

ITU-D第4/2号课题输出成果报告

电信/信息通信技术设备： 一致性和互操作性、打击 假冒和盗窃移动设备的行为

2022-2025年研究期



ITU-D第4/2号课题输出成果报告

电信/信息通信技术设备： 一致性和互操作性、打击假 冒和盗窃移动设备的行为

2022-2025年研究期



电信/信息通信技术设备：一致性和互操作性、打击假冒和盗窃移动设备的行为：ITU-D第4/2号课题2022-2025年研究期输出成果报告

ISBN 978-92-61-41185-5（电子版）

ISBN 978-92-61-41195-4（EPUB版）

© 国际电信联盟 2025

International Telecommunication Union, Place des Nations, CH-1211 Geneva, Switzerland

保留部分权利。本作品采用知识共享署名 – 非商业性使用 – 相同方式共享3.0 IGO许可证（CC BY-NC-SA 3.0 IGO）向公众授权。

根据本许可条款，您可以出于非商业目的复制、重新分发和改编本作品，但前提是按如下所示对作品进行适当的引用。使用本作品时，不得暗示国际电联认可任何特定组织、产品或服务。未经授权，不得使用国际电联的名称或标识。如果您改编本作品，则必须根据相同或等效的知识共享许可协议授权您的作品。如果您翻译本作品，则应在建议的引用之外添加以下免责声明：“本译文并非由国际电信联盟（国际电联）创作。国际电联对本译文的内容或准确性不承担任何责任。原英文版应为具有约束力的正式版本”。更多信息，请访问：

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

建议引用内容。电信/信息通信技术设备：一致性和互操作性、打击假冒和盗窃移动设备的行为：ITU-D第4/2号课题2022-2025年研究期输出成果报告。日内瓦：国际电信联盟，2025年。许可：CC BY-NC-SA 3.0 IGO。

第三方资料。如果您希望重复使用本作品中归属于第三方的材料，例如表格、图表或图像，您有责任确定是否需要获得许可，并获得版权所有者的许可。因侵犯作品中任何第三方拥有的内容而导致的索赔风险完全由用户承担。

一般免责声明。本出版物中采用的名称和材料的呈现方式并不代表国际电信联盟（ITU）或国际电联秘书处对任何国家、领土、城市或地区或其当局的法律地位、或其边界划定的任何意见。

提及特定公司或某些制造商的产品并不意味着国际电联赞同或推荐这些公司或这些产品，而非其它未提及的同类公司或产品。除错误和遗漏外；专有产品的名称以首字母大写区分。

国际电联已采取一切合理的谨慎措施来核实本出版物中包含的信息。但是，所发布材料的分发没有任何明示或暗示的保证。资料的解释和使用责任由读者自负。

本出版物中表达的意见、调查结果和结论不一定反映国际电联或其成员的观点。

封面图片来源：Adobe Stock

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在此汇聚一堂，开发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的基础上编写报告、导则和建议。研究课题每四年由世界电信发展大会（WTDC）确定。国际电联成员于2022年6月在基加利举行的WTDC-22上商定，在2022-2025年期间，第2研究组将在数字化转型的总体范围内处理七项课题。

本报告是针对第4/2号课题“**电信/信息通信技术设备：一致性和互操作性，打击假冒和盗窃移动设备的行为**”编写的，由ITU-D第2研究组的管理班子进行全面指导和协调。该研究组由主席Fadel Digham先生（阿拉伯埃及共和国）领导，并得到以下副主席的支持：Abdelaziz Alzarooni先生（阿拉伯联合酋长国）、Zainab Ardo女士（尼日利亚联邦共和国）、Javokhir Aripov先生（乌兹别克斯坦共和国）、Carmen-Mădălina Clapon女士（罗马尼亚）、Mushfig Guluyev先生（阿塞拜疆共和国）、Hideo Imanaka先生（日本）、Mina Seonmin Jun女士（大韩民国）、Mohamed Lamine Minthe先生（几内亚共和国）、Víctor Antonio Martínez Sánchez先生（巴拉圭共和国）、Alina Modan女士（罗马尼亚）、¹Diyor Rajabov先生（乌兹别克斯坦共和国）、¹巫彤宁先生（中华人民共和国）和Dominique Würges先生（法国）。

本报告由第4/2号课题报告人Ibrahima Sylla先生（几内亚共和国）领导编写，他是第1章的作者，其它章节的作者如下：副报告人Tharalika Livera女士（斯里兰卡民主社会主义共和国）为第2章作者；Serigne Abdou Lahatt Sylla先生（塞内加尔共和国）为第3章作者；阎军智先生（中华人民共和国）为第4章作者；Awa Koko Valéry Nadège Traore Epouse Goue女士（科特迪瓦共和国）为第5章作者；Sergei Melnik先生（国际电信学院）为第6章作者。此外，还要感谢积极贡献者Gordon Gillerman先生（美利坚合众国）和Turhan Muluk先生（英特尔公司）。

本报告是在ITU-D第4/2号课题联系人、编辑以及出版物制作团队和ITU-D第2研究组秘书处的支持下编写的。

¹ 在本研究期内卸任。

目录

鸣谢	iii
内容提要.....	viii
缩写词和首字母缩略语	ix
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 引言	1
1.2 ICT产品对社会的相关性.....	2
1.3 ICT设备的社会经济应用.....	2
1.4 遵循公认标准/遵守公认的ICT质量和互操作性标准	3
1.5 新冠疫情对审批程序的影响.....	6
第2章 – 一致性和互操作性.....	7
2.1 引言	7
2.2 关键问题的考虑	8
2.3 技术规范和标准	9
2.3.1 国家和区域层面C&I应用展示.....	9
2.3.2 良好做法	9
2.3.3 建立联合C&I的潜在协作机制.....	10
2.3.4 技术合作	11
2.4 关于一致性评定的相互认可安排/协议	11
2.4.1 什么是相互认可安排/协议？	11
2.4.2 MRA在C&I领域的作用.....	11
2.4.3 与国际MRA有关的问题	12
2.5 建立强大的C&I框架的必要性.....	12
2.5.1 高质量C&I框架的基本基础设施：技术标准与必要的立法修订	12
2.5.2 联邦测试的概念	13
2.6 市场监督	13
2.6.1 提高监测意识	13
2.6.2 监测与合作	14
2.7 新技术的一致性评定.....	14

2.7.1 新技术挑战	15
2.7.2 预合规性测试	16
2.7.3 预期影响	16
第3章 – 打击设备的非法使用行为：移动设备的假冒、质量缺陷和盗窃.....	17
3.1 假冒设备扩散的挑战.....	17
3.2 导则	17
3.3 移动设备盗窃	18
3.4 难题和问题	19
3.5 国家案例研究	20
3.5.1 赞比亚共和国	20
3.5.2 几内亚	21
3.5.3 乍得共和国	23
3.5.4 斯里兰卡	23
3.5.5 卢旺达	23
第4章 – 物联网的一致性和互操作性.....	24
4.1 引言	24
4.2 IoT生态系统和应用场景.....	24
4.2.1 IoT生态系统	24
4.2.2 应用场景	25
4.2.3 IoT设备的分类	25
4.3 与C&I相关的IoT挑战.....	26
4.4 IoT产品的法规和政策	27
4.5 新IoT设备的合规标准	28
第5章 – 知识转移.....	30
5.1 引言	30
5.2 C&I培训需求和机会.....	30
5.3 响应知识获取与留存需求的措施.....	32
5.4 开展一致性和互操作性项目的导则.....	34
第6章 – 一致性和互操作性问题：挑战、解决方案和前景	35
6.1 超出监管/测试程序的新技术	35

6.2	5G的C&I.....	39
6.2.1	对实验室和认证机构进行认可，以使用5G技术	39
6.2.2	实施基于数字计量的远程测试机制.....	40
6.3	对已认证的ICT设备进行的软件修改及其对现有C&I框架的影响	40
6.4	程序的有效协调和技术协作.....	42
6.5	如何确定设备/型号核准型号的优先排序，同时在用户信心和适用监 管措施之间取得平衡.....	44
6.6	新冠疫情期间C&I面临的挑战和机遇.....	44
6.7	新技术如何助力改善国际C&I框架和ICT设备的贸易和使用？	45
Annexes		46
Annex 1:	Conformance and interoperability frameworks: data by country	46
Annex 2:	Summary of the workshop on compliance and interoperability challenges for digital transformation.....	49
Annex 3:	Summary of the workshop on techniques designed to promote harmonization of C&I regimes	52
Annex 4:	List of contributions and liaison statements received on Question 4/2	55

表和图目录

表

表1: 制定或认可国际标准的组织.....4

图

图1: 可持续发展目标.....1

图2: 市场监督在加纳的推广14

图3: 加纳C&I机制的构成31

图4: 加纳C&I机制的目标31

图5: 肯尼亚C&I机制的目标32

图6: 国际电联-NCA非洲培训项目33

图7: PDCA循环.....35

图8: PDCA循环的计划阶段.....36

图9: PDCA循环的执行阶段.....37

图10: PDCA循环的检查阶段38

图11: PDCA循环的处置阶段.....39

Figure 12: Percentage of countries with established C&I mechanisms.....47

Figure 13: Mapping distribution to chapters.....59

内容提要

编写本报告的总体原则：1) 利用一致性和互操作性（C&I）提升发展中国家公民获取信息通信技术（ICT）的机会；2) 避免对贸易造成不必要的障碍。

第八届世界电信发展大会于2022年6月6日至16日在卢旺达共和国基加利举行，主题为“**将未连接者连接起来，实现可持续发展**”，本内容提要重点阐述了大会宣言中提出的主要问题。以下是所提出的要点：

- **ICT的重要性**：在当今数字世界中，ICT设备不可或缺。
- **网络的互操作性**：国际电信网络对互操作性的需求是1865年创建国际电报联盟的主要原因，这仍然是国际电联战略规划的主要总体目标之一。
- **标准的协调统一**：全球标准的协调统一对于确保网络和设备的互操作性至关重要。
- **C&I项目**：所有国家都在实施C&I项目，但进度各不相同。利用和认可现有的国际惯例（例如美国、欧盟及其他地区已确立的惯例）是有益的。
- **ITU-D的协助**：国际电联电信发展部门（ITU-D）协助成员国应对与ICT设备的C&I相关的技术和经济挑战。
- **监管机构的作用**：监管机构在管理C&I框架以确保安全和控制方面发挥着至关重要的作用。
- **未来发展**：新技术的出现，尤其是与物联网（IoT）相关的技术，在C&I方面带来了更多挑战。
- **新的网络技术**：有必要通过组织讲习班和其他能力建设活动，支持成员国，特别是发展中国家，提高对解耦式、开放和可互操作的网络技术的认识 and 了解，如开放式无线接入网（Open RAN）和其他技术。
- **数字技能**：需要制定有效计划，以培养和提升在线世界所需的数字能力和技能，否则数字鸿沟将继续扩大。
- **良好做法**：本报告探讨了在C&I方面寻找最优解决方案的良好做法。

总之，报告强调了在ICT的C&I领域协助发展中国家的重要性，以及与这一不断演进的领域相关的挑战和机遇。

缩写词和首字母缩略语

缩写词	术语
3G	第三代移动技术
3GPP	第三代伙伴关系项目
4G	第四代移动技术
5G	第五代移动技术
6G	第六代移动技术 ²
AB	认可机构
AI	人工智能
ANSI	美国国家标准学会
ANSSI	几内亚国家信息系统安全局
API	应用程序接口
C&I	合规性/一致性/一致性和互操作性
CAB	一致性评定机构
DMIS	尺寸测量接口标准
DMSC	数字计量标准联盟
EMC	电磁兼容性
ETSI	欧洲电信标准化协会
GDP	国内生产总值
GDPR	通用数据保护条例
GSMA	全球移动通信系统协会
HPHC	高处理高连接
IAF	国际认可论坛
ICT	信息通信技术
IEC	国际电工委员会
IECERS	综合电子通信设备登记系统

² 尽管本文件注意正确使用和指称各代IMT的官方定义（见ITU-R第56号决议“国际移动通信的命名”），但本文件的一些部分包含了成员提供的采用常用市场名称“xG”的材料。此材料不一定对应到特定的某一代IMT，因为成员的基本标准是未知的，但总的来说，IMT-2000、IMT-Advanced、IMT-2020和IMT-2030分别称为3G/4G/5G/6G。

(续)

缩写词	术语
IEEE	电气电子工程师学会
IETF	互联网工程任务组
ILAC	国际实验室认可合作组织
IMEI	国际移动设备标识
IMT	国际移动通信
ISDN	综合业务数字网
ISO	国际标准化组织
IoT	物联网
ITU	国际电信联盟
ITU-D	国际电联电信发展部门
ITU-R	国际电联无线电通信部门
ITU-T	国际电联电信标准化部门
JTC	联合技术委员会
KEBS	肯尼亚标准局
LEO	低地球轨道
LoRaWAN	长距离广域网
LPHC	低处理高连接
LPLC	低处理低连接
LPWAN	低功率广域网
LTE	长期演进
M2M	机器对机器
MRA	相互认可安排/协议
NCA	加纳国家通信管理局
PDCA	计划、执行、检查、处置
QIF	质量信息框架
RAN	无线接入网络
RF	射频
SDG	可持续发展目标
SIPs	会话发起协议
SWG 5	第5特别工作组

(续)

缩写词	术语
TBT	技术性贸易壁垒
TIA	电信行业协会
TRCSL	斯里兰卡电信监管委员会
W3C	万维网联盟
WSN	无线传感器网络
WTDC	世界电信发展大会
WTO	世界贸易组织
WTSA	世界电信标准化全会

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 引言

可持续发展目标（SDG）是全球致力于应对我们这个时代最紧迫的挑战（从扶贫到环境可持续性）的核心所在。信息通信技术（ICT）在实现这些目标方面发挥着至关重要的作用，为有效且可持续地应对这些挑战提供了工具和创新解决方案。

ICT产品能够助力实现所有SDG。例如，移动应用可用于改善教育资源的获取，基于传感器的监测系统有助于水资源管理，电子商务平台可促进包容性经济增长。

此外，ICT通过赋能个人和组织在全球范围内交换信息、协调行动并调动资源，从而鼓励协作并提高意识。这有助于以全面综合的方式实现SDG，促进政府、私营部门、民间团体和公民之间的合作。

通过投资于ICT产品的开发和使用以实现SDG，可以利用科技的力量为所有人创建一个更加公正、可持续和繁荣的未来。

图1：可持续发展目标



来源：联合国³

³ <https://www.un.org/zh/teach/SDGs>

1.2 ICT产品对社会的相关性

ICT产品在我们的现代社会中发挥着关键作用，提供了大量的益处和机遇。ICT产品与社会的相关性体现在以下几个层面：

- **改善连通性：**智能手机和电脑等ICT产品能够促进个人、社区和国家之间的沟通和连接，从而促进信息交流、合作并强化社会纽带。
- **获取信息：**ICT提供了快速便捷地获取不同主题的大量信息的途径，助力学习、研究以及知情决策。
- **完善公共服务：**政府正在利用ICT产品提升公共服务的效率与可及性，例如电子卫生服务、远程教育系统以及交通管理平台等。
- **创新与经济发展：**ICT通过便利企业创立、助力进入全球市场以及推动业务流程自动化，驱动创新与经济发展。
- **社会包容性：**ICT产品有助于弥合数字鸿沟，提供公平获取技术的机会，并将边缘化群体与经济和社会机遇连通起来。
- **助力SDG：**可利用ICT产品应对众多社会与环境挑战，如扶贫、推动教育发展、管理自然资源以及减少不平等现象等。

由此可见，ICT产品对社会至关重要，因为它们能够促进连通性、信息获取、高效政府服务、经济创新、社会包容性并助力实现SDG。

1.3 ICT设备的社会经济应用

当一个社会的社会性目标与经济可行性高度融合且被同步考虑，ICT设备有助于将社会企业的原则与科技带来的可能性相结合，从而对社会产生积极且可持续的影响。以下是ICT设备在此背景下的一些使用方式：

- **扩大可及性：**通过使用ICT，社会经济举措能够触及更广泛的受众，从而扩大其影响力。价格可承受的智能手机和电脑等技术，可以让更多的人获得服务，包括来自边缘化或低收入社区的群体。
- **社会创新：**ICT设备正在推动开发并实施创新解决方案，以应对社会问题。例如，可以设计移动应用，为农村地区提供负担得起的医疗服务，或帮助弱势社区获得教育机会。
- **能力建设：**可以利用ICT设备和终端，为社会经济组织配备管理、监测和评估工具，从而加强这些组织的能力。项目管理软件、数据收集平台和在线通信工具可以帮助这些组织优化运营并衡量其影响力。
- **数字包容性：**通过提供ICT设备使用和数字技能方面的培训，社会经济举措可以促进数字包容性，弥合社区中的数字鸿沟。
- **弥合性别鸿沟：**ICT和ICT产品是实现性别平等以及增强所有妇女和女童权能的重要途径。

- **环境可持续性：**在一个社会经济体系中，还能以对环境负责的方式使用ICT设备。例如，电子产品回收举措有助于减少电子垃圾，促进环境可持续性。通过将ICT设备融入经济社会的模式，可以打造出创新、可及且可持续的解决方案，以满足社区的社会、经济和环境需求。

ICT产品带来的益处日益受到发展中国家的欢迎，其中大多数国家正在ICT领域开展大规模的发展项目。

正是在这一背景下，中非共和国⁴正努力填补重大的监管和制度空白，以充分利用数字技术作为增长引擎和支持减贫的工具。最终目标是解决与假冒和伪造ICT设备相关的问题，最重要的是，到2030年实现与产业、创新和基础设施相关的SDG（SDG 9）。

最终，为了支持国家层面的技术研究、开发和创新，并大幅增加公众获取负担得起的宽带技术和服务的机会，中非共和国决定：

- a) 完善电信业的法律和监管框架；
- b) 加强数字经济、邮政和电信部以及电信监管机构－电子通信和邮政监管局的能力；
- c) 建立一个能力完备且经过认证的实验室，以测试或认可ICT设备；
- d) 电子通信和邮政监管局推动电信基础设施共享和部署，以降低部署成本。

1.4 遵循公认标准/遵守公认的ICT质量和互操作性标准

在ICT造福社会的背景下，遵循公认标准对于确保产品和服务的质量、安全性和互操作性至关重要。ICT产品必须遵守的公认标准的示例包括：

- **ISO 27001－信息安全：**该国际标准化组织（ISO）标准定义了实施、维护和改进信息安全管理体系的要求。其目标是保护敏感信息免受黑客攻击、数据丢失或隐私泄露等威胁。
- **ISO 9001－质量管理：**ISO 9001标准确立了有效质量管理体系（QMS）的标准。它面向ICT产品供应商，旨在确保客户满意度、持续改进和监管合规性。
- **万维网联盟（W3C）**为开发HTML、CSS和JavaScript等web技术制定标准和建议。遵循这些标准可确保ICT产品与现代web浏览器兼容，并可供广大受众获取。
- **《通用数据保护条例》（GDPR）：**对于处理个人信息的ICT产品而言，遵守GDPR以确保尊重用户的隐私权和数据保护权至关重要。
- **电气电子工程师协会（IEEE）**为ICT的各个方面制定标准，包括无线网络、以太网通信和编码标准。
- **ISO/IEC 17025 “检测和校准实验室能力的通用要求”：**该ISO和国际电工委员会（IEC）标准规定了实验室合格、公正和持续运作的通用要求。实验室客户、监管机构、采用同行评审的组织和制度、认可机构（AB）及其他机构使用本文件来确

⁴ 中非共和国提交的SG2RGQ/17号文件。

认或认可实验室的能力。ICT供应商通过由国际实验室认可合作组织相互认可安排（ILAC MRA）签署方AB认可的合格实验室（按照国际电联电信标准化部门（ITU-T）建议书等标准）对其ICT产品进行测试，从而在C&I方面赢得客户的信任。

- 关于高速移动通信的5G（国际移动通信（IMT）-2020）和4G长期演进（LTE）标准。
- 关于云计算和参考架构标准的ISO/IEC 17788和ISO/IEC 17789标准。
- 关于人工智能（AI）术语和概念的ISO/IEC 22989标准。

表1：制定或认可国际标准的组织

编号	组织	描述	链接
1	ITU	国际电信联盟制定全球电信和ICT标准	https://www.itu.int/ITU-T
2	ISO	国际标准化组织发布各行业（包括ICT）的国际标准。	https://www.iso.org
3	IEC	国际电工委员会专注于电气、电子及相关技术的标准。	https://www.iec.ch
4	IEEE	电气电子工程师协会为包括ICT和网络在内的众多行业制定标准。	https://www.ieee.org
5	ETSI	欧洲电信标准化协会为欧洲和全球的ICT系统和服务制定标准。	https://www.etsi.org
6	ANSI	美国国家标准学会负责监督美国自愿性共识标准的制定工作。	https://www.ansi.org
7	W3C	万维网联盟制定网络标准，确保网络的长期发展和互操作性。	https://www.w3.org

要点：

- **遵循标准**可确保ICT产品和服务符合全球质量、安全性和互操作性基准。
- **合规性**表明符合国际公认的规范，促进市场准入和用户信任。
- **互操作性**：实现不同系统和技术之间的无缝集成和通信。

有必要与在标准制定和国际认可中发挥关键作用的主要外部组织建立更多伙伴关系并加强信息交流。以下是一些行动方案：

- 与IEEE、ISO、IEC和互联网工程任务组（IETF）等组织**建立专门联络点**，以促进定期信息共享。
- **积极参与论坛和工作组**（如第三代伙伴关系项目（3GPP）、互联网任务组、IEEE等），以确保本地需求更好地融入国际标准。
- **建立后续机制**，从这些外部预算中收集相关数据，并将其纳入今后的报告。
- 通过合作协议或战略伙伴关系**加强机构间联络**，以确保相互交流专业知识和资源。

全球评定项目需要具有适应性和前瞻性，例如Wi-Fi联盟的例子。以下是一些可能的行动：

- **确定具体项目：**例如，Wi-Fi联盟颁发的Wi-Fi CERTIFIED®认证可确保产品的互操作性、安全性及性能。⁵
- **强调重要性：**描述这些项目如何促进标准的采用，并确保不同设备和技术之间的兼容性。
- **整合其他类似举措：**提及蓝牙特别兴趣组（SIG）、LoRa联盟或其他致力于新兴技术互操作性的联盟所开展的项目。
- **分析区域影响：**评估这些项目如何影响本地市场及其对报告所涉区域的技术和经济发展的相关性。

为发挥数字平台及流程的变革性潜力，应考虑以下几种发展途径：

- **定义数字平台：**解释什么是数字平台，它如何促进不同参与者、产品和服务的互联互通（如支付平台、通信平台和电子商务）。
- **展示数字平台的益处：**
 - 1) **提高效率：**优化业务流程并降低运营成本。
 - 2) **提高可及性：**便利远程服务的获取，从而提高包容性和连通性。
 - 3) **持续创新：**通过集成新兴技术，实现新产品和服务的快速开发。
- **探索数字化流程：**
 - 1) **流程自动化：**集成自动化技术以提高生产率并减少人为错误。
 - 2) **商业模式转型：**采用数字工具以促进企业和公共行政部门内部的信息管理、沟通及协作。
 - 3) **公共服务数字化：**探讨政府服务数字化转型的影响（如电子政务、电子卫生、电子教育）。
- **成功的数字平台和流程示例：**
 - 1) **协作平台：**如电子教育或远程医疗平台。
 - 2) **公共部门的数字化流程：**实施数字化公共服务以简化行政程序。
 - 3) **具体领域：**金融（金融科技）、交通（出行即服务）等领域的应用。
- **挑战与机遇：**
 - 1) **挑战：**数据安全、网络安全、隐私、基础设施要求、数字包容性。
 - 2) **机遇：**发展数字经济、提高竞争力和促进创新。

⁵ <https://www.wi-fi.org/zh-hans/why-wi-fi-certified>

1.5 新冠疫情对审批程序的影响

新冠疫情对包括ICT领域在内的众多领域的授权程序产生了重大影响。疫情对这些程序的一些主要影响包括：

- **采用数字化程序：**随着旅行限制和保持社交距离措施的实施，许多授权程序已经转向完全数字化的程序。管理部门建立了在线平台来提交和处理许可申请，减少了对实体文件和面对面会议的需求。
- **处理时间缩短：**在许多情况下，疫情加快了许可处理时间，因为政府寻求促进快速部署ICT解决方案，以应对与疫情有关的紧急需求，如远程办公、电子学习和远程医疗。
- **灵活性提高：**鉴于疫情相关的特殊情况，管理部门在评估授权申请时展现出了更大的灵活性。在某些情况下，这可以简化程序或放宽资格标准，以鼓励创新和快速实施技术解决方案。
- **安全性提高：**尽管转向数字化流程，但管理部门也加强了安全措施，以保护敏感数据，防止滥用。这涉及实施强有力的安全协议，以确保作为授权申请的一部分所提交的信息的完整性和保密性。
- **国际协作：**疫情鼓励在ICT评估和监管方面加强国际协作。管理部门分享良好做法、数据和资源，以应对疫情带来的共同挑战，并在全球范围内推广协调一致的办法。

第2章 – 一致性和互操作性

2.1 引言

在产品、服务和基础设施创新的推动下，电信/ICT行业快速演进。随着这些技术的互连互通，利益攸关方必须确保C&I。一致性评定可确保ICT设备符合技术规范和标准，这对于网络环境中的性能评估和兼容性至关重要。互操作性测试确保多种产品能够无缝集成和通信，支持具体的通信协议。互操作性测试旨在通过遵循电信和ICT行业的具体通信协议，利用国际电联等国际组织和区域工作组的知识，确定两种或多种产品是否符合技术规范，这是成功集成所必需的。本章强调了C&I举措运作的复杂环境，从传统网络信令问题到假冒移动电话的扩散。本章还涉及一致性评定的相互认可安排/协议（MRA），促进测试结果和认证的跨境认可，鼓励国际贸易与合作。本章还重点介绍了预一致性测试在主动评定产品是否符合适用标准方面的作用、市场监管的重要性，以及提高供应商和用户对符合质量标准和打击假冒产品的认识。

MRA可以是AB之间的多边协议，这些机构经过同行评估确定其在评定一致性评定机构（CAB）（如ICT产品测试实验室）能力方面具备对等能力。此类MRA有助于成员所代表的经济体之间相互接受测试结果，从而有助于克服技术性贸易壁垒（TBT）。MRA还可以是政府与政府之间签订的协议，通过相互接受产品以及各自经济体中经其国家AB认可的实验室出具的测试报告来促进贸易。

ICT设备合规性的强制性验证是确保电信网络完整性、稳定性和安全性的关键工具。然而，必须减少检查次数，缩短ICT设备的上市时间。外国实验室测试结果的MRA可以起到帮助作用，但由于需要对测试协议进行海牙认证（Apostille）翻译，这一过程往往成本高昂且耗时较长。

一个潜在的解决方案是建立国家ICT专业知识体系，由政府批准的实体负责合规性验证。这种方法可最大限度地缩短检查时间并降低成本，因为无需对设备进行全面测试。此类检查的成本远低于进行全面的ICT设备测试的成本。

1) C&I:

- 合规性测试确保ICT设备符合技术标准和规范。
- 互操作性测试验证产品能否成功集成到网络中。
- 这些测试对于识别可能影响网络质量的不合规设备至关重要。

2) 技术规范和标准:

- 标准由服务提供商、运营商和国家监管机构制定。
- 遵守这些标准可确保互操作性，减少厂商锁定，提高市场竞争力。
- 世界贸易组织（WTO）技术性贸易壁垒委员会强调标准制定的透明度、公开性、公正性和一致性。

3) MRA:

- MRA促进各国之间对合规性测试结果的认可，减少重复测试和成本。
- MRA旨在实现“一次测试，全球公认”，但面临着法律障碍、缺乏对等以及一些国家资源不足等挑战。

4) 国家ICT专业知识:

- 国家ICT专业知识体系可确保符合国家和国际标准。
- 该体系建立问责制，防止假冒产品，并通过避免全面测试降低成本。
- 该体系需要监管框架、认可规则和合格专家。

5) 挑战和解决方案:

- 各国在ICT实施方面的差异增加了相互认可的复杂性。
- 国家专业知识体系可以通过提供本地化的合规性验证来应对这些挑战。⁶

2.2 关键问题的考虑

现有智能网络信令中的互操作性问题可归因于不同的因素:

- 1) 不同厂商设备之间缺乏C&I;
- 2) 非标准接口或协议; 以及
- 3) 来自单一制造商的软件修订。

这可能导致会话发起协议(SIP)不兼容。语音、数据和视频容量也可能受到现有网络过载的影响。复杂网络中的互操作性可以通过网络和设备的集成来实现。但是，一些厂商可能无法提供必要的基础设施和支持团队来实现与其他运营商的互操作性。在所有平台上采用标准、管理通话详单并实施新功能和服务也带来了挑战。此外，还有缺乏测试中心、训练有素的人员，综合业务数字网(ISDN)支持问题，用户终端问题以及客户使用的服务和终端设备的互操作性问题。

此外，在区域和国家层面发现的一些挑战包括:

- 在开发和实施假冒电话解决方案方面缺乏区域合作;
- 缺乏基准数据，无法为打击假冒设备的区域贸易战略的制定和实施过程提供信息;
- 在移动电话可负担性方面持续面临挑战;
- 对假冒手机问题的认知度低;
- 假冒设备对发展中国家的国家数字化转型计划构成了潜在威胁;

⁶ 国际电信学院提交的ITU-D SG2 [2/140](#)号文件。

- 假冒设备造成的经济影响还可能降低ICT行业对一个国家国内生产总值（GDP）的贡献；以及
- 假冒设备损害了安全性、网络性能和服务质量，并使民众面临多种健康风险；

对移动电话及其永久拥有权的需求的增长，超越了城市和农村社区等地理因素以及收入差异和文化水平等社会因素的限制，但这些因素共同推动了假冒移动电话流入市场。⁷

2.3 技术规范和标准

2.3.1 国家和区域层面C&I应用展示

展示应用的C&I对于了解国家和区域的经验以及推广良好做法至关重要。这些展示包括认可和认证机构的指定/认可、国际标准和做法的指定/认可、测试实验室的指定/认可以及注册/认证。此类展示可为成功实施战略、应对面临的挑战和吸取经验教训提供宝贵的见解。

AB的指定或认可的先决条件之一是其ILAC/国际认可论坛（IAF）MRA签署方身份，该身份正式证明其程序和规范符合认证机构和测试实验室的国际标准。

分享AB在推广一致性评定做法和促进合规产品和服务的市场准入方面的成功故事，可以建立信任，减少贸易壁垒。认证机构的指定/认可旨在制定评估一个产品符合适用标准和法规的程序和要求。

展示测试实验室的能力、公正性和持续运作，可以建立对其能够生成有效测试结果的能力的信任。在难以建立包含所有各种要素的国家项目的情况下，各国可以依靠已有项目的良好做法甚至认证。

注册/认证解释了证明符合适用法规和标准的产品、服务或系统的注册或认证的流程 and 标准。展示经过认证的产品可以展示注册或认证标志是质量、安全性和可靠性的象征，使消费者能够做出明智的购买决定。认可来自成熟的、管理完善的和国际公认的项目的认证标志，作为一致性的证明，可以大幅减少消费者的成本、时间以及国家管理部门的成本。

2.3.2 良好做法

- **颁发经销商证书：**确保ICT设备经销商获得官方认可的证书，以提高透明度和合规性。
- **建立综合注册系统：**建立电子通信设备综合参考和登记系统，以提高可追溯性并改进监管监督。
- **消费者获取国际移动设备标识（IMEI）验证：**通过短代码为消费者提供验证IMEI号码的便捷手段，加强设备验证并帮助防范欺诈。

⁷ 赞比亚提交的ITU-D SG2 [SG2RGQ/37](#)号文件。

- **有关假冒趋势的区域报告：**促进提供关于披露数量和趋势（如最容易被假冒的手机型号）的区域报告，以提高消费者的认识。
- **认可国际测试和认证标准：**确保测试结果和认证符合国际标准和良好做法，以提高互操作性和市场接受度。

2.3.3 建立联合C&I的潜在协作机制

服务提供商和运营商对其用来服务客户的设备和系统实施协调统一的标准和规范。国家监管机构为部署在本国境内的设备和系统的协调标准和规范制定法规。用户、服务提供商和国家监管机构必须获得不可撤销的证明，证实此类设备和系统符合相应的互操作性标准、要求和规范。

为推动国际标准、指南和建议的制定，世界贸易组织TBT委员会确立了以下六项原则：

- 1) **透明度：**该原则要求，至少应向所有WTO成员领土上的所有相关方提供有关正在进行的工作计划，以及正在审议的标准提案、指南和建议及最终结果的所有基本信息。该原则鼓励制定程序，为提交书面意见提供充足的时间和机会。关于这些程序的信息应得到有效传播。

为提供基本信息，透明度程序应：为相关方提供充足的时间提交书面意见，并在随后审议标准时予以考虑；标准一经通过立即公布；定期发布工作计划，其中包含有关正在制定和通过的标准的消息。

- 2) **开放性：**该原则要求，国际标准化机构的成员资格应无歧视地向至少所有WTO成员国的相关机构开放，既可参与政策制定层面的工作，也可参与标准制定的各个阶段。

因此，国际标准化机构的任何成员，特别是发展中国家成员，如果对某一具体标准化活动感兴趣，都应有机会切实参与所有阶段的标准制定工作。

- 3) **公正性和协商一致：**该原则强调，WTO成员的所有相关机构都应有机会为国际标准的制定做出有意义的贡献，从而使标准的制定过程不会偏袒或有利于一个或多个特定供应商、国家或区域的利益。该原则承认，应建立协商一致的程序，以考虑所有相关方的意见并调和相互冲突的论点。

- 4) **有效性和相关性：**国际标准应具有相关性，并能针对各国在监管及市场方面的需求，以及科技的发展情况做出有效回应，从而促进国际贸易，避免出现不必要的贸易壁垒。

国际标准不应扭曲全球市场，不应公平竞争产生不利影响，也不应阻碍创新和技术发展。此外，当其他国家或区域存在不同需求或利益时，国际标准不应偏袒特定国家或区域的特征或要求。国际标准应尽可能基于性能而非设计或描述性特征。

- 5) **一致性：**该原则要求国际标准化机构避免与其他国际标准化机构的工作出现重叠或重复，以避免制定相互冲突的国际标准。在这方面，与其他相关国际机构的合作与协调至关重要。

- 6) **发展维度：**该原则表明，在标准制定过程中应考虑发展中国家面临的制约因素，特别是阻碍发展中国家有效参与标准制定的制约因素。因此，该原则鼓励寻求促进发展中国家参与国际标准制定的方法，例如利用技术援助和能力建设。

2.3.4 技术合作

- **能力建设与培训：**开发国家和区域项目，开展培训活动，以支持各国政府实施有效措施打击假冒设备的流入。
- **政策与监管支持：**协助制定和加强政策、法规以及执法机制，以遏制不合规ICT设备的流通。
- **跨境协作：**在国家与区域层面，推动监管机构、执法机构和行业利益攸关方开展合作，以加强打击假冒的工作。
- **技术与基础设施提升：**支持部署先进的设备认证、追踪和验证技术，以提升市场诚信度。

2.4 关于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？

MRA是各方（私营或公共实体）之间认可一致性评定结果（有关程序和过程）的合同约定。

- **互信**可加强监管机构之间的技术合作。

ITU-T Q.4068建议书提出了一套面向可互操作测试床联邦的开放应用程序接口（API），这些API不仅能够处理联邦内测试床之间的互联与互操作性，还能管理资源的公告发布、分配及配置。API的设计旨在管理参与联邦的用户（如试验人员），并为用户分配角色。同样，资源使用也通过可互操作的测试床联邦的开放API分配给试验人员。试验的一个典型用例是测试床联邦及其相关需求。类似用例也可在Fed4FIRE这样的测试床联邦中实施。

2.4.2 MRA在C&I领域的作用

MRA用于：

- 认可第三方执行国家监管或许可程序的能力；
- 避免重复测试成本，提高透明度；
- 为进入国外市场提供便利；
- 缩短上市时间，降低生产成本；
- 打击掠夺性做法，消除市场准入壁垒；
- 简化程序和方法，大幅降低生产者在几个市场的成本。

最终目标：“一次测试，全球公认”。

2.4.3 与国际MRA有关的问题

不幸的是，使用MRA经常遇到困难：

- 许多国家缺乏使用另一国制定的文件的法律机制，也没有目标国使用的语言的海牙认证翻译。
- 并非所有国家都有所需的物力和人力来进行自己的测试。在这种情况下，无法实现测试和研究结果的相互认可，单方面认可也是不可接受的。在这种情况下，各国可以认可由拥有声誉良好、完善、有据可查的国家或区域项目的国家或国际管理机构所提供的测试结果和认证。这将允许合法使用基于国家通信主管部门授权组织的专家意见的所有测试和研究结果。
- ICT因国家而异。国家通信主管部门制定ICT的实施目标。遵循ICT使用目标的工作应由国家通信主管部门授权的机构进行。
- 在有争议的情况下，测试和研究结果的错误可能会造成损失，因此很难起诉一个按照另一个国家的法律开展工作的组织。

有鉴于此，有必要建立并普遍应用有关测试结果和研究的国家专业知识机制。同时，提供专家意见的组织应根据所在国法律承担责任。借鉴成功实施MRA国家的良好做法和经验也很重要。

2.5 建立强大的C&I框架的必要性

2.5.1 高质量C&I框架的基本基础设施：技术标准与必要的立法修订

一个强大的C&I框架对于确保ICT系统的无缝集成、促进创新以及保护消费者至关重要。由于在技术标准、监管要求和立法政策方面存在差距，发展中国家在建立这种框架时经常面临挑战。结构合理的基础设施，包括技术、立法和监管方面的内容，对于有效实施C&I项目至关重要。

目标

本节的主要目标是重点介绍高质量C&I框架所需的基本基础设施。这包括制定技术标准、建立监管机制以及必要的立法修订，以支持发展中国家的一致性评定和互操作性工作。加强这些要素将提高ICT生态系统的可靠性、安全性和效率。

影响

定义明确的C&I基础设施具有重大的社会经济和技术影响。它能确保ICT解决方案的互操作性，降低市场壁垒，增强消费者信心，促进公平竞争。此外，它通过使国家标准与全球良好做法保持一致，使发展中国家能够更有效地参与全球数字经济，促进国际贸易。

作用

通过解决这些关键领域问题，发展中国家可以为高质量C&I框架奠定坚实基础，最终推动数字化转型和经济增长。

2.5.2 联邦测试的概念

最近随着互联网相关技术的发展，在现实世界中进行测试和使用变得更加复杂。更多样的情况需要得到考虑并评估可扩展性。为了在实际条件下测试新的用例，在测试台中进行实验的需求变得愈发重要。这一进展使得采用、互连不同的测试床变得越来越必要且切实可行。然而，这种强大的方法缺乏清晰的标准化API来支持现有测试床和资源的联合，以支持对新技术、服务和解决方案进行实验、测试和验证，从而提高测试床的互操作性。

2.6 市场监督

2.6.1 提高监测意识

提高终端设备厂商和用户的认识对于改善电信业的标准监督至关重要。这不仅能提高产品质量和可靠性，还能促进互操作性、提升监管合规性和消费者信心。供应商通过了解相关标准，可以培育质量和可靠性文化，从而提高产品质量、减少缺陷并增强可靠性。用户可以做出明智的购买决策，选择符合其需求和期望的产品，从而提高对终端设备可靠性和性能的满意度和信心。

厂商可以通过设计符合行业标准和协议的产品来促进互操作性，促进不同系统与平台之间的无缝通信和兼容性。用户了解监管标准也有好处，因为这有助于确保其终端设备符合监管机构规定的安全、保障和隐私要求。

获得消费者的信任对供应商至关重要，因为这表明了他们对质量、可靠性和客户满意度的承诺。精明的用户更有可能信任符合公认标准和认证的设备，从而培养忠诚度和正面的品牌认知。市场监督对于电信市场的正常运作至关重要，因为它保护消费者和工人免受不合规产品带来的风险，并保护公司免受不公平竞争的影响。

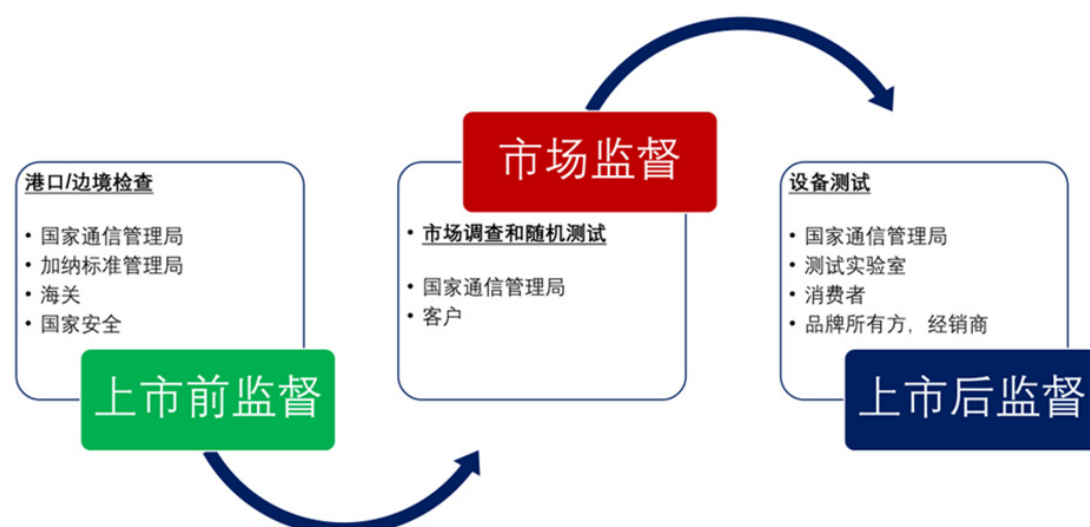
市场监督：该程序旨在确保投放市场或在市场中的电子通信设备符合上市前批准的标准。⁸

三管齐下的方法：

- 上市前监督，包括入境清关程序、实体港口检查；
- 市场监督，包括市场调查和随机测试；
- 上市后监督活动。

⁸ Roland Yaw Kudozia, 加纳, [通过C&I测试和市场监督打击假冒ICT设备](#), ITU-D关于数字化转型面临的一致性和互操作性挑战讲习班, 2023年6月2日, 日内瓦。

图2：市场监管在加纳的推广



2.6.2 监测与合作

市场监管情报和经验对于确保电信业的监管合规性、公平竞争和维护消费者利益至关重要。通过交换信息、与其他国家开展咨询以及提供早期预警，监管机构能够加强市场监管力度、简化执法活动并促进各方之间的协作。知识交流和区域合作是此类咨询的关键要素。

监管机构可从分享其他国家的良好做法、经验教训和监管知识中获益。这有助于推动区域合作、促进监管方法协调统一、加强执法的一致性并减少监管碎片化。咨询还提供了能力建设机会，使监管机构能够更好地了解新兴技术、趋势和执法手段。

可向合作伙伴发送早期预警，以降低风险、优化资源配置并促进合规。这些预警还可用作教育工具，提高对监管要求的认识并鼓励自愿合规。通过提供明确的指导和及时的信息，监管机构使各方将其活动与监管预期保持一致、降低合规性风险并助力营造公平的市场竞争环境。

参与的主要利益攸关方包括：

- 政府/监管机构；
- AB；
- CAB；
- 制造商、进口商、厂商和服务提供商。

2.7 新技术的一致性评定

一致性评定是确保新的电信/ICT符合行业标准、法律要求和客户期望的必要工具。在设备和网络互联的时代，确保安全性、可靠性和互操作性至关重要。通过一致性评定，政策制定机构、企业和消费者可以对电信和ICT产品及服务的性能和质量放心。

一致性评定涵盖了评定ICT和电信技术各种特性的多种方法。这些方法包括认可、认证、测试和检验。测试是在受控环境中对产品或系统进行严格检查，以确定其是否符合公认的技术标准。检验的主要目标是通过验视、文件审查和现场评估来确认合规性。认证过程是颁发许可或官方声明，证明符合特定的规则或法律。测试、检验和认证活动由CAB进行，这些机构被证明公正且具备能力，并被视为认可程序的一部分。

国际公认的标准和健全的监管框架是进行有效一致性评定的前提条件。监管机构制定标准和导则，以确保电信和ICT系统的互操作性、安全性和可靠性。为促进兼容性并推动全球的协调统一，国际电联、IEEE、IETF、IEC、欧洲电信标准化协会（ETSI）和ISO等标准化机构制定技术规范和协议。遵循这些导则在鼓励整个ICT和电信业创新的同时，还确保整个ICT和电信业的一致性和问责制。

2.7.1 新技术挑战

新兴技术的复杂性

新的ICT和电信技术的复杂性是一致性评定面临的主要障碍之一。AI和IoT等技术的组件、协议和能力的多样性给标准化测试技术的开发带来了挑战。这些技术的快速演进和多样性可能导致传统的一致性评定技术难以维持，进而可能导致按照既定标准对这些技术进行一致性评定出现缺口。现代电信系统相互连接，这增加了额外的复杂性。因此，需要全面的评估框架来考虑互操作性和系统级因素。

缺乏协调统一的标准

不同司法辖区和区域之间缺乏协调统一的标准是一个重大障碍。全球电信/ICT市场中提供的产品和服务跨越了国际边界。然而，法律框架和标准的多样性给一致性评定结果的相互认可和互操作性带来了困难。标准之间的差异可能导致市场碎片化、合规成本增加以及测试工作重复。为了促进电话和ICT行业的互操作性、便利国际贸易以及减少监管壁垒，需要实现标准的协调统一并达成MRA。

技术快速过时

技术的快速过时显然是ICT和电话领域一致性评定面临的一大障碍。新技术常常使现有的标准和测试程序过时，需要持续不断地进行更新和调整。为了保持相关性和有效性，CAB需要快速适应新技术和不断变化的监管要求。但这种需要不断适应的要求可能会造成知识和资源方面的压力，尤其是对于小型一致性评定企业而言。此外，部分技术的寿命较短，可能会限制测试设备和参考资料的可获取性，这将使一致性评定举措面临更大挑战。

互操作性和兼容性问题

在ICT和电信技术的一致性评定中，互操作性和兼容性问题是重大障碍。在由不同设备、网络 and 平台组成的互连生态系统中，无缝互操作性对于提供可靠且一致的服务至关重要。然而，互操作性测试具有挑战性，需要大量资源，尤其是在存在专有协议和过时系统的异构环境中。缺乏标准化的接口和协议进一步阻碍了互操作性工作，导致互操作性存在差距以及服务中断。为了克服这些障碍，一致性评定必须实施强调ICT和电信堆栈不同层级之间互操作性的详细测试程序。

2.7.2 预合规性测试

预合规性测试是制造商采用的一种主动策略，用于在申请官方认证前评估其产品是否符合适用标准和法规。通过预合规性测试，制造商能够在开发周期的前期发现潜在的合规性问题，包括可能导致上市时间延迟以及经常被建议的重新设计或召回情况。此外，预合规性测试能让制造商深入了解其产品的性能特性，确保产品具备最佳的功能性和可靠性。在快速变化的电信和ICT行业，标准在不断演变，创新在迅速发展，预合规性测试有助于制造商保持敏捷性和适应性。

预合规性测试是确定适用于具体电信/ICT设备的标准和法规的过程。基于这些标准，制定全面的测试计划，说明具体的测试和评估内容。测试设置对于获得准确可靠的结果至关重要。预合规性测试包括电磁兼容性（EMC）测试、电气安全测试、射频（RF）性能测试以及环境测试。根据预先确定的验收标准记录和分析数据，从而确定与标准的偏差并确定合规状态。制造商可以通过重新设计组件、调整参数或改进保护机制，来纠正不符合项。在整个过程中会编制全面的文档，详细记录测试程序、结果、纠正措施以及观察到的偏差或异常情况。通常会采用迭代测试方法来改进产品、解决剩余的不符合项并优化性能。这一过程有助于制造商对产品进行微调，并确保产品符合适用的标准和法规。

电信和ICT设备的预合规性测试必须遵循良好做法和行业标准，其中包括提前与监管专家接触、实现全面测试覆盖、定期校准和验证、采用真实的测试场景、跨职能团队之间开展协作，以及进行稳健的文档管理和跟踪。早期参与有助于更好地理解监管要求并简化测试流程。全面测试覆盖可确保对设备合规性进行整体评估。定期校准和验证可确保测试的准确性和可靠性。真实的测试场景可模拟现实世界的运行条件和环境变量。跨职能团队之间的协作可促进知识共享和问题解决。在预一致性测试反馈的基础上进行持续改进，以完善产品设计并优化合规性。

2.7.3 预期影响

在当今这个互连互通的世界中，C&I对于企业的成功至关重要。C&I使公司能够打造智能产品组合，确保产品之间实现无缝集成与互补。这将构建一个有凝聚力的生态系统，提升用户体验和客户满意度。从产品开发流程伊始就将C&I融入其中，有助于解决兼容性问题，简化集成工作，并加快产品上市时间。这种方法能够降低产品在生命周期后期进行费用昂贵的重新设计或升级的风险。

了解C&I测试所需的人力和物力资源，对于有效规划和执行测试至关重要。配备恰当的专业知识、基础设施以及支持，可最大程度减少延误、降低成本并优化资源利用。

监管机构可通过提倡在各主管部门之间签订MRA来支持新兴产品和行业，此类协议通过认可不同司法辖区或行业的一致性评定结果，简化监管合规性流程。这有助于创新产品进入市场，并促进全球协作。

监管机构还可以通过提供建议、资源和教育举措，促进与企业家的知情对话。这能够增进监管机构与企业家之间的信任、透明度和协作，从而带来更好的监管结果和有利于创新和业务增长的环境。总体而言，在当今这个互连互通的世界中，C&I对于企业的成功至关重要。

第3章 – 打击设备的非法使用行为：移动设备的假冒、质量缺陷和盗窃

3.1 假冒设备扩散的挑战

对于消费者、合法行业、政府和国际组织来说，假冒残次设备的扩散是一个日益严重的问题。假冒设备往往是在不符合安全和质量标准的情况下制造的，对发展中国家的国家数字化转型计划构成了潜在威胁。除了损害安全性、网络性能和服务质量，假冒设备还会使公众面临诸多健康和环境风险。假冒电子设备的经济影响还会降低ICT行业对一个国家GDP的贡献。

打击假冒设备需要采取多管齐下的方法，并制定导则，使政府、企业和国际组织能够共同努力，减少假冒设备的扩散，并提高各国电子产品的安全和质量。

本章以各国经验（案例研究）为重点，制定定义和导则，打击假冒残次设备的流入。

将本章所讨论的不同方法结合起来的主要目的是营造一种环境，让消费者能够获得正宗且优质的电子产品，同时降低与假冒和制造残次假冒产品相关的风险。

打击假冒残次设备的扩散：

- 旨在保护消费者免受使用这些产品所带来的潜在危害，如健康、安全和性能风险，同时维护合法行业的诚信和合法品牌的声誉。

打击这种扩散的工作可包括：

- 加强电子产品的认证和可追溯性；
- 政府、行业和国际组织开展合作。

3.2 导则

应制定相关导则，更好地打击假冒残次设备在发展中国家的扩散，包括：

- **认证和可追溯性：**为合法电子产品建立认证和可追溯性计划，增加篡改和分销假冒产品的难度；
- **公私伙伴关系：**鼓励与授权制造商、行业协会和国际组织协作，以识别和消除假冒产品供应链；
- **区域和国际协作：**鼓励与其他国家和国际组织协作，分享打击假冒产品方面的信息和良好做法；

- **培训和能力建设：**投资于执法机构的培训和能力建设，以提高其打击假冒行为的有效性；
- **推广举报机制：**建立消费者举报假冒产品的机制，鼓励主管部门进行调查并采取行动；
- **企业社会责任：**鼓励公司采取负责任的商业做法，承诺不在其供应链中使用假冒产品，并为宣传和培训项目做出贡献。

3.3 移动设备盗窃

移动设备盗窃是一个全球性问题，对个人和企业都有影响。随着智能手机、笔记本电脑、平板电脑和其他手持设备的普及，它们对犯罪分子的吸引力急剧增加。这些设备通常包含敏感信息，如个人、银行和业务数据，使其不仅成为实物盗窃的主要目标，也成为数字攻击的主要目标。要打击这一祸患，需要采取综合方法，将技术、立法和公众意识提升措施结合起来。

移动电话盗窃的统计数据⁹

移动电话盗窃是一个不断加剧的全球现象，对个人和企业都造成了影响。

根据各种研究和报告：

- 全球每年约有7 000万部智能手机被盗或丢失。
- 大约10%的移动电话用户会在设备的使用寿命期内成为盗窃或丢失的受害者。
- 在一些主要城市，智能手机失窃案占报案总数的50%。
- 只有7-10%的被盗设备能被失主找回。
- 大约40%的手机盗窃发生在公共交通工具上或繁忙的公共场所。

这些数字表明了问题的严重性，并强调了预防和保护措施的重要性。

安全和隐私影响

移动电话盗窃是一个令人担忧的问题，因为它不仅造成实物设备的损失，还对个人和企业数据的安全和隐私构成严重威胁。窃贼可以利用存储在设备上的个人、银行和业务信息。

未经授权访问敏感数据的安全影响包括：

- **网络攻击和欺诈风险：**犯罪分子可利用手机访问在线账户、进行欺诈性购物或冒充机主。
- **公司数据泄露：**在企业环境中，被盗手机可提供机密数据的访问权限，从而危及组织的网络安全。

⁹ GSMA, [移动设备盗窃 – 事态发展报告](#), 2025年2月。

- 犯罪用途：一些被盗手机被用于非法活动，如电话诈骗或网络犯罪。
- 个人信息泄露：存储的照片、视频、信息和文档可能被用于恶意目的。
- 侵犯隐私：社交媒体和消息应用可能被泄露，导致身份盗窃和通信隐私泄露。
- 在黑市上出售数据：手机中包含的信息可在黑网上转售，危及用户的数字安全。

缓解措施

为了最大限度地降低手机盗窃带来的风险，可以采取以下几种策略：

- 使用安全锁进行预防和保护：激活PIN码、使用高强度密码和生物特征认证（指纹、面部识别）。
- 数据加密：保护敏感文件可防止其在被盗后遭到恶意利用。
- 用户意识：学习良好安全做法，如避免在危险场所暴露手机。
- 加强监控：确保永远不要让手机无人看管，尤其是在公共交通工具上和公共场所。
- 远程跟踪和擦除以应对盗窃：使用“查找我的iPhone”（苹果）或“查找我的设备”（安卓）等服务进行远程查找、锁定或清除数据。
- IMEI屏蔽：向移动运营商报告盗窃情况，以停用设备，使其在网络上无法使用。
- 投诉备案：向管理部门报告失窃事件，尝试找回设备并防止可能的欺诈性使用。
- 立即更改密码：更改与手机关联的应用和服务的登录凭证，防止未经授权的访问。
- 运营商屏蔽被盗设备的监管和技术措施：建立国际数据库，防止激活被盗手机。
- 要求制造商集成防盗解决方案：提供在多次尝试登录失败后自动清除数据等功能。
- 加强立法：通过法律以惩罚接收和转售被盗设备的行为。

3.4 难题和问题

- 敏感数据丢失：移动设备被盗后，用户有可能丢失关键的个人和业务信息，从而导致隐私泄露。
- 身份盗窃：存储在被盗设备中的数据可能被用于欺诈或身份盗窃活动。
- 服务无法接入：设备被盗可能会切断用户对基本服务的访问，从而影响他们的日常活动。
- 黑市转售：被盗设备通常会在全球黑市上被转售，逃避监管，加剧犯罪问题。
- 立法应对措施缺乏标准化：各国的法律和制裁措施各不相同，因此很难在国际层面采取协调一致的应对措施。
- 设备追回工作：目前的追踪装置并不总能保证追回被盗设备。

- **电信运营商的作用：**运营商在屏蔽被盗设备接入网络方面发挥着关键作用，但各区域采取的措施有所不同。
- **用户意识和教育：**开展宣传活动，提高公众对移动设备失窃风险和良好数字安全做法（如启用设备锁定和追踪机制）的认识至关重要。
- **加强立法：**政府必须制定强有力的法律来遏制移动设备盗窃行为，在国际层面上统一处罚措施，并与运营商和制造商合作，防止被盗设备的使用。
- **溯源技术：**应鼓励广泛采用远程设备跟踪和锁定技术。制造商也应在其产品中融入更有力的防盗措施。
- **电信运营商的参与：**运营商必须建立机制，快速屏蔽被盗设备，并增加其与其他网络上使用的难度。运营商还应积极参与国际被盗设备数据库的工作。
- **国际协调：**需要在国际层面加强打击移动设备盗窃行为的力度，建立中央数据库以追踪被盗设备，并建立国家间信息共享机制。

通过实施这些导则，政府、企业和国际组织可以共同努力，减少假冒设备的扩散，提高各国尤其是发展中国家电子产品的安全 and 质量。

3.5 国家案例研究

成员国和利益攸关方提交的文稿在本报告的编写过程中发挥了基础性作用。这些文稿基于各国的经验、现有数据和现行做法，旨在有效打击假冒设备的扩散。

所有文稿提交方一致认为，制定适当的政策、法律和监管框架对于应对这一挑战至关重要。

此外，一些文稿提交方建议采用经过验证的技术解决方案，包括实施国际标准、运用市场监督技术，以及建立数据库和集中化平台来屏蔽假冒设备。

特别强调的是，需要支持发展中国家实施C&I项目，同时加大力度打击假冒ICT设备和盗窃移动设备的行为。

此外，若干文稿提交方建议在区域和次区域层面加强努力，汇集各种方法和技术，以便更有效地打击设备假冒行为。

3.5.1 赞比亚共和国

赞比亚提交的一份文件指出，假冒和改装移动电话的扩散对发展中国家，特别是赞比亚的数字化转型计划构成了重大威胁。这些设备不仅危及安全、网络性能和服务质量，还使民众面临健康风险，并降低了ICT行业对GDP的贡献。

已确定的挑战

- 在打击假冒行为方面缺乏区域合作。
- 缺乏指导国家和区域战略的基准数据。

- 正品手机存在经济可及性问题。
- 消费者对假冒设备相关风险的认识不足。

赞比亚案例

- 赞比亚有8个邻国，且对手机的需求不断增长，因此特别容易受到假冒设备流入的影响。
- 政府已采取措施，例如：
 - 通过电子通信法；
 - 对ICT设备进行型号核准；
 - ICT管理部门、移民、海关和税务部门之间开展协作；
 - 开发综合电子通信设备登记系统（IECERS）。

正在实施的举措

- 赞比亚正在探索使用全球移动通信系统协会（GSMA）的IMEI验证服务，使消费者能够在购买前验证设备的真伪。
- 这项举措旨在减少对假冒设备的需求，并提高消费者的认识。

建议

- 区域解决方案：鼓励成员国之间采取协作方式打击假冒手机贸易。
- 培训和项目：制定国家和区域计划，加强政府能力。
- 区域报告：发布有关假冒产品数量和趋势的数据，以便更好地向消费者提供信息。
- 区域平台：建立被盗设备快速报告系统，保护消费者。

结论

打击假冒手机需要采取综合方法，结合技术解决方案、区域合作和提高消费者认识的活动。赞比亚通过相关举措和采用GSMA的IMEI服务等技术，正在为其他发展中国家的效仿铺平道路。¹⁰

3.5.2 几内亚

引言

随着技术的快速发展以及新型移动设备、应用和服务的涌现，公民越来越依赖ICT，但往往并未意识到其中涉及的风险。各国必须制定一致的国家政策来保护公民。

¹⁰ 赞比亚提交的ITU-D SG2 [SG2RGQ/37](#)号文件。

背景

在几内亚，公民经常成为移动设备盗窃、网络攻击和欺诈活动的受害者。管理部门采取的措施包括：

- 通过关于网络安全和个人数据保护的第2016/037/AN号法律。
- 成立国家信息系统安全局（ANSSI）。
- 开展建立国家计算机应急响应小组（CERT）和安全运营中心（SOC）的可行性研究。

尽管如此，在设备丢失或被盗的情况下，公民仍然容易受到伤害，在恢复数据或恢复SIM卡方面面临重重困难。假冒设备充斥市场，加剧了欺诈和服务质量问题。

打击欺诈

在几内亚邮电监管局（ARPT）的协调下，成立了一个监督委员会，以打击未经授权和假冒的设备。采取的行动包括：

- 开展进口设备认证活动。
- 在2023年发现并断开了1 000个欺诈号码。
- 在科纳克里拆除了六个SIMBOX站点。

打击设备盗窃

ANSSI和ARPT协作追踪窃贼和被盗设备。一个集中的移动设备识别和SIM卡注册平台已经建立，以管理移动终端并识别那些不合规、克隆或被盗的移动终端。

结论

为了有效打击这一祸患，建议采取以下措施：

- 制定统一的国家战略，打击设备盗窃、假冒和网络攻击行为。
- 在国际电联成员国之间分享经验和良好做法。
- 国际电联提供支持，帮助发展中国家制定共同战略并实施国家CERT。

要点

- 几内亚公民面临与设备盗窃、假冒和网络攻击相关的风险。
- 已采取措施，包括成立ANSSI和建立检测和设备管理平台。
- 区域和国际协作对于加强打击这些行为至关重要。¹¹

¹¹ 几内亚提交的ITU-D SG2 [SG2RGQ/115](#)号文件。

3.5.3 乍得共和国

在乍得，数字鸿沟的缩小推动移动电话用户和互联网用户数量的大幅增加。然而，这种增长也带来了重大挑战，包括假冒或伪造手机的扩散以及设备盗窃事件的增多。这些问题损害了用户安全、电信服务质量以及网络性能。

乍得政府通过电信和数字经济部采取了措施，旨在实现基础设施现代化并缩小数字鸿沟。然而，市场上充斥着未经验证的设备，这些设备往往未经检查就进口进来，使用户面临安全和质量风险。乍得电子通信和邮政监管局（ARCEP）在监管该行业方面发挥着关键作用，但缺乏有效验证设备以及打击盗窃和假冒行为的技术手段。

为应对这些挑战，提出了若干建议，其中包括：

- 建立符合GSMA标准的认证实验室。
- 加强ARCEP、海关署和运营商之间的协作，在设备进入市场之前进行验证。
- 开展宣传活动，让消费者了解假冒或被盗设备的相关风险。
- 制定区域性协议，加强被盗设备的追踪以及国家间的合作。

总之，尽管已经做出了努力，但乍得打击手机盗窃和假冒行为的工作仍然处于早期阶段。包括技术、监管和区域性措施在内的统筹协调方法对于保护用户和提高电信服务质量至关重要。¹²

3.5.4 斯里兰卡

斯里兰卡电信监管委员会（TRCSL）根据1991年《斯里兰卡电信法案》（第25号）监管移动设备的进口。获得许可的运营商必须保留设备标识寄存器（EIR），以确保仅激活合法进口的支持IMEI的设备。TRCSL要求对电信设备进行型号核准，并为合法进口的设备维护IMEI数据库。最近，对违规行为的罚款大幅增加。现在有一个在线系统让公众能够报告手机丢失或被盗，从而提高效率并降低成本。TRCSL还运行了一个IMEI验证系统，供客户通过SMS验证设备，尽管针对非法进口的执法行动面临挑战。¹³

3.5.5 卢旺达

在过去的二十年中，卢旺达在包括移动技术在内的ICT行业取得了长足进步，扩大了移动设备市场。然而，这种增长也导致假冒移动设备的大量扩散。如果这一问题管理不当，可能会带来安全威胁，阻碍经济增长，引发运营风险并对用户信任产生负面影响。为了解决这些问题，卢旺达根据国际电联的建议，通过工具、法律框架和机构协作来打击假冒和被盗设备。海关署、消费者保护机构、电信运营商和安全实体等关键利益攸关方共同努力，确保只使用合法设备。公众对数据保护的不情愿和意识低下仍然是障碍。联合宣传活动和机构间协作已显示出巨大的潜力。¹⁴

¹² 乍得提交的ITU-D SG2 [SG2RGQ/112](#)号文件。

¹³ 斯里兰卡提交的ITU-D SG2 [2/367](#)号文件。

¹⁴ 卢旺达提交的ITU-D SG2 [2/352](#)号文件。

第4章 – 物联网的一致性和互操作性

4.1 引言

IoT是信息社会的一种全球性基础设施，基于现有的和不断演进的、可互操作的ICT实现实体和虚拟物品的相互连接，提供先进服务。¹⁵

IoT技术应用于众多行业，并通过处理数十亿台互联设备生成数据的平台影响IoT用户的日常生活。IoT Analytics开展的一项研究显示，目前有167亿台活跃的IoT端点，预计到2027年，IoT连接数量将超过290亿。¹⁶

4.2 IoT生态系统和应用场景

4.2.1 IoT生态系统

IoT是实体物品或设备构成的网络，这些实体物品或设备配备有电子元件、软件、传感器和网络连接功能，使其能够收集和交换数据。这些设备利用各种现有技术收集有用的数据，并在其他设备之间自动传输数据。利益攸关方对连接和设备的安全性及可靠性，以及存储和传输数据的隐私性表示关切。IoT生态系统包括：

- **设备和传感器：**IoT的核心要素，它们是配备了传感器和执行器的实体对象，能够从周围环境中收集数据，或根据接收到的指令执行特定操作。例如温度传感器、运动传感器、可穿戴设备、智能仪表等。
- **连接：**它为设备提供了相互通信以及与核心系统或云端系统（进行额外数据处理）通信的手段。所采用的技术包括Wi-Fi、蓝牙、蜂窝（LTE、5G）、低功率广域网（LPWAN）（长距离广域网（LoRaWAN）、Sigfox）等。
- **数据处理设备：**这些设备处理传感器收集的数据，然后将其发送到云服务器或本地服务器进行更密集的计算。实施方式包括边缘计算设备进行数据预处理，以减少延迟和带宽使用。
- **平台：**平台是IoT系统的骨干，集成不同的设备，管理设备的通信并实现设备之间的数据流动。功能包括设备管理、数据收集和应用激活。
- **云服务器与数据中心：**它们提供了存储大量IoT数据和运行复杂分析模型以提炼可操作洞察所需的基础设施。它们通常与AI和机器学习功能相结合，用于高级预测性分析。

¹⁵ ITU-T [Y.4000/Y.2060](#) (06/2012)建议书，物联网（IoT）概述。

¹⁶ IoT Analytics, [2024年IoT状况：全球连接IoT设备增长13%，达到188亿台](#)，2024年9月3日。

- **用户界面：**它包括仪表盘、移动应用和其他用户界面，使用户与IoT系统进行交互，配置设置，并以易于理解的格式查看数据。它可以根据特定需求进行定制，为用户提供相关信息和控制。
- **安全：**它旨在保护IoT数据和系统的完整性和机密性免受网络威胁。指标包括加密、双因素身份认证、安全启动和定期安全更新。
- **标准与法规：**标准化确保设备的互操作性和兼容性。它遵循有关数据保护、隐私、数据跨境自由流动以及设备跨不同行业操作的区域和国际法规。

4.2.2 应用场景

近年来出现了许多新的IoT应用。最相关且活跃的应用场景如下：

- 通过可远程控制和监控的恒温器、照明和安全系统等互联设备实现家居环境的智能自动化；
- 远程患者监测系统、可穿戴健康设备和远程医疗解决方案，可改善患者护理和健康管理；
- 农业精耕技术利用传感器测量土壤湿度、天气状况和作物健康状况，提高产量和资源效率；
- 智能工厂配备了传感器和自动化机械，以提高生产效率、进行预测性维护、优化供应链；
- 运输和物流车队管理解决方案，实时车辆跟踪和智能交通管理系统，优化物流和减少拥堵；
- 智能库存管理系统、新型店内ICT设备及个性化营销，改善零售服务和客户体验；
- 智慧城市整合了交通、废弃物管理和能源消耗等城市服务的管理系统，以改善可持续性和城市生活；
- 智能电网和新型ICT设备，用于改善家庭、建筑和城市的能源效率和管理。

4.2.3 IoT设备的分类

IoT设备的类别根据其计算能力和通信能力分为三类：¹⁷

- 低处理低连接（LPLC）设备；
- 低处理高连接（LPHC）设备；
- 高处理高连接（HPHC）设备。

ITU-T Y.4108建议书涉及标签等无处理能力的设备。

¹⁷ ITU-T [Y.4460](#)建议书（06/2019年）。物联网应用设备架构参考模型。

HPHC设备功能实体：

传感/执行/数据捕获功能实体；消息传递功能实体；网关接入功能实体；物资管理功能实体；与云服务/应用交互的功能实体；连接管理功能实体；应用执行引擎功能实体；设备管理功能实体；信息共享功能实体；数据分析功能实体；数据存储功能实体。

LPHC设备功能实体：

传感/执行/数据捕获功能实体；消息传递功能实体；网关接入功能实体；物资管理功能实体；与云服务/应用交互的功能实体；连接管理功能实体。

LPLC设备功能实体：

传感/执行/数据捕获功能实体；LPLC消息处理功能实体；网关接入功能实体；物资管理功能实体。

ISO/IEC第一联合技术委员会（JTC1）的IoT报告提供了有关该主题的一般信息，包括IoT技术驱动因素、监管、安全、隐私和治理的示例。

4.3 与C&I相关的IoT挑战

与满足IoT具体需求相关的一些问题和挑战，如质量、可靠性、覆盖和低功耗，在ITU-D第4/2号课题（2018-2021年研究期）最后报告中有所涉及。¹⁸近年来，新趋势不断涌现，势头强劲，增加了IoT平台和协议的复杂性。IoT认证方案必须接受定期审查，以确保符合最新发展趋势。在IoT设备和系统的技术选择和部署过程中，需要考虑更多因素。

增加卫星连接的比例

随着卫星发射成本的降低，通过低地球轨道（LEO）卫星进行连接变得日益普遍。通过LEO卫星实现连接具有更低的路径损耗，因此对终端功率的要求更低，且所需的天线指向性也更低，使设计和部署IoT设备的难度和成本更低。研究表明，卫星IoT市场将继续呈现出日益激烈的竞争态势，并增长至10亿美元的市场规模。然而，卫星IoT连接的最佳应用场景仍然是在偏远和孤立地区进行部署。在可预见的未来，卫星IoT市场的总规模仍将是整个IoT市场的一小部分。

AI和IoT的融合

预计到2027年，近一半的IoT应用将具备AI功能。¹⁹将AI融合IoT应用将会强劲增长，预计未来几年将会大幅增长。

AI与IoT的融合，即AIoT，随着AI技术的大规模应用，正在快速发展。AI技术可以为IoT应用提供更精确的数据分析和处理能力，帮助用户更好地管理和控制IoT设备。IoT设备为AI提供了更多的数据和应用来源，使其能够更好地理解环境，识别模式，并改善各个领域的决策。

¹⁸ ITU-D, ITU-D第2研究组第4/2号课题2018-2021研究期最后报告, [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ICT设备和盗窃移动设备的行为](#), 国际电联, 2021年。

¹⁹ <https://iot-analytics.com/how-enterprise-iot-market-is-evolving/>

例如，AI和IoT的融合，给智能家居带来更多的机会。AI可以实时监控家居环境，通过连接不同的家居设备进行智能调节。在智慧城市场景中，AI可以收集关于城市的实时信息，并通过连接城市中的各种基础设施和设备来支持智能规划和决策。交通系统可以实时调整交通信号灯，并通过AI算法优化交通流量。

4.4 IoT产品的法规和政策

IoT就其本质而言，要求监管框架和治理政策进行调整，以管理IoT给ICT行业带来的新动态。以下是一些需要考虑的关键方面：

- **国际互操作性标准：**包括国际电联、ISO、IEEE在内的多个组织正在努力制定有关IoT设备互操作性的全球标准。这些标准旨在确保技术协调统一，促进IoT解决方案的大规模部署。
- **IoT安全法规：**面对连接对象的激增，需要协调统一的法规来确保这些设备的安全。各国政府正在制定法律，要求制造商遵守最低安全协议，以保护ICT网络免受恶意入侵。
- **数据保护政策：**随着IoT产生的数据增加，监管机构正在实施严格的数据保护义务，如欧洲的GDPR。这些法律要求IoT企业确保通过其设备收集的个人信息隐私和安全。
- **认证举措：**为了确保IoT产品符合C&I标准，一些司法辖区鼓励或要求认证流程。此类认证可涵盖技术兼容性以及与消费者保护和环境可持续性相关的内容。

IoT监管框架是一套政策、标准和导则，旨在监督IoT技术的开发、部署和管理。有效的监管框架对于确保IoT设备和数据的安全性、隐私性、互操作性和合乎道德的使用至关重要。

新ICT的监管框架必须规定：

- 制定安全标准；
- 隐私保护；
- 制定互操作性要求；
- 制定服务质量和可靠性标准；
- 消费者保护法；
- 遵守国际标准；
- 制定道德导则。

首先，当地监管机构应该提供：

- 设备和网络认证；
- 频谱管理；

— 数据治理和主权。

设备认证确保设备在投放市场前符合监管标准。网络认证是强制性的，确保IoT设备在网络基础设施内安全运行。

频谱管理规范无线电频率的使用，以避免干扰并确保IoT设备的可靠通信。

数据治理定义了数据的所有权、共享和传输的规则，尤其是在跨境业务中。数据主权标准确定如何存储、处理和保护数据。

4.5 新IoT设备的合规标准

世界各地的标准制定组织致力于为新ICT设备建立全面的框架，以确保其安全性、互操作性和有效性。这些标准是这些组织共同努力的成果，旨在为开发和实施新的ICT提供明确的指导。它们涵盖了许多方面，包括物理层、网络层、会话层和应用层的要求，以及对安全性和保密性的考虑。国际电联、IEEE和ISO等标准制定组织正积极致力于制定和维护标准，以确保新ICT设备的合规性。

国际电联提供以下标准：ITU-T Y.4000/Y.2060 (06/2012) – 物联网概述；²⁰ITU-T Y.4100/Y.2066 (06/2014) – 物联网通用要求。²¹

ISO和IEC提供以下标准：ISO/IEC 30141 (2024)：物联网（IoT）– 参考架构；²²ISO/IEC 27400 (2022)：网络安全 – IoT安全和隐私 – 导则。²³

ETSI提供以下标准：技术规范ETSI TS 103 645 (01/2024) – 消费者物联网的网络安全：基础要求，提供有关消费者IoT安全的高级指导；²⁴欧洲标准ETSI EN 303 645 (09/2024) – 消费者物联网的网络安全：基础要求，为消费者IoT设备建立网络安全标准，以保护用户隐私和个人数据。²⁵

美国国家标准学会（ANSI）和电信行业协会（TIA）提供以下标准：ANSI/TIA-942-C (07/2024) – 数据中心的电信基础设施标准，规定了数据中心的电信基础设施标准，并考虑IoT部署；²⁶ANSI/TIA-1179-B (06/2023) – 医疗机构电信基础设施标准，制定支持IoT设备的医疗设施电信基础设施的标准。²⁷

3GPP提供以下标准：TS 22.368 (04/2025) – 机器类型通信（MTC）的服务要求，包括IoT内容；²⁸TS 23.682 (03/2025) – 促进分组数据网和应用通信的增强架构，介绍了促进IoT和机器对机器（M2M）通信的增强架构。²⁹

²⁰ ITU-T [Y.4000/Y.2060](#) (06/2012)建议书，物联网概述。

²¹ ITU-T [Y.4100/Y.2066](#) (06/2014)建议书，物联网通用要求。

²² ISO/IEC [30141](#) (2024)，物联网（IoT）– 架构参考。

²³ ISO/IEC [27400](#) (2022)，网络安全 – IoT安全和隐私 – 导则。

²⁴ ETSI [TS 103 645](#)，消费者物联网的网络安全：基础要求。

²⁵ ETSI [EN 303 645](#)，消费者物联网的网络安全：基础要求。

²⁶ ANSI/TIA-[942-C](#)，数据中心的电信基础设施标准。

²⁷ ANSI/TIA-[1179-B](#)，医疗机构电信基础设施标准。

²⁸ 3GPP [22.368](#)，机器类型通信（MTC）的服务要求。

²⁹ 3GPP [23.682](#)，促进分组数据网和应用通信的增强架构。

OneM2M提供了通用M2M服务层的技术规范，可以集成到硬件和软件中实现设备的连接。OneM2M还提供TS-0004服务层核心协议，该协议规定了oneM2M兼容系统、M2M应用和/或其他M2M系统的通信协议。³⁰

ISO/IEC JTC1第5特别工作组（SWG 5）负责研究IoT及相关技术，包括智能电网，并交换信息以加强协作。该工作组于2014年解散，由ISO/IEC JTC 1第10工作组继续开展工作，直至2016年ISO/IEC JTC1第41分委员会接手第10工作组的工作计划。

具体的技术报告和活动提供了以下标准：努力确保IoT设备符合医疗保健领域现行的X73标准，特别是个人健康设备（IEEE 11073标准）。对IoT领域的ISO/IEC和IEEE标准进行基准测试，确保不同制造商的设备和系统之间的C&I。

用例是无线传感器网络（WSN）的实验，该网络由使用无线协议相互通信的IoT设备组成。该实验的目的是评估这些IoT设备在真实条件下和不同环境中的性能。应使用多个测试床，每个测试床代表安装无线IoT设备的特定环境。可远程接入测试床基础设施，以准备和控制无线IoT实验。在这种无线网络中，通常需要测量的参数包括可靠性、时延、无线电占空比、跳数、同步性以及带宽。该实验需要以下条件：

- 相关性：要测量的测试和参数必须与工业部署中遇到的真实条件相关。
- 再现性：实验必须在不同的测试台上和不同的条件下重复进行。
- 重复性：实验必须在相同的条件下重复进行。
- 自动化：实验必须自动运行。

诸如Fed4FIRE+之类的测试床联邦提供了满足这些要求所需的所有工具和服务，使得实验可在预定义的条件下进行和重复。

³⁰ OneM2M [TS-0004](#)，服务层核心协议。

第5章 – 知识转移

5.1 引言

为成功转移C&I知识和技术专长，有必要评估现有能力，明确知识差距，而最为重要的是，提供有效和适当的培训。

5.2 C&I培训需求和机会

《迪拜行动计划》（WTDC-14）中忆及电信/ICT设备和系统的广泛一致性和互操作性增加了市场机会，提高了可靠性，促进了一体化并简化了国际贸易。

然而，这种概括凸显了在获取和拥有合规程序方面，或为实现目标而需评估的程序方面存在的差异与问题。

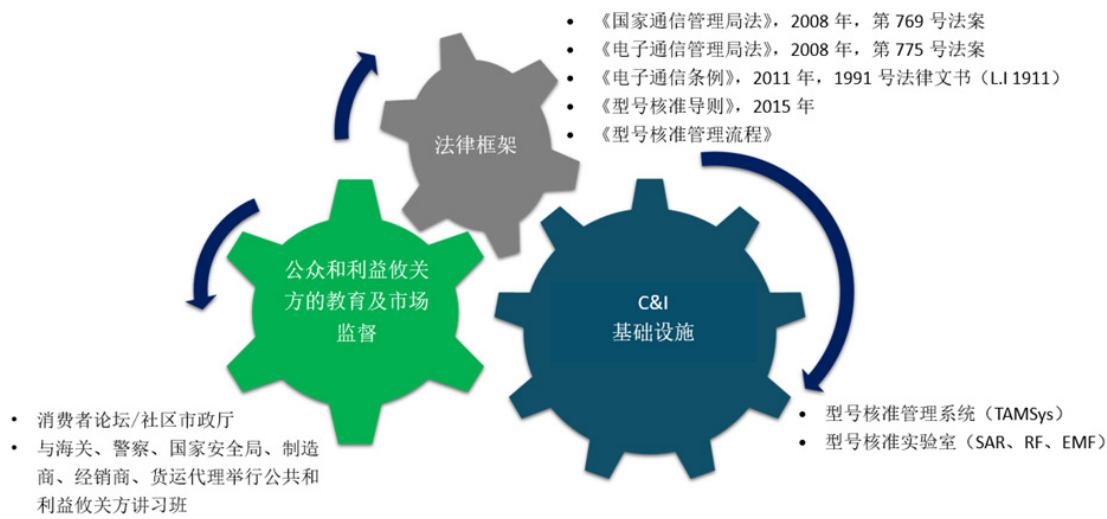
与ICT设备的一致性、互操作性或性能不佳相关的问题会产生多方面的影响。在建立有效的知识转移框架时，必须考虑到用户的安全、技术人员的认证、制造商级设计过程的标准化、对政府决策的支持以及网络服务的质量。

有关数字技术的持续创新和发展表明，需对合规性领域利益攸关方开展培训与教育工作，以确保符合法规要求并防范不合规的相关风险。

除了掌握创新技术设备、理解和制定法律框架、获取和实施C&I基础设施以及监督合同等挑战之外，还有其他一些挑战可以通过具体的培训和知识转移项目来解决。

加纳国家通信管理局（NCA）介绍了其C&I机制通过C&I测试和市场监督打击假冒ICT设备的目标、挑战、指标、构成、技术标准、规范和要求、监管要求以及基础设施。

图3：加纳C&I机制的构成



来源：加纳³¹

图4：加纳C&I机制的目标



来源：加纳³²

作为加纳案例研究的后续行动，肯尼亚共和国与Diplo基金会协作，提供了非洲一致性评定活动监管框架的一个实例。

该框架以肯尼亚负责制定和实施标准以及一致性评定程序的国家标准化机构 – 肯尼亚标准局（KEBS）的活动以及肯尼亚ICT监管机构 – 通信管理局的活动为基础。

³¹ Roland Yaw Kudozia，加纳，[通过C&I测试和市场监督打击假冒ICT设备](#)，ITU-D关于数字化转型面临的一致性和互操作性挑战讲习班，2023年6月2日，日内瓦。

³² 同上。

图5：肯尼亚C&I机制的目标



来源：Diplo基金会³³

5.3 响应知识获取与留存需求的措施

根据WTDC-17通过的《布宜诺斯艾利斯宣言》，通过相关项目、政策和决定的落实而广泛实现的电信/ICT设备和系统的C&I，能够增加市场机遇，提高可靠性，并促进全球一体化和贸易活动。

因此，鼓励成员国和ITU-D部门成员通过研究探寻弥合标准化差距的方法、解决WTDC第47号决议（2022年，基加利，修订版）、世界电信标准化全会（WTS）第44号决议（2024年，新德里，修订版）以及全权代表大会第177号决议（2022年，布加勒斯特，修订版）中提出的各项相关问题，相互提供协助和指导。

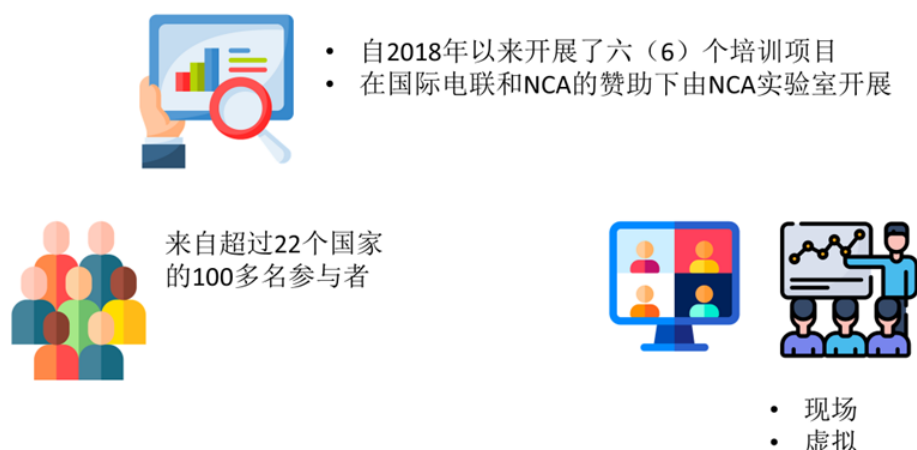
为了满足这种协作的需要，并协助国际社会实现SDG，已经采取了若干举措来发展C&I方面的能力。电信发展局（BDT）报告了与国际电联协作开展的这些举措。

这些文稿介绍了非洲区域在能力建设领域的经验，并向国际电联成员通报了已开发的未来数字网络和基础设施（包括活动、行动、事件和/或资源，如培训和导则）。

自2018年以来，在国际电联（通过国际电联学院）和NCA的赞助下，加纳NCA实验室为非洲组织了六次C&I培训项目。

³³ Mwende Njiraini, Diplo基金会, [非洲的一致性和互操作性评定：肯尼亚案例研究](#)。ITU-D数字化转型面临的一致性和互操作性挑战讲习班，2023年6月2日，日内瓦。

图6：国际电联-NCA非洲培训项目



来源：加纳³⁴

这种经验交流有助于应对与以下方面有关的具体合规问题：

- 法规和法律方面，包括MRA和EMC。
- 在获取基本C&I基础设施以促进型号核准和市场监督时遇到的难题。
- 参与者需要技术合作。
- 在解释不同电信设备的测试报告等方面存在困难。

2021年7月，埃及发起了埃及非洲电信监管培训中心（EG-ATRC），旨在提高非洲ICT行业专业人员的技能，推动数字非洲的进程。这家国际电联认可的中心通过现场和在线会议提供了理论和实践培训。培训课程涵盖网络安全、智慧城市和通信设备认证流程等领域，以确保符合国际标准。50多个国家参加了该项目，迄今已有381人接受了培训。该中心的项目促进了面向非洲监管机构的知识转移，并为整个非洲大陆的数字战略和监管框架的发展做出了贡献。³⁵

除了各成员国采取的国家举措（这些举措是交流经验与知识的切实手段）之外，国际电联还向成员提供电信发展局（BDT）在ICT基础设施领域的工作信息，并向它们提供了已经或正在开发的资源，以促进各国和各区域采纳ICT基础设施政策和战略。

国际电联对成员国的这种支持加快了连通性，利用了地方、国家和区域的知识，并有助于实现在全世界建设包容性数字社会的共同目标。这些资源涵盖各种主题，如ICT网络（ICT基础设施测绘和地理空间分析、ICT业务规划工具包、IMT 2020/5G）、新兴技术、面向成员国的技术援助、培训机会（IPv6、IoT、5G、交换点……）、C&I、最后一英里连接、暴露于电磁场等。³⁶

³⁴ Roland Yaw Kudozia，加纳，[通过C&I测试和市场监督打击假冒ICT设备](#)，ITU-D关于数字化转型面临的一致性和互操作性挑战讲习班，2023年6月2日，日内瓦。

³⁵ 埃及提交的ITU-D SG2 [2/329](#)号文件。

³⁶ 国际电联BDT提交的ITU-D SG2 [2/48](#)、[2/189](#)、[2/253](#)、[SG2RGQ/49](#)和[SG2RGQ/194](#)号文件。

关于C&I，国际电联学院为非洲区域组织了有关测试报告分析的一致性和互操作性、EMC测试的监管问题的培训课程。

5.4 开展一致性和互操作性项目的导则

总之，通过实施确保广泛实现电信/ICT设备和系统的C&I的项目，结合发展中国家和最不发达国家的实际需求和能力，可以实现各项发展目标。

但是，为了开展这些项目，必须遵循以下导则：

- 提供发展中国家和最不发达国家当前C&I情况的最新概述，以便有效地应对挑战，并根据实际需要做出响应。
- 向成员国提供国际电联和其他标准组织的相关信息，以提高对合规性益处的认识。
- 对培训课程进行更好的分类和细分，以更好地满足初学者和专业人士的需要。
- 开发和完善培训模块，以提升每个人的技能。

第6章 – 一致性和互操作性问题：挑战、解决方案和前景

6.1 超出监管/测试程序的新技术

超出监管和测试程序的发展需要一个单一的机制来在最短的时间内实现最佳结果。

计划、执行、检查、处置（PDCA）循环是一个持续改进的循环，也称为戴明循环或戴明轮。它是一种解决问题、改进流程或优化项目的结构化方法。这种方法将统一超出监管和测试程序的开发程序，并确保这些流程的有效性、完整性和充分性。

缩短上市时间，逐步实施新技术的规则和程序

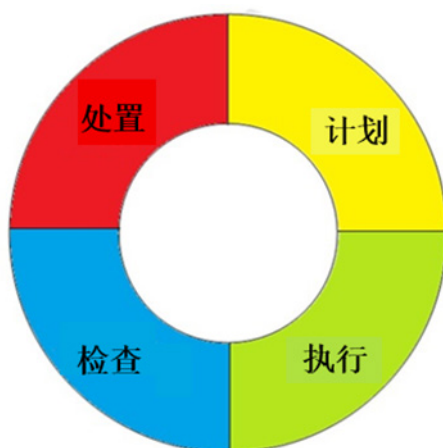
- 步骤1：结合分析程序，使用设备制造商提供的测试协议。
- 步骤2：部署兼容性测试的测试区域。
- 步骤3：制定既定的要求，并在经过认可的实验室进行测试。新技术超出了监管和测试程序。

开发新技术和采用新的ICT标准总是需要时间的，因为需要确立新的监管要求并组织测试过程。

为了解决这个问题，可以采用一种过程方法，正如ISO 9001所介绍的那样。

PDCA循环模式如图7所示：

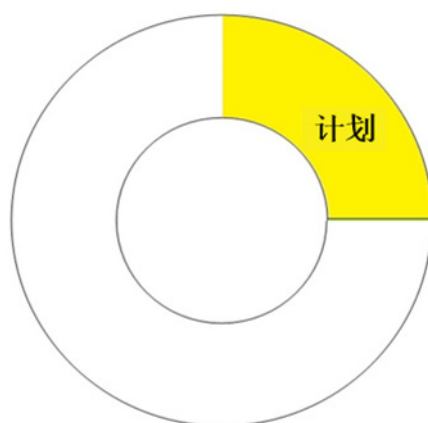
图7：PDCA循环



步骤1 – 计划

作为第一步，有必要确定近期将实施哪些新的ICT标准。根据分析结果，可以编制一份报告，列出在新设备强制一致性评定和兼容性测试的背景下，为更新当前监管框架、设定新要求 and 开发测试方法所需的文件清单。

图8：PDCA循环的计划阶段



第一阶段说明

应在计划阶段制定一套文件。

文件必须说明：

- 1) 将设备进口到该国境内的程序。
- 2) 确保人、动物和环境安全所需的设备规范。
- 3) 用来确保通信网络的完整性、可持续性和安全性的设备。
- 4) 新的ICT所需的许可（如果要求）。
- 5) 商用设备投入使用的程序。
- 6) 在强制一致性评定和新设备与通信网络上现有设备的兼容性测试背景下新ICT的测试方法。
- 7) 测试实验室设备规范。
- 8) 实验室认可/确认所需的工作，以启动测试和使用新方法。
- 9) 负责开发和测试新ICT的工作人员所需的培训和认证水平。
- 10) 制定/增加控制和监测措施，同时确保符合既定要求。

所有这些措施都需要时间和物质资源。这些过程可能需要1到2年。为避免在此期间拖慢ICT的发展，应使用审查机制。

通信管理局向当地公司发放许可，其通过分析制造商的文件来验证设备是否符合要求。通过检查后，进口、安装和调试设备。这将消除试点地区部署的障碍，并最大限度地缩短设备投入商业部署所需的时间。

步骤2 – 执行

在第二阶段，根据编制的法规文件开展工作，包括进口、测试、安装和维护新的ICT。规划跟进和监督活动，确保符合既定要求。按照详细的课程开展人员培训和认证。

图9：PDCA循环的执行阶段



第二阶段说明

在行动阶段，上一步规划和确定的程序需要运作起来。这包括：

- 1) 认证设备符合人类、动物和环境安全的要求。
- 2) 认证设备符合确保通信网络完整性、可持续性和安全性的要求。
- 3) 确保新的ICT设备的进口符合相关的新的进口要求。
- 4) 核实具备使用新的ICT所需的许可（如果要求）。
- 5) 确保设备按照规定的需求实现商业可获取。
- 6) 确保测试实验室采用新方法。
- 7) 培训和认证参与开发和测试新ICT的工作人员。
- 8) 计划和实施控制和监督措施，以确保符合既定要求。

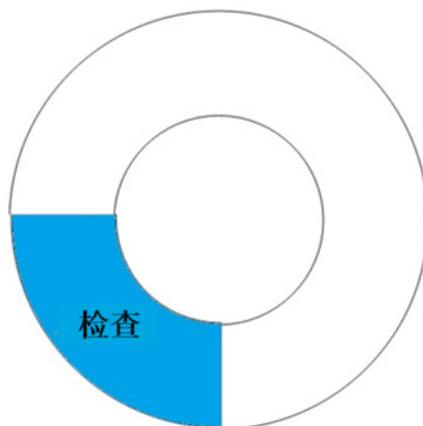
收集所有与ICT相关的活动和统计数据，包括最终用户投诉。在第二阶段，当参数不会对人类、动物或环境安全造成重大风险时，也允许使用强制设备和项目审查机制。

步骤3 – 检查

在对有关新ICT使用情况的统计数据以及终端用户的反馈进行分析之后，可以制定一项修改当前监管框架的计划。引入修改，并依据这些修改引进、测试、安装及运行新的

ICT。规划监测和控制活动，以确保符合调整后的要求。如果必要，对员工认证和培训项目进行修改。

图10：PDCA循环的检查阶段



第三阶段说明

在纠正措施阶段，对统计数据 and 最终用户反馈进行分析。基于此分析，计划对以下现有流程进行变更并加以实施：

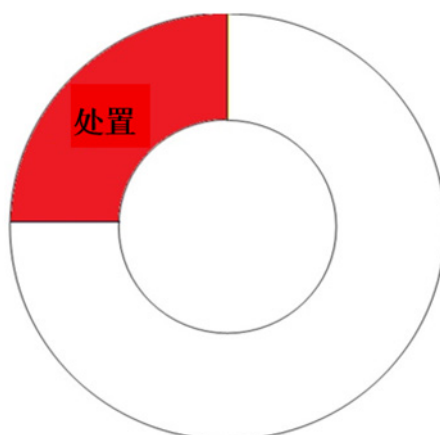
- 1) 设备符合人、动物和环境安全要求的强制性认证。
- 2) 设备符合确保通信网络的完整性、可持续性和安全性要求的强制性认证。
- 3) 进口新ICT设备的程序。
- 4) 培训和认证负责开发和测试新ICT的工作人员。
- 5) 后续和控制措施，确保符合既定要求。

根据纠正措施的结果，起草报告并收集统计数据。

步骤4 – 处置

讨论第三阶段制定的纠正措施的影响，并确定相关ICT的未来使用情况。

图11：PDCA循环的处置阶段



这种循环会一直持续，直到做出决定停止使用这些ICT及拆除设备。然后，有必要制定安全拆除和移除设备的要求，以及对操作设备的人员进行再培训的要求。

第四阶段说明

在处置或决策阶段，对上一步的报告和统计数据进行分析。

基于此分析，计划对以下现有流程进行变更并加以实施：

- 1) 培训和认证负责开发和测试新ICT的工作人员。
- 2) 后续和控制措施，以确保符合既定要求。

在对整个流程的数据进行全面分析后，可以决定是否停用ICT。

6.2 5G的C&I

6.2.1 对实验室和认证机构进行认可，以使用5G技术

对（从事5G相关技术工作）实验室和认证机构的预定评定必须由AB进行，同时顾及现行的国家法律和监管要求。负责执行要求/法规的政府机构必须与经济体的AB以及实验室和认证机构密切合作。这将有助于控制和监测5G产品的质量和互操作性。主管部门可以考虑从5G技术的最佳做法和协调统一中受益。必须考虑购买必要的新设备和培训专家所需的过渡期。在过渡时期，建议使用强制审查机制。借鉴其他国家的良好做法和经验非常重要。

5G技术的一个特点在于大量的IoT对象。应为这些设施建立远程测试机制。与人类用户不同，它们无法自己报告潜在问题。

考虑到使用5G技术的通信设施和服务的测试设备价格昂贵，并需要高素质专家的干预，建议设立区域中心，集中必要的资源。

使用强制审查机制前景广阔，在经济上可行。

6.2.2 实施基于数字计量的远程测试机制

质量信息框架（QIF）标准由数字计量标准联盟（DMSC™, Inc.）制定。

QIF 3.0于2018年被采纳为ANSI标准，并于2019年初由技术委员会提交至ISO。

基于QIF方法，ANSI和ISO制定并通过了ISO 23952:2020标准。³⁷

为了实施该标准，制定了尺寸测量接口标准（DMIS），DMIS在计算机系统和控制设备之间提供控制数据的双向传输。它可以作为通用控制系统编程语言的基础。DMIS提供了一种编程语言语法，用于将控制程序传输到测量设备，并将测量和处理数据反馈到分析、采集或存档系统。DMIS定义了一种中性数据交换格式，是为人工监测而设计。

反过来，所有这些机制都需要校准通信信道，以便在远程站点使用。例如，数字计量是ICT的一部分。

引入数字计量机制的技术基础是创建一个测量探测器的框架。探针安装在域边界，提供中转流量的完整分析，包括来源（形成数据包的设备实际地址）以及所有其他参数（与测量设备交互生成和分析参考流量时）。

没有数字计量，就不可能确保数字主权，因为数据包的原始数据不具有法律上的重要地位，也不可能适用国际法的现行规范。

6.3 对已认证的ICT设备进行的软件修改及其对现有C&I框架的影响

对已认证的ICT设备进行的软件修改会对现有的C&I框架产生重大影响。这些框架旨在确保设备满足关于安全性、保障性、互操作性和性能的具体标准。关于软件修改的影响，以下是一些需要考虑的要点：

符合认证标准

- **初始认证：**当一个ICT设备通过认证时，将根据具体的标准和法规对其进行评估。认证后进行的任何软件修改都有可能改变设备对这些标准的符合性。
- **再认证：**根据修改的性质，设备可能需要进行再认证，以确保它仍然符合要求的标准。这可能是一个昂贵且耗时的过程。

国际电信学院提出了一个新的ITU-T建议书项目，旨在改进ICT设备符合国际电联标准的合规性测试。该提案以ITU-T Q.4068建议书为基础，说明了测试过程，但其面临实际应用的挑战。目标是制定一份新的建议书，以澄清和规范认证机制。³⁸

³⁷ ISO 23952:2020，自动化系统和集成 – 质量信息框架（QIF） – 制造质量信息集成模型。

³⁸ 国际电信学院提交的ITU-D SG2 2/79号文件。

要点

1) 当前测试系统的组织方式

- 测试系统基于ITU-T Q.4068建议书，该建议书为可互操作的测试床联邦定义了开放API接口。
- 技术进步，特别是在IoT方面，使测试变得更加复杂，需要通过试验床互连互通模拟真实世界的条件。
- 开放API支持管理：联邦中测试床的互联和互操作性；资源的公布、分配和配置；用户角色（实验人员）。

2) 用例：在测试床联邦中进行的实验

- 一个具体示例是由IoT设备组成的WSN的实验。
- 测试床通过测量可靠性、时延和无线电频谱使用等参数，支持在各种环境下对IoT设备进行性能测试。
- 要求包括实验的相关性、再现性、重复性和自动化。
- 试验床联邦，比如Fed4FIRE+，提供了满足这些需求的必要工具。

3) 用例：认证系统

- 现行制度有缺点，特别是如果测试实验室归运营公司所有，会产生利益冲突。
- 测试结果只具有信息性，没有法律地位，限制了其在发生纠纷时的使用。
- 该提案主张由经认可的独立第三方认证机构参与，以确保：
 - 资金的透明度（通过认证机构）。
 - 消除利益冲突。
 - 测试结果的合法有效性。

4) 提案和解决方案

新的建议书

制定ITU-T建议书，阐明认证机制并实现联邦测试床API接口的标准化。

独立的认证机构

- 与经认可的机构合作，确保测试的公正性、透明度和法律效力。
- 应在国家立法的基础上进行认证，同时要考虑到现有的国际良好做法。

提高互操作性

实现API接口的标准化，以促进试验床互联，并实现可重复和自动化的实验。

建议的解决方案旨在实现ICT设备测试和认证流程的现代化和标准化。它基于ITU-T Q.4068建议书，提出了解决当前挑战的解决方案，挑战包括IoT测试复杂性、利益冲突和测试结果缺乏法律有效性。通过新的建议书和独立认证机构的参与将提高符合性测试的可靠性、透明度和互操作性。³⁹

安全影响

- **漏洞风险：**软件更新或修改可能会引入新的漏洞，或暴露已有漏洞，进而可能危及设备的安全。
- **补丁管理：**定期更新和补丁对于解决安全漏洞至关重要。但是，必须小心管理这些更新，以确保它们不会无意中引入新的风险或不合规问题。

互操作性

- **兼容性：**软件更改会影响设备与其他设备和系统的互操作能力。在不同制造商的多种设备需要无缝协作的环境中，这一点尤为重要。
- **遵从标准：**修改必须遵从行业标准，以保持互操作性。偏离这些标准会导致兼容性问题，破坏现行的C&I框架。

性能和可靠性

- **功能：**软件修改会影响设备的性能和可靠性。影响设备功能的更改可能会导致故障或性能下降，这可能与最初的认证标准不符。
- **测试和验证：**修改后测试对于确保设备继续按预期运行并满足必要的性能基准至关重要。

管理软件修改的良好做法

- **变更管理：**实施一个稳健的变更管理过程来评估、测试和记录软件修改。
- **持续监控：**确立持续监控机制，及时检测 and 解决软件变更引起的任何问题。
- **利益攸关方参与：**与利益攸关方协作，了解软件修改产生的影响，并确保与C&I框架保持一致。

总之，对已认证的ICT设备进行的软件修改会对现行的C&I框架产生深远的影响。谨慎管理这些变更以维护合规性、安全性、互操作性和性能，同时调整C&I框架以适应软件更新的动态特性，这一点至关重要。

6.4 程序的有效协调和技术协作

程序的技术协作和有效协调在任何组织或伙伴关系中对于确保无缝运营、促进创新和实现共同目标至关重要。以下是实现这一目标的关键策略：

³⁹ 同上。

确立明确的目标和标准

- **定义目标：**清楚地阐明协调和协作的目的，确保与组织或项目目标一致。
- **标准化程序：**制定标准化的协议、工作流程和文档，以确保团队或合作伙伴之间的一致性。
- **采用良好做法：**利用行业标准和良好做法来创建一个通用的协作框架。

促进开放沟通

- **定期会议：**安排定期检查、更新和反馈会议，以保持透明度并及时解决问题。
- **统一平台：**使用协作工具（如Slack、Microsoft Teams或项目管理软件）集中沟通和信息共享。
- **跨职能团队：**鼓励部门或合作伙伴之间的协作，打破孤岛，促进知识交流。

利用技术

- **集成系统：**实施可互操作的工具和平台，以简化数据共享和工作流程集成。
- **自动化：**使用自动化来减少手动错误，提高重复任务的效率。
- **数据分析：**利用数据驱动的洞察来识别瓶颈、优化流程并衡量协调工作的影响。

打造协作文化

- **共同愿景：**确保所有利益攸关方理解并致力于共同的愿景和目标。
- **信任和尊重：**营造一个信任、尊重和包容的环境，鼓励公开对话和合作。
- **认可和奖励：**认可和奖励激励团队和强化积极行为的协作努力。

提供培训和支持

- **技能培养：**提供培训项目，以确保所有团队成员精通所使用的工具、技术和程序。
- **变更管理：**通过提供资源、指导和解决问题来支持团队完成过渡。
- **辅导：**将有经验的团队成员与新成员配对，以促进知识转移和技能培养。

监测和评估进展

- **KPI和指标：**确立关键绩效指标（KPI），跟踪协调和协作工作的成功进展。
- **反馈循环：**不断收集利益攸关方的反馈，确定需要改进的地方。
- **适应性：**准备好根据不断变化的需求和挑战调整程序和策略。

确保治理和问责制

- **明确角色和责任：**定义角色和责任，避免重复工作，确保问责制。

- **合规性：**确保所有程序和协作符合法规要求和组织政策。
- **解决冲突：**确立建设性地解决争端或分歧的机制。

促进创新和持续改进

- **鼓励实验：**为团队打造一个安全的空间来实验新的想法和方法。
- **迭代过程：**定期审查和完善程序，以纳入经验教训和新趋势。
- **知识共享：**记录和分享成功与失败，打造持续学习的文化。

通过实施这些策略，组织可以实现程序的有效协调和技术协作，从而提高效率、创新和整体成功。

6.5 如何确定设备/型号核准型号的优先排序，同时在用户信心和适用监管措施之间取得平衡

为了在用户信心（如通过型号核准）和遵守监管措施之间取得适当的平衡，必须：

- 与合格的员工合作，确保型号核准测试的质量和有效性
- 确保型号核准测试的独立性
- 确保测试样品的中性标记
- 在不同实验室中进行对比测试

型号核准程序中的所有流程必须由当地或区域主管部门确定。

该主管部门必须建立并维护公司活动的认可和验证系统，开展型号核准测试工作。

6.6 新冠疫情期间C&I面临的挑战和机遇

新冠疫情展现了C&I如何能够在一次疫情期间提供：

- 预警系统；
- 户外门禁系统；
- 室内门禁系统；
- 场外追踪系统；
- 采集系统，存储和分析关于疫情参数的信息；
- 采集系统，存储和分析患者护理信息；
- 采集系统，存储和分析医务人员的工作信息；
- 采集系统，存储和分析医疗设备信息；

- 采集系统，储存和分析预防感染/疫苗接种的信息；
- 运送患者和患者住院的物流系统；
- 媒体管理系统；
- 国际/区域间互动系统。

6.7 新技术如何助力改善国际C&I框架和ICT设备的贸易和使用？

以下是新技术帮助改善国际C&I框架以及ICT设备的贸易和使用的一些方式：

- 建立许可设备的国际和区域间电子登记册。
- 建设电子文档登记系统。
- 通过实施数字计量机制，进行远程测试/测量。
- 实施边境和海关服务通用电子登记册。
- 协调有关保护个人数据和个人信息的国际立法。
- 建设国际/区域间信息系统
- 确保信息安全，保护公民、公司和国家机关。
- 维护统一的国际/区域间假冒产品登记册。
- 实施远程医疗机制，帮助各国人民。
- 实施国际/区域间灾害和紧急情况预警系统。

Annexes

Annex 1: Conformance and interoperability frameworks: data by country

Understanding how countries organize themselves to ensure proper C&I levels for ICT networks and device deployment can help C&I operators establish efficient collaboration mechanisms. This is evident in existing effective technical collaboration agreements, such as those in Europe and the Asia-Pacific region.

Data indicates that most countries have established C&I frameworks to ensure trust in the safe and interoperable use of ICT devices by networks and citizens. However, the procedures and the strictness of the requirements (e.g. recognition of certification, use of proxies, self-declaration and local testing) can vary significantly.

Under Pillars 3 (Capacity building) and 4 (Assistance in the establishment of test centres and C&I programmes in developing countries) of the ITU C&I programme, data was collected from 116 countries between 2022 and 2025. The research focused on key C&I infrastructure variables, namely:

1. C&I frameworks
2. ICT standards and technical requirements
3. Conformance assessment and bodies
4. Testing laboratories
5. Quality and metrology

Key findings (2022-2025):

1. C&I frameworks:
 - **85 per cent of countries** have established formal C&I frameworks.
 - **65 per cent** of these frameworks are aligned with international standards (e.g. ITU, GSMA, IEEE).
 - **Regional collaboration** has increased, with **40 per cent of countries** participating in MRAs.
2. ICT standards and technical requirements:
 - **70 per cent of countries** have adopted ICT standards based on ITU recommendations.
 - **50 per cent** have implemented additional national technical requirements to address local needs.
 - **Challenges:** the lack of harmonization in standards across regions remains a barrier to interoperability.
3. Conformance assessment and bodies:
 - **75 per cent of countries** have designated conformance assessment bodies.
 - **60 per cent** of these bodies are accredited by international organizations (e.g. ISO/IEC 17065).
 - **Gaps:** limited capacity in developing countries to conduct advanced testing and certification.

4. Testing laboratories:
 - **60 per cent of countries** have established accredited testing laboratories.
 - **45 per cent** of these labs are equipped to test advanced technologies (e.g. 5G, IoT).
 - **Challenges:** high costs and lack of skilled personnel hinder the expansion of testing capabilities.
5. Quality and metrology:
 - **55 per cent of countries** have integrated quality assurance and metrology into their C&I frameworks.
 - **40 per cent** have adopted digital tools for monitoring and reporting quality metrics.
 - **Opportunities:** the use of AI and blockchain for quality assurance is increasing.

Visual representation: histogram

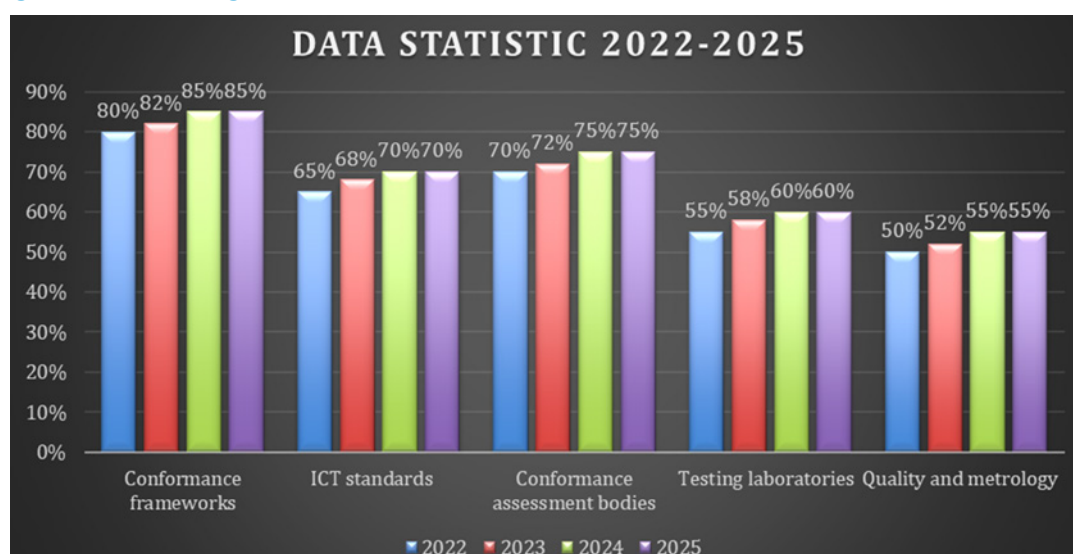
Below is a conceptual representation of the data using a bar diagram and spiral diagram to highlight trends and comparisons.

Bar diagram:

- **X-axis:** C&I infrastructure variables (frameworks, standards, assessment bodies, testing labs, quality).
- **Y-axis:** Percentage of countries with established mechanisms (2022-2025).

Variable	2022	2023	2024	2025
Conformance frameworks	80%	82%	85%	85%
ICT standards	65%	68%	70%	70%
Conformance assessment bodies	70%	72%	75%	75%
Testing laboratories	55%	58%	60%	60%
Quality and metrology	50%	52%	55%	55%

Figure 12: Percentage of countries with established C&I mechanisms



- The histogram illustrates the growth trajectory of C&I frameworks and infrastructure from 2022 to 2025.
- Each loop represents a year, with the size of the loop indicating the percentage of countries adopting C&I mechanisms.
- Key variables (frameworks, standards, assessment bodies, testing labs, quality) are colour-coded for clarity.

Recommendations for 2025 and beyond:

1. **Strengthen regional collaboration:** encourage more countries to join MRAs and harmonize standards.
2. **Build capacity:** invest in training programmes for conformance assessment bodies and testing laboratories.
3. **Adopt advanced technologies:** promote the use of AI, IoT and blockchain for quality assurance and interoperability testing.
4. **Provide funding and support:** provide financial and technical assistance to developing countries to establish and upgrade C&I infrastructure.
5. **Monitor and evaluate:** develop a global dashboard to track progress and share good practices.

Conclusion:

The study period 2022-2025 has seen significant progress in the establishment of C&I frameworks worldwide. However, challenges such as lack of harmonization, limited testing capabilities and high costs, persist. A coordinated global effort, supported by ITU and other stakeholders, is essential to address these gaps and ensure the safe and interoperable use of ICT devices and networks.

Annex 2: Summary of the workshop on compliance and interoperability challenges for digital transformation

Friday, 2 June 2023, 0900 – 1200 hours

Workshop programme: [link](#)

This workshop was organized by the Management Team of ITU-D Study Group Question 4/2. It aimed to identify and discuss issues related to Conformance and Interoperability (C&I) of ICT equipment, with a focus on challenges facing developing countries. Discussions focused on topics related to ICT product compliance in the age of digital transformation. Participation in the workshop was open to ITU Member States, Sector Members, Associates and academia, as well as anyone wishing to contribute to the work. This included people who were also members of international, regional and national organizations.

The workshop was opened by Mr Ibrahima Sylla (Guinea), Rapporteur for Question 4/2.

SESSION 1: Future challenges and adoption in telecommunications/ICTs and digital skills enhancement for C&I

This session focused on questions related to challenges and adoption of telecommunications/ICTs and improving digital skills in developing countries for C&I, such as:

- New technologies exceeding regulations/testing procedures;
- Regulatory aspects for the adoption of openness and interoperability related to 5G;
- Software modifications of ICT devices after certification and their impacts on existing C&I frameworks;
- How new technologies can contribute to improving the international C&I framework and the trade and use of ICT devices.

Co-moderators:

- Mr Serigne Abdou Lahatt Sylla (Senegal), Vice-Rapporteur for Question 4/2
- Mr Vladimir Daigle (ITU), BDT Focal Point for Question 4/2

The first report, New conformity assessment framework for telecommunication products, was presented by Mr Leonardo Marques Campos (Brazil).

This report described how the system for confirming the conformity of communications in Brazil was arranged. Equipment was divided into groups depending on its level of influence on the communication network: either more critical or less critical. Less critical equipment shall be declared. More critical equipment was subject to certification. Particular attention was being paid to new areas - digital transformation and globalization. Voluntary cyber security certification was being offered.

The second report, Conformance and interoperability assessment in Africa: case study of Kenya, was presented by Ms Mwende Njiraini (DiploFoundation).

The report outlined how to implement compliance validation functions in a digital transformation and globalization environment, using Kenya's experience as an example.

The third report, ICT equipment certification in Russia and the Commonwealth of Independent States (CIS) region, was presented by Mr Sergei Melnik (International Telecommunication Academy).

In the report, Mr Melnik noted that in the Russian Federation and the CIS region, an approach similar to the one presented in the Brazilian report was applied to confirming the conformity of communications. Algorithms for the operation of declaration and certification were given. It was

noted that cyber security problems were also proposed to be solved through voluntary certification. The need to introduce digital metrology mechanisms for remote testing was especially worth noting.

SESSION 2: C&I infrastructure and applications

This session focused on:

- the basic infrastructure needed to obtain a quality C&I framework, from technical standards/requirements to legislative and regulatory framework revisions that would be necessary to implement appropriate C&I programmes by developing countries;
- demonstrations of C&I applications for the purposes of the mandate on national and regional experiences in C&I, good practices and possible mechanisms of collaboration for the establishment of joint programmes of C&I and technical cooperation;
- the importance of raising awareness among suppliers and users of terminal equipment in the context of improved monitoring of equipment and use of compliant equipment.

Moderator: Mr Sergei Melnik (International Telecommunication Academy), Vice-Rapporteur for Question 4/2

The first report, Combat counterfeiting through the use of RF, SAR and EMC laboratories, was presented Mr Mourad Belmrissi (Rohde & Schwarz).

The report covered the capabilities of Rohde & Schwarz equipment, advanced testing methods and the peculiarities of equipping EMC laboratories.

Mr Melnik shared his opinion on the merits of Rohde & Schwarz equipment from his own experience, especially in the field of measurement automation.

The second report, Combating counterfeit ICT devices through C&I testing and market surveillance, was presented by Mr Roland Yaw Kudozia (Ghana).

The report outlined the C&I regime in Ghana: its objective and components, technical standards and requirements, technical specifications documents, regulatory requirements, C&I testing infrastructure, market surveillance and its associated challenges, C&I awareness, the joint programme and technical cooperation with ITU, and the ITU-NCA C&I training for Africa. The speaker paid great attention to the issue of training specialists. The experience of Ghana could be very rewarding for everyone.

The third report, Conformity and interoperability of electronic communications equipment and systems: what are the contributions to digital transformation? – case of Mauritania, was presented by Mr Tidjani Oudaa (Mauritania).

Achieving these objectives necessarily required the establishment of an effective and harmonized C&I system that could assess the compliance of ICT equipment with standards and the interoperability between competing systems, in order to build a high-quality, reliable, durable and resilient ICT infrastructure, to serve and achieve the objectives of the policy declaration for the telecommunications sector in Mauritania.

Through the analysis and evaluation of the C&I regime in Mauritania, it was clear that the country lacked the capacities and infrastructures necessary to implement conformity assessment programmes for ICT equipment and systems.

The fourth report, ICT compliance assessment in the digital transformation scenario, was presented by Mr Victor Vellano Neto (Centro de Pesquisa e Desenvolvimento em Telecomunicações).

The report concluded that, due to the use of several technologies in communications, hardware and software, conformity assessment was an essential part of a successful transition. Test facilities and regulatory compliance testing were therefore critical to the success of adopted solutions.

The fifth report, Overview of ITU-T SG11 activities on C&I, including C&I programme, was presented by Mr João Alexandre Zanon (Brazil & ITU-T Study Group 11 Working Party 4).

The report presented the results of the work. Standards for ITU-T testing had been developed. Laboratories for testing had been accredited. Mechanisms for placing and displaying test reports had been created. These mechanisms and results could be used by all countries concerned.

After the session, Mr Denis Andreev (ITU Telecommunication Standardization Bureau) spoke further about ITU-T SG11, ITU-T, how laboratories could be accredited to conduct tests and compliance with ITU-T standards, and how to view test reports in an electronic system. He invited everyone to take part in the webinar on the work of the test system.

Annex 3: Summary of the workshop on techniques designed to promote harmonization of C&I regimes

Friday, 10 May 2024, 1430 - 1730 hours

Workshop programme: see [link](#)

Background information

This workshop was designed to tackle the challenges faced by developing countries in ensuring the C&I of ICT equipment, with a special focus on countering the theft and counterfeiting of mobile devices and the regulatory aspects of IoT technologies.

The workshop was opened by Mr Ibrahima Sylla (Guinea), Rapporteur for Question 4/2.

SESSION 1: Theft of mobile devices and importance of raising awareness among equipment suppliers and users

This session explored the growing challenges of mobile device theft and the crucial importance of raising awareness among both providers and users of telecommunication/ICT equipment. With the proliferation of mobile devices in our daily lives, the risk of theft and counterfeiting of the devices had increased considerably, requiring concerted action by the entire technological ecosystem. Speakers in the session shared their knowledge and expertise on various aspects of mobile device security, including the latest technologies for tracking and combating counterfeiting, effective awareness-raising strategies, existing regulations and the need for collaboration among industry stakeholders. By focusing on preventing device theft and promoting the use of conforming equipment, the session aimed to inform participants on good practices and measures to be taken to protect data and ensure user safety.

The session was moderated by Mr Sergei Melnik (International Telecommunication Academy), Vice-Rapporteur for Question 4/2.

Theft of mobile devices and importance of raising awareness among equipment suppliers and users in Kenya

Ms Mwende Njiraini (DiploFoundation)

Ms Mwende Njiraini addressed the issue of mobile device theft in Kenya and the critical role of raising awareness among both suppliers and users. She outlined the intricacies of the regulatory framework in Kenya, which included KEBS for ISO ICT standards and the Communications Authority of Kenya for ITU recommendations. She detailed the process of type approval, the challenges faced due to the lack of a local testing laboratory, and the limited number of MRAs due to the absence of such facilities. She also discussed initiatives in Kenya to monitor and combat counterfeit ICT equipment, highlighting the KenTrade system for import verification, market surveillance efforts, and the proposed Device Management System, which had faced legal challenges but was ultimately upheld by the Supreme Court, to address counterfeit, stolen and illegal ICT devices.

Q&A session:

Questions were raised regarding the operational aspects of the Device Management System, the establishment of a laboratory for counterfeit management and the verification of documents supplied during the type-approval process. Ms Njiraini responded by explaining the collaboration with various regulatory organizations, the proposed laboratory's role, and the current operational challenges, including trusting the authenticity of documents in the absence of a local laboratory.

Mr Papa Gueye (École Nationale de Cybersécurité à Vocation Régionale, Senegal)

Mr Papa Gueye provided insights into the approach of Senegal to tackling the issue of counterfeit ICT devices, highlighting the security threats they posed, including spying and data theft. He detailed legislative measures, such as competition laws, intellectual property protections, and telecommunications regulations, aimed at consumer protection. He also emphasized the need for international cooperation, public awareness campaigns and enhanced investigative capabilities to effectively combat counterfeit goods, which had significant negative impacts on national security and economic stability.

Q&A session:

An inquiry was made regarding the policy of Senegal on the protection of private data in relation to IoT devices. Mr Gueye confirmed the existence of a Data Protection Act in Senegal, which was overseen by a designated body, ensuring the safeguarding of personal data within the country.

Mobile Device Registration System

Ms Zeynep Nehir Sarıgöl (Dekob Technology)

(Ms Sarıgöl had to cancel her participation due to unexpected circumstances. Participants were invited to review the presentation available and contact her for more information.)

Overview of ITU-T activities on combating counterfeiting and stolen ICT

Mr João Alexandre Zanon (Brazil & ITU-T Study Group 11 Working Party 4)

Mr João Alexandre Zanon could not be present due to his involvement in the ITU-T SG11 Plenary occurring at the same time. Nevertheless, he provided, through a video recording, an insight into ITU-T's activities on combating counterfeit and stolen ICT devices. He brought attention to two significant resolutions, Resolutions 188 and 189 (Rev. Bucharest, 2022) of the Plenipotentiary Conference, targeting counterfeit ICT devices and mobile device theft. He discussed the work of ITU-T Study Group 11, which, since 2017, had developed various relevant recommendations, technical reports, and supplements. He emphasized the importance of a global infrastructure enabling communication between devices as well as the interoperability between various lists used in tracking problems with counterfeit and stolen devices.

Q&A session:

A question was asked about the implementation and monitoring mechanisms planned for the proposed recommendations against counterfeit ICT devices. The importance of not just presenting well-analysed propositions but also ensuring there was a system or radar in place to track the application of and adherence to these recommendations was emphasized.

As the Q&A could not be conducted in real-time due to his absence, participants were encouraged to submit their questions, which would be forwarded to him for a response.

SESSION 2: Internet of things and regulatory aspects for the adoption of the opening of C&I

This session provided an in-depth exploration of the specific regulatory challenges for the integration of IoT in the field of ICT. It brought together experts to discuss legal implications, conformance standards and interoperability strategies in the context of the increasing use of IoT in ICT infrastructures and services.

This session was moderated by Mr Sergei Melnik (International Telecommunication Academy), Vice-Rapporteur for Question 4/2.

Internet of things and regulatory aspects for the adoption of the opening of C&I

Mr Roland Yaw Kudozia (Ghana)

Mr Roland Yaw Kudozia explored the regulatory aspects and challenges pertaining to the adoption of IoT technologies. He highlighted IoT's potential for improving socio-economic conditions in developing countries, despite facing obstacles such as digital divides, security and privacy concerns, interoperability issues, and infrastructure gaps. He stressed the need for strategic planning and collaboration between governments, industry and international partners to overcome the challenges of IoT and maximize its benefits.

Q&A session:

Questions were asked about the prevalence of security flaws in IoT devices and the policies in place to protect private data. Mr Kudozia acknowledged the lack of reliable statistics on the regularity of network attacks via IoT but cited examples of devices transmitting data to unexpected servers. He confirmed that Ghana had a Data Protection Act to safeguard personal data.

A comment was also raised about the opportunity for coordination on security matters concerning new technologies and suggested that the aspects presented would be beneficial for cross-Question discussions, in particular with Question 3/2.

Conclusion

The workshop concluded with an emphasis on the multifaceted challenges of promoting C&I regimes and the pivotal role of international standards and cooperation. Participants recognized the importance of harmonized regulatory frameworks, effective MRAs, vigilant market surveillance and comprehensive consumer education to combat the theft and counterfeiting of mobile devices. Additionally, the workshop highlighted the critical need for addressing interoperability issues, particularly in the rapidly advancing IoT landscape. The consensus underscored the need for a collaborative approach by Member States, Sector members, academia, and regional and international organizations to effectively tackle the issues. The successful deployment of IoT technologies in developing countries illustrated the potential for economic development, improved access to health care and education, and enhanced resource management. However, the challenges presented by the digital divide, and the need for infrastructure development were acknowledged as significant barriers that had to be addressed through comprehensive policies, regulations and international cooperation.

Overall, the workshop served as a crucial platform for exchanging knowledge, experiences and good practices among various stakeholders in the ICT sector. The discussions reinforced the necessity of developing robust and adaptable regulatory frameworks that could keep pace with technological advancements. The workshop's outcomes pointed towards the need for ongoing dialogue, research and collaboration to create a more harmonized and global ICT environment, which was particularly vital for the sustainable growth and development of ICT infrastructure in developing countries.

In summary, the workshop provided valuable insights into the complexities of C&I regimes and set the stage for future actions and collaborations aimed at enhancing the C&I of ICT equipment worldwide. It underlined the importance of leveraging international standards, fostering collaboration and implementing good practices to navigate the challenges and opportunities presented by emerging technologies such as IoT, ensuring their beneficial integration into society.

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

Contributions on Question 4/2

Web	Received	Source	Title
2/398	2025-04-22	BDT Focal Points for Questions 4/2 and 7/2	BDT report on the implementation of ICT Infrastructure work since the last ITU-D Study Group meeting
2/367	2025-03-31	Sri Lanka	Combating counterfeiting and theft of mobile devices
2/361 (Rev.2)	2025-05-09	Rapporteur for Question 4/2	Draft Output Report on Question 4/2
2/352	2025-03-05	Rwanda	Enhancement of institution and collaboration in combating the use of counterfeit, theft, and tampered ICT mobile devices in Rwanda
2/329	2024-10-29	Egypt	Egypt capacity building centre for African countries (EG-ATRC)
2/296	2024-10-22	China	Base station antenna OTA conformance testing practice
2/280	2024-10-28	Rapporteur for Question 4/2	Draft Output Report on ITU-D Question 4/2
2/269	2024-09-26	Sri Lanka	Proposed text for Question 4/2 Final Report, Chapter 2 "Compliance and interoperability"
2/267	2024-09-25	International Telecommunication Academy	Proposed text for Question 4/2 Final Report, Section 7.3 "Intelligent object communication paradigms"
2/266	2024-09-25	International Telecommunication Academy	Proposed text for Question 4/2 Final Report, Section 7.2 "Regulatory aspects for open and interoperable adoption related to 5G"
2/253	2024-09-19	BDT Focal Points for Questions 1/1, 2/1, 4/2, 5/1 and 7/2	BDT report on the implementation of ICT Infrastructure work since the last ITU-D Study Group meeting
2/230	2024-09-26	Rapporteur for Question 4/2	Annual progress report for Question 4/2 for November 2024 meeting
RGQ2/216	2024-04-22	Rapporteur for Question 4/2	Revised table of contents for the Final Report of Question 4/2
RGQ2/210	2024-04-18	Guinea	Draft Chapter 1 ("ICT products for the Sustainable Development Goals (SDGs)") for the Final Report of Question 4/2
RGQ2/204	2024-04-16	Vice-Rapporteur for Question 4/2	Draft Chapter 3 - Countering the proliferation of counterfeit and poor quality devices for the final report of Question 4/2
RGQ2/203	2024-04-16	Côte d'Ivoire	Draft text for the Q4/2 Final Report, Chapter 6 ("Review of information transfer, know-how and training")

(continued)

Web	Received	Source	Title
RGQ2/194	2024-04-16	BDT Focal Points for Questions 1/1, 2/1, 4/2, 5/1 and 7/2	BDT report on the implementation of ICT Infrastructure work since the last ITU-D Study Group meeting
RGQ2/186	2024-04-15	International Telecommunication Academy	Proposed text for Q4/2 Final Report, Section 7.1 ("New technologies beyond regulatory/testing procedures")
RGQ2/115	2024-02-27	Guinea	Combating counterfeiting and theft of mobile devices in Guinea
RGQ2/112	2024-02-21	Chad	Combating mobile phone theft in Chad
2/193	2023-10-16	Telecommunications Management Group, Inc.	Frameworks of conformance and interoperability to support wireless power transmission via radiofrequency beam (beam WPT)
2/189	2023-10-16	BDT Focal Points for Questions 1/1, 2/1, 4/2, 5/1 and 7/2	BDT report on the implementation of ICT Infrastructure work since the last ITU-D Study Group meeting
2/140	2023-10-03	International Telecommunication Academy	National expertise for the compliance of the ICT devices and services with the ITU standards
2/124	2023-09-14	Rapporteur for Question 4/2; Vice-Rapporteurs for Question 4/2	Annual progress report for Question 4/2 for October-November 2023 meeting
2/114	2023-09-05	Sri Lanka	Registration of legitimate mobile devices and combating counterfeiting and theft of mobile devices
2/99	2023-08-04	Liberia	Public policy challenge to combat mobile crime in Liberia
RGQ2/49	2023-04-25	BDT Focal Points for Questions 1/1, 2/1, 4/2, 5/1 and 7/2	BDT report on Future Network and Digital Infrastructure work including activities, and resources since the last ITU-D Study Group meetings
RGQ2/37	2023-04-07	Zambia	Combating the influx of counterfeit phones
RGQ2/22	2023-03-23	Madagascar	Importance of awareness-building among suppliers and users of terminal equipment in the context of improved monitoring of equipment and compliance of equipment in use
RGQ2/17	2023-03-20	Central African Republic	SDG 9 in relation to impact of counterfeit and fake telecommunications/ICTs and devices trafficked to developing countries
2/TD/5	2022-12-06	Rapporteur for Question 4/2	Proposed workplan and table of contents for Question 4/2

(continued)

Web	Received	Source	Title
2/79	2022-11-24	International Telecommunication Academy	Certification system for ICT devices and services compliance with ITU standards
2/48	2022-10-18	BDT Focal Points for Questions 1/1, 2/1, 4/2, 5/1 and 7/2	BDT report on the implementation of ICT Infrastructure work since the last ITU-D Study Group meeting
2/46	2022-10-17	Inter-Sector Coordination Group	Mapping of ITU-D Questions to ITU-T Questions and ITU-R Working Parties

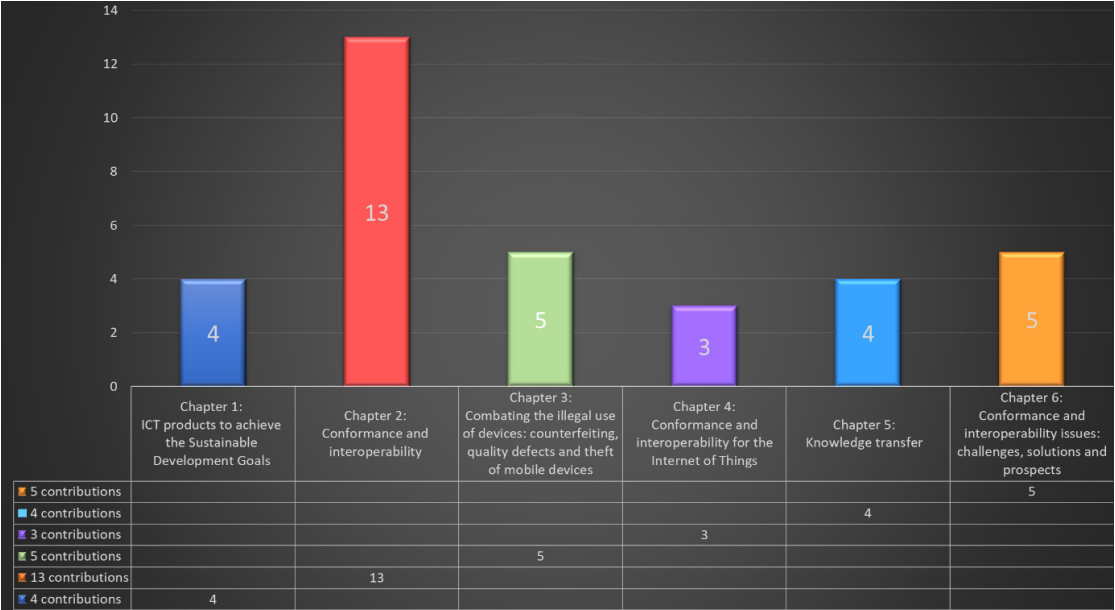
Incoming liaison statements for Question 4/2

Web	Received	Source	Title
2/357 +Ann.1	2025-03-13	International Laboratory Accreditation Cooperation	Liaison statement from the International Laboratory Accreditation Cooperation (ILAC) to ITU-D Study Group 2 Question 4/2 on the draft Final Report of Question 4/2
2/349	2025-03-20	ITU-R Working Party 5D	Liaison statement from ITU-R Working Party 5D to ITU-D Study Group 2 Question 4/2 and Working Party 1C on base station antenna OTA conformance testing
2/217 +Ann.1-2	2024-05-21	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Group 2 Question 4/2 on the progress of the work on Combating Counterfeit and Stolen Telecommunication/ICT devices/software
RGQ2/202 +Ann.1-10	2024-04-16	ITU-T Focus Group on Testbeds Federations for IMT-2020 and beyond	Liaison statement from ITU-T Focus Group on Testbeds Federations for IMT-2020 and beyond (FG-TBFxG) to ITU-D Study Groups 1 and 2 on deliverables of FG-TBFxG
2/208 +Ann.1-2	2023-10-26	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Group 2 Question 4/2 on the agreement of ITU-T Q Suppl.76 and new draft Recommendation ITU-T Q.GIR
2/207 +Ann.1	2023-10-26	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Group 2 Question 4/2 on the agreement of the Technical Report ITU-T QSTR-MCM-UC "Use Cases on the combat of Multimedia Content Misappropriation"
2/206	2023-10-26	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Group 2 Question 4/2 on ITU Workshop "Episode 2: "Global approaches on combating counterfeiting of telecommunication/ICT devices and mobile device theft"
2/203	2023-10-24	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Group 2 Question 4/2 on ITU Tutorial on Testing Laboratories Recognition Procedure

(continued)

Web	Received	Source	Title
2/93	2023-06-05	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Group 2 Question 4/2 on telecommunication/ICT equipment
RGQ2/59	2023-05-03	ITU-T Study Group 15	Liaison statement from ITU-T Study Group 15 to ITU-D Study Groups 1 and 2, Question 1/1 and Question 4/2 on contributions from developing countries
2/25 +Ann.1-4	2022-07-18	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Group 2 Question 4/2 on ITU recognition of testing laboratories
2/21 +Ann.1	2022-06-16	ITU-T Focus Group on Testbeds Federations for IMT-2020 and beyond	Liaison statement from ITU-T Focus Group on Testbeds Federations for IMT-2020 and beyond (FG-TBFxG) to ITU-D Study Groups 1 and 2 on call for use cases on testbeds federation
2/15 +Ann.1-2	2022-04-14	ITU-T Focus Group on Testbeds Federations for IMT-2020 and beyond	Liaison statement from ITU-T Focus Group on Testbed Federations for IMT-2020 and beyond (FG-TBFxG) to ITU-D Study Groups 1 and 2 on the outcomes of the first meeting of the Focus Group
2/10 +Ann.1	2021-12-21	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Groups 1 and 2 on establishment of a new ITU-T Focus Group on Testbeds Federations for IMT-2020 and beyond (FG-TBFxG) and first meeting (virtual, 4-7 April 2022)
2/8	2021-12-16	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Group 2 Question 4/2 on the progress on the combat of counterfeit and stolen ICT
2/6 +Ann.1-3	2021-12-10	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Group 2 Question 4/2 on ITU Testing Laboratory Recognition Procedure

Figure 13: Mapping distribution to chapters



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****区域代表处**

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****区域代表处**

SAUS Quadra 6 Ed. Luis Eduardo
Magalhães,
Bloco "E", 10º andar, Ala Sul
(Anatel)
CEP 70070-940 Brasilia - 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****区域代表处**

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

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: itu-ro-cis@itu.int
电话: +7 495 926 6070

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**

4th floor NBTC Region 1 Building
101 Chaengwattana Road
Laksi,
Bangkok 10210,
Thailand

电子邮件: itu-ro-asiapacific@itu.int
电话: +66 2 574 9326 – 8
+66 2 575 0055

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

塞内加尔**国际电联****地区办事处**

8, Route du Méridien Président
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**

Gedung Sapta Pesona
13th floor
Jl. Merdeka Barat No. 17
Jakarta 10110
Indonesia

电子邮件: bdt-ao-jakarta@itu.int
电话: +62 21 380 2322

津巴布韦**国际电联****地区办事处**

USAF POTRAZ Building
877 Endeavour Crescent
Mount Pleasant Business Park
Harare
Zimbabwe

电子邮件: itu-harare@itu.int
电话: +263 242 369015
电话: +263 242 369016

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 Cía
Apartado Postal 976
Tegucigalpa
Honduras

电子邮件: itutegucigalpa@itu.int

电话: +504 2235 5470
传真: +504 2235 5471

印度**国际电联****地区办事处和****创新中心**

C-DOT Campus
Mandi Road
Chhatrapur, Mehrauli
New Delhi 110030
India

电子邮件: itu-ao-southasia@itu.int
地区办事处: itu-ic-southasia@itu.int
创新中心: ITU Innovation Centre in New Delhi, India
网址: ITU Innovation Centre in New Delhi, India

国际电信联盟
电信发展局
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN: 978-92-61-41185-5



9 789261 411855

瑞士出版
日内瓦，2025

图片鸣谢: Adobe Stock