ITUPublications
Study period 2018-2021

International Telecommunication Union
Development Sector

Study Group 2 Question 4

Assistance to developing countries for implementing conformance and interoperability programmes and combating counterfeit ICT equipment and theft of mobile devices

Output Report on ITU-D Question 4/2

Assistance to developing countries for implementing conformance and interoperability programmes and combating counterfeit information and communication technology equipment and theft of mobile devices

Study period 2018-2021

Assistance to developing countries for implementing conformance and interoperability programmes and combating counterfeit information and communication technology equipment and theft of mobile devices: Output Report on ITU-D Question 4/2 for the study period 2018-2021

978-92-61-34131-2 (Electronic version)
978-92-61-34141-1 (EPUB version)
978-92-61-34151-0 (Mobi version)

Suggested citation. Assistance to developing countries for implementing conformance and interoperability programmes and combating counterfeit information and communication technology equipment and theft of mobile devices: Output Report on ITU-D Question 4/2 for the study period 2018-2021. Geneva: International Telecommunication Union, 2021. Licence: CC BY-NC-SA 3.0 IGO.

Third-party materials. If you wish to reuse material from this work that is attributed to a third party, such as tables, figures or images, it is your responsibility to determine whether permission is needed for that reuse and to obtain permission from the copyright holder. The risk of claims resulting from infringement of any third-party-owned component in the work rests solely with the user.

General disclaimers. The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of ITU or its secretariat concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The mention of specific companies or of certain manufacturers' products does not imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned. Errors and omissions excepted, the names of proprietary products are distinguished by initial capital letters.

All reasonable precautions have been taken by ITU to verify the information contained in this publication. However, the published material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader. In no event shall ITU be liable for damages arising from its use.

Cover photo credits: Shutterstock

Acknowledgements

The study groups of the ITU Telecommunication Development Sector (ITU-D) provide a neutral platform where experts from governments, industry, telecommunication organizations and academia from around the world gather to produce practical tools and resources to address development issues. To that end, the two ITU-D study groups are responsible for developing reports, guidelines and recommendations based on input received from the membership. Questions for study are decided every four years at the World Telecommunication Development Conference (WTDC). The ITU membership, assembled at WTDC-17 in Buenos Aires in October 2017, agreed that for the period 2018-2021, Study Group 2 would deal with seven Questions within the overall scope of "Information and communication technology services and applications for the promotion of sustainable development."

This report was prepared in response to Question 4/2: **Assistance to developing countries for implementing conformance and interoperability programmes and combating counterfeit information and communication technology equipment and theft of mobile devices** under the overall guidance and coordination of the management team of ITU-D Study Group 2 led by Mr Ahmad Reza Sharafat (Islamic Republic of Iran), as Chairman, supported by the following Vice-Chairmen: Mr Nasser Al Marzouqi (United Arab Emirates)(resigned in 2018); Mr Abdelaziz Alzarooni (United Arab Emirates); Mr Filipe Miguel Antunes Batista (Portugal)(resigned in 2019); Ms Nora Abdalla Hassan Basher (Sudan); Ms Maria Bolshakova (Russian Federation); Ms Celina Delgado Castellón (Nicaragua); Mr Yakov Gass (Russian Federation)(resigned in 2020); Mr Ananda Raj Khanal (Republic of Nepal); Mr Roland Yaw Kudozia (Ghana); Mr Tolibjon Oltinovich Mirzakulov (Uzbekistan); Ms Alina Modan (Romania); Mr Henry Chukwudumeme Nkemadu (Nigeria); Ms Ke Wang (China); and Mr Dominique Würges (France).

The report was developed under the leadership of the Rapporteur for Question 4/2, Mr Cheikh Tidjani Oudaa (Mauritania), in collaboration with the following Vice-Rapporteurs: Mr Ahmadou Dit Adi Cissé (Mali); Ms Amel Khiar (Algeria); Mr Joseph Onaya (Kenya); Mr Brillant Harivony Rakotoratsimanjefy (Madagascar); and Mr Serigne Abdou Lahatt Sylla (Senegal).

Special thanks go to chapter coordinators for their dedication, support and expertise.

This report has been prepared with the support of the BDT focal points, editors, as well as the publication production team and the ITU-D study group secretariat.

Table of contents

List of table and figures

Table

Figures

Executive summary

Global reliance on and confidence in ICT devices

Information and communication technology (ICT) devices are the essential gateways to the digital world. Global coordination on and compliance with standards are vital to ensure that networks are interoperable and users and machines can interconnect.

The implementation of conformance and interoperability (C&I) programmes and advanced techniques to combat the proliferation of counterfeit ICT equipment and the theft of mobile devices is moving forward in all countries, with some making more rapid progress than others.

The ITU Telecommunication Development Sector (ITU-D) has been helping Member States to evaluate the technical and economic issues related to ensuring conformance and interoperability of ICT devices, focusing on assistance, capacity building and sharing best practices from ITU Member States. ITU-D has been collaborating closely on these matters with the ITU Radiocommunication Sector (ITU-R) and the ITU Telecommunication Standardization Sector (ITU-T) to build synergies in those efforts and bring about a bigger impact.

Additionally, in a society increasingly connected through ICT devices, the use of C&I frameworks continues to be an important issue widely debated by developers, manufacturers, importers, operators and users. The role of the regulatory authorities in this regard is crucial to balancing the levels of security and control needed.

Finally, another important issue for the future of C&I is the emergence of new technologies in all industries driven by the Internet of Things (IoT), and the standards to be taken into account when developing countries are implementing or revising C&I frameworks.

In this context, the present report discusses best practices for achieving optimal solutions.

Background work in the field of C&I

During previous study periods, ITU had focused on the important issue of assistance on conformance and interoperability for developing countries. Several important outputs were produced that are still relevant to ITU-D's work on Question 4/2. The previous report on Question 4/2 can be found at https://www.itu.int/pub/D-STG-SG02.04.1-2017 and additional ITU-D activities on assistance to developing countries, such as the national and regional C&I framework database, regional assessments and capacity-building events, can be found at https://itu.int/go/CI_Development.

Chapter 1 – Information and communication technology products enabling the achievement of the Sustainable Development Goals

1.1 Relevance of ICT products to society

Digital transformation is enabling rapid change across all industries and in every aspect of life. Mobility, broadband and the cloud, the three fundamental forces of information and communication technologies (ICTs), are reshaping value chains, spurring the digitalization of business models and overcoming distances. A new service economy is thus emerging where people are increasingly able to, for example, share goods and services instead of buying and owning them – an illustration of how the digital age is unleashing innovative new business models and changing lives.[1]

The main benefits of ICTs are increased access, connectivity and efficiency gains for individuals, communities and economies:[2]

- *Access* to information and services: Through ICT devices and infrastructure and the use of technologies including mobile phones, cellular telecommunication networks (such as 3G and LTE), the Internet and broadband, ICTs can improve universal access to information and services for individuals globally, in both rural and urban areas.
- *Connectivity* between individuals and organizations: Instantaneous or near-instantaneous connectivity between individuals, organizations and networks can increase productivity and innovation across multiple sectors and communities, and facilitate the real-time communication needed for the rapid scaling of critical services.
- *Efficiency gains* from improved productivity and resource efficiency.
- Adoption of *green standards* through conformance to effectively reduce climate change.
- Ability of ICTs to unlock and leverage *productivity gains* by improving access to information and communication between individuals (thereby reducing the resources wasted on travel and the manual collection of data) and by providing the infrastructure needed for collecting and analysing large sets of data (big data).

1.2 ICT devices: Proxies for the social economy backbone

A strategic framework is necessary in order to pursue coherent policies and reinforce ICT-enabled development initiatives. ICTs must be integrated into every aspect of public policy and economic activity. To achieve this, it will be necessary to:

- develop public policies and regulations to enable full ICT utilization;

[1] As stated by Hans Vestberg, President and CEO, Ericsson, in his Foreward to ICT & SDGs – Final Report: How Information and communications technology can accelerate action on the Sustainable Development Goals. The earth Instutute, Colombia University, and Ericsson.

[2] Huawei. 2017 ICT Sustainable Development Goals Benchmark. Huawei, 2017.

- rapidly expand and upgrade the ICT infrastructure;
- promote public-private partnerships to incubate new ICT start-ups that will provide locally appropriate services;
- address ICT interoperability issues;
- build capacity to manage ICT systems;
- ensure that policies and regulations keep pace with the rapid innovation and deployment of ICTs.

1.3 Connecting and protecting ICT users and networks through conformance to recognized standards

Investments in infrastructure and innovation are crucial drivers of economic growth and development. Technological progress is also key to finding lasting solutions to economic and environmental challenges, such as creating jobs and promoting energy efficiency. Fostering sustainable industries and investing in scientific research and innovation are all important ways to facilitate sustainable development.[3]

SDG 9: Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation

Targets:

9.1 – Develop quality, reliable, sustainable and resilient infrastructure, including regional and transborder infrastructure, to support economic development and human well-being, with a focus on affordable and equitable access for all.

9.a – Facilitate sustainable and resilient infrastructure development in developing countries through enhanced financial, technological and technical support to African countries, least developed countries, landlocked developing countries and small island developing States.

9.b – Support domestic technology development, research and innovation in developing countries, including by ensuring a conducive policy environment for, *inter alia*, industrial diversification and value addition to commodities.

9.c – Significantly increase access to information and communication technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020.

To protect ICT users and networks, it is vital to focus on:

- quality
- safety
- interoperability
- interference-free spectrum environment
- national rules
- sustainability
- reliability
- resilience

[3] United Nations Development Programme (UNDP). Sustainable Dvelopment Goals. SDG 9: Industrial innovation and infrastructure.

- affordability (through the economies of scale made possible by conformance and interoperability, or C&I).

To that end, issues relating to ICT equipment and systems must be taken into account, including:

- technical requirements and standards
- conformity assessment
- control of equipment
- post-market surveillance
- promotion of mutual recognition agreements.

Innovative methods for assessing C&I are therefore needed, including:

- new or shared testing laboratories
- virtual laboratory services
- mutual recognition agreements (MRAs) reflecting local and regional requirements and limitations
- post-market surveillance
- smart testing solutions
- harmonization of standards.

Tasks include:

- raising awareness
- creating a networking platform on C&I for the ITU-D membership
- promoting collaboration, research and sharing of experience on matters covered by the Question
- ensuring ITU-D member representation in other forums dealing with C&I (e.g. ISO/CASCO STAR group meetings)
- producing a questionnaire to collect country data and to track progress on C&I
- developing guidelines
- issuing recommendations.

1.4 Impact of COVID-19 pandemic on type-approval procedures

The COVID-19 pandemic has had – and continues to have – a significant impact on international trade and the conformity assessment of products, including ICT devices. Type-approval activities have been severely affected by border closures and difficulties in accessing facilities (such as physical testing labs and experts in the field). This has led to a need to find innovative ways to certify the conformance and quality of products. Regulators, manufacturers and operators have been developing ad hoc solutions to keep businesses running and avoid trade chain disruptions. The time has come to harness the potential of digital technologies to provide solutions for conformity assessment.

Chapter 2 – Conformity and interoperability

2.1 Introduction

Conformity assessment guarantees that ICT equipment complies with technical specifications and standards. Compliance helps vendors and users evaluate how the equipment will perform when integrated into a network with other devices to provide a network service. Interoperability testing measures if two or more products correctly implement the technical specifications necessary to ensure successful integration supporting particular communication protocols.

C&I testing is important to identify features of equipment on an ICT network that may not comply with recognized industry standards, and may thus affect the quality of the network service provided. The availability of advanced high-quality products for commercial use contributes to the widespread deployment of network technologies and associated network services.

2.2 Review of critical issues/priorities in countries and regions

C&I issues are driven by a variety of concerns and problems, including but not limited to:[4]

- legacy intelligent network signalling (interoperability problems) services behaviour when replacing equipment, signalling in mobile networks (e.g. access, core, SMS);
- lack of conformity and interoperability between equipment from different vendors;
- non-standardized interfaces or protocols in equipment from different manufacturers;
- different software revisions in equipment from a single manufacturer, resulting in incompatible session initiation protocol (SIP)
- clients;
- conformity of set-top box (STB) equipment made by different Internet protocol television (IPTV) middleware manufacturers;
- bandwidth, namely the transmission capacity for voice, data and video as users overload the existing network;
- achievement of interoperability in complex networks through the integration of networks and devices;
- services launched by certain providers that do not provide infrastructure and support teams to enable interoperability with other operators;
- methodology for adopting standards;
- management of call detail records for billing;
- implementation of new features and services on all platforms;
- existence of different charging models;
- new technology that is not interoperable with legacy equipment;
- lack of testing centres and facilities;
- lack of trained personnel to undertake C&I tasks;

[4] ITU-D. Final Report on ITU-D Study Group 2 Question 4/2 for the study period 2014-2017. Assistance to developing countries for implementing conformance and interoperability programmes. ITU, 2017.

- ISDN support problems;
- user terminal problems for different systems;
- interoperability issues for services and terminal equipment used by customers;
- vendors using proprietary and non-standard interfaces;
- costs;
- lack of human resources capacity and training opportunities;
- weak institutional systems;
- lack of awareness on standardization;
- interoperability challenges.

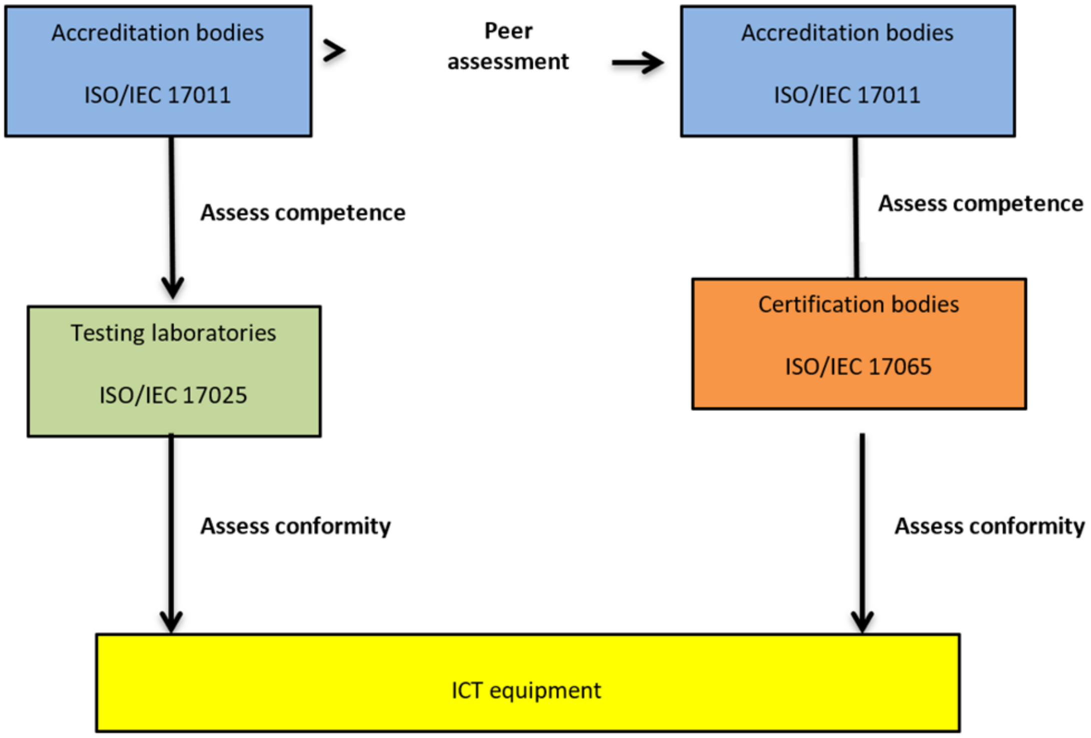
Conformity assessment activities

Conformity assessment activities include:

- appointment/recognition of accreditation bodies
- designation/recognition of certification bodies
- designation/recognition of testing laboratories
- registration/certification.

Conformity assessment activities are shown in **Figure 1**.

Figure 1: Conformity assessment activities



2.3 Technical requirements and standards

Service providers and operators specify the standards and requirements for equipment and systems that they use to provide services to their customers. National regulators establish regulations, standards and specifications for equipment and systems deployed in their territories.

Users, service providers and national regulators require evidence and proof that the equipment and systems conform to the appropriate standards and specifications, and that they are able to interoperate as specified.[5]

To foster the development of international standards, guides and recommendations, the World Trade Organization (WTO) Committee on Technical Barriers and Trade (TBT) established six principles:[6]

- transparency
- openness
- impartiality and consensus
- relevance and effectiveness
- coherence
- the development dimension.

The importance of standards

Conformity with technical standards:

- is essential for the interoperability of equipment and networks;
- reduces the risks of being locked into a particular technology or supplier;
- ensures that legitimate objectives are met, including those relating to safety and non-interference;
- contributes to regional integration;
- contributes to market aggregation, competitiveness and trade.

New procedures

New procedures include a combination of:

- manufacturers' declarations of compliance, compliance testing by commercial test houses, and market surveillance;
- global standards and MRAs on standards and approvals between countries or among groups of countries.

2.4 Mutual recognition arrangements/agreements on conformity assessment

2.4.1 What is a mutual recognition arrangement/agreement?

A mutual recognition arrangement/agreement on conformity assessment (hereafter MRA) is a voluntary arrangement/agreement (on procedures and processes) between parties (private or public entities) on the recognition of conformity assessment results.

A mutual recognition *agreement* constitutes a formal legal commitment by parties to recognize conformity assessment results for telecommunication equipment. It deals with regulatory requirements and it is referred to below as a "regulatory MRA". Such agreements are often made on a bilateral, regional or multilateral basis, by two or more governments.

[5] ITU. Establishing conformity and interoperability regimes: Complete guidelines. February, 2015.
[6] WTO. Committee on Technical Barriers to Trade. Document G/TBT/9. November, 2000.

A mutual recognition *arrangement* is a voluntary arrangement between parties to recognize conformity assessment results for telecommunication equipment. It deals with non-regulatory requirements and it is referred to below as a "non-regulatory MRA". An example of a mutual recognition arrangement is a commitment made by accreditation bodies to mutually recognize the conformity assessment results from accredited conformity assessment bodies.

Parties to an MRA are obliged to put in place processes and procedures to implement the MRA for their mutual benefit. This applies to both regulatory and non-regulatory MRAs.

An MRA does not undermine regulatory authority within the jurisdiction of the parties to the agreement/arrangement. The MRA should specify the various bodies involved in its implementation:

- *party*: An entity that has agreed to participate in the MRA;
- *designating authority*: A government authority or recognized competent body appointed by the party for the purpose of designating a conformity assessment body to assess conformity under the MRA;
- *accreditation body*: A body responsible for assessing and recognizing the specific competences of testing laboratories and/or certification bodies in accordance with international standards;
- *conformity assessment body*: A body designated to assess conformity to another party's telecommunication requirements under the MRA (it may be a third party or a supplier's testing laboratory or a certification body);
- *joint committee*: A committee established by the parties for the purpose of managing the drafting and implementation of the MRA, adjusting it as and when necessary, and addressing any other matters relating to the smooth operation of the MRA, including future changes and adjustments;
- *regulatory authority*: An entity with legal authority responsible for telecommunications.

2.4.2 Role of MRAs in the C&I regime

MRAs serve to:

- recognize the competence of third parties to carry out national regulatory/type-approval processes;
- avoid the cost of duplicate testing and promote transparency;
- facilitate access to foreign markets;
- cut time to market and production costs;
- tackle predatory practices and obstacles to market entry;
- streamline procedures and methods, and thus significantly reduce costs for producers who sell on multiple markets.

Ultimate goal: "one test, done once, valid worldwide".

2.5 Virtual infrastructure

2.5.1 Virtual testing[7]

In the ICT sector, services are increasingly being provided virtually, through the Internet. This new reality also applies to emerging mechanisms for assessing the connectivity of ICT equipment over IP networks, and is aligned with the requirements of new converged networks.

Virtual laboratories can offer timely, affordable and sustainable testing services to developing countries that lack testing capabilities of their own.

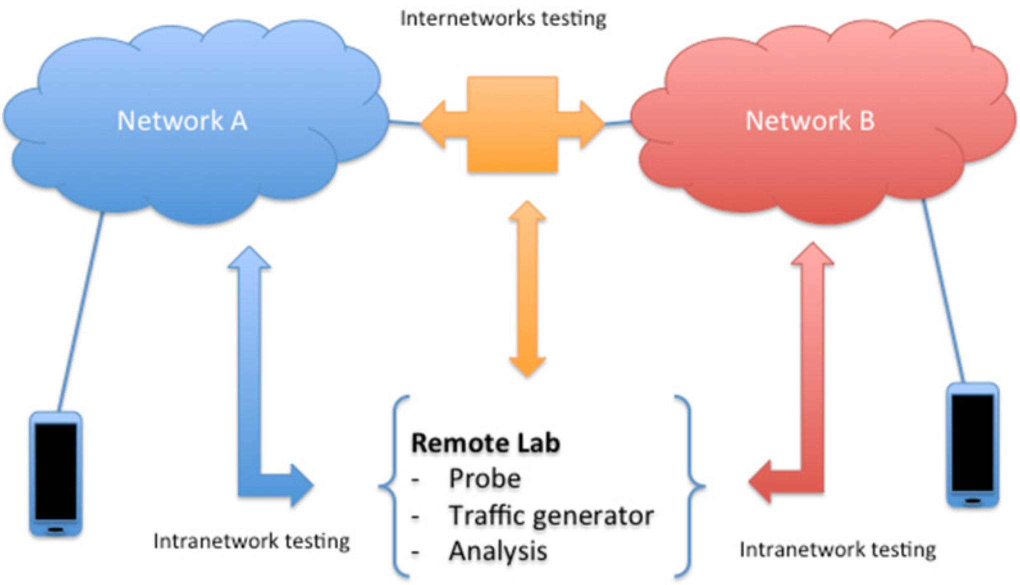
Two applications of virtual testing are described below: remote interoperability testing and remote type-approval testing.

2.5.2 Remote interoperability testing

Objective: *To assess the networks of operators in different countries/regions for interoperability*

Global experience has confirmed the need for standardized testing and certification procedures for ICT-based products and systems to prevent the numerous problems that are otherwise caused to users and operators.

Figure 2: Remote interoperability testing



Lack of interoperability can cause a host of problems, including:

- reduced communication rate;
- low communication reliability;
- shortened useful life of devices and equipment;
- high energy consumption;
- interference of one service with another (especially in wireless systems);

[7] ITU-D. Final Report on ITU-D Study Group 2 Question 4/2 for the study period 2014-2017. Op. cit.

- substandard equipment, hampering evolution and compatibility with new technologies and protocols;
- equipment incompatibilities resulting in communication bottlenecks (often very difficult to diagnose);
- fluctuations in network performance owing to lack of procedures for monitoring changes in equipment and software;
- interconnection difficulties between equipment from different manufacturers and between national networks.

Concrete objectives of remote testing may include: product development, regulatory authority certification, pre-conformance and interoperability testing for ICT products, compliance evaluation for mobile devices and IP protocols, and field service.

Target audience: telecommunication operators, equipment manufacturers and users (variety of needs – customers, operators, associations and regulators, etc.).

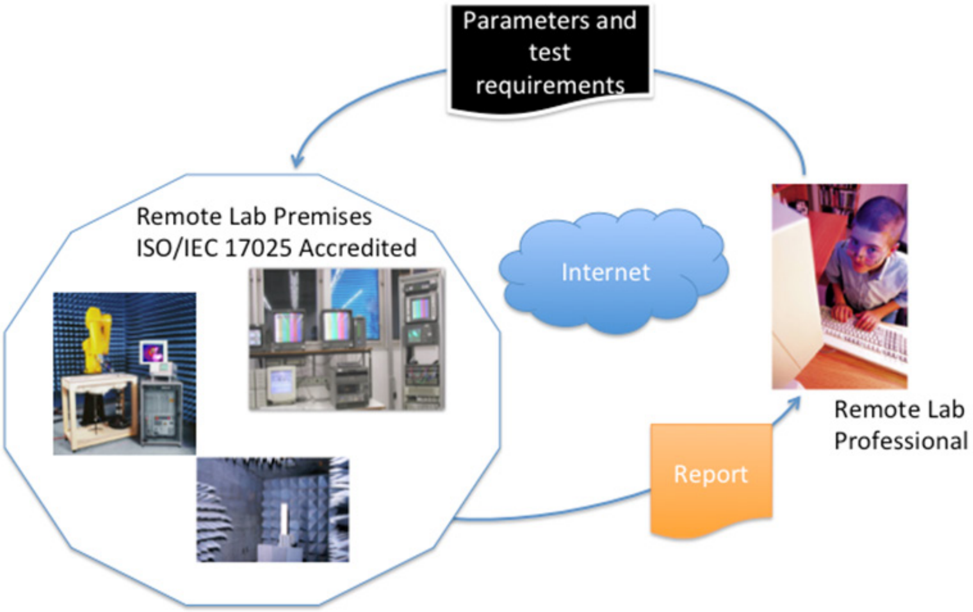
A strong, close partnership with major manufacturers of testing and measurement systems is desirable, to ensure the infrastructure can be updated rapidly when required.

2.5.3 Remote type-approval testing

Objective: *To provide access to physical test infrastructure at a distance for the purposes of type approval.*

Remote type-approval testing allows laboratory development, pre-conformance, conformance and interoperability testing of samples of ICT products by remote or virtual means using the infrastructure of other labs. The samples will be supplied by other entities (community involvement).

Figure 3: Remote type-approval testing



The level of laboratory services provided can be adapted through several phases:

- Phase 1: Remote training.

- Phase 2: Conducting tests on the samples with video transmission of each step and sending data for composition of reports.
- Phase 3: The local laboratory is increasingly involved in testing certain types of products, in particular core network products (to maximize the benefit in terms of addressing core infrastructure needs).
- Phase 4: Infrastructure is provided for remote testing (investments in suitable test measurement infrastructure).
- Phase 5: Consulting and training to prepare for moving to local acquisition of testing infrastructure (if judged advisable).

Requirements: applicable standards, testing, screening, etc.

2.6 Market surveillance

The objective of market surveillance of deployed telecommunication equipment is to ensure that products brought onto the market do not cause electromagnetic interference, damage the public telecommunication network, endanger public health or safety or harm public interest in any other way. In practice, market surveillance covers any measures (including prohibition, withdrawal or recalls) necessary to stop the circulation of products that fail to comply with the requirements set out in the relevant legislation and regulations, ensure product compliance, and impose sanctions. Market surveillance is vital to the smooth functioning of the telecommunication marketplace. It is essential to protect consumers and workers against risks posed by non-compliant products. In addition, market surveillance helps to protect responsible businesses against unfair competition from unscrupulous economic operators who ignore the rules or cut corners. Many regulatory bodies throughout the world have specific legal requirements relating to the organization of market surveillance. Regulations typically set out clear obligations for market-surveillance authorities, including that they must have the necessary powers, resources and knowledge to properly perform their functions. Procedures must be put in place for following up complaints, monitoring accidents, verifying that corrective action has been taken and gathering scientific and technical knowledge concerning safety issues.

2.6.1 Key stakeholders

The key stakeholders are:

- governments/regulators
- accreditation bodies (ABs)
- conformity assessment bodies (CABs)
- manufacturers, importers, vendors and service providers.

2.6.2 Consultations on market-surveillance intelligence and experience

Activities include:

- Sharing information and consulting with other countries that have established market-surveillance and enforcement programmes, particularly within the region, where there is a common language and perhaps common spectrum management and frequency assignments for services.
- Sending notices or advance warnings to partners regarding compliance problems with technologies and products which may be deployed early in a particular country or region, alerting partners to potential compliance issues when the products or technologies are

deployed more broadly and making it possible to target inspection and audit efforts more precisely.

2.7 Conformance assessment of new technologies

As ICT services and applications are used in all aspects of people's lives and the proliferation of new technologies (IoT, 5G, etc.) becomes a reality, conformance and interoperability will pose a serious problem for developing countries, if they fail to prepare in time.

The anticipation of a future where everything is connected is driving demand for C&I. Developing countries are looking for innovative ways to meet the challenges that arise, including by:

- establishing common technical requirements;
- identifying the main technical points of reference at the international level (standards);
- developing policies for robust C&I frameworks to promote collaboration in a multistakeholder ICT environment (e.g. through the establishment of mechanisms including the acceptance of suppliers' declarations and mutual recognition agreements).

2.7.1 New technology challenges

The challenges include:

- Impact of interoperability issues on scaling efforts:
    - awareness at the regulator level
    - perception of regulations as a barrier to entry
- Developer awareness and perception of C&I:
    - monetary cost
    - safety and human cost
- Limited funding and resources for projects/products:
    - certification costs
    - markets still in their infancy.

2.7.2 Pre-compliance testing

Pre-compliance testing requires:

- Awareness of C&I:
    - relevant to specific product design
    - at each stage of a product's journey to market
- Awareness of the impact of C&I:
    - appreciation of the costs (monetary, time, technical) to a start-up
    - regulations as a benefit rather than a barrier.

2.7.3 Intended impact[8]

C&I can improve the prospects for success by:

- facilitating a smart product mix;
- incorporating C&I from the outset;
- knowing what people and resources will be needed and when.

It can help regulators boost emerging products and businesses by:

- advocating cross-cutting MRAs;
- promoting informed engagement with entrepreneurs.

[8] ITU. Topical session for Question 4/2. 16 October 2019.

Chapter 3 – Combating the proliferation of counterfeit, substandard and tampered devices

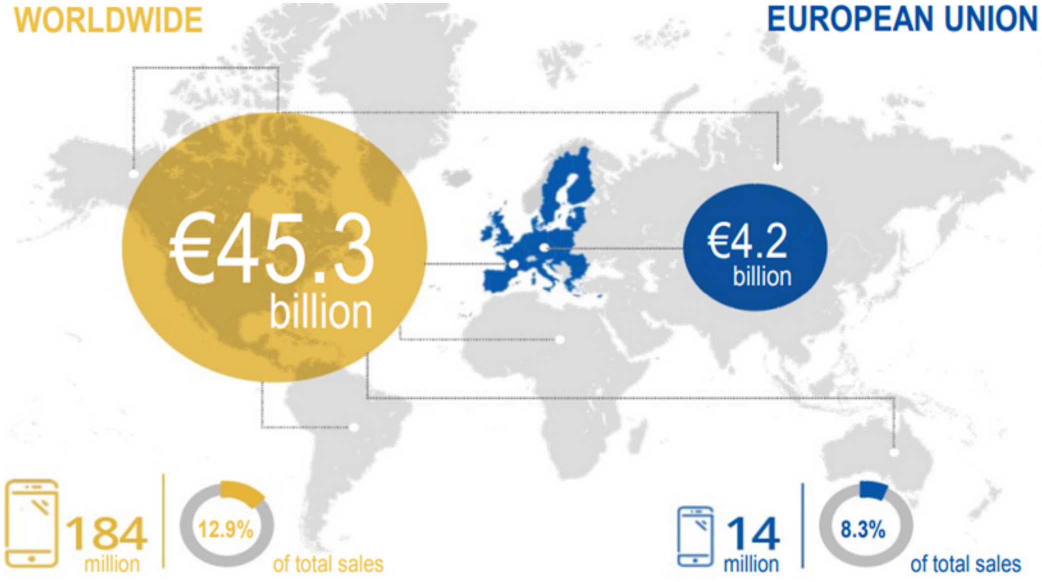
Today, the counterfeit ICT market and the trade in counterfeit mobile devices is a global socio-economic problem with negative repercussions for innovation, investment, economic growth, health and employment. There is also a danger of resources being diverted to organized crime.

The 2017 World Telecommunication Development Conference (WTDC-17) in its Resolution 79 (Rev. Buenos Aires, 2017) identified the fight against the proliferation of counterfeit equipment and devices as a priority under Question 4/2. This chapter describes the problems caused by counterfeit telecommunication/ICT devices and offers guidelines for identifying and combating their use.

3.1 Problems and issues

The counterfeiting of telecommunication/ICT equipment, especially mobile phones, is a global challenge for users, manufacturers and governments, as well for innovation, investment and economic growth. The European Union Intellectual Property Office (EUIPO) has estimated the revenue loss to smartphone sales due to counterfeits at EUR 45.3 billion in 2015.[9]

Figure 4: Lost sales due to fake smartphones: EU and worldwide



On the user side, the incentives driving the proliferation of counterfeit terminals include:

- Counterfeit and tampered devices may be more affordable than genuine ones and offer access to networks.

[9] EUIPO. Study on fake smartphones. October 2018.

- Such devices offer users convenient functionalities such as multiple SIM cards, TV, FM radio and various convenient mobile Internet services (chat, video calls, web browsing, money transfers, etc.) at a low cost.

The negative impact of counterfeit terminals on human health, on the quality of networks and services and on finances arises from a number a number of factors, including the following (non-exhaustive list):

- unreliable devices posing a threat to human health and the environment due to hazardous components (e.g. lead or cadmium), a high specific absorption rate (SAR) or batteries that are an explosion hazard;
- degraded quality of service (QoS) including voice accessibility problems, dropped calls, mobility problems (handover) and lower speed;
- financial losses for manufacturers of genuine terminals (loss of sales, negative impact on price);
- fiscal losses (customs revenue and taxes);
- copyright and trademark violations, unfair competition;
- loss of warranty and technical support;
- disruptions to telecommunication network performance, such as loss of control over power.

On the network performance issue, a report by Qualcomm[10] demonstrated how counterfeit equipment has a negative impact on networks by:

- reducing network capacity: long-term evolution (LTE) data capacity has been reduced by 23 per cent, high-speed packet access (HSPA) data capacity by 6 per cent, and Universal Mobile Telecommunications System (UMTS) voice capacity by 27 per cent.
- reducing support available for the latest LTE features, such as LTE-CA (carrier aggregation), MIMO (multiple-input and multiple-output) 4x4 and 256 QAM (quadrature amplitude modulation), with a negative impact on the overall user experience;
- increasing network site count requirements, which entails capital and operating expenses, negatively impacting the business case for mobile operators.

Problems relating to counterfeit devices with invalid IMEI codes include:

- Difficulties in identifying and blocking counterfeit mobile devices, as many have legitimate-looking IMEI codes. Counterfeiters customarily use IMEI number ranges in their products that correspond to those of legitimate device manufacturers, making it difficult to distinguish between legitimate and counterfeit products.
- Threats to public security. Such devices could potentially facilitate criminal activities and terrorism.
- Disruptions caused by the blocking of sold counterfeit devices often penalize users, rather than those who trade in fake products.

3.2 Definitions

- **Terminal**: Equipment connected to a telecommunication network to provide access to one or more specific services (Recommendation ITU-R V.662-3).[11]
- **IMEI** (International Mobile Equipment Identity): A unique code allocated to each IMT-2000 mobile terminal by the manufacturer and used to identify the IMT-2000 terminal to the network for the purpose of terminal equipment validation or similar tasks.

[10] Qualcomm. Combating mobile counterfeiting and theft. October, 2018.

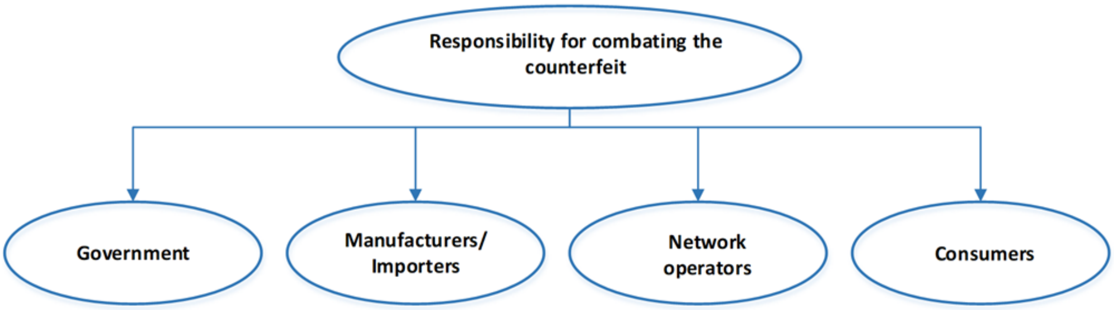
[11] ITU Radiocommunication Sector (ITU-R). Recommendation ITU-R V.662-3 (05/2000). Terms and definitions.

- **EIR** (Equipment Identity Register): A register to which user equipment identity may be assigned for record purposes. The nature, purpose and use of this information is an area for further study.
- **Whitelist**: A register of the devices authorized for use in a country (including devices that have been legally imported or manufactured in that country).
- **Blacklist**: A register of devices for which services must be denied on the telecommunication network.

3.3 Guidelines

It is important for all stakeholders (i.e. governments, manufacturers, network operators and consumers) to work together to fight the proliferation of counterfeit telecommunication/ICT equipment.

Figure 5: Responsibility for combating counterfeiting



Collaboration is essential for establishing a regulatory and technical framework to combat the proliferation of counterfeit products. To that end:

- Governments and regulators should develop regulatory frameworks that implement standard procedures and deploy a technology platform to enforce regulations; organize awareness-raising campaigns, in particular on risks for users of counterfeit devices, such as health risks and poor QoS; and promote market surveillance to prevent trade in black-market devices.
- Governments should consider lowering taxes and fees on legitimate imported ICT devices. This may also reduce the cost of ownership.
- At the national level, regulators should work with manufacturers and network operators to determine the extent of counterfeit device use on the local market.
- Customs and security services should be given the resources necessary to combat illicit traffic and verify the legitimacy of identifiers on devices at the point of import.
- Manufacturers and importers should register all imported and locally manufactured equipment and respect the type-approval procedures established by the regulator.
- Manufacturers should enhance the security of IMEI codes by complying with the technical design principles for IMEI security implementation and participating in the GSM Association (GSMA) process for reporting and correcting IMEI security vulnerabilities.
- Operators can contribute to the fight against the proliferation of counterfeit devices by: providing device network data to the regulator and government stakeholders; setting up an EIR database to support IMEI blacklist and whitelist functionality so as to deny access to counterfeit devices; and informing subscribers of their devices' status by SMS, if necessary.
- Customers can contribute by verifying the legitimacy of the devices they plan to purchase by referring to verification services provided by other stakeholders; registering individually imported devices; and reporting counterfeit devices to the authorities.

- A conformity assessment regime should be established, as well as a centralized national database that contains all device information (identifiers, technical specifications, device lifecycles, and so on) to contribute to effective market surveillance.

The experience of countries such as Rwanda (see **Section 3.4.4**) suggests that, at the regional level:

- It is important to conclude mutual recognition agreements between countries for conformity assessment and market surveillance.
- A centralized equipment control system could significantly reduce the number of counterfeit and substandard devices entering the market.
- Regionally recognized test centres could aid significantly in implementing conformity assessment through certification and supplier declarations of conformity.

3.4 National experience (case studies)

Contributions from Member States and stakeholders have been vital in the preparation of this report. The contributions draw on national experience, data and existing practices to combat the proliferation of counterfeit devices.

All contributors agree on the need to establish enforceable political, legal and regulatory frameworks.

Some contributors propose using existing technical solutions, such as international standards and market-surveillance techniques, and establishing central databases and platforms to block counterfeit devices.

Additionally, several contributors propose broadening efforts to the regional and subregional levels, in order to pool different techniques for fighting the counterfeiting of devices.

3.4.1 Madagascar

In Madagascar, 25 per cent of active devices on mobile networks are counterfeit products.[12]Even if these devices provide certain benefits, being affordable, offering access to universal services and reducing the digital divide, those advantages are outweighed by the various risks they pose to human health (e.g. hazardous emission levels), to operators (QoS, interference, etc.) and to the country's economy.

In order to prevent digital development having a detrimental impact on human health and the economy, Madagascar has adopted measures to:

- increase user awareness of the dangers of counterfeit devices;
- shut down black markets and enforce customs measures;
- prohibit counterfeit terminals and ensure certification of imported ICT equipment;
- use a platform to analyse and identify IMEI codes and block counterfeit devices as of 30 June 2019.

[12] ITU-D SG2 Document 2/45 from Madagascar.

3.4.2 Guinea

The contribution from the Government of Guinea highlights concerns relating to the certification of telecommunication equipment and infrastructure, and the interoperability of telecommunication services.[13] Since 2015, the government has promulgated telecommunication laws that have restructured the sector. The reforms have brought benefits such as increasing the telephone pool, improving QoS, increasing the sector's contribution to the gross domestic product, and providing control in the digital market and certification sector.

The government has laid down very strict rules for the certification of telecommunication equipment, with countermeasures and sanctions to deter offences. The Regulatory Authority for Posts and Telecommunications (ARPT) assesses terminal equipment for conformity with core requirements, demanding very detailed administrative and technical submissions before conformity certificates are issued. The measures taken in Guinea include:

- rigorous and ongoing monitoring of ITU work on standardization;
- action by a range of actors, including ARPT, customs, tax authorities and ministries;
- approval of telecommunication equipment, granted for a renewable period of five years;
- establishment of a labelling system for approved equipment;
- seizure of equipment or dismantling of facilities involved in counterfeiting, at the offender's expense;
- confiscation of counterfeit equipment, as ordered by a competent court;
- penalties for failure to register: anyone holding terminal equipment or radio equipment within the meaning of the law with a view to its sale or distribution free of charge or for payment, or selling such equipment, and anyone connecting such equipment to a public telecommunication/ICT network in violation of the certification regime or without prior approval, is liable to a fine of between GNF 10 million and GNF 200 million;
- doubled fines for repeat offences.

3.4.3 Senegal

In addition to effectively combating piracy, counterfeiting and the theft of telecommunication/ICT devices, and taking steps to adapt to changes in the legal environment, the Government of Senegal has undertaken important initiatives in collaboration with continental and intercontinental communities, multinationals, telecommunication and ICT regulators and Internet service providers (ISPs) to fight against this modern scourge, which is an obstacle to technological innovation, job and wealth creation and foreign direct investment.[14]

Senegal has put in place measures of a legislative and regulatory nature and taken other steps to improve the protection of individual property, including:

- a legislative framework based on a series of laws;
- a regulatory framework based on a series of decrees;
- a national brigade for combating piracy and counterfeiting;
- the Senegalese Agency for Industrial Property and Technological Innovation;
- the Regulatory Authority for Telecommunications and Posts (ARTP);
- the national customs authority;

[13] ITU-D SG2 Document SG2RGQ/9(Rev.1) from Guinea.

[14] ITU-D SG2 Document SG2RGQ/66(Rev.1) from Senegal [in French].

- the involvement of national and multinational manufacturers and distributors of telephones, tablets, smartphones and decoders.

3.4.4 Rwanda

Aware of the danger that counterfeit devices pose to the consumer, the industry and the economy, the Government of Rwanda has developed a strategy to combat the proliferation of counterfeit devices and has set out a roadmap at the regional level, together with Member States belonging to the East African Community (EAC).[15] The government's proposals include:

- Mutual agreements among EAC Member States: Reviewing the legal and regulatory instruments of Member States with a view to concluding mutual recognition agreements for conformity assessment and enhanced market surveillance.
- A centralized monitoring system: Establishing a real-time control system based on EIR SIM Lock, IMEI pre-authorization, IMEI authorization and EIR alert as the best approach to fighting the proliferation of illegal devices at the regional level.
- Regional testing centres: Setting up accredited regional testing centres would facilitate conformity assessment in EAC Member States through certification with the supplier declaration of conformity. This will cut the cost of certification for regional assembly plants and reduce the cost of the final product. The establishment of mutual agreements among countries will facilitate the creation of specialized labs in different countries.

3.4.5 Zimbabwe

All mobile network operators in Zimbabwe have the capability to detect counterfeit devices with duplicate IMEI codes on their networks and to disconnect them. However, given the importance of counterfeit devices for operator revenues – these devices account for the majority of network users – actual disconnection is rare.[16] Nevertheless, the following measures have been taken in Zimbabwe to combat the proliferation of counterfeit devices and the theft of mobile devices:

- prohibition on the use of any device not meeting type-approval requirements;
- obligation for mobile network subscribers to register newly purchased SIM cards with the mobile network operator (MNO) before the card can be activated on the network;
- acquisition of a subscriber registration database to ensure that all SIM cards activated in the country are correctly registered, which also facilitates the detection of counterfeit devices and fake mobile phones;
- testing and certification of all new ICT devices at the regional level by an independent testing laboratory operated by the Independent Communications Authority of South Africa (ICASA).

3.4.6 Ghana

In Ghana, type approval is used to protect telecommunication/ICT devices, users and networks.[17] To that end, the National Communications Authority (NCA) has created a type-approval regime to certify and test communication equipment to ensure compliance with international standards:

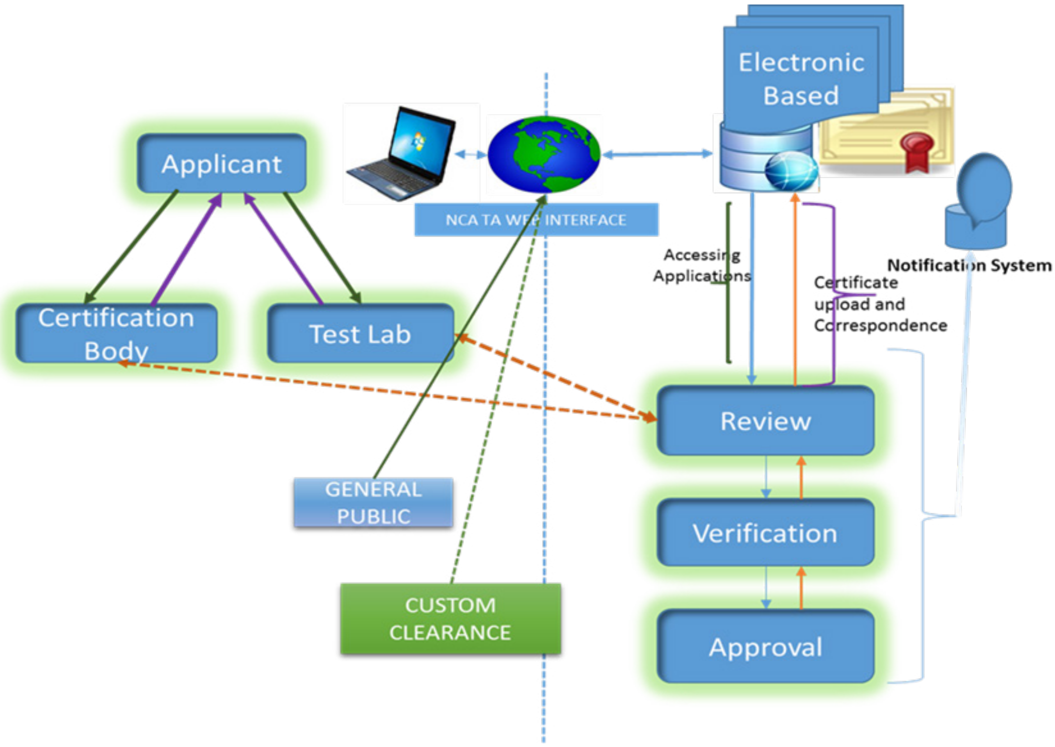
- implementation of an approval procedure based on technical documentation which contains test reports and compliance requirements relating to consumer protection,

[15] ITU-D SG2 Document SG2RGQ/69 from Rwanda.
[16] ITU-D SG2 Document SG2RGQ/85 from Zimbabwe.
[17] ITU-D SG2 Document SG2RGQ/82 from Ghana.

environmental protection, network disruption, integrity and interoperability, as well as provisions to ensure conformity with the National Frequency Allocation Plan;

- attribution of the type-approval certificate (TAC) and NCA mark, with details of the equipment published on the NCA website;
- implementation of a dealership licensing system, integrated into the approval regime, to streamline the activities of electronics and communication equipment (ECE) dealers and to ensure that only approved ICT devices are used;
- arrangements to strengthen national market surveillance;
- establishment of testing laboratories for measurements relating to specific absorption rate (SAR), electromagnetic field (EMF), digital terrestrial television (DTT) and radio frequency and signalling (RF&Sig).

Figure 6: The type-approval process

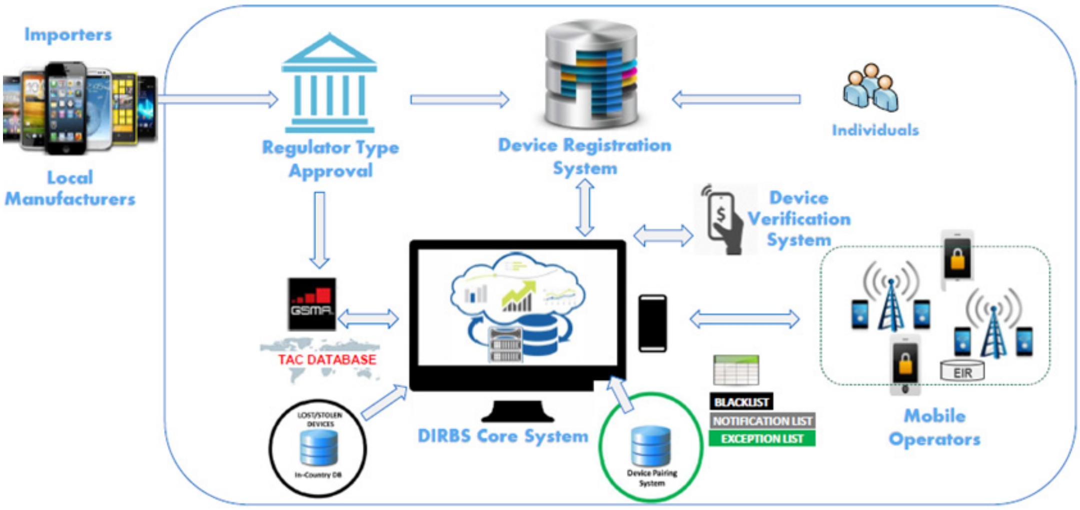


3.4.7 Pakistan

The Pakistan Telecommunication Authority has launched, in collaboration with Qualcomm, an open-source technology platform called the Device Identification, Registration and Blocking System (DIRBS) to ensure that only approved, legal devices can operate on mobile networks in the country.[18] DIRBS allows the identification of all devices; captures an installed base of devices; monitors all new device activations; addresses illegal and counterfeit devices, including mobile theft; and allows for exceptions/amnesties.

[18] More information on DIRBS is available on the websites of the Pakistan Telecommunication Authority (PTA) and the Pakistan Federal Board of revenue (FBR).

Figure 7: Device Identification, Registration and Blocking System (DIRBS)



3.4.8 The GSM Association

The GSM Association (GSMA) manages the International Mobile Equipment Identity Database, a global central database containing basic information on the serial number (IMEI) ranges of millions of mobile devices.[19]

GSMA provides a "device check" service to device traders, recyclers and insurers, and to law-enforcement agencies (in some markets, consumers can also access the service directly). It allows users to find out instantly whether a device has been reported lost or stolen through the device status registry, as reported to GSMA by its mobile network operator members worldwide.

GSMA seeks to connect as many MNOs as possible to the IMEI database.

In September 2016, the GSM Association partnered with the World Customs Organization (WCO) to combat counterfeiting and fraudulent mobile commerce. The integration of the IMEI database will facilitate the cross-checking and filtering of counterfeit devices identified by their IMEI at the point of import.

3.4.9 Brazil

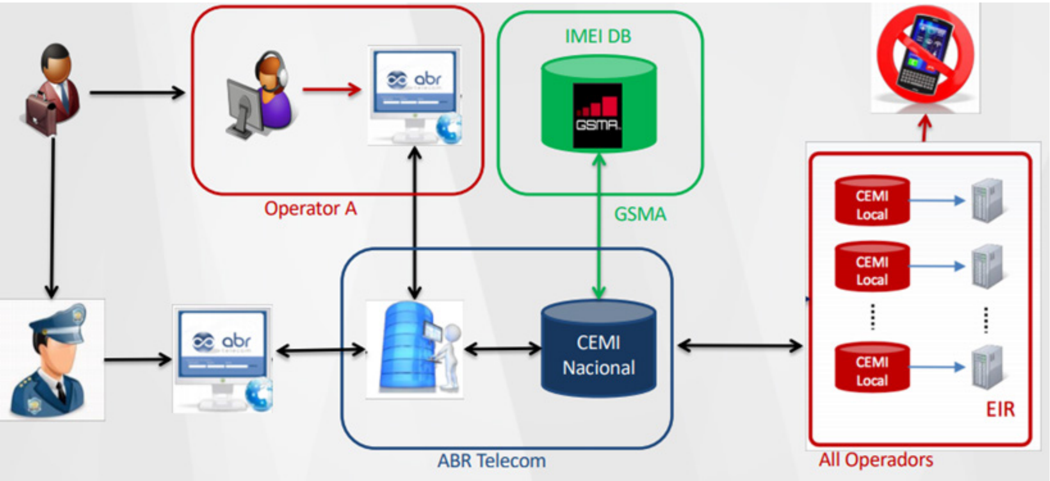
To combat the use of stolen, falsified and uncertified unique identifiers, the Government of Brazil has launched the *Celular Legal* initiative, coordinated by the *Agência Nacional de Telecomunicações* (ANATEL) and involving all stakeholders.[20] The measures implemented under that initiative are organized around two modules:

- The CEMI module (*Cadastro de Estações Móveis Impedidas*) allows mobile operators and the police to block stolen devices at the request of the user.

[19] ITU-D SG2 Document SG2RGQ/80 from the GSM Association (GSMA).

[20] João Zanon. Combating the use of stolen and counterfeit ICT devices. *ITU-D Workshop on combating counterfeit ICT devices*, Geneva, 4 October 2018.

Figure 8: CEMI workflow



- The SIGA module (*Sistema Integrado de Gestão de Aparelhos*) is used to identify and block devices linked to other types of fraud: tampering, cloning, non-certified devices, irregular unique identifiers, etc. *Celular Legal* has an online tool that can check the status of a device based on its IMEI code.[21]

3.4.10 Oman

Of the mobile devices registered on the national network of Oman, almost 2 million have invalid IMEI codes. Some IMEI numbers have been repeated almost 10 times, because more than 10 devices carry the same IMEI.[22] This creates a technical problem in terms of registering these devices on local networks and increases the financial burden on consumers in general, by undermining confidence in these products.

Regulators are keen to ensure that all off-the-shelf ICT devices from dealers and importers fully comply with relevant orders and decisions issued by the regulatory authority. To this end, the Telecommunications Regulatory Authority (TRA) inspection body is responsible for ensuring compatibility and compliance with applicable standards and technical specifications for ICT equipment sold on the national market.

The TRA has set up a helpline together with local operators to enable customers to verify IMEI codes. Still, the organization faces difficulties, including the lack of access to an international database of IMEI codes, because full access to the GSMA database is not granted to regulators, but only manufacturers and operators in a given country.

3.4.11 International standards and recommendations

- ISO 12931:2012: Performance criteria for authentication solutions used to combat counterfeiting of material goods.
- ISO 16678:2014: Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade.
- ITU-T Q.5050 (03/2019): Combating counterfeiting and stolen ICT devices.
- ITU-T Y.4808 (08/2020): Digital entity architecture framework to combat counterfeiting in IoT.

[21] *Agência Nacional de Telecomunicações* (ANATEL). Celular Legal.
[22] ITU-D SG2 Document 2/326 from Oman.

Chapter 4 – Mobile device theft

4.1 Introduction

Growth in the use of mobile devices worldwide has been accompanied by an increase in the use of stolen devices, both domestically and across borders. Global initiatives are needed to keep stolen devices off networks around the world.

The scale of harm that the use of fraudulent devices is causing throughout the ecosystem has made governments and industries take a growing interest in the search for remedies. Governments are implementing regulations that address a wide range of issues, including:

- mobile theft
- security risks
- tax revenue losses
- consumer privacy
- network quality
- intellectual property rights.

For many years, GSMA has been a leader for industry initiatives involving the sharing of data to block stolen or lost mobile devices from accessing networks worldwide. Using the unique IMEI code, GSMA manages a blacklist of suspect devices (i.e. those reported as lost or stolen), which is made available to operators all over the world.[23]

4.2 Problems and issues

Device theft is a global problem that requires cross-border alignment and action to make theft economically unattractive. Although industry initiatives have had a positive impact, further efforts are needed as most activities to date have been based on global non-proprietary standards and certain countries have yet to align their efforts on global industry practice. In that regard, countries need to have a unified approach for global alignment with industry efforts. Lack of action undermines the effectiveness of some of the measures implemented.

The requirements for addressing device theft fall under the following headings.

Regulations and enforcement

- Develop a regulatory framework
- Implement standard operating procedures
- Deploy and administer a technology platform to enforce regulations
- Conduct awareness-raising campaigns.

Technical platform

- Classify existing devices:
  - analyse device data from network information

[23] ITU-D SG2 Document SG2RGQ/80 from GSMA.

  - classify devices by IMEI (valid/invalid, unique/duplicate)

- Allow existing devices:
  - pair existing fraudulent IMEI codes with International Mobile Subscriber Identity (IMSI) codes and Mobile Station International Subscriber Directory Number (MSISDN)
- Register new devices:
  - require type approval with unique device identifiers
  - register imported and locally produced devices with valid and unique identifiers only
- Detect IMEI code falsification:
  - analyse network data
  - identify devices with fraudulent IMEI codes
- Enable network blocking:
  - monitor access of non-compliant devices/non-registered devices through network control.

Technical system implementation[24]

- convenience for all stakeholders, especially consumers
- a standalone system alleviating the need for mobile network integration and interoperability that entail unnecessary costs, capacity constraints and resource burdens on operators
- no requirement for strict device-customer binding
- flexibility/configurability to adapt to national regulations without the need for customization.

4.2.1 Device crime and fraud

Device crime and fraud have a negative impact on various groups of stakeholders:

- Consumers: Risk of harm in connection with theft, property loss, loss of personal information
- Governments: More crime, lower tax revenue
- Traders: Unwitting purchase of stolen goods, network performance issues
- Insurers: Increased underwriting costs, transfer of title to stolen goods
- Operators: Subscriber churn, subsidy loss, insurance underwriting costs
- Law enforcement: Organized crime, drain on resources.

4.2.2 Stakeholders' roles and responsibilities

Various stakeholders can play an important role in the fight against device theft.

Governments can develop a regulatory framework, implement standard operating procedures, deploy and manage technology to enforce regulations, and conduct awareness-raising campaigns.

[24] Mohammad Raheel Kamal. An Open Source CEIR to Combat Counterfeit and Stolen ICT Devices. *Third ITU-T Study Group 11 Regional Workshop for Africa on "Counterfeit ICT devices, conformance and interoperability testing challenges in Africa"*, Tunis, 30 September 2019.

Manufactures/importers can obtain device type approval from the government/regulator, register all devices to be imported, and register all locally manufactured devices.

Operators can provide device-related network data to the government, ensure Equipment Identity Register (EIR) support, support blacklisting of valid/invalid IMEI codes and allow exceptions, and notify subscribers of their device status via SMS as required.

Consumers can verify their device status (via SMS, application or web interface), register individually imported devices, report device theft to the authorities, and submit proof (invoices) for genuine devices, if required.

4.2.3 Essential tools to combat device theft

To fight against device theft, various things can be done at the network level and the device level.

Device-based protection:

- capability to delete contacts and photos and block mobile payments
- factory reset functionality to wipe all data
- remote wipe function.

Network-based protection:

- block stolen phone from accessing the network.

Device status checking:

- check device status before recycling
- make phone theft unprofitable.

4.3 Guidelines

Multistakeholder involvement

Users can report stolen devices to their network operators, enable antitheft features on their devices and, in countries where operators are connected to the GSMA IMEI operator blacklist, users can be encouraged to check the IMEI status of used devices that they plan to buy.[25]

Mobile network operators can block stolen devices from their networks and connect to the GSMA IMEI operator blacklist to share and collect blacklist data and encourage their device suppliers to adequately protect the integrity of the IMEI implementations in their products.

Device manufacturers/brand owners can ensure the integrity of the IMEI codes in all of their products, design more secure devices (i.e. make it impossible to reprogram IMEI codes) and implement kill-switch functionality to allow users to remotely disable lost and stolen devices.

App store operators can obtain the IMEI codes of stolen devices from GSMA and use them to deny app store access to devices that have been reported stolen.

[25] James Moran (GSMA). Combating device crime together – Best practice to combat mobile device theft. *ITU Workshop on Global approaches on combating counterfeiting and stolen ICT devices*, Geneva, 23 July 2018.

All stakeholders (governments, manufacturers, network operators and consumers) must work together to fight against the theft of mobile devices, in particular through:

- engagement with and involvement of law enforcement;
- policing of distribution channels to tackle trafficking of stolen devices;
- legislative and judicial support for antitheft initiatives;
- focus on devices, minimal inconvenience for users;
- renewed emphasis on collective efforts, with all countries playing their role;
- measures to support existing capabilities rather than replicating/undermining them;
- measurement and reporting on the effectiveness of the approaches adopted;
- analysis of action taken to determine what works and what doesn't;
- adoption of emerging technologies and solutions to bridge gaps.

Governments and regulators must work together to ensure that:

- operators deploy EIRs to block stolen devices on local networks;
- best-practice guidelines for blocking devices and sharing data are followed;
- operator EIRs connect to the IMEI database to ensure international blocking;
- IMEI security levels are strengthened and problems are reported and resolved;
- IMEI codes are checked by law-enforcement officials, customs officers, retailers and consumers;
- enforcement action is taken against criminals (IMEI tampering, theft and trading);
- measures are taken to educate consumers and promote kill-switch capabilities;
- measurement metrics to track the progress of these efforts are agreed and reporting is instituted.

4.4 National experiences (case studies)

4.4.1 Central African Republic

As part of its ICT infrastructure development policy, the Government of the Central African Republic has opened up the ICT market to four mobile operators and one fixed operator to ensure maximum coverage of the national territory and to offer quality services to the population.[26]

Failures in the implementation of this policy by the Regulatory Authority for Electronic Communications and Posts (ARCEP) have led to the unregulated development of infrastructures, difficulties in checking the conformity and interoperability of ICT equipment, and a rise in counterfeiting and theft of mobile terminals. Investment and sector revenue have suffered as a result.

To address these problems, the Government of the Central African Republic has:

- adopted and promulgated the Electronic Communications Law and its implementing texts;
- adopted and promulgated the law to establish the Regulatory Authority for Electronic Communications and Post (ARCEP);
- drafted the cybercrime and cybersecurity bill;
- created a trafficking control, antifraud and location centre for mobile terminals;

[26] ITU-D SG2 Document SG2RGQ/144 from the Central African Republic.

- established the Permanent Secretariat for the Governance of Electronic Communications to ensure technological monitoring;
- completed the international fibre-optic infrastructure backbone project connecting the capital city Bangui with the Republic of the Congo and Cameroon;
- implemented the national digitalization project *Centrafrique digital 2025*;
- implemented a national strategic plan for the development of very high-speed broadband infrastructures;
- created a national ICT agency and a national data centre.

The Central African Republic recommends that ITU provide assistance and support to help countries build capacity with regard to compliance and interoperability programmes and to deal with counterfeit products and mobile equipment theft.

4.4.2 Mexico

To combat the theft of mobile terminal equipment, the Federal Institute of Telecommunications (IFT), the national regulatory body for telecommunications and broadcasting of Mexico, has put in place regulatory obligations. Several initiatives have been launched at the national and international levels to control IMEI codes.[27]

At the international level, the Government of Mexico, through its ministries and departments, has signed bilateral and regional conventions to exchange information on the IMEI codes of stolen or lost devices and prohibit their reuse. An agreement has been concluded with GSMA to implement the IMEI device check system, allowing users of mobile devices to check the GSMA IMEI number database in real time.

At the national level, IFT published in the Official Journal a technical provision (IFT-011-2017) with guidelines for collaboration on security and justice, relating to the suspension of service for mobile terminal equipment or devices reported stolen or lost. IFT strengthened this collaboration with the implementation of technical provisions, including specifications for mobile terminals connected to telecommunication networks and compliance control:

- conformity assessment;
- update of the conformity certificate;
- database of IMEI codes of approved devices;
- control of compliance with certification requirements.

IFT checks compliance with the requirements of the above-mentioned technical provision by following the test methods described in the provision.

4.4.3 Iran University of Science and Technology

To prevent fraud and combat the sale and use of illegal devices, including stolen phones and phones for which customs fees have not been paid, the Islamic Republic of Iran in 2017 developed a mobile phone registry plan.[28]

When the device is turned on to access a service, it is evaluated; if the required information is not available on the legal list, the device will be identified as illegal and added to a blacklist.

[27] ITU-D SG2 Document 2/166 from Mexico.

[28] ITU-D SG2 Document 2/83 from the Islamic Republic of Iran.

Under the comprehensive trade system of the Islamic Republic of Iran, imported phones are registered at customs borders, with each handset assigned a unique activation code. The Iran University of Science and Technology has developed the HAMTA system, an online database which permits the activation of the device with a unique code and provides users with two main features:

- reporting the status of currently active mobile phones in the country, confirming the authenticity of a mobile phone and verifying that the unit is legal and activated;
- activating new and legally imported phones.

The data on registered equipment in the HAMTA system is transmitted to the Communications Regulatory Authority of the Islamic Republic of Iran and mobile operators. Only registered devices authenticated by the HAMTA system are considered legal and allowed to access services provided by operators; all others are blacklisted.

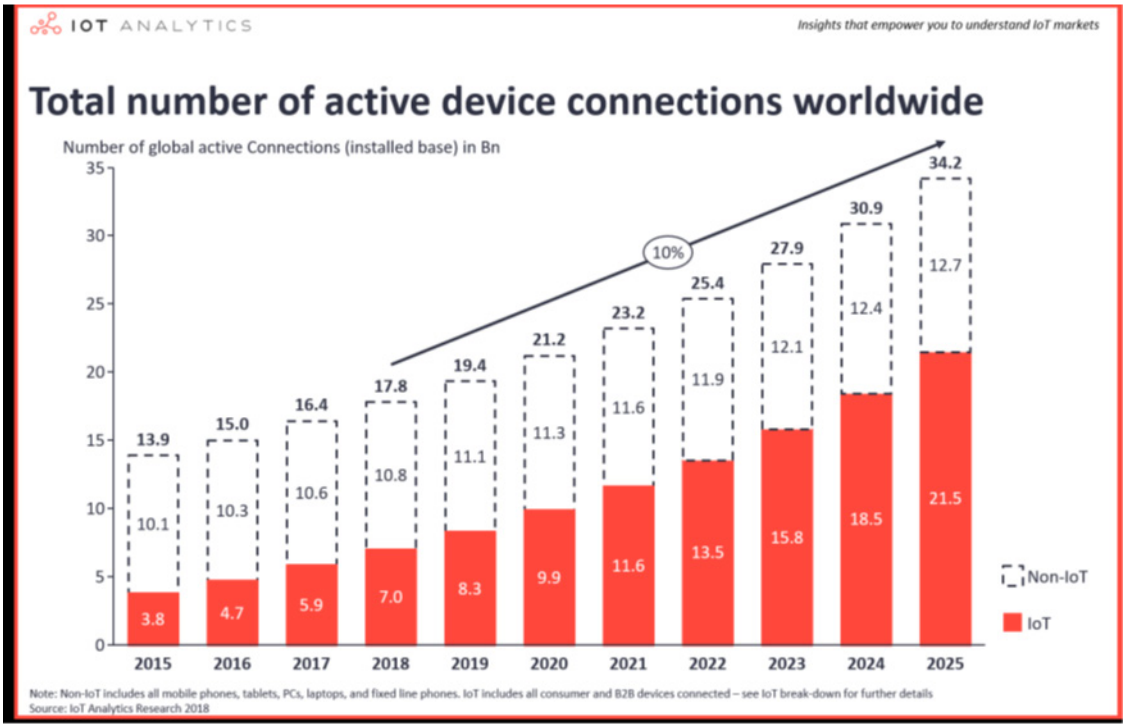
Chapter 5 – The Internet of Things and C&I

5.1 Introduction

ITU defines the Internet of Things (IoT) as *"a global infrastructure for the information society enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving, interoperable information and communication technologies"*.[29,30]

IoT technologies can be found in different industry sectors and affect people's daily lives via platforms that process data generated by billions of connected devices. A study carried out by IoT Analytics indicates that the total number of active device connections worldwide will increase dramatically. In 2020, of the 21.2 billion active device connections worldwide, 9.9 billion are IoT connections. This figure may rise to 21.5 billion by 2025.[31]

Figure 9: Number of active device connections worldwide



Note: Non-IoT includes all mobile phones, tablets, PCs, laptops, and fixed line phones. IoT includes all consumer and B2B devices connected – see IoT break-down for further details
Source: IoT Analytics Research 2018

5.2 Impact of IoT on C&I and ICT preparation

Certain issues and challenges have to be addressed in order to meet the specific needs of IoT, which include quality, reliability, coverage and low power consumption.

[29] Recommendation ITU-T Y.2060 (06/2012): Overview of the Internet of Things.
[30] Recommendation ITU-T Y.2069 (07/2012): Terms and definitions for the Internet of Things.
[31] IoT Analytics. State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating. August 2018.

5.2.1 Challenges of IoT

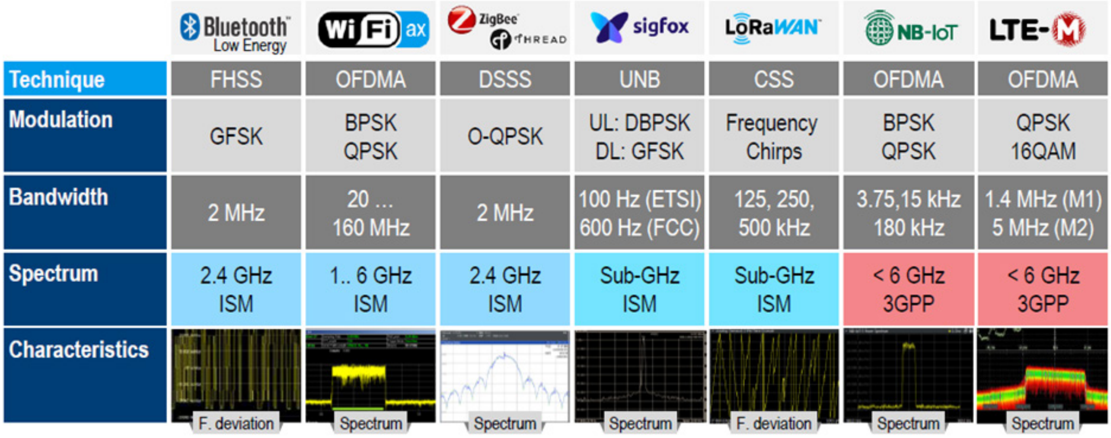
It is not enough to have good data-collection sensors; it is also necessary to ensure good connectivity to transmit data, and implement a platform to analyse and process them.

Among the many challenges associated with IoT, the following are of particular interest.

Choice of technology: Key to the success of IoT

In the future, IoT applications requiring total coverage and mobility will focus on cellular technology, such as LTE-M and NB-IoT technologies based on 4G and 5G. Others, such as Sigfox or LoRaWAN, will make use of low-power technologies operating in the unlicensed bands. Most applications will use short or medium-range wireless technologies, such as Bluetooth®, WLAN/Wi-Fi and Zigbee. IoT wireless technologies are shown in **Figure 10**.[32]

Figure 10: IoT wireless technologies



	Bluetooth Low Energy	WiFi ax	ZigBee THREAD	sigfox	LoRaWAN	NB-IoT	LTE-M
Technique	FHSS	OFDMA	DSSS	UNB	CSS	OFDMA	OFDMA
Modulation	GFSK	BPSK QPSK	O-QPSK	UL: DBPSK DL: GFSK	Frequency Chirps	BPSK QPSK	QPSK 16QAM
Bandwidth	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)
Spectrum	2.4 GHz ISM	1.. 6 GHz ISM	2.4 GHz ISM	Sub-GHz ISM	Sub-GHz ISM	< 6 GHz 3GPP	< 6 GHz 3GPP
Characteristics	F. deviation	Spectrum	Spectrum	Spectrum	F. deviation	Spectrum	Spectrum

Design that responds to IoT needs, i.e. quality, reliability, extended coverage, latency, etc.

The design must also respond to users' expectations, particularly in the area of confidentiality and personal data protection, and build trust by employing security standards in the IoT ecosystem.

The need for certification of IoT platforms and devices

Platforms and devices need to be certified by assessing their conformity with international standards and regulations.

5.2.2 Constraints of IoT

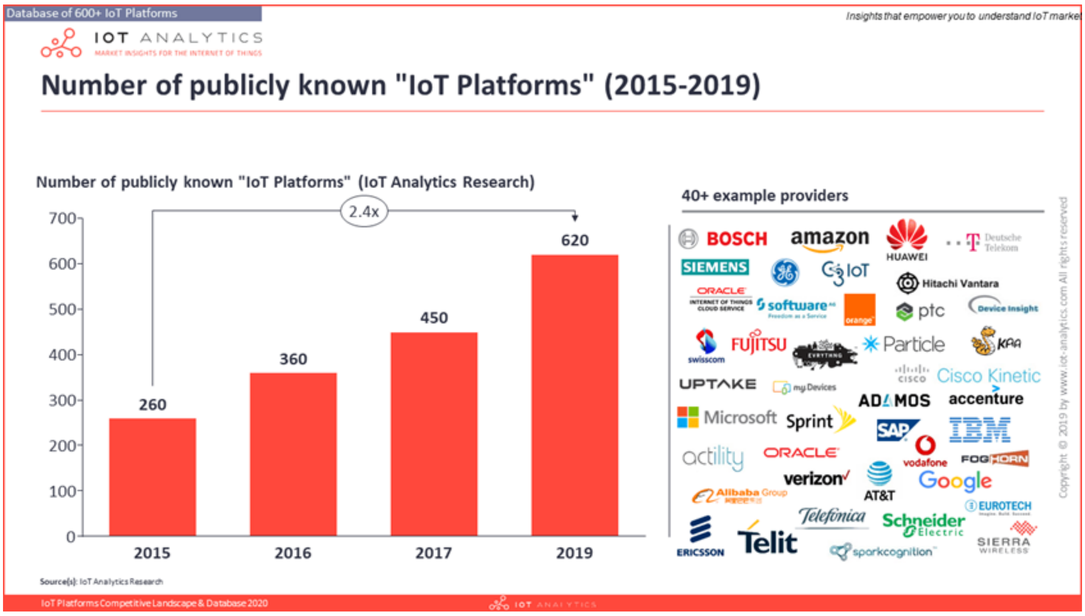
IoT is based essentially on the object (sensor), network (connectivity), data and the operating applications. The resulting constraints include:

- **Multiple IoT platforms**: Statistics generated by IoT Analytics show that in 2019 there were 620 IoT platforms and more than 40 providers (see **Figure 11**).[33]

[32] Joerg Koepp (Rohde & Schwarz, Germany). Ensuring reliable and secure communication in a hyper-connected world. *ITU-D Question 4/2 Session on ICT conformance and interoperability: challenges for developing countries*, Geneva, 16 October 2019.

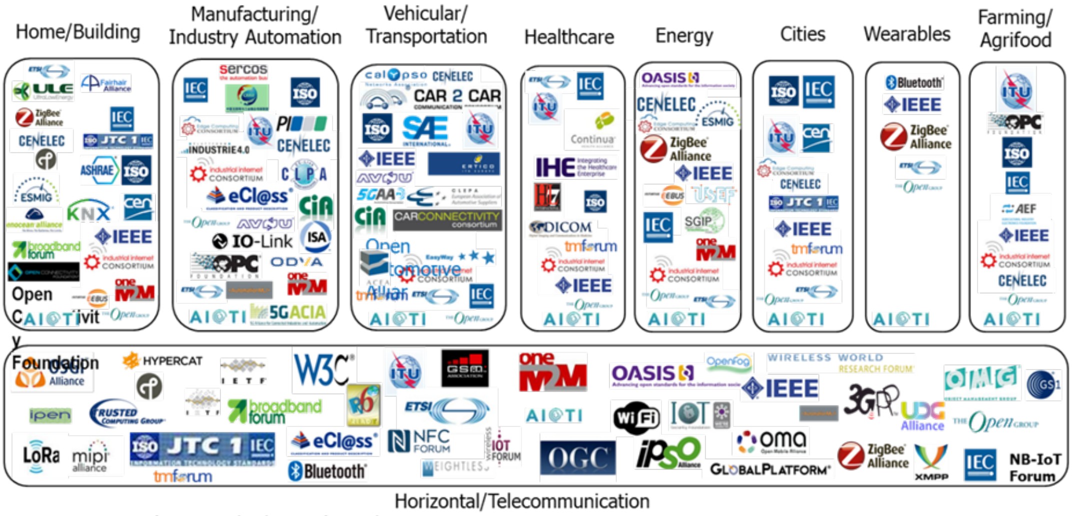
[33] IoT Analytics. IoT Platform Companies Landscape 2019/2020: 620 IoT Platforms globally. December 2019.

Figure 11: Number of publicly known IoT platforms



– **Multiple IoT protocols**: There are multiple data-sharing protocols, depending on standards development organizations (SDOs) and manufacturers of IoT products. Each IoT standard has its own normative framework, leaving IT professionals to choose from a multitude of options (see **Figure 12**).[34]

Figure 12: The landscape of IoT standards development organizations and alliances (vertical and horizontal domains)


Home/Building
Manufacturing/ Industry Automation
Vehicular/ Transportation
Healthcare
Energy
Cities
Wearables
Farming/ Agrifood
Horizontal/Telecommunication

Source: AIOTI WG3 (IoT Standardisation) – Release 2.9

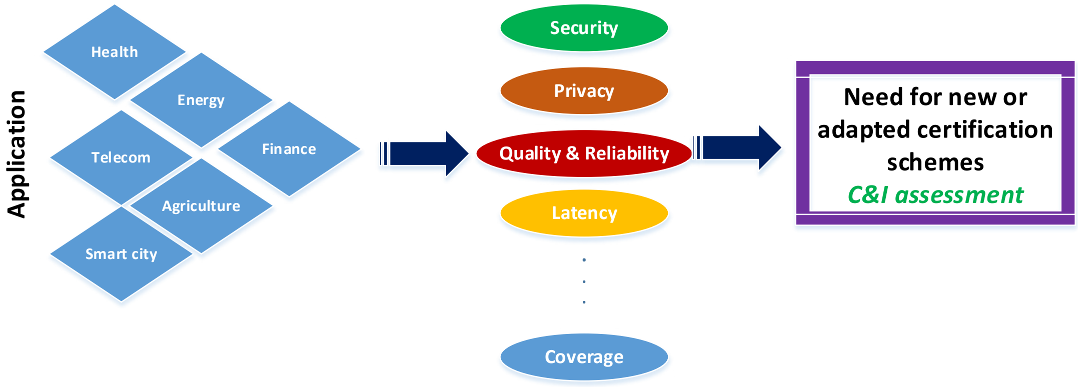
At present, IoT is far from standardized, with a wide range of incompatible standards and solutions.[35] Given the proliferation of IoT platforms and protocols facilitating object communication, IoT technical standards have evolved in a variety of contexts, involving different applications and stakeholders with differing requirements and objectives. A big challenge is

[34] Alliance for Internet of Things Innovation (AIOTI). IoT LSP Standard Framework Concepts. Release 2.9, 2019.

[35] ITU. Document ITU-T SG20-TD1722. *ITU Webinar on Accelerating cities' transformation through standards*, 25 June 2020.

therefore to ensure interoperability, scalability, robust international standards and end-to-end security (see **Figure 13**).

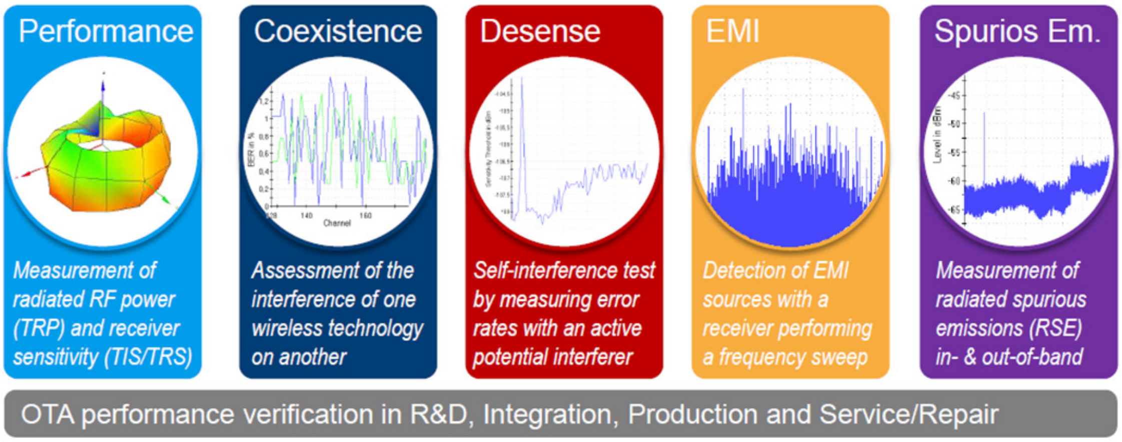
Figure 13: Need for adapted certification schemes



5.2.3 Example: Rohde & Schwarz IoT test

For Rohde & Schwarz, over-the-air (OTA) measurements help to guarantee performance and regulatory compliance. The tests focus on performance, coexistence, interference testing, electromagnetic interference (EMI) and measuring radiated spurious emissions (RSEs) in band and out of band (see **Figure 14**).[36]

Figure 14: OTA measurements


Performance
Measurement of radiated RF power (TRP) and receiver sensitivity (TIS/TRS)
Coexistence
Assessment of the interference of one wireless technology on another
Desense
Self-interference test by measuring error rates with an active potential interferer
EMI
Detection of EMI sources with a receiver performing a frequency sweep
Spurios Em.
Measurement of radiated spurious emissions (RSE) in- & out-of-band
OTA performance verification in R&D, Integration, Production and Service/Repair

5.2.4 Standards development organizations

The adoption of a unified approach to IoT systems as a means of fostering industry development has prompted SDOs to work towards establishing a standard architecture that ensures the interoperability of systems, applications, devices and sensors.

[36] Joerg Koepp (Rohde & Schwarz). Op. cit.

International Telecommunication Union

ITU-T has developed the Y-series Recommendations, covering the global information infrastructure, aspects of Internet protocol, next-generation networks, IoT and smart cities. ITU-T Study Group 20 (SG20) has been working on international standards to promote interoperability between digital infrastructures and IoT applications.

In March 2020, ITU published Recommendation ITU-T Y.4459[37] introducing a digital entity architecture. This defines a minimum set of architectural components and services needed to provide generic information and service interoperability. It will facilitate interoperability for the identification, description, representation, access, storage and security of IoT devices. This architecture framework fosters the use of a common security and management interface across different IoT applications.

For C&I testing, ITU-T Study Group 11 (SG11) and the Conformity Assessment Steering Committee are working together with SG20 on a network model for IoT tests.[38]

The International Organization for Standardization and the International Electrotechnical Commission

In 2018, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) published standard ISO/IEC 30141, a harmonizing standard reference architecture for IoT, described as "the complex assemblage of billions of smart devices connected through the Internet".[39]

In 2019, ISO and IEC published standard ISO/IEC 21823-1,[40] which provides an overview of interoperability as it applies to IoT systems.

Institute of Electrical and Electronics Engineers

The Institute of Electrical and Electronics Engineers (IEEE) has published standard 2413-2019, "IEEE Standard for an Architectural Framework for the Internet of Things (IoT)".[41] Standard P2413.1 provides an architectural blueprint for smart-city implementation by leveraging cross-domain interaction and interoperability among different smart-city components and domains.[42] This standard builds on the architectural framework established for IoT in draft standard IEEE P2413, which is based on international standard ISO/IEC/IEEE 42010.

[37] ITU-T. Recommendation ITU-T Y.4459 (12/2020): Digital entity architecture framework for Internet of things interoperability.

[38] Kofi Ntim Yeboah-Kordieh (Ghana). ITU-T SG11 Work Updates and Activities. *ITU-D Question 4/2 workshop on ICT conformance and interoperability: Challenges for developing countries*, Geneva, 16 October 2019.

[39] ISO. ISO/IEC 30141:2018. Internet of Things (IoT) – Reference Architecture. August 2018.

[40] ISO. ISO/IEC 21823-1:2019. Internet of Things (IoT) – Interoperability for IoT systems – Part 1: Framework. February 2019.

[41] IEEE. IEEE 2413-2019. IEEE Standard for an Architectural Framework for the Internet of Things (IoT). May 2019.

[42] IEEE IEEE P2413-1. Standard for a Reference Architecture for Smart City (RASC). August 2018.

5.3 Regulations and policies for IoT and ICTs

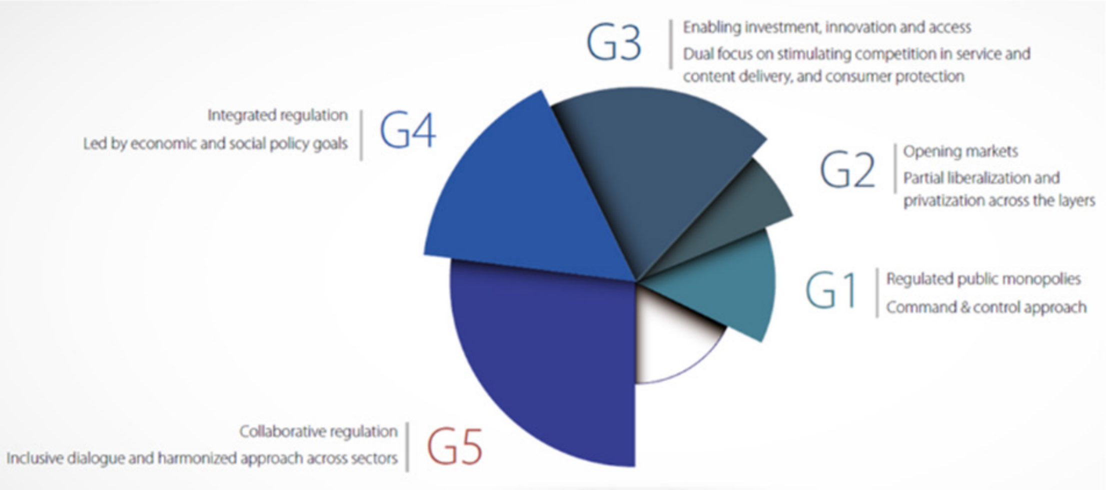
Regulators must be aware of the impact of C&I on IoT. Although testing laboratories contribute to ensuring product performance, conformity and interoperability, regulations are also necessary.

Today, IoT technologies are deployed by public and private entities in different sectors, including healthcare, telecommunications, education, agriculture, finance and media, as well as in smart cities. Establishing a cross-sectoral regulatory environment, adapted to IoT, is therefore of paramount importance and requires fifth-generation regulation (i.e. collaborative regulation).

5.3.1 Overview of collaborative regulation

Regulation has already evolved considerably between the first and fourth generations: from regulated monopolies to basic reforms and market liberalization, followed by the regulation of an environment that stimulates innovation and access, and then to the fourth generation of integrated regulation centred on Internet-related issues (see **Figure 15**).[43]

Figure 15: Generations of ICT regulation – a conceptual framework

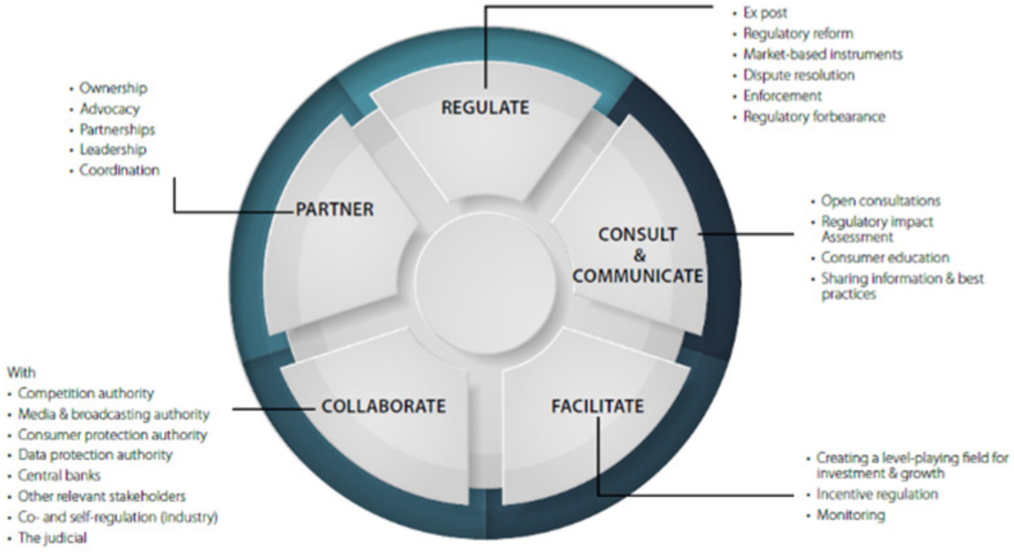

G3
Enabling investment, innovation and access
Dual focus on stimulating competition in service and content delivery, and consumer protection
Integrated regulation
Led by economic and social policy goals
G4
G2
Opening markets
Partial liberalization and privatization across the layers
G1
Regulated public monopolies
Command & control approach
Collaborative regulation
Inclusive dialogue and harmonized approach across sectors
G5

Fifth generation, or collaborative, regulation is flexible and driven by consensus. Collaborative regulation promotes innovation, efficiency, QoS, data sharing and security, and overcomes obstacles such as interoperability challenges. In addition, it builds on sharing expertise, guiding principles and best practices and identifying mechanisms for cross-sector cooperation to more effectively address common challenges (see **Figure 16**).[44]

[43] ITU-D. ITU Global ICT Regulatory Outlook 2017.

[44] Ibid.

Figure 16: Collaborative regulation



The ITU GSR-19 Best Practice Guidelines focused on collaborative regulation as a means of ensuring successful digital transformation.[45]

5.3.2 IoT regulation

Many governments are encouraging innovation in IoT and wish to reform their regulatory framework to avoid impinging on its growth. However, as there is still a degree of regulatory uncertainty concerning IoT market, regulatory innovations and adjustments will be made in phases.

IoT is different from the connectivity that ICT regulators are striving to enable. Connectivity is the principal service, whereas the IoT also covers associated applications, devices and sensors.

In general, although all regulations apply to IoT, this technology might give rise to additional requirements. Policies and regulations must address issues specific to IoT, such as:

- confidentiality, data protection and security
- standards and interoperability of systems, platforms and connected objects
- spectrum management and licensing (in many cases, IoT devices use wireless technologies)
- numbering and number portability
- the need to migrate from IPv4 to IPv6
- costs, reliability, QoS and quality of experience (QoE)
- measures to manage competition.

ICT regulations have become increasingly complex, owing to issues relating to security, confidentiality and data protection. Many countries may need to update out-of-date or excessively restrictive regulations, and scaling up efforts are affected by interoperability.

In order to improve interoperability and reduce costs, professionals are calling for an open IoT ecosystem built on open-source, non-proprietary platforms, applications and standards, thereby promoting economic growth and innovation.

[45] ITU. Global Symposium for Regulators (GSR). Best practice guidelines 2019. Port Vila, 2019.

5.4 Conclusion

Standardization is critical to establishing a single IoT market where any device can be plugged in and communicate from any location. Standardization facilitates interoperability, compatibility, reliability and security; it stimulates the emergence of new ecosystems and innovation; and it boosts competitiveness.

Regulators must recognize the impact of new IoT technologies, and the significant role that they play in the development of these technologies, through creating more opportunities by ushering in a new era of collaborative regulation in which ICT regulators operate more as facilitators, working to improve connectivity and collaborate with other stakeholders to promote the use of ICTs across all domains.

In conclusion, a strategy built on a progressive regulatory framework can protect and provide a boost to all stakeholders through the deployment of expertise and financial and other resources. In addition, such a strategy can promote this new technology, a competitive market and rapid innovation.

Chapter 6 – Transfer of information, know-how and knowledge

6.1 C&I learning needs and educational opportunities

C&I requires a specialized set of skills, and trained professionals are required to run C&I programmes. Moreover, certain challenges are inherent to the field, including:

- A lack of formal holistic C&I education programmes. Large institutions train staff on C&I by pairing them with experienced workers. Although it can be useful, this approach tends to provide a narrow breadth of experience with no formal quality checks. Moreover, it cannot be implemented in smaller institutions.
- The various C&I practitioners, including regulators, licensees, certification requesters (importers and manufactures) and conformity managers must also have a clear understanding of legal, technical, international trade and economic issues.
- Rapidly evolving technological products represent an ongoing challenge for C&I frameworks (e.g. with respect to IoT and software configuration).

Resolution 177 (Rev. Dubai, 2018) of the ITU Plenipotentiary Conference highlighted the need for the continued provision of on-the-job C&I capacity-building activities, in collaboration with recognized institutions and taking advantage of the ITU Academy ecosystem, including activities on preventing radiocommunication interference caused or received by ICT equipment.[46]

The experiences of 2020 have demonstrated the urgent global need for digital learning through reliable ICT networks. In the aftermath of the COVID-19 pandemic, the use of ICTs for educational purposes is being viewed more than ever as a public good. As proposed in Resolution 177 (Rev. Dubai, 2018), the ITU Academy offers online training solutions for trainers that should be explored by the global C&I community.

6.2 Responding to needs relating to knowledge acquisition/retention

A collaborative platform based on quality-assurance mechanisms should be considered as a way of fostering the development of a broader set of skills, following the example of the ITU proposal for a conformance and interoperability training programme (CITP).[47]

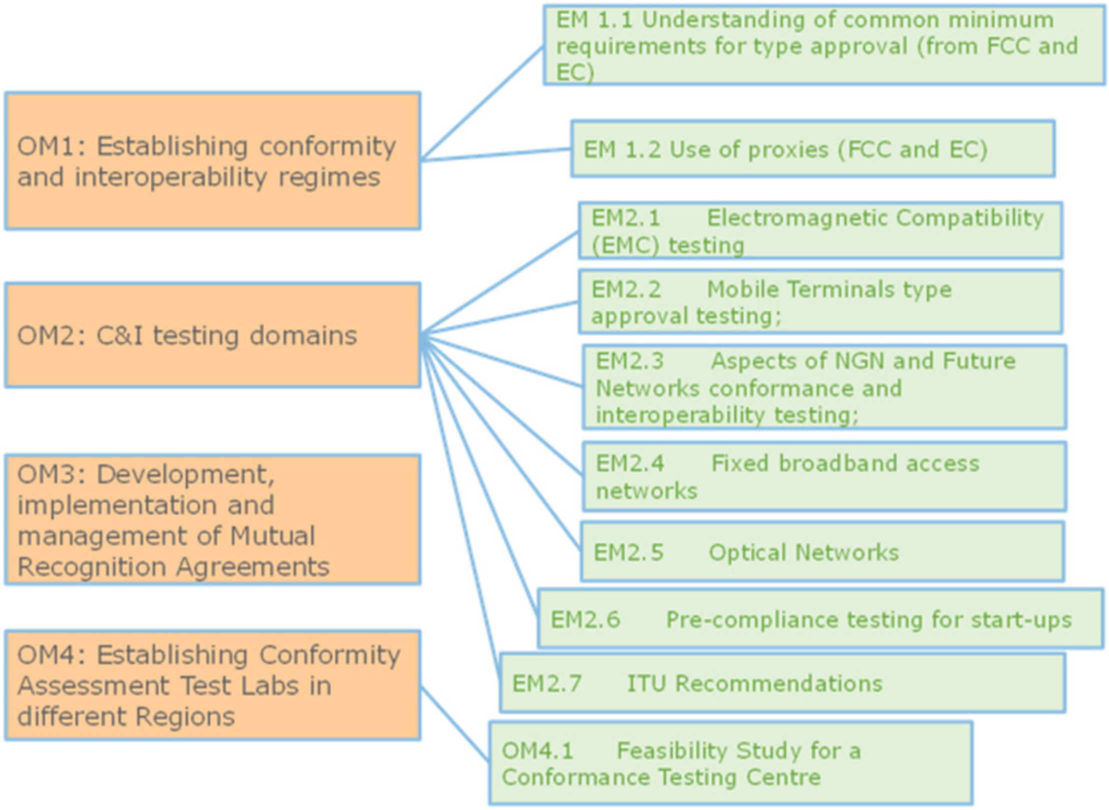
CITP is based on previous successful C&I training events, such as on-the-job regional training activities on C&I programmes and test domains, together with partner laboratories.[48] The programme also takes into account lessons learned from ITU publications, including the final report on Question 4/2 for the previous study period,[49] and published guidelines.[50]

[46] ITU. Resolution 177 (Rev. Dubai, 2018) of the Plenipotentiary Conference, on conformance and interoperability.
[47] These concepts were presented to Question 4/2 in October 2019 in ITU-D SG2 Document SG2RGQ/194+Annex from the BDT Focal Point for Question 4/2.
[48] ITU-D. Conformance and interoperability events.
[49] ITU-D. Final Report on ITU-D Study Group 2 Question 4/2 for the study period 2014-2017. Op. cit.
[50] ITU-D. Publications and deliverables – C&I.

Work to develop CITP is following the model established by the ITU Academy's quality-assurance mechanism, which includes a package of high-level materials prepared by subject-matter experts, a peer-review process, and templates prepared by professional trainers for writing syllabus cards and training outlines.

A proposed training structure, offering tailored learning paths, is outlined below:

Figure 17: CITP training modules (OM are obligatory modules, EM are eligible modules)


EM 1.1 Understanding of common minimum requirements for type approval (from FCC and EC)
OM1: Establishing conformity and interoperability regimes
EM 1.2 Use of proxies (FCC and EC)
EM2.1 Electromagnetic Compatibility (EMC) testing
EM2.2 Mobile Terminals type approval testing;
OM2: C&I testing domains
EM2.3 Aspects of NGN and Future Networks conformance and interoperability testing;
EM2.4 Fixed broadband access networks
OM3: Development, implementation and management of Mutual Recognition Agreements
EM2.5 Optical Networks
EM2.6 Pre-compliance testing for start-ups
OM4: Establishing Conformity Assessment Test Labs in different Regions
EM2.7 ITU Recommendations
OM4.1 Feasibility Study for a Conformance Testing Centre

The training structure is organized around four main topics and divided into sub-topics to support the selected learning path and to ensure the modular transfer of knowledge required by students.

1) **Designing and establishing conformity and interoperability regimes/frameworks**

   This module focuses on understanding minimum technical requirements and the use of existing C&I structures and proxies to find the right balance between trust and control of ICT devices.

2) **Testing domains covering a broad range of laboratory services**

   The scope of testing domains is potentially endless, and can cover topics such as new technology approval and supporting young developers to help them achieve international recognition of their products.

   There is a clear understanding that training modules should be developed in response to existing needs and priorities.

3) **Regional collaboration on and harmonization of standards and type-approval processes, including mutual recognition agreements**

   As indicated in the previous chapter, collaboration is key, and this module promotes sharing resources and mechanisms that are already in place to certify ICT product conformance to international and national technical requirements.

4) **Establishment and maintenance of testing laboratories**

   This module focuses on quality procedures and strategic assessments, such as business planning optimization.

6.3 Conclusions

In summary, a comprehensive analysis of how to develop a training programme on the transfer of information, know-how and knowledge needs to take into account:

- collaboration with experts in the field, which will include ITU study groups (ITU-D SG2 Q4/2, ITU-T SG11, and Radiocommunication Bureau contributors), testing professionals, type-approval managers, trade experts;
- training materials based on ITU publications on the C&I programme, including guidelines and ITU Recommendations developed by ITU-R and ITU-T;
- work on knowledge transfer by international, regional and national organizations;
- easy access to C&I training and ensuring a forward-looking, professional approach;
- a course design that is universally accessible, to both beginners and specialists;
- a modular and adaptive approach, providing the level of knowledge appropriate to the task at hand and ensuring that content responds to current C&I needs.

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).

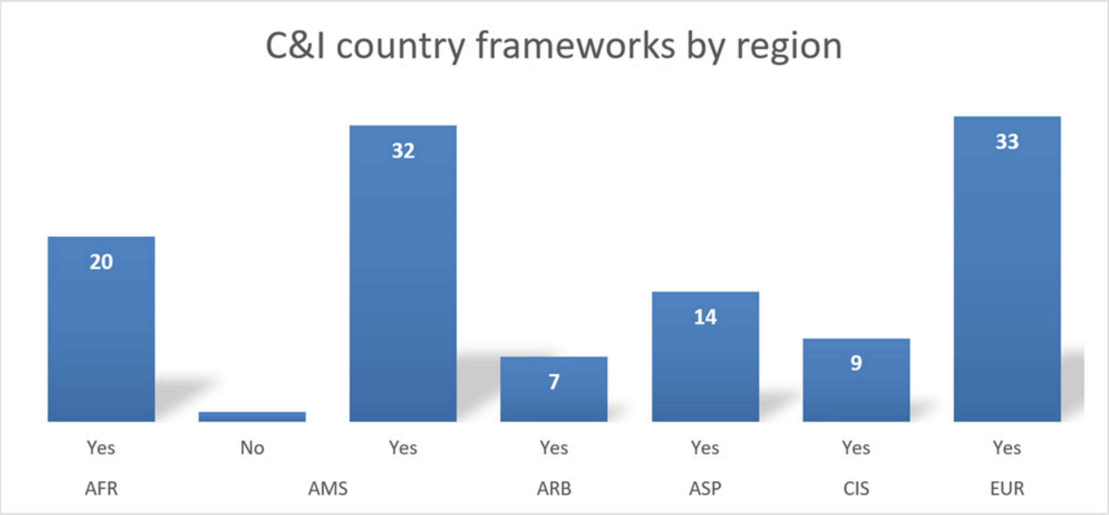
Data show that most of the countries have in place a C&I arrangement aiming to ascertain trust on safe and interoperable use of ICT devices by networks and citizens. Note that procedures and strictness levels of requirements (e.g. recognition of certification and use of proxies, self-declaration, local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

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



[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.

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 SG2RGQ/38+Annex from the BDT Focal Point for Question 3/1.

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

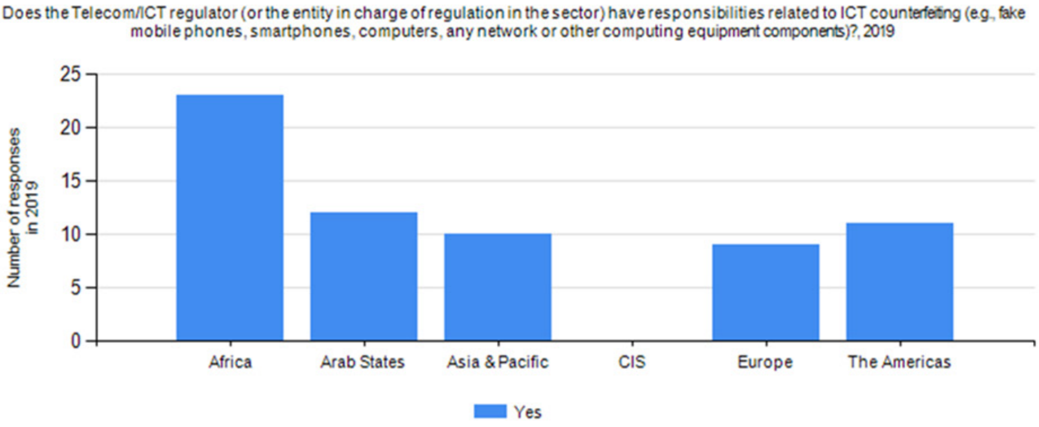


Figure 3A: Regional distribution of responses from survey – Question 2

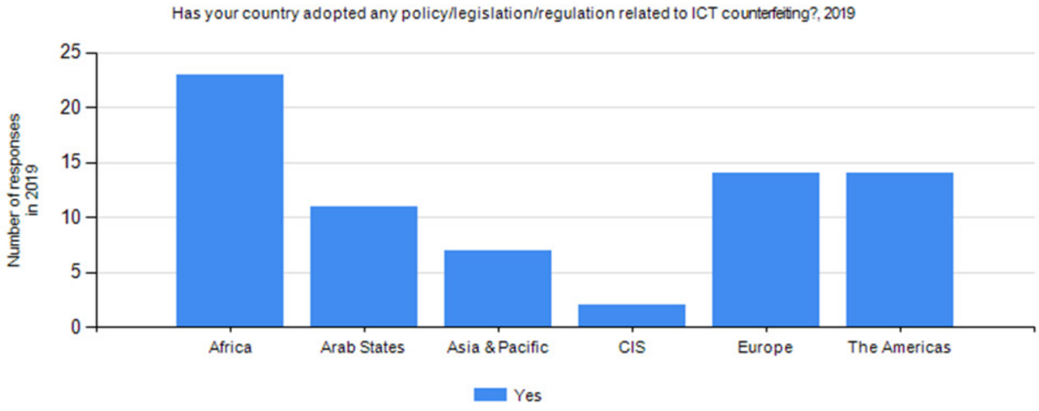
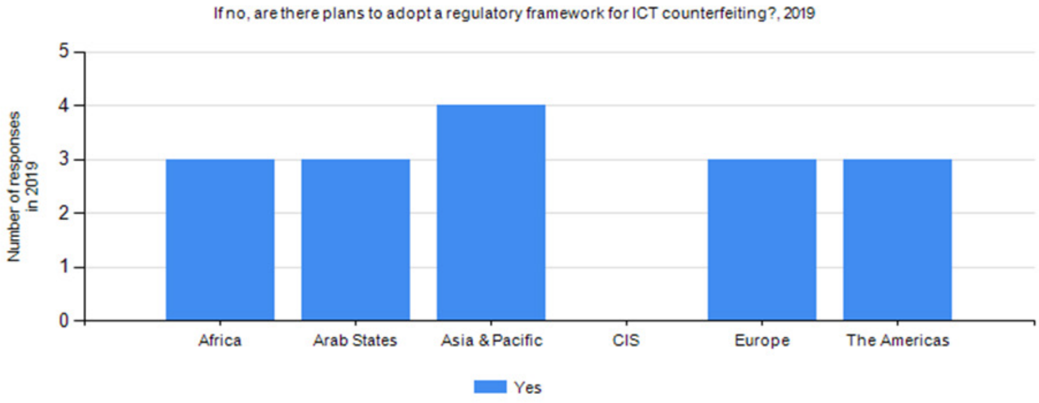


Figure 4A: Regional distribution of responses from survey – Question 3



Annex 3: Initiatives in the fight against equipment counterfeiting and mobile terminal theft in Burundi[54]

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.

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.

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.
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.

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

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.

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)

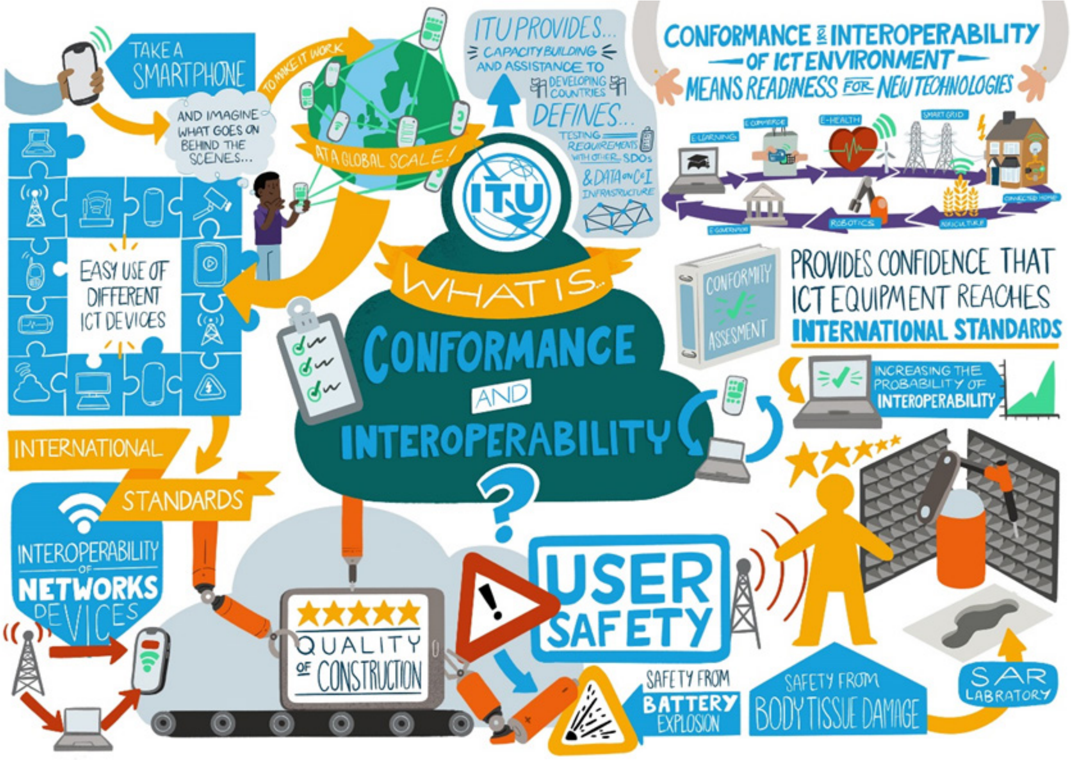

TAKE A SMARTPHONE
AND IMAGINE WHAT GOES ON BEHIND THE SCENES...
TO MAKE IT WORK
AT A GLOBAL SCALE!
ITU PROVIDES... CAPACITY BUILDING AND ASSISTANCE TO DEVELOPING COUNTRIES
DEFINES... TESTING REQUIREMENTS WITH OTHER SDOs & DATA ON C&I INFRASTRUCTURE
ITU
CONFORMANCE AND INTEROPERABILITY OF ICT ENVIRONMENT MEANS READINESS FOR NEW TECHNOLOGIES
E-LEARNING
E-COMMERCE
E-HEALTH
SMART GRID
CONNECTED HOME
AGRICULTURE
ROBOTICS
E-GOVERNMENT
EASY USE OF DIFFERENT ICT DEVICES
WHAT IS...
CONFORMANCE AND INTEROPERABILITY ?
CONFORMITY ASSESMENT
PROVIDES CONFIDENCE THAT ICT EQUIPMENT REACHES INTERNATIONAL STANDARDS
INCREASING THE PROBABILITY OF INTEROPERABILITY
INTERNATIONAL
STANDARDS
INTEROPERABILITY OF NETWORKS DEVICES
QUALITY OF CONSTRUCTION
USER SAFETY
SAFETY FROM BATTERY EXPLOSION
SAFETY FROM BODY TISSUE DAMAGE
SAR LABRATORY

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

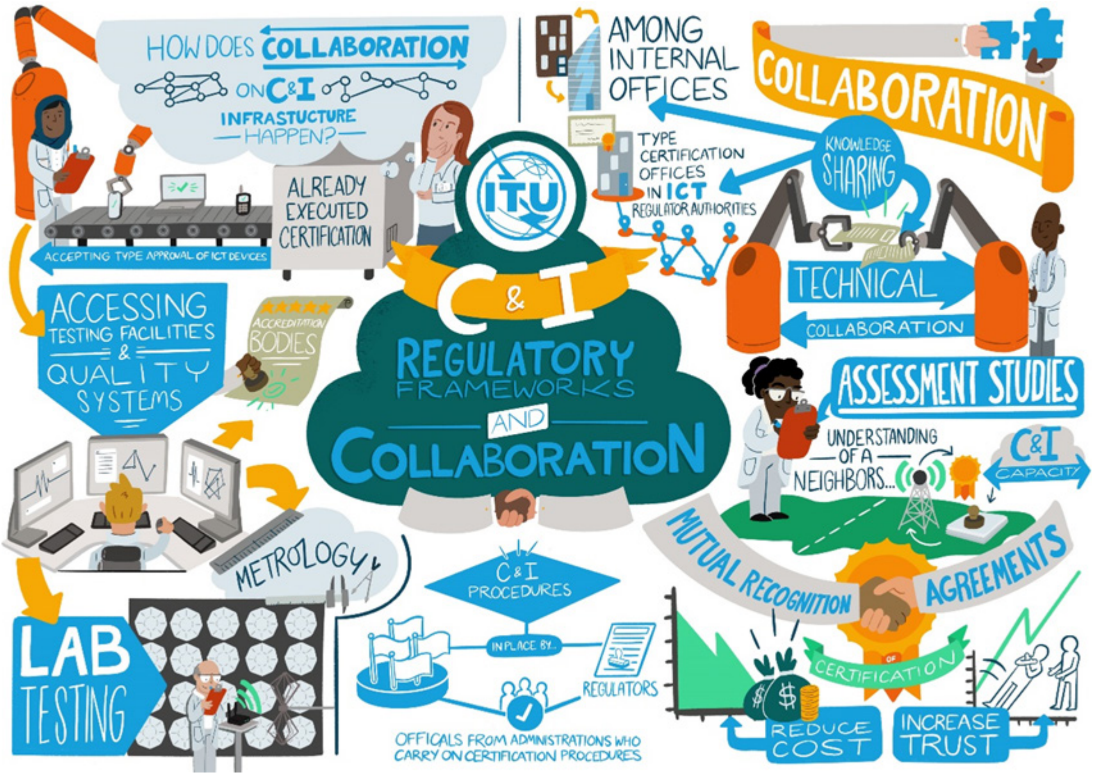

HOW DOES COLLABORATION ON C&I INFRASTUCTURE HAPPEN?
ACCEPTING TYPE APPROVAL OF ICT DEVICES
ALREADY EXECUTED CERTIFICATION
AMONG INTERNAL OFFICES
TYPE CERTIFICATION OFFICES IN ICT REGULATOR AUTHORITIES
COLLABORATION
KNOWLEDGE SHARING
TECHNICAL COLLABORATION
ITU
C & I
REGULATORY FRAMEWORKS AND COLLABORATION
ACCESSING TESTING FACILITIES & QUALITY SYSTEMS
ACCREDITATION BODIES
METROLOGY
LAB TESTING
C&I PROCEDURES
IN PLACE BY...
REGULATORS
OFFICALS FROM ADMINISTRATIONS WHO CARRY ON CERTIFICATION PROCEDURES
ASSESSMENT STUDIES
UNDERSTANDING OF A NEIGHBORS...
C&I CAPACITY
MUTUAL RECOGNITION AGREEMENTS
OF CERTIFICATION
REDUCE COST
INCREASE TRUST

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

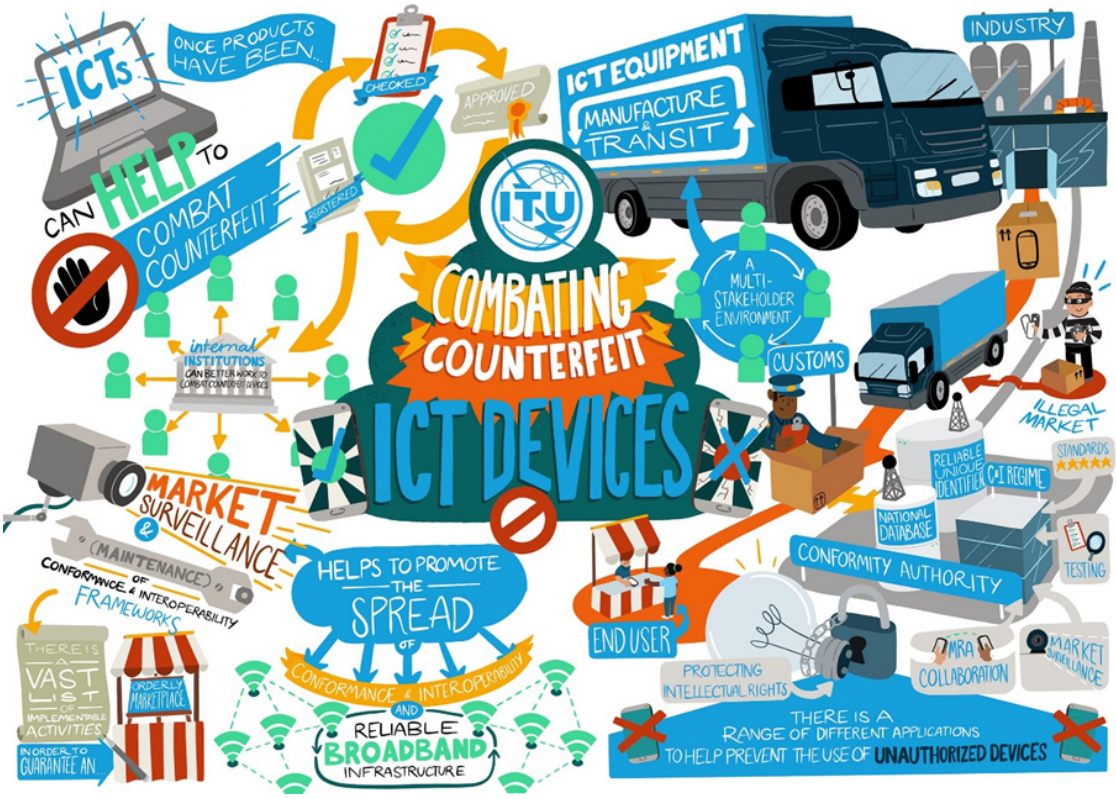
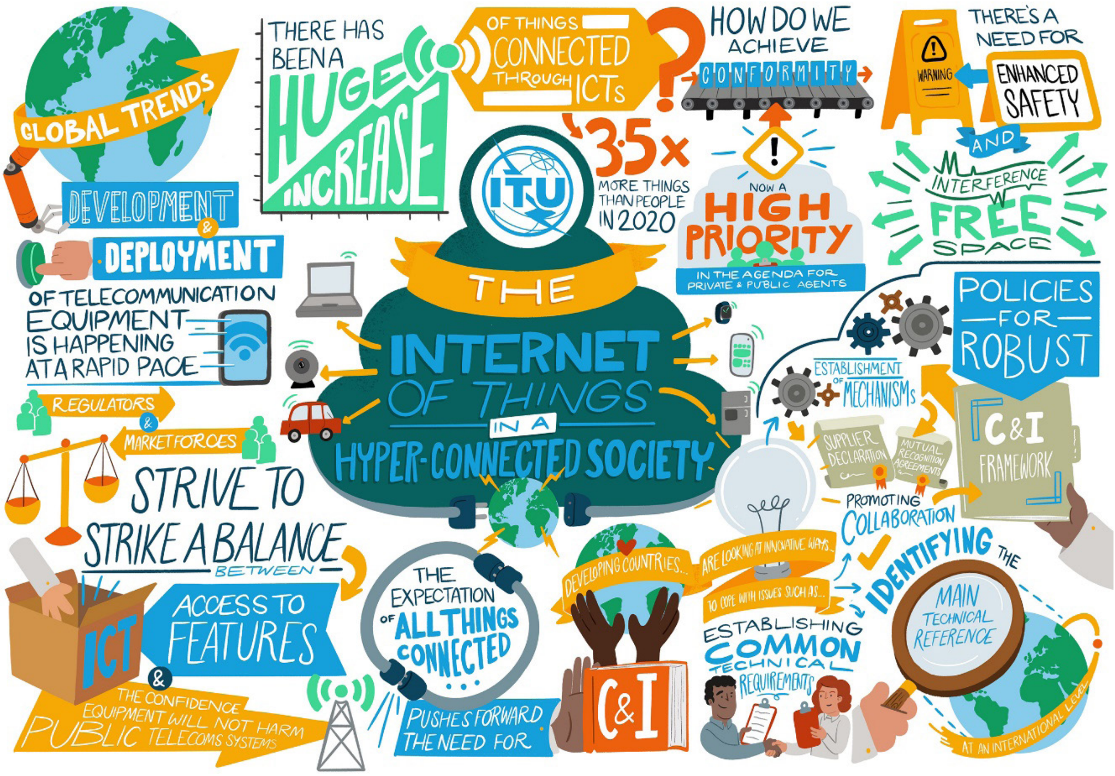

ICTs CAN HELP TO COMBAT COUNTERFEIT
ONCE PRODUCTS HAVE BEEN...
CHECKED
APPROVED
REGISTERED
ICT EQUIPMENT
MANUFACTURE & TRANSIT
INDUSTRY
ITU
COMBATING COUNTERFEIT ICT DEVICES
A MULTI-STAKEHOLDER ENVIRONMENT
CUSTOMS
ILLEGAL MARKET
internal INSTITUTIONS CAN BETTER WORK TO COMBAT COUNTERFEIT DEVICES
MARKET SURVEILLANCE & (MAINTENANCE) OF CONFORMANCE & INTEROPERABILITY FRAMEWORKS
RELIABLE UNIQUE IDENTIFIER
C&I REGIME
STANDARDS
NATIONAL DATABASE
TESTING
CONFORMITY AUTHORITY
HELPS TO PROMOTE THE SPREAD OF CONFORMANCE & INTEROPERABILITY AND RELIABLE BROADBAND INFRASTRUCTURE
END USER
PROTECTING INTELLECTUAL RIGHTS
MRA COLLABORATION
MARKET SURVEILLANCE
THERE IS A VAST LIST OF IMPLEMENTABLE ACTIVITIES
IN ORDER TO GUARANTEE AN...
ORDERLY MARKETPLACE
THERE IS A RANGE OF DIFFERENT APPLICATIONS TO HELP PREVENT THE USE OF UNAUTHORIZED DEVICES

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


GLOBAL TRENDS
DEVELOPMENT
&
DEPLOYMENT
OF TELECOMMUNICATION EQUIPMENT IS HAPPENING AT A RAPID PACE
THERE HAS BEEN A
HUGE INCREASE
OF THINGS CONNECTED THROUGH ICTs
3.5x
MORE THINGS THAN PEOPLE IN 2020
ITU
THE
INTERNET OF THINGS
IN A
HYPER-CONNECTED SOCIETY
REGULATORS
&
MARKET