备状况。
- 用户可以通过参考其他利益攸关方提供的核实服务验证其计划购买设备的合法性；单独登记进口设备；向管理部门报告假冒设备情况。
- 应该建立一致性评估制度，以及一个包含所有设备信息（标识符、技术规格、设备生命周期等）的中央国家数据库，以便开展有效的市场监管。

卢旺达等国家的经验表明（参考3.4.4节），在区域层面：

- 国家之间缔结一致性评估和市场监管相互认可协议非常重要。
- 集中式设备控制系统可以大大减少进入市场的假冒和低劣设备的数量。
- 区域内认可的测试中心通过认证和供应商合格声明，可以显著促进一致性评估的实施。

3.4 国家经验（案例研究）

成员国和利益攸关方提交的文稿对编写本报告至关重要。这些文稿吸收了国家经验、数据和现有做法，以打击假冒设备的扩散。

所有投稿者一致认同，需要建立强制性的政治、法律和法规框架。

一些投稿者建议使用现有的技术解决方案，如国际标准和市场监管技术，建立中央数据库和平台来阻截假冒设备。

此外，数名文稿贡献者提议将工作扩展到区域和次区域层面，以便汇集不同的技术来对抗设备造假。

3.4.1 马达加斯加

马达加斯加移动网上25%的活跃设备是假冒设备。¹²即便这些设备有一定的价值，如价格低廉、可接入普遍服务、缩小数字鸿沟等，但其潜在的风险却远超过益处，会对人体健康（如信号辐射水平）、运营商（QoS、网络中断等）以及国家经济造成危害。

马达加斯加已采取了一系列措施，避免数字化发展对人身健康和国家经济造成危害：

- 提升用户对假冒设备危害性的认识；
- 关闭黑市并实施海关措施；
- 禁止假冒终端，对进口ICT设备开展认证；

¹² ITU-D SG2马达加斯加提交的2/45号文件。

- 2019年6月30日起，利用相关平台分析鉴别IMEI，封堵假冒设备。

3.4.2 几内亚

几内亚政府提交的文稿强调了与电信设备和基础设施的认证以及电信业务之间的互操作性问题。¹³2015年以来，几内亚政府已颁布了旨在调整行业结构的电信法。电信改革带来有利影响包括：加大了电话基数、改善了服务质量、提高了行业对国内生产总值（GDP）的贡献率，并实现了对数字市场和认证行业的管控。

几内亚政府对电信设备认证采取非常严格的措施，对违规者采取压制措施，甚至进行制裁。终端设备符合基本要求的评估是由邮政和电信管理局（ARPT）进行的，该局要求申请方提交非常详细的行政和技术文件，之后才颁发一致性证书。采取的措施包括：

- 对符合国际电联标准化的工作进行严格和持续跟踪；
- 包括ARPT、海关、税务和其它相关部委等相关参与方开展行动；
- 批准电信设备器材，有效期5年；
- 实施认可设备标签制度；
- 没收设备或拆除假冒设施，费用由违法者承担；
- 根据主管法院命令，没收假冒设备；
- 对未注册者进行处罚：任何人持有待售或分销本法规定的终端设备或无线电设备，违反认证机制或未经事先批准将其连接到公众电信/信息通信技术网络，将被处以1000万至2亿几内亚法郎的罚款；
- 二次犯罪，罚金加倍。

3.4.3 塞内加尔

除了有效打击盗版、假冒和盗窃电信/信息通信技术设备行为，并采取措施适应法律环境的环境外，塞内加尔还与大陆和洲际组织、跨国公司、电信和ICT监管机构和互联网服务提供商（ISP）开展合作，采取了重要举措打击这一现代祸患。这一祸患是技术创新、创造就业和财富以及外国直接投资的真正障碍。¹⁴

塞内加尔实施了各种措施，包括立法和监管框架以及一系列措施，以更好地保护个人财产，包括：

- 通过一系列法律建立法律框架；
- 通过一系列法令建立监管框架；
- 打击盗版和假冒行为的国家稽查大队；
- 塞内加尔工业产权和技术创新局；

¹³ ITU-D SG2几内亚提交的SG2RGQ/9(Rev.1)号文件。

¹⁴ ITU-D SG2塞内加尔提交的SG2RGQ/66(Rev.1)号文件[原文为法文]。

- 电信和邮政管理局（ARTP）；
- 国家海关；
- 电话、平板电脑、智能手机和解码器的国内和跨国制造商和分销商参与其中。

3.4.4 卢旺达

卢旺达政府意识到假冒设备对消费者、行业和经济带来的危险，因此制定了一项打击假冒设备扩散的战略，并与东非共同体（EAC）¹⁵的成员国一道在区域层面制定了路线图。政府的建议包括：

- 东非共同体成员国之间的相互协议：审查成员国的法律和监管文书，以期缔结相互认可协议用于开展一致性评定，加强市场监管。
- 集中监控系统：建立基于EIR SIM锁、IMEI预授权、IMEI授权和EIR警报的实时控制系统，作为在区域层面打击非法设备扩散的最佳方法。
- 区域测试中心：建立获得认可的区域测试中心，通过供应商一致性声明认证，促进EAC成员国的一致性评定。这将减少区域组装厂的认证成本，并降低最终产品的成本。国家间建立相互协议有助于促进在不同国家建立专门实验室。

3.4.5 津巴布韦

津巴布韦的所有移动网络运营商（MNO）均有能力检测出网络中使用重复IMEI码的假冒设备，并且能够切断网络。然而，考虑到假冒设备对运营商收入十分重要，因为大多数网络用户都使用此类设备，实际断开连接的情况十分少见。¹⁶尽管如此，津巴布韦还是采取了以下行动来打击假冒和盗窃移动设备的行为：

- 任何不符合型号核准要求的设备均不得使用；
- 购买新SIM卡的移动网络用户必须在网络上激活之前向移动网络运营商（MNO）注册；
- 获取用户注册数据库系统，以确保在该国激活的所有SIM卡均已正确注册。该系统还有助于检测假冒设备和假冒手机；
- 南非独立通信管理局（ICASA）运营一家独立的测试实验室，对所有区域一级ICT设备开展测试认证。

3.4.6 加纳

加纳开展了选型措施用于保护电信/ICT设备、用户和网络。¹⁷为此，国家通信管理局（NCA）建立了选型制度，以对通信设备进行认证和测试，确保其符合国际标准：

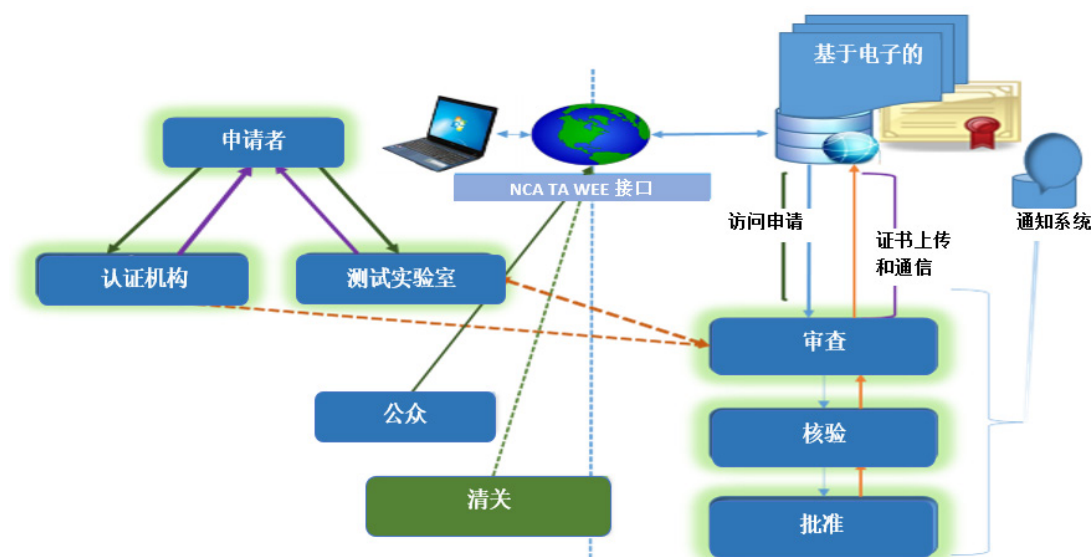
¹⁵ ITU-D SG2卢旺达提交的SG2RGQ/69号文件。

¹⁶ ITU-D SG2津巴布韦提交的SG2RGQ/85号文件。

¹⁷ ITU-D SG2加纳提交的SG2RGQ/82号文件。

- 根据技术文件执行批准程序，其中包含有关消费者保护，环境保护，网络中断，完整性和互操作性的测试报告和合规性要求，以及确保符合《国家频率分配计划》的规定；
- 对选型证书（TAC）和NCA标志进行归类，以及在NCA网站上发布设备的详细信息；
- 实施整合到批准制度中的经销商许可制度，以简化电子和通信设备（ECE）经销商的活动，并确保仅使用经批准的ICT设备；
- 加强国家市场监管的安排；
- 建立测试实验室，用于测量比吸收率（SAR），电磁场（EMF），数字地面电视（DTT）以及射频和信号（RF & Sig）。

图6：型号批准进程

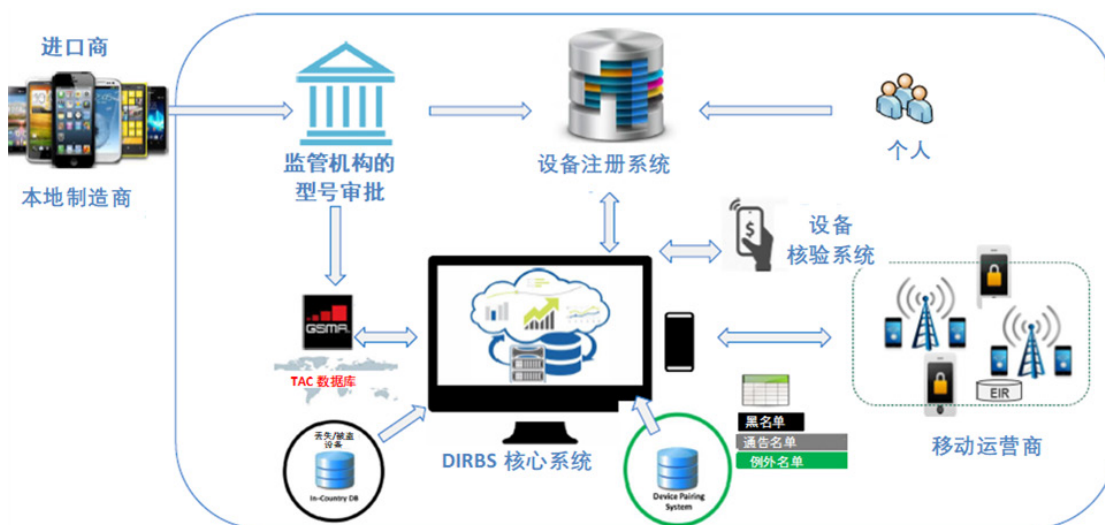


3.4.7 巴基斯坦

巴基斯坦电信管理局（PTA）与高通公司合作，通过开放源代码启动了一个名为“设备识别、注册和阻止系统”（DIRBS）的技术平台，以确保只有经过批准的合法设备才能在该国的移动网络上运行。¹⁸DIRBS可以方便识别所有设备；捕获已安装设备的基数；监督所有新设备的激活情况；解决非法和假冒设备问题，包括失窃的移动设备问题；并允许有例外/特赦情况。

¹⁸ 关于DIRBS的更多信息请参见巴基斯坦电信局（PTA）和巴基斯坦联邦收入委员会（FBR）的网站。

图7：设备识别、注册和阻止系统（DIRBS）



3.4.8 GSM协会

GSM协会（GSMA）管理国际移动设备识别数据库，这是一个全球中央数据库，其中包含有关数百万个移动设备的序列号（IMEI）范围的基本信息。¹⁹

GSMA向设备贸易商，回收商和保险公司以及执法机构提供“设备检查”服务（在某些市场中，消费者也可以直接使用该服务）。它使用户能够立即通过设备状态注册表发现设备是否已报告丢失或被盗，正如其全球移动网络运营商成员向GSMA报告的那般。

GSMA试图将尽可能多的移动网络运营商与IMEI数据库相连接。

GSMA和世界海关组织（WCO）于2016年9月合作打击假冒和欺诈性移动商务活动。IMEI数据库的集成将便于交叉检查和过滤进口时由其IMEI识别的假冒设备。

3.4.9 巴西

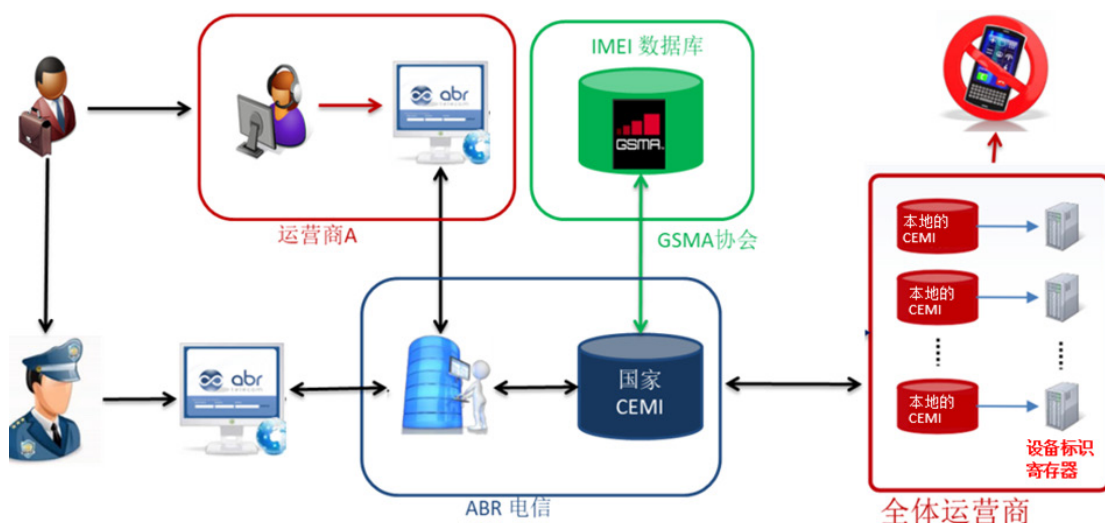
为了打击盗用，伪造和未经认证的唯一标识符的使用，巴西政府发起了由国家通信管理局（ANATEL）协调并由所有利益相关者参与的Celular Legal举措。²⁰根据该举措实施的措施围绕两个模块展开：

- CEMI（阻止登记的移动设备）模块允许移动运营商和警察根据用户的要求阻截被盗设备。

¹⁹ ITU-D SG2 GSM协会（GSMA）提交的SG2RGQ/80号文件。

²⁰ João Zanon, [打击使用被盗及假冒ICT设备行为](#), ITU-D打击假冒ICT设备讲习班, 日内瓦, 2018年10月4日。

图8: CEMI工作流程



- SIGA模块（综合手机管理系统）用于识别和阻止与其他类型的欺诈相关的设备：篡改，克隆，未经认证的设备，不规则的唯一标识符等。Cellular Legal提供了一个在线工具，可以根据设备的IMEI代码检查设备的状态。²¹

3.4.10 阿曼

在阿曼国家网络上注册的移动设备中，将近200万具有无效的IMEI码。一些IMEI号码已经重复了将近10次，因为有10多个设备带有相同的IMEI码。²²就在本地网络上注册这些设备而言，这产生了技术问题，并且由于破坏了消费者对这些产品的信心，总体上增加了消费者的经济负担。

监管机构特别希望能够确保经销商和进口商提供的所有现成的ICT设备都完全遵守监管机构发布的相关命令和决定。为此，电信监管局（TRA）检查机构负责确保在国内市场上出售ICT设备的兼容性，且这些设备符合相关标准和技术规范。

TRA已与当地运营商建立了一条求助热线，以使客户能够验证IMEI码。尽管如此，该组织仍面临困难，包括无法访问IMEI代码的国际数据库，因为对GSMA数据库的完全访问权限不授予监管机构，而仅授予指定国家/地区的制造商和运营商。

3.4.11 国际标准和建议书

- [ISO 12931:2012](#): 用于打击假冒商品的身份验证解决方案的性能标准
- [ISO 16678:2014](#): 用于阻止假冒和非法交易的互操作对象识别和相关认证系统指南
- [ITU-T Q.5050 \(03/2019\)](#): 打击假冒伪劣和失窃ICT设备
- [ITU-T Y.4808 \(08/2020\)](#): 打击物联网中假冒行为的数字实体架构框架。

²¹ 国家通信管理局（ANATEL）。Cellular Legal

²² ITU-D SG2阿曼提交的2/326号文件。

第4章 – 盗窃的移动设备

4.1 简介

随着全球移动设备使用量不断增长，在国内和跨境使用失窃设备的情况也随之增加。需要在全球范围内采取措施，屏蔽失窃设备联网使用。

使用假冒设备对整个生态系统造成极大危害，政府和行业愈发重视开展补救措施。各国政府正在实施能够解决一系列问题的法规，包括：

- 手机盗窃
- 安全隐患
- 税收损失
- 消费者隐私
- 网络质量
- 知识产权。

多年来，GSMA领导了多项共享数据以屏蔽失窃或丢失的移动设备访问全球网络的行动。通过使用唯一的IMEI码，GSMA管理可疑设备（即那些被报告为丢失或失窃的设备）黑名单，供全球运营商参考。²³

4.2 难题和问题

设备盗窃是一个全球性问题，需要采取跨境协调和行动以使盗窃行为无利可图。尽管一些行业举措已经产生了积极的影响，但由于迄今为止大多数活动都是基于全球非专属标准，并且某些国家还没有将其行动调整到与全球行业做法同步，因此仍需要继续努力。在这方面，各国需要采取整齐划一的办法，与业界努力保持一致。不作为会让一些已实施措施失效。

解决设备盗窃行为的要求可划分为以下几类。

法规与执行

- 制定监管框架
- 执行标准作业程序
- 部署和管理技术平台用于执行法规

²³ ITU-D SG2 GSMA提交的SG2RGQ/80号文件。

- 开展提高认识的活动。

技术平台

- 对现有设备分类：
 - 从网络信息分析设备数据
 - 按IMEI对设备进行分类（有效/无效，唯一/重复）
- 承认现有设备：
 - 将现有假冒IMEI码与国际移动用户识别码（IMSI）和移动台国际用户目录号码（MSISDN）配对
- 注册新设备：
 - 需要使用唯一设备标识符进行选型操作
 - 仅使用有效和唯一标识符注册进口和本地生产的设备
- 检测IMEI码篡改行为：
 - 分析网络数据
 - 识别假冒IMEI码的设备
- 启用网络屏蔽：
 - 通过网络控制监视不兼容设备和未注册设备的访问行为。

技术系统实现²⁴

- 给所有利益攸关方，尤其是消费者带来便利
- 移动网络集成和互操作性给运营商带来了不必要的成本、容量限制和资源负担，独立系统可以缓解这一需求
- 不需要严格的设备-客户绑定
- 无需定制即可适应国家法规的灵活性/可配置性。

4.2.1 设备犯罪和诈骗

设备犯罪和欺骗对各利益攸关方群体都会产生负面影响：

- 消费者：与失窃、财产损失、个人信息丢失有关的伤害风险
- 政府：犯罪增加、税收减少

²⁴ Mohammad Raheel Kamal, [打击假冒和被盜ICT设备的开源CEIR](#), 第三届ITU-T第11研究组非洲区域讲习班, 主题为“非洲的假冒ICT设备、一致性和互操作性测试挑战”, 突尼斯, 2019年9月30日。

- 贸易商：不知情购买失窃物品、网络性能问题
- 保险公司：承保成本增加、所有权转移到失窃物品
- 运营商：用户流失、补贴损失、保险承保费用
- 执法：有组织犯罪、资源消耗。

4.2.2 利益攸关方的角色和责任

各利益攸关方能够在打击盗窃设备行为中发挥重要作用。

政府可以制定监管框架，实施标准操作程序，部署和管理技术，以便于执行规定，并开展提高意识活动。

制造商/进口商可以从政府/监管机构获得设备型号核准，注册所有要进口的设备，并注册所有本地制造的设备。

运营商可以向政府提供设备相关网络数据，确保设备标识注册（EIR）支持，支持将有效/无效IMEI码列入黑名单并允许例外情况，并根据需要通过SMS通知用户其设备状态。

消费者可以验证设备状态（通过SMS、应用程序或网页界面），单独注册进口设备，向监管部门报告设备失窃情况，并根据需要提交正版设备证据（发票）。

4.2.3 打击盗窃设备行为的基本工具

为了防止设备失窃，可以在网络层级和设备层级完成各种操作。

基于设备的保护：

- 删除联系人和照片并阻止移动支付的能力
- 利用恢复出厂设置功能擦除所有数据
- 远程擦除功能。

基于网络的保护：

- 阻止失窃手机访问网络。

设备状态检查：

- 回收前检查设备状态
- 使盗窃手机行为无利可图。

4.3 导则

各种利益攸关方的参与

用户可以向网络运营商报告设备失窃，在设备上启用防盗功能，而且对于运营商已连通GSMA IMEI运营商黑名单的国家/地区，可以鼓励用户检查计划购买的二手设备的IMEI状态。²⁵

移动网络运营商可以阻断失窃设备访问网络，并连接至GSMA IMEI运营商黑名单，共享和收集黑名单数据，并鼓励设备供应商充分保护其产品上IMEI应用的完整性。

设备制造商/品牌所有者可以确保其所有产品中IMEI码的完整性，设计更安全的设备（即无法改动IMEI码）并实现“终止开关”功能，支持用户远程禁用丢失和失窃的设备。

应用程序商店运营商可以从GSMA获取失窃设备的IMEI码，从而拒绝失窃设备访问应用程序商店。

所有利益攸关方（政府部门、制造商、网络运营商和消费者）需要携手努力，打击假冒电信/ICT设备，特别是在以下方面：

- 融入和参与执法
- 监管分销渠道以应对贩运失窃设备行为
- 给予防盗举措立法和司法支持
- 重点关注设备，尽可能减少给用户带来的不便
- 重申所有国家共同努力发挥作用的重要性
- 支持现有功能而不是复制/破坏现有功能的措施
- 衡量和报告所采用方法的有效性
- 对已采取的措施进行分析以便确定哪些措施有效，哪些无效
- 采用新技术和解决方案弥合差距。

政府和监管机构必须通力协作，以确保：

- 运营商部署EIR屏蔽失窃设备访问本地网络；
- 遵循设备屏蔽和共享数据的最佳做法导则；
- 运营商EIR连接到IMEI数据库以确保国际屏蔽；
- 提高IMEI安全水平，确保问题得到上报和解决；

²⁵ James Moran（GSMA）。[莫兰共同打击设备犯罪-打击移动设备盗窃的最佳做法](#)，国际电联关于打击伪造和被盗ICT设备的全球方法讲习班，日内瓦，2018年7月23日。

- 执法人员、海关人员、零售商和消费者共同检查IMEI码；
- 对篡改、盗窃并交易IMEI的犯罪分子采取执法行动；
- 采取措施教育消费者并宣传终止开关功能；
- 商定跟踪工作进展的衡量标准，并建立报告制度。

4.4 国家经验（案例研究）

4.4.1 中非共和国

作为国家ICT基础设施发展政策的一部分，中非共和国政府已向4个移动运营商和1个固网运营商开放ICT市场，以便最大程度地覆盖全国并为民众提供优质服务。²⁶

电子通信和邮政监管局（ARCEP）未能执行此政策，导致基础设施的发展未得到充分监管，检查ICT设备的一致性和互操作性面临困难，假冒移动终端和盗窃行为不断增加，投资和行业收入受损。

为了解决这些问题，中非共和国政府采取了以下措施：

- 通过并颁布了《电子通信法》及实施文本；
- 通过并颁布了法律，建立了电子通信和邮政监管局（ARCEP）；
- 起草了网络犯罪和网络安全法案；
- 建立了移动终端贩运控制、反欺诈和定位中心；
- 建立了电子通信管理常设秘书处，以保证技术监测；
- 完成了连接首都班吉与刚果共和国及喀麦隆的国际光纤基础设施骨干项目；
- 实施了名为Centrafrique digital 2025的国家数字化项目；
- 实施了发展超高速宽带基础设施的国家战略计划；
- 建立了国家ICT机构和国家数据中心。

中非共和国建议国际电联提供援助和支持，以帮助各国开展合规性和互操作性计划能力建设，应对假冒产品和移动设备盗窃行为。

4.4.2 墨西哥

为了打击移动终端设备盗窃行为，墨西哥国家电信和广播监管机构联邦电信协会（IFT）落实了监管义务。在国家和国际层面采取了一些举措管控IMEI码。²⁷

²⁶ ITU-D SG2中非共和国提交的SG2RGQ/144号文件。

²⁷ ITU-D SG2墨西哥提交的2/166号文件。

在国际层面，墨西哥政府已通过其各部委与它国签署了双边和区域公约，交换失窃或丢失设备的IMEI码信息，并禁止复用。该国已与GSMA达成协议，实施IMEI设备检查系统，支持移动设备用户实时检查GSMA IMEI号码数据库。

在国家层面，IFT在官方公报上发布了一项技术规定（IFT-011-2017），针对中止向失窃或丢失的移动终端设备或装置提供服务事宜确立了安全和司法合作导则。IFT通过实施技术规定（包括与电信网络连接的移动终端的规范和合规控制）加强了上述合作：

- 一致性评估
- 一致性证书更新
- 已核准设备的IMEI码数据库
- 符合认证要求的控制。

IFT遵循技术规定中描述的测试方法，检查是否符合上述规定的要求。

4.4.3 伊朗科技大学

为了防范欺诈行为并打击销售和使用非法设备（包括失窃手机和尚未支付海关费用的手机）的行为，伊朗于2017年制定了手机注册计划。²⁸

打开设备访问服务时，有关部门将对其进行评估；如果合法列表无法提供所需信息，该设备将被认定为非法设备并被添加进黑名单中。

在伊朗全面贸易体系下，进口手机在海关边境登记，每部手机分配到一个唯一的激活码。伊朗科技大学开发了HAMTA系统，该在线数据库支持具备唯一代码的设备进行激活操作，并为用户提供两个主要功能：

- 报告该国当前活跃手机的状态，确认手机真伪，并验证该装置是否合法并已激活；
- 激活合法进口的新手机。

HAMTA系统中已注册设备的数据将被传输至伊朗通信管理局和移动运营商。只有经HAMTA系统认证的注册设备才被视为合法设备，允许访问运营商提供的服务；其他设备都会被列入黑名单。

²⁸ ITU-D SG2提伊朗伊斯兰共和国提交的2/83号文件。

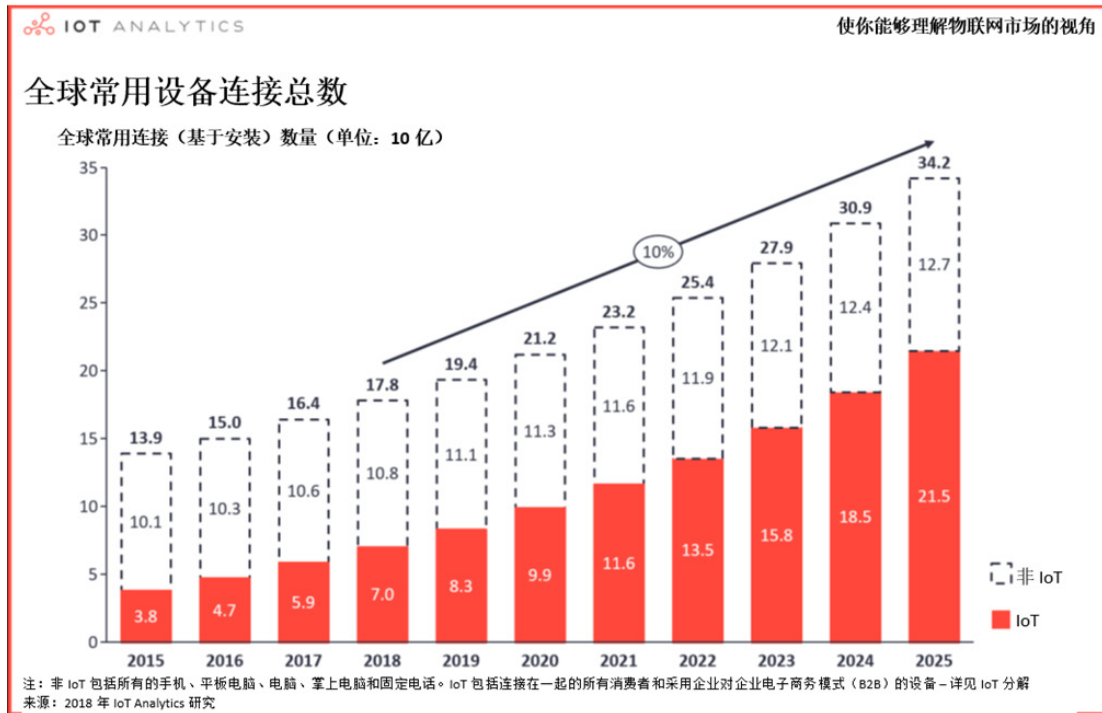
第5章 – 物联网与一致性和互操作性 (C&I)

5.1 介绍

国际电联将物联网 (IoT) 定义为“信息社会的一种全球基础设施，基于现有的和正在出现的、可互操作的信息通信技术实现 (物理和虚拟) 物品相互连接，提供先进服务”。^{29, 30}

物联网技术应用于各行各业，并通过处理数十亿个互联设备生成数据处理平台影响人们的日常生活。物联网研究机构“物联网分析”进行的一项研究表明，全球常用设备连接总数将急剧增加。到2020年，全球212亿常用设备连接中，有99亿为物联网连接。到2025年，这一数字可能会增加到215亿。³¹

图9：全球常用设备连接数



²⁹ ITU-T Y.2060 (06/2012) 号建议书：物联网概述。

³⁰ ITU-T Y.2069 (07/2012) 号建议书：物联网的术语和定义。

³¹ 物联网分析。2018年物联网的状况：物联网设备的数量-现在是7B-市场加速，2018年8月。

5.2 物联网对C&I和ICT准备的影响

为了满足物联网的特定需求，必须解决包括质量、可靠性、覆盖范围和低功耗在内的一些问题和挑战。

5.2.1 物联网的挑战








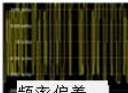
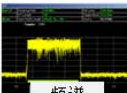
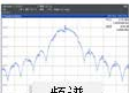
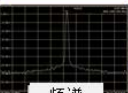
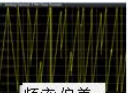
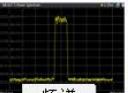
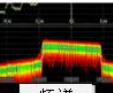
仅拥有好的数据收集传感器是不够的；还必须保证具备传输数据的良好连接性和建立能够分析和处理数据的平台。

物联网相关众多挑战中，以下值得特别关注。

技术选择：物联网成功的关键

未来，需要全面覆盖和移动性的物联网应用将专注于蜂窝技术，如基于4G和5G技术的LTE-M和NB-IoT技术。其他技术，如Sigfox或LoRaWAN，将利用在免许可频段运行的低功耗技术。大多数应用程序将使用短程或中程无线技术，如Bluetooth®、WLAN/Wi-Fi和Zigbee。物联网无线技术如图10所示。³²

图10：物联网无线技术

							
技术	FHSS	OFDMA	DSSS	UNB	CSS	OFDMA	OFDMA
调制	GFSK	BPSK QPSK	O-QPSK	UL: DBPSK DL: GFSK	Frequency Chirps	BPSK QPSK	QPSK 16QAM
带宽	2 MHz	20 ... 160 MHz	2 MHz	100 Hz (ETSI) 600 Hz (FCC)	125, 250, 500 kHz	3.75, 15 kHz 180 kHz	1.4 MHz (M1) 5 MHz (M2)
频谱	2.4 GHz ISM	1.. 6 GHz ISM	2.4 GHz ISM	Sub-GHz ISM	Sub-GHz ISM	< 6 GHz 3GPP	< 6 GHz 3GPP
特点							
	频率偏差	频谱	频谱	频谱	频率偏差	频谱	频谱

响应物联网需求的设计，即质量、可靠性、扩展范围、延迟等。

设计还必须响应用户期望，特别是在保密性和个人数据保护方面，并通过在物联网生态系统中采用安全标准来建立信任。

物联网平台和设备认证的需求

需要通过评估平台和设备与国际标准和法规的一致性来对其开展认证。

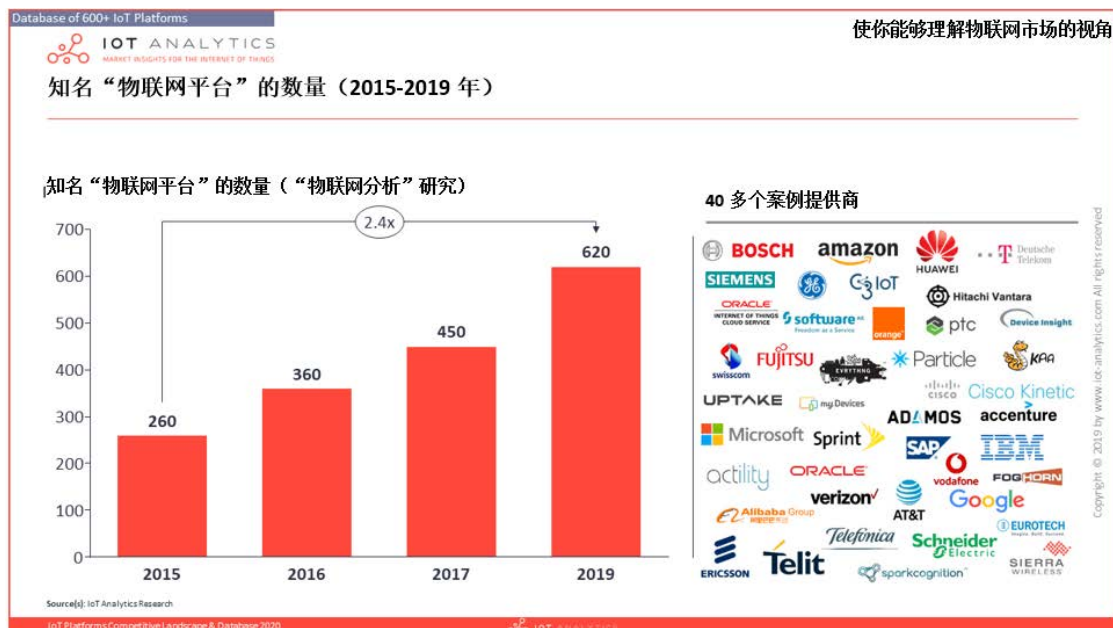
³² Joerg Koepp（罗德与施瓦茨公司，德国）。在[一个超级连接的世界中确保可靠和安全的通信](#)，ITU-D第4/2号课题会议，关于ICT的一致性和互操作性：发展中国家的挑战，日内瓦，2019年10月16日。

5.2.2 物联网受到的制约

本质上看，物联网基于对象（传感器）、网络（连接性）、数据和操作应用程序。因此受到的制约包括：

- **多个物联网平台：**“物联网分析”统计数据显示，2019年共有620个物联网平台和40多个提供商（参见图11）。³³

图11：知名物联网平台数量

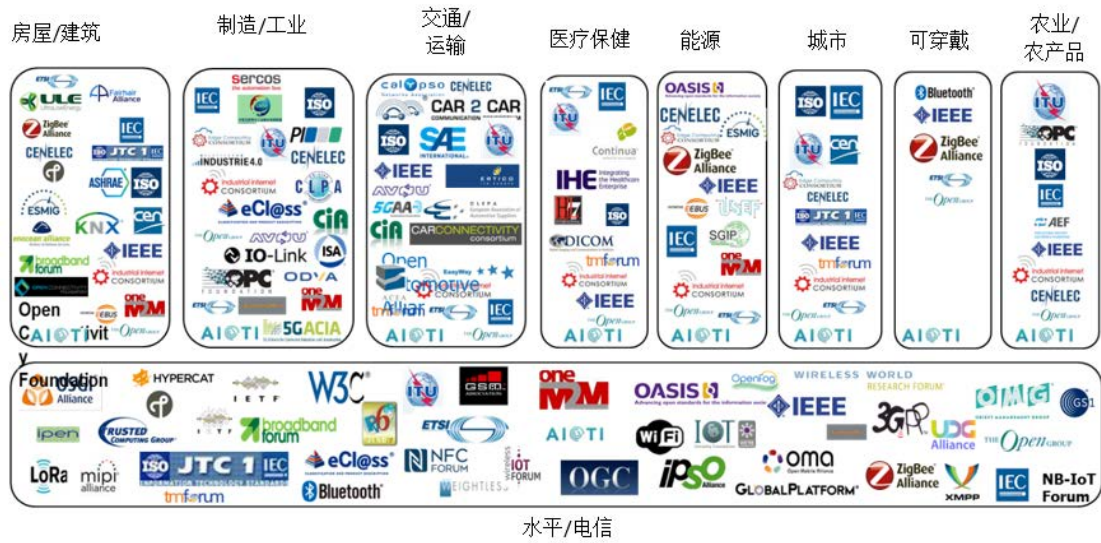


- **多种物联网协议：**存在多种数据共享协议，具体取决于标准制定组织（SDO）和物联网产品制造商。每项物联网标准都有自己的规范框架，供IT专业人员选择（参见图12）。³⁴

³³ 物联网分析。2019/2020年物联网平台公司概况：全球620家物联网平台，2019年12月。

³⁴ 物联网创新联盟（AIOTI）。IoT LSP标准框架概念，2.9版，2019年。

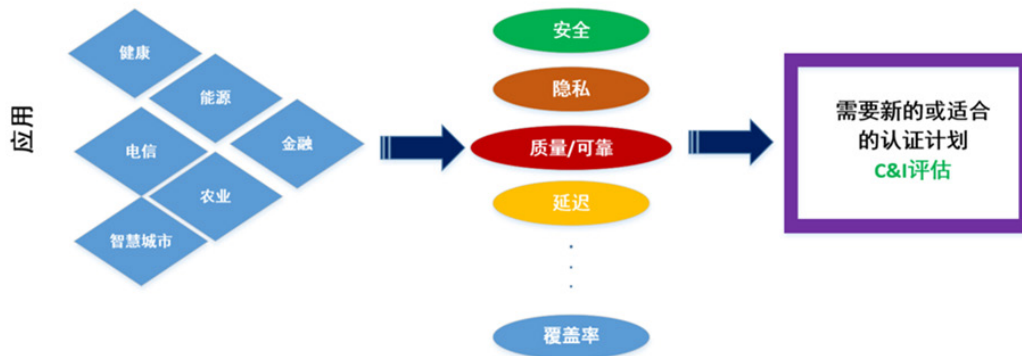
图12：物联网标准制定组织和联盟概况（垂直和水平域）



来源：AIOTI WG3（物联网标准化）- 第2.9版

当前，物联网还远未达到标准化，存在各种不兼容的标准和解决方案。³⁵ 鉴于促进对象通信的物联网平台和协议的激增，物联网技术标准在各种情形下发展，应用于各种情景，利益攸关方也有着各不相同的要求和目标。因此，一项较为严峻的挑战是保证互操作性、可扩展性、强健的国际标准和端到端安全性（参见图13）。

图13：适合的认证方案需求



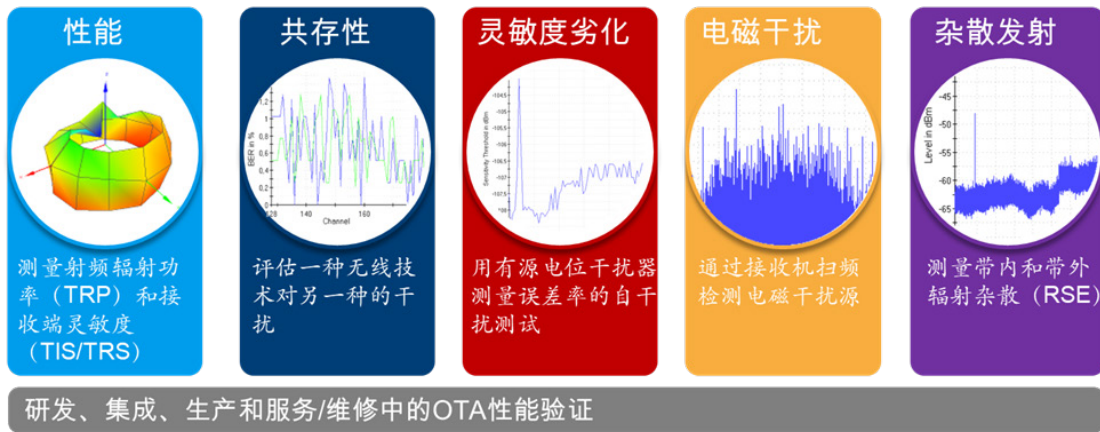
5.2.3 示例：罗德与施瓦茨（Rohde & Schwarz）物联网测试

对于罗德与施瓦茨（Rohde & Schwarz）公司而言，无线（OTA）测量有助于确保性能并做到符合监管规定。测试重点是性能、共存性、干扰测试、电磁干扰（EMI）以及测量段内和段外的辐射杂散（RSE）（参见图14）。³⁶

³⁵ 国际电联。ITU-T SG20-TD1722号文件，“国际电联通过标准加速城市的转型网络研讨会”，2020年6月25日。

³⁶ Joerg Koeppe（罗德与施瓦茨公司），见前文。

图14: OTA测量



5.2.4 标准制定组织

物联网系统将采用统一方法作为促进行业发展的手段，这推动了标准制定组织建立一套能够保证系统、应用程序、设备和传感器之间互操作性的标准架构。

国际电信联盟

ITU-T制定了Y系列建议书，涵盖了全球信息基础设施、互联网协议、下一代网络、物联网和智慧城市等方面。ITU-T第20研究组（SG20）致力于制定国际标准，以提升数字基础设施与物联网应用间的互操作性。

2020年3月，国际电联发布了介绍数字实体架构框架的ITU-T Y.4459建议书³⁷规定了提供通用信息和服务互操作性所需的最小规模的一组架构组件和服务。建议书将促进物联网设备识别、描述、代表性、访问、存储和安全性的互操作性。该架构框架促进了行业使用跨不同物联网应用的通用安全和管理接口。

在C&I测试方面，ITU-T第11研究组（SG11）和合格评定指导委员会正在与第20研究组合作研究用于物联网测试的网络模型。³⁸

国际标准化组织和国际电工委员会

2018年，国际标准化组织（ISO）和国际电工委员会（IEC）发布了标准ISO/IEC 30141，是物联网统一标准参考架构，被称为“通过互联网连接的数十亿智能设备的复杂集合”。³⁹

在2019年，ISO和IEC发布了标准ISO/IEC 21823-1，⁴⁰该标准概述了适用于物联网系统的互操作性。

³⁷ ITU-T. [ITU-T Y.4459 \(12/2020\)](#)号建议书：物联网互操作性的数字实体架构框架。

³⁸ Kofi Ntim Yeboah-Kordieh（加纳）。[ITU-T SG11工作更新和活动](#)。ITU-D第4/2号课题关于ICT一致性和互操作性的讲习班：发展中国家的挑战，日内瓦，2019年10月16日。

³⁹ ISO. [ISO/IEC 30141:2018](#)。物联网（IoT）-参考架构。2018年8月。

⁴⁰ ISO. [ISO/IEC 21823-1:2019](#)。物联网（IoT）-物联网系统的互操作性-第1部分：框架。2019年2月。

电气电子工程师学会

电气和电子工程师协会（IEEE）已发布标准2413-2019，“用于物联网（IoT）架构框架的IEEE标准”。⁴¹标准P2413.1通过充分利用不同智能城市组件和域间的跨域交互和互操作，为智能城市实施描绘了体系结构蓝图。⁴²该标准建立在草案标准IEEE P2413中物联网架构框架的基础上，后者建立在国际标准ISO/IEC/IEEE 42010的基础上。

5.3 物联网和ICT的法规和政策

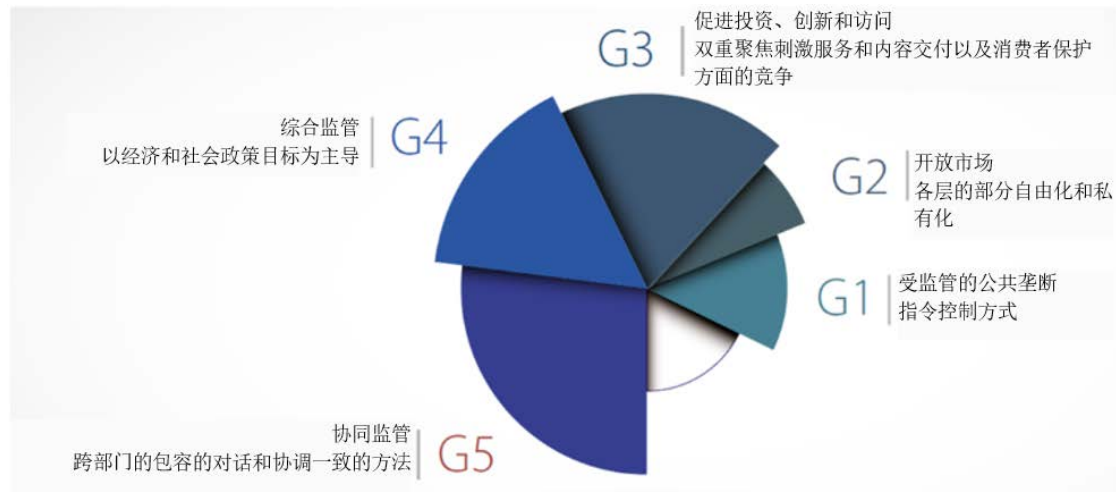
监管机构必须意识到C&I对物联网的影响。尽管测试实验室有助于保证产品性能、一致性和互操作性，但也需要制定法规。

如今，公共部门和私营部门在包括医疗保健、电信、教育、农业、金融和媒体以及智慧城市在内的不同部门部署物联网技术。因此，建立适合物联网的跨部门监管环境至关重要，这就需要第五代监管（即协作监管）。

5.3.1 协作监管概述

从第一代监管到第四代监管，已经有了相当大的发展：从受监管的垄断到基本改革和市场自由化，随后是对鼓励创新的环境进行监管，然后到以互联网相关问题为中心的第四代综合监管（参见图15）。⁴³

图15：各代ICT监管 – 概念框架



第五代监管或协作监管灵活性强，由共识驱动。协作性法规可促进创新，提升效率，改善服务质量（QoS），推进数据共享和安全性，克服互操作性挑战等障碍。此外，协作监管建立在共享专业力量、指导原则和最佳做法以及跨部门合作确认机制的基础上，以便更有效地应对共同挑战（参见图16）。⁴⁴

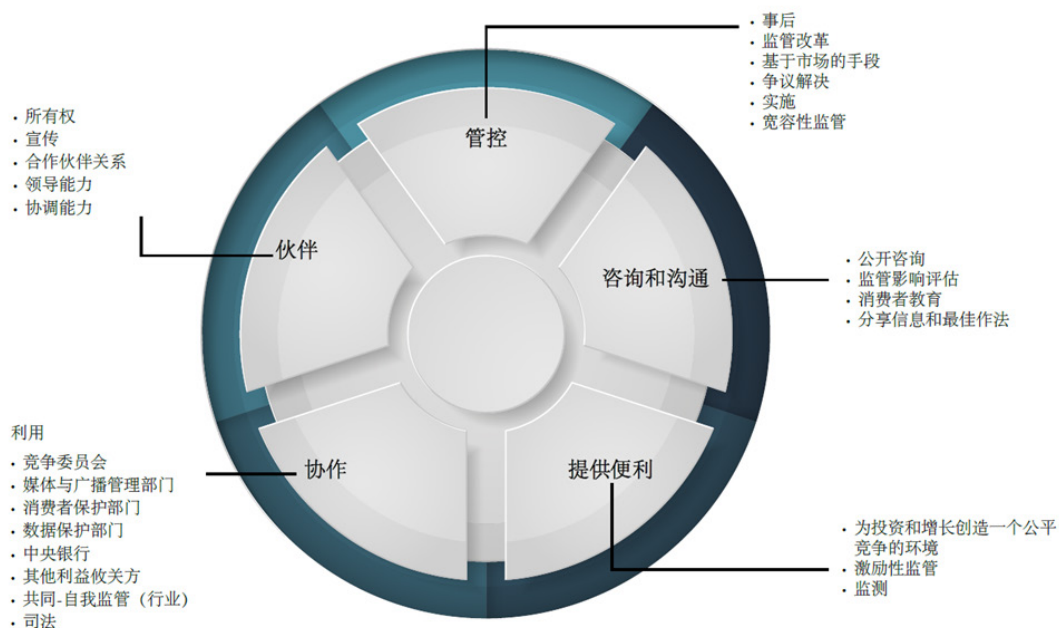
⁴¹ IEEE。IEEE 2413-2019。IEEE物联网（IoT）架构框架标准。2019年5月。

⁴² IEEE。IEEE P2413-1。智慧城市参考架构标准（RASC）。2018年8月。

⁴³ ITU-D。国际电联2017年全球ICT监管展望

⁴⁴ 同上。

图16: 协作监管



国际电联GSR-19最佳作法导重点关注协作监管，以确保数字变革取得成功。⁴⁵

5.3.2 物联网监管

许多政府鼓励物联网创新，并希望改革监管框架，避免阻碍物联网发展。但是，由于物联网市场监管仍存在一定程度的不确定性，因此应分阶段开展监管创新和调整。

物联网的含义不全在于ICT监管机构努力实现的连通性。连接是主要服务，而物联网还涵盖相关的应用、设备和传感器。

总的来说，尽管所有规定都适用于物联网，但物联网技术可能会催生其他要求。政策和法规必须要解决专属于物联网的各类问题，例如：

- 保密性、数据保护和安全性
- 系统、平台和连接对象的标准和互操作性
- 频谱管理和许可（许多情况下，物联网设备使用无线技术）
- 编号和号码便携性
- 从IPv4迁移到IPv6的需要
- 成本、可靠性、QoS和体验质量（QoE）
- 管理竞争的措施。

⁴⁵ 国际电联全球监管机构专题研讨会（GSR）。[2019年最佳实践导则](#)，Port Vila，2019年。

由于涉及安全性、保密性和数据保护问题，ICT规定变得越来越复杂。许多国家可能需要更新过时或过于严格的规定，而且互操作性会影响到升级换代工作。

为了提升互操作性并降低成本，专业人员呼吁建立在开源非专有平台、应用程序和标准之上的开放式物联网生态系统，从而促进经济增长和创新。

5.4 结论

标准化对于建立任何设备都可以接入并从任何位置进行通信的单个物联网市场至关重要。标准化有助于提升互操作性、兼容性、可靠性和安全性；鼓励新生态系统和创新；提升竞争力。

对物联网新技术的影响和自身在技术开发中所扮演的重要角色，监管者必须有清晰的认识，要开创协作监管的新时代来创造更多机会，ICT监管者要更多地充当促进者的角色，投身改善连通性，并与其他利益攸关方合作，推进在所有领域使用ICT。

总之，建立在渐进式监管框架上的策略可以通过部署专业力量、财务和其他资源来保护所有利益攸关方，并为之提供推动力。此外，这种策略还可以推广这项新技术，形成竞争市场，推动快速创新。

第6章 – 信息、知识技能和知识的转让

6.1 C&I学习需求和教育机会

C&I需要一套专门技能，并且需要经过培训的专业人员来运行C&I计划。此外，该领域固有的挑战包括：

- 缺乏正规的综合性C&I教育计划。大型机构通过将拟培训员工与经验丰富的员工配对来开展C&I培训。尽管这种方式可以起到一定效果，但往往这种方法提供的经验较为狭窄，无法做到正规的质量检查。此外，规模较小的机构也无法实施。
- C&I从业者，包括监管者、许可证持有人、认证请求人（进口商和制造商）以及一致性管理者，对法律、技术、国际贸易和经济问题也应当有清晰的了解。
- 快速发展的技术产品对C&I框架构成了持续的挑战（如IoT和软件配置）。

国际电联全权代表大会第177号决议（2018年，迪拜，修订版）强调，需要与经认可的机构合作并利用国际电联学院生态系统的优势，持续开展在职C&I能力建设活动，包括防范ICT设备造成或接收到的无线电通信干扰活动。⁴⁶

2020年的经验表明，全球迫切需要通过可靠的ICT网络开展数字学习。在新冠病毒大流行之后，人们比以往更多地将使用ICT开展教育视为一种公益事业。根据第177号决议（2018年，迪拜，修订版）建议，国际电联学院为培训人员提供由全球C&I社区开发的在线培训解决方案。

6.2 响应知识获取/保留的相关需求

以国际电联关于一致性和互操作性培训计划（CITP）的建议为例，可以考虑建设基于质量保证机制的协作平台，作为推动发展更广泛技能的一种方式。⁴⁷

之前国际电联与合作伙伴实验室共同开展的C&I培训（如C&I计划和测试领域的在职区域培训活动）十分成功，CITP就建立在这些培训基础上。⁴⁸该计划还考虑到从国际电联出版物中汲取经验教训，包括前一个研究期第4/2号课题的最后报告，⁴⁹并发布了导则。⁵⁰

开发CITP工作遵循了国际电联学院质量保证机制建立的模型，该模型包括由主题专家准备的一整套高级材料、同行评审流程以及由专业培训师准备的用于编写教学大纲卡和培训大纲的范本。

⁴⁶ 国际电联全权代表大会第177号决议（2018年，迪拜，修订版），关于一致性和互操作性。

⁴⁷ BDT第4/2号课题联络人于2019年10月在ITU-D SG2的SG2RGQ/194+附件号文件中向第4/2号课题提出了这些概念。

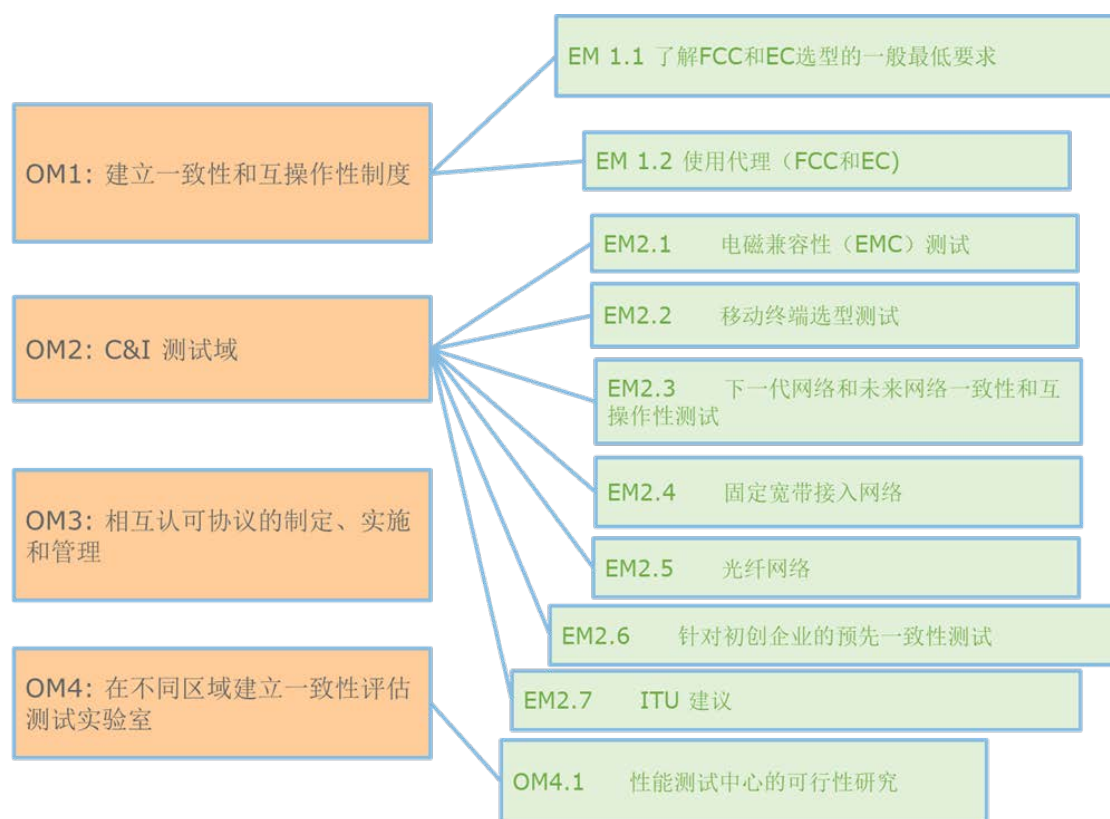
⁴⁸ ITU-D。一致性和互操作性会议

⁴⁹ ITU-D第2研究组2014-2017年研究期第4/2号课题最后报告。见前文。

⁵⁰ ITU-D。出版物和实际成果 – C&I

建议的培训结构提供了量身定制的学习路径，概述如下：

图17: CITP培训模块（OM是必修模块，EM是合格模块）



培训结构围绕四个主要主题进行组织，并分为子主题，为所选择学习路径提供支持，保证学生所需知识能够实现模块化传输。

1) 设计和建立一致性和互操作性制度/框架

本模块重点关注了解最低技术要求以及使用现有C&I结构和代理，在ICT设备的信任和控制之间找到适当平衡。

2) 涵盖广泛实验室服务的测试域

测试领域的范围可以无限广阔，并且可以涵盖如新技术批准、支持年轻开发人员帮助他们获得产品国际认可之类的主题。

应根据现有需求和优先事项开发培训模块，这一点要有明确的认识。

3) 在涵盖相互认可协议在内的标准和选型程序方面开展区域合作和协调

如前一章所述，协作是关键，该模块促进共享资源和已存在的机制，以证明ICT产品符合国际和国家技术要求。

4) 建立和维护测试实验室

本模块侧重于质量程序和战略评估，如业务计划优化。

6.3 结论

总之，综合分析如何制定一个能够传递信息、知识技能和知识的培训计划，要考虑以下几点：

- 与该领域专家的合作：这将包括国际电联研究组（ITU-D第4/2号课题第2研究组，ITU-T第11研究组和无线电通信局的供稿人）、测试专业人员、选型主管、贸易专家；
- 在国际电联C&I计划出版物的基础上编写培训材料，包括导则和由ITU-R和ITU-T制定的国际电联建议书；
- 国际、区域和国家组织的知识转让工作；
- 轻松获得C&I培训，并确保采用前瞻性的专业方法；
- 无论是初学者还是专家都可以获得课程设计；
- 模块化的自适应方法，提供的知识水平适合手头任务，确保内容能够满足当前C&I需求。

Annexes

Annex 1: Conformance and interoperability frameworks: Country data

Understanding how countries organize themselves for guaranteeing proper levels of conformance and interoperability for the deployment of ICT networks and devices can help C&I operators to establish efficient mechanisms for collaboration. This can be verified in effective technical collaboration agreements in some regions (e.g. Europe, APEC-MRA).

Data show that most of the countries have in place a C&I arrangement aiming to ascertain trust on safe and interoperable use of ICT devices by networks and citizens. Note that procedures and strictness levels of requirements (e.g. recognition of certification and use of proxies, self-declaration, local testing, etc.) can differ significantly.

Various events undertaken under Pillars 3 (capacity building) and 4 (assistance to developing countries)⁵¹ of the ITU C&I Programme made it possible to gather relevant information from 116 countries.⁵²

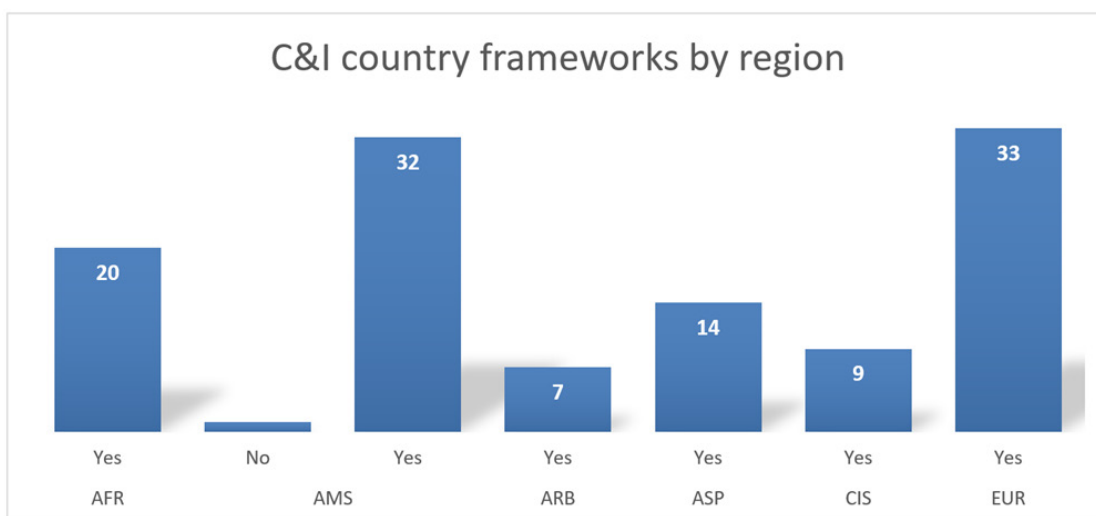
Data research and organization of essential information considered different C&I infrastructure variables, such as:

- 1) Conformance and interoperability frameworks.
- 2) ICT standards and technical requirements.
- 3) Conformance assessment and bodies.
- 4) Testing laboratories.
- 5) Quality and metrology.

⁵¹ The source material used for the data research is currently available on the ITU website, from: [C&I events](#); [Assessment studies](#); ITU-D Study Group Question 4/2 inputs as national and regional case studies.

⁵² ITU-D SG2 Document [SG2RGQ/274+Annex](#) from the BDT Focal Point for Question 4/2.

Figure 1A: C&I legal frameworks from 114 countries that provided information



The figure above displays the number of C&I country frameworks per region from 116 countries: 115 countries indicated the existence of a legal document and a level of procedure for accepting ICT products in their markets (importation fees and taxes not included); only one country, in the Americas region, indicated the absence of any legal procedures for ICT products.

The complete dataset display is a work-in-progress, and complete analysis will be provided through the ITU-C&I development portal (https://itu.int/go/ci_development).

Annex 2: Counterfeiting – a survey of national frameworks and practices

The annual ITU World Telecommunication/ICT Regulatory Survey (edition 2019) included data on regulatory practices related to the distribution and use of counterfeit ICTs.

The data series featured are as follows:

- 1) Responsibilities of telecom/ICT regulators related to ICT counterfeiting.
- 2) Types of counterfeit ICTs overseen by the telecom/ICT regulator.
- 3) Policy/legislation/regulation related to ICT counterfeiting adopted.
- 4) Areas covered in ICT counterfeiting regulations.
- 5) Plans to adopt a regulatory framework for ICT counterfeiting.⁵³

Table 1A: Summary of ITU World Telecommunication/ICT Regulatory Survey (edition 2019): Survey on regulatory practices related to the distribution and use of counterfeit ICTs

Summary								
Question	Answer	Africa	Arab States	Asia & Pacific	CIS	Europe	The Americas	Total
Does the Telecom/ICT regulator (or the entity in charge of regulation in the sector) have responsibilities related to ICT counterfeiting (e.g., fake mobile phones, smartphones, computers, any network or other computing equipment components)?	Yes	23	12	10	0	9	11	65
	No	10	3	10	2	28	14	67
Has your country adopted any policy/legislation/regulation related to ICT counterfeiting?	Yes	23	11	7	2	14	14	71
	No	10	5	15	3	20	12	65
If no, are there plans to adopt a regulatory framework for ICT counterfeiting?	Yes	3	3	4	0	3	3	16
	No	4	0	8	4	11	5	32
Region size		44	22	40	9	46	35	196
* This question allows multiple answers per country/economy								
Year: 2019 or latest available data.								
Source: ITU World Telecommunication/ICT Regulatory Database								
ITU ICT-Eye: http://www.itu.int/icteye								

⁵³ ITU-D SG2 Document [SG2RQG/38+Annex](#) from the BDT Focal Point for Question 3/1.

Figure 2A: Regional distribution of responses from survey – Question 1

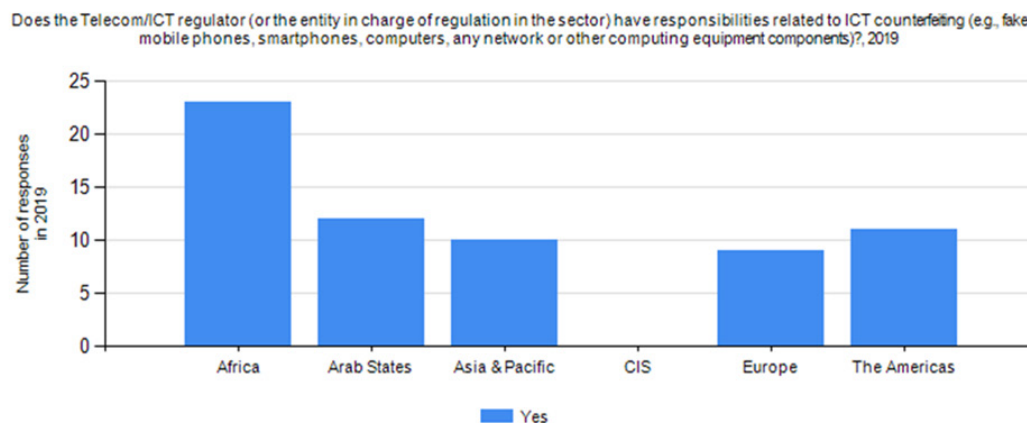


Figure 3A: Regional distribution of responses from survey – Question 2

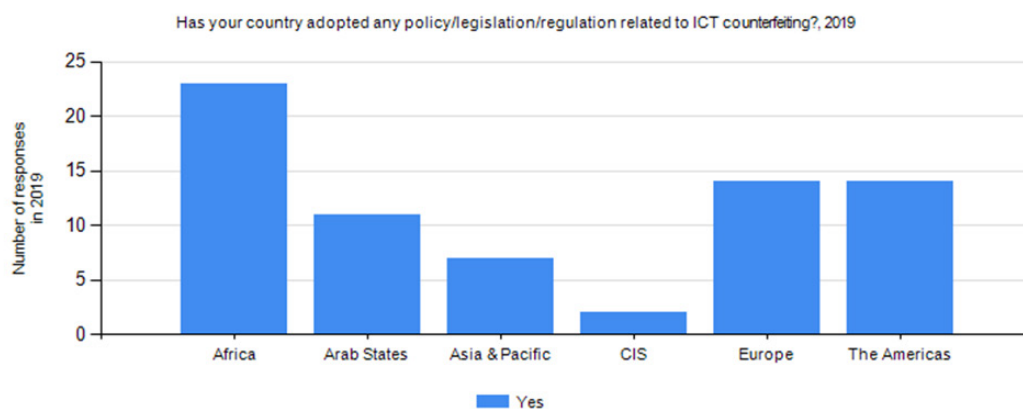
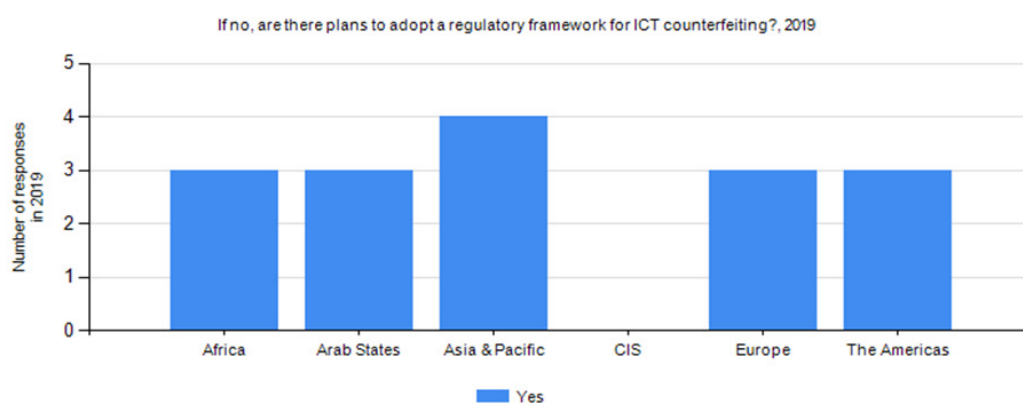


Figure 4A: Regional distribution of responses from survey – Question 3



Annex 3: Initiatives in the fight against equipment counterfeiting and mobile terminal theft in Burundi⁵⁴

A3.1 Introduction

Counterfeiting of mobile phones has numerous negative effects on industry, society, governments and in particular consumers of ICT services. Primarily, it leads to a lower quality of service of mobile telecommunications and safety hazards associated with the use of defective second-hand terminals due to inferior quality or unsuitable technical characteristics.

A3.2 Impact of the proliferation and use of counterfeit mobile terminals

The use of counterfeit mobile terminals by consumers and rising dissatisfaction among mobile subscribers faced with the growing phenomenon of mobile terminal theft has undesirable consequences in the short and long term, including:

- Lowering the QoS of mobile telecommunication services, which in turn has an impact on the experience of consumers and businesses.
- Compromising the security of digital transactions and that of mobile terminal users.
- Increasing evasion from applicable taxes and duties, which has a negative effect on tax revenues.
- Creating risks to the environment and consumer health due to the use of hazardous substances recovered from waste electrical and electronic equipment (WEEE).
- Facilitating the drugs trade, terrorism and other local, regional and international criminal activity.
- Infringing on manufacturers' trademarks.
- Significantly affecting the ICT market by proposing poor-quality, low-cost products that tend to have a greatly reduced lifetime, whence the accumulation of WEEE.

A3.3 National initiatives in the fight against mobile terminal theft and equipment counterfeiting

To combat the use of counterfeit terminals more effectively, the *Agence de régulation et de contrôle des télécommunications* (ARCT) (Telecommunication Regulatory and Control Agency of Burundi) has instituted the following measures:

- 1) Creation of certification procedures for telecommunication equipment.
- 2) Registration of the characteristics of telecommunication equipment.
- 3) Issuance of import certificates for vendors of telecommunication equipment.

⁵⁴ ITU-D SG2 Document [2/390](#) from Burundi [in French].

- 4) Enforcement of the requirement that telecommunication equipment vendors be licensed and display their vendor's licence on the establishment's walls, that terminals be certified by ARCT, and that equipment be guaranteed for at least six months.
- 5) Regular inspections to verify compliance and respect of technical standards and regulations.
- 6) Creation of a toll-free number (151) for members of the public to report telephone sales where there is a problem with the IMEI number of the phone and that on the package.
- 7) Organization of public awareness campaigns on the dangers of using counterfeit mobile terminals.
- 8) Inspection of electronic communication terminal equipment in use by public and private organizations.
- 9) Inspection of providers of value-added services who use numbering resources.

To combat the use of stolen mobile terminals more effectively, ARCT has initiated the following activities:

- 1) Registration of all mobile telecommunication service subscribers: ARCT regularly assesses compliance with the circular on the registration of subscribers by the telecommunication operators, in order to combat fraud.
- 2) Automation of the service for requisitioning expert testimony: A management application for processing and managing requisitions for expert testimony in cases of mobile communication terminal theft has been designed and implemented.
- 3) Combating theft and crimes committed using mobile telephones: ARCT invites members of the public to report the numbers used to send suspicious messages and to forward them to ARCT for systematic verification and deactivation if necessary.

A3.4 Conclusion

It is crucial to put into action all effective means for combating counterfeit terminals being sold or connected to the telecommunication network, so as to protect the consumers of ICT services. This will also enhance security for users, improve the quality of service of networks and stimulate digital economy and financial growth of the country.

Annex 4: Illustrations for chapters of the Output Report on Question 4/2

The following illustrations summarize concepts for Chapters 2, 3 and 5 of the Output Report.

Definitive, high-level resolution images of the illustrations are available at https://itu.int/go/CI_development.

Figure 5A: Illustration for Chapter 2 – What is conformance and interoperability (C&I)



Figure 6A: Illustration for Chapter 2 – C&I frameworks



Figure 7A: Illustration for Chapter 3 – Combating the proliferation of counterfeit, substandard and tampered devices



Figure 8A: Illustration for Chapter 5 – The Internet of Things and C&I



Annex 5: Ideas for the future of the Question

Having regard to the role of C&I in a hyperconnected world where billions of people and objects connect with each other, the study group's work on C&I could focus on:

- **Efforts to manage the increasing number of devices sharing the same limited resources**
- **Measures to cover costs related to conformity procedures and controls of ICT products to allow only approved products to access markets**
- **Harmonization of procedures and collaboration**
 - Robust C&I frameworks: Making sure every country has or is part of a robust C&I framework at minimal cost (e.g. agreements on the shared use of national C&I infrastructure, such as testing facilities and certificates of conformity).
 - Collaboration: Are MRAs effective tools to pursue in the future? What aspects of MRAs need to be adapted to improve existing collaboration agreements or develop new ones? The group could focus on innovative collaboration structures to improve access to high-quality and safe ICT products.
- **Trends**
 - Future challenges for C&I, such as:
 - New technologies outpacing regulation/testing procedures
 - Regulatory aspects for open RAN and interoperability adoption related to 5G
 - Smart objects able to communicate through ICTs
 - Software tampering/hacking vulnerabilities
 - Effective harmonization of procedures and technical collaboration, etc.
 - Means of prioritizing device/type-approval models to achieve a good balance between trust and control.
 - C&I challenges and opportunities during the COVID-19 pandemic.
 - Ways in which new technologies (such as blockchain and artificial intelligence) can help to improve trust in the international C&I framework and trade in and use of ICT devices.

Annex 6: List of contributions and liaison statements received on Question 4/2

Contributions on Question 4/2

Web	Received	Source	Title
2/423	2021-03-18	Rapporteur for Question 4/2	Proposed liaison statement from ITU-D Study Group 2 Question 4/2 to ITU-T Study Group 11, ITU-R WP1A and WP6A, and ISO/CASCO
2/390	2021-02-03	Burundi	Initiatives de lutte contre les équipements de contrefaçon et le vol des terminaux mobiles au Burundi
RGQ2/277	2020-09-22	Algérie Télécom SPA (Algeria)	Revisions to Draft Chapter 3 for the Final Report of Question 4/2
RGQ2/274 +Ann.1	2020-09-22	BDT Focal Point for Question 4/2	C&I Database – updated summary
RGQ2/269	2020-09-22	Rapporteur for Question 4/2	Draft text for new chapter (Ideas for the Future of the Question) of the Output Report for Question 4/2
RGQ2/265	2020-09-22	Rapporteur for Question 4/2	Draft text for Chapter 1 Section 1.4 on COVID-19 impact to type approval procedures
RGQ2/264	2020-09-22	Kenya	Proposed draft text for Chapter 4 of the Output Report for Question 4/2
RGQ2/233	2020-08-20	Algérie Télécom SPA (Algeria)	Proposed text for Chapter 5: Internet of Things and C&I
2/345	2020-02-11	BDT Focal Point for Question 4/2	ITU Conformance and Interoperability Training Programme
2/337	2020-02-11	Algérie Télécom SPA (Algeria)	Revisions to draft Chapter 3 for the Final Report of Q4/2
2/332 +Ann.1	2020-02-11	Kenya	Device Management System – Kenyan Case
2/326	2020-02-10	Oman	Problem of increasing use of fake IMEI
2/323 (Rev.1)	2020-02-07	Ghana	Achieving quality C&I regimes – Challenges from basic Infrastructure to legislative and regulatory frameworks. The experience of Ghana
2/311	2020-01-28	International Telecommunication Academy (Russian Federation)	Regulation on the system to confirm the compliance of communication facilities and services with the ITU standard
2/290	2020-01-08	Mauritania	Mauritania (Islamic Republic of)
2/261	2019-12-24	Guinea	Conformance and interoperability (C&I)
2/257	2019-12-20	Mauritania	Proposed draft text for Chapter 2 of the Final Report for Question 4/2

(continued)

Web	Received	Source	Title
2/250	2019-12-08	Comoros	Progress of activities for implementing conformance and interoperability programmes in the Union of the Comoros
RGQ2/194 +Ann.1	2019-09-24	BDT Focal Point for Question 4/2	ITU Conformity and Interoperability Training Programme (CITP)
RGQ2/171	2019-09-18	Algérie Télécom SPA (Algeria)	Implementation of Plenipotentiary Conference (PP-18) Resolution 177 (Rev. Dubai, 2018)
RGQ2/170	2019-09-15	Mauritania	Conformité et interopérabilité des équipements TIC dans les pays en développement: normes et procédures – cas de la Mauritanie
RGQ2/144	2019-08-20	Central African Republic	Assistance to developing countries for implementing conformance and interoperability (C&I) programmes and combating counterfeit ICT equipment and theft of mobile devices
RGQ2/139	2019-08-06	Guinea	Assistance to developing countries for implementing conformance and interoperability (C&I) programmes and combating counterfeit ICT equipment
2/TD/24	2019-03-29	Rapporteur for Question 4/2	Proposed outgoing liaison statements from Q4/2
2/TD/22 +Ann.1-3	2019-03-27	Rapporteur for Question 4/2	Proposed updates to work plan, table of contents and areas of responsibilities, matrix of contributions received and proposal for second focus session
2/210	2019-03-12	BDT Focal Point for Question 4/2	C&I Programme – Pillars 3 & 4 implementation report
2/202 +Ann.1	2019-03-08	BDT Focal Point for Question 4/2	Summary on national C&I topics
2/177	2019-02-07	Rapporteur for Question 4/2	Draft Chapter 3 for Final Report on Question 4/2
2/166	2019-02-06	Mexico	Regulatory obligations to help combat the theft of mobile devices
2/149	2019-01-24	Guinea	Assistance to developing countries for implementing conformance and interoperability programmes, portability and combating counterfeit ICT equipment and theft of mobile devices
2/142	2019-01-16	Madagascar	Implementing conformance and interoperability programmes

(continued)

Web	Received	Source	Title
2/133	2019-01-10	Comoros	Realization of a programme for assistance to developing countries for implementing conformance and interoperability programmes: case of Union of the Comoros
RGQ2/TD/8	2018-09-25	South Sudan	Challenges and proposals to deal with counterfeit ICT equipment and mobile device theft in South Sudan and region
RGQ2/TD/7	2018-10-01	Russian Federation	ITU-D SG1 and SG2 coordination: Mapping of ITU-D Study Group 1 and 2 Questions
RGQ2/86 +Ann.1	2018-09-18	BDT Focal Point for Question 4/2	ITU C&I programme: implementation update
RGQ2/85	2018-09-18	Zimbabwe	Actions to combat counterfeit and theft of mobile devices in Zimbabwe
RGQ2/82	2018-09-18	Ghana	Ghana's Type Approval Regime – a sustainable approach to connecting and protecting users of telecommunications/ ICTs and networks through conformance assessment
RGQ2/80	2018-09-18	GSM Association	GSMA' s IMEI database and services
RGQ2/69	2018-09-17	Rwanda	Regional effort to fight illegal devices, improve the quality of services and minimize health hazard to consumers
RGQ2/66 (Rev.1)	2018-09-16	Senegal	Lutte contre la contrefaçon et le vol de téléphone
RGQ2/38 +Ann.1	2018-08-18	BDT Focal Point for Question 3/1	ITU data on regulatory practices related to counterfeit ICTs
RGQ2/9 (Rev.1)	2018-07-05	Guinea	Implementing conformance and interoperability programmes and combating counterfeit ICT equipment and theft of mobile devices
2/TD/10	2018-05-10	Rapporteur for Question 4/2	Draft reply liaison statements from ITU-D Study Group 2 Question 4/2
2/TD/8	2018-05-09	Rapporteur for Question 4/2	Draft work plan, Table of Contents (ToC) and responsibilities for ITU-D Question 4/2
2/97 (Rev.1)	2018-05-06	Chairman, ITU-D Study Group 2	List of proposed Rapporteurs and Vice-Rapporteurs of ITU-D Study Group 2 study Questions for the 2018-2021 period
2/92 +Ann.1	2018-04-24	BDT Focal Point for Question 4/2	ITU C&I Programme status – Pillars 3 and 4
2/90	2018-04-24	Mauritania	Draft work plan for ITU-D Study Group 2 Question 4/2

(continued)

Web	Received	Source	Title
2/88 +Ann.1	2018-04-23	BDT	Implementation of ITU C&I Programme and ITU-T activities on combatting counterfeiting and stolen ICT devices
2/83	2018-04-23	Iran University of Science and Technology (Islamic Republic of Iran)	HAMTA: A system for combating counterfeit ICT equipment and theft of mobile devices
2/58	2018-03-22	Algérie Télécom SPA (Algeria)	Conformance and interoperability
2/45	2018-03-12	Madagascar	Monitoring counterfeit terminal devices, building a healthy network that brings in revenues for the Stat

Incoming liaison statements for Question 4/2

Web	Received	Source	Title
RGQ2/219	2020-08-06	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on updates on the current work at ITU-T Q15/11 "Combating counterfeit and stolen ICT equipment"
RGQ2/205 +Ann.1-2	2020-03-25	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on updates on the current work at ITU-T Q15/11 "Combating counterfeit and stolen ICT equipment"
RGQ2/204 +Ann.1	2020-03-25	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on contribution on conformance and interoperability
RGQ2/115 +Ann.1	2019-06-14	ITU-T Study Group 5	Liaison statement from ITU-T SG5 to ITU-D SG2 Q4/2 and Q7/2 on work being carried out under study in ITU-T Study Group 5 Question 3/5
RGQ2/113	2019-05-29	ITU-T Study Group 20	Liaison statement from ITU-T SG20 to ITU-D SG2 Q4/2 on SG20 activities on IoT and Smart Cities & Communities
RGQ2/111 +Ann.1-3	2019-04-21	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on collaboration
2/TD/22 +Ann.1-3	2019-03-27	Rapporteur for Question 4/2	Proposed updates to work plan, table of contents and areas of responsibilities, matrix of contributions received and proposal for second focus session
2/TD/19 +Ann.1-3	2019-03-21	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on collaboration
2/TD/17 +Ann.1	2019-03-20	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on updates to the Technical Report on the Combat of Counterfeit Devices

(continued)

Web	Received	Source	Title
2/TD/16 +Ann.1	2019-03-20	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on creation of new work item on "Reliability of IMEI identifier"
2/TD/15	2019-03-20	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on impact of counterfeit mobile devices on Quality of Service
2/139	2019-01-16	ITU-T Study Group 20	Liaison statement from ITU-T SG20 on SG20 activities on IoT and Smart City & Community
RGQ2/16 +Ann.1-3	2018-08-02	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on progress and collaboration on the combat of counterfeit and mobile device theft
2/35	2017-12-01	ITU-T Study Group 11	Liaison Statement from ITU-T SG11 to ITU-D SG2 Question 4/2 on ongoing collaboration

**国际电信联盟 (ITU)
电信发展局 (BDT)
主任办公室**

Place des Nations
CH-1211 Geneva 20
Switzerland

电子邮件: bdtdirector@itu.int
电话: +41 22 730 5035/5435
传真: +41 22 730 5484

数字网络和社会部 (DNS)

电子邮件: bdt-dns@itu.int
电话: +41 22 730 5421
传真: +41 22 730 5484

非洲

埃塞俄比亚

**国际电联
地区代表处**
Gambia Road
Leghar Ethio Telecom Bldg, 3rd floor
P.O. Box 60 005
Addis Ababa
Ethiopia

电子邮件: itu-ro-africa@itu.int
电话: +251 11 551 4977
电话: +251 11 551 4855
电话: +251 11 551 8328
传真: +251 11 551 7299

美洲

巴西

**国际电联
地区代表处**
SAUS Quadra 6 Ed. Luis Eduardo
Magalhães,
Bloco "E", 10^o andar, Ala Sul
(Anatel)
CEP 70070-940 Brasília - DF
Brazil

电子邮件: itubrasilia@itu.int
电话: +55 61 2312 2730-1
电话: +55 61 2312 2733-5
传真: +55 61 2312 2738

阿拉伯国家

埃及

**国际电联
地区代表处**
Smart Village, Building B 147,
3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
Cairo
Egypt

电子邮件: itu-ro-arabstates@itu.int
电话: +202 3537 1777
传真: +202 3537 1888

欧洲

瑞士

**国际电联
欧洲处**

Place des Nations
CH-1211 Geneva 20
Switzerland

电子邮件: euregion@itu.int
电话: +41 22 730 5467
传真: +41 22 730 5484

**副主任兼行政和运营
协调部负责人 (DDR)**

Place des Nations
CH-1211 Geneva 20
Switzerland

电子邮件: bdtdeputydir@itu.int
电话: +41 22 730 5131
传真: +41 22 730 5484

数字化发展合作伙伴部 (PDD)

电子邮件: bdt-pdd@itu.int
电话: +41 22 730 5447
传真: +41 22 730 5484

数字知识中心部 (DKH)

电子邮件: bdt-dkh@itu.int
电话: +41 22 730 5900
传真: +41 22 730 5484

喀麦隆

**国际电联
地区办事处**
Immeuble CAMPOST, 3^e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé
Cameroon

电子邮件: itu-yaounde@itu.int
电话: +237 22 22 9292
电话: +237 22 22 9291
传真: +237 22 22 9297

巴巴多斯

**国际电联
地区办事处**
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown
Barbados

电子邮件: itubridgetown@itu.int
电话: +1 246 431 0343
传真: +1 246 437 7403

亚太

泰国

**国际电联
区域代表处**
Thailand Post Training Center
5th floor
111 Chaengwattana Road
Laksi
Bangkok 10210
Thailand

邮寄地址:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210, Thailand

电子邮件: ituasiapacificregion@itu.int
电话: +66 2 575 0055
传真: +66 2 575 3507

塞内加尔

**国际电联
地区办事处**
8, Route des Almadies
Immeuble Rokhaya, 3^e étage
Boîte postale 29471
Dakar - Yoff
Senegal

电子邮件: itu-dakar@itu.int
电话: +221 33 859 7010
电话: +221 33 859 7021
传真: +221 33 868 6386

智利

**国际电联
地区办事处**
Merced 753, Piso 4
Santiago de Chile
Chile

电子邮件: itusantiago@itu.int
电话: +56 2 632 6134/6147
传真: +56 2 632 6154

印度尼西亚

**国际电联
地区办事处**
Sapta Pesona Building
13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10110
Indonesia

邮寄地址:
c/o UNDP - P.O. Box 2338
Jakarta 10110, Indonesia

电子邮件: ituasiapacificregion@itu.int
电话: +62 21 381 3572
电话: +62 21 380 2322/2324
传真: +62 21 389 5521

津巴布韦

**国际电联
地区办事处**
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792
Belvedere Harare
Zimbabwe

电子邮件: itu-harare@itu.int
电话: +263 4 77 5939
电话: +263 4 77 5941
传真: +263 4 77 1257

洪都拉斯

**国际电联
地区办事处**
Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cia
Apartado Postal 976
Tegucigalpa
Honduras

电子邮件: itutegucigalpa@itu.int
电话: +504 2235 5470
传真: +504 2235 5471

独联体国家

俄罗斯联邦

**国际电联
区域代表处**
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

电子邮件: itumoscow@itu.int
电话: +7 495 926 6070

国际电信联盟
电信发展局

Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN: 978-92-61-34135-0



9 789261 341350

瑞士出版
2021年,日内瓦

图片来源: Shutterstock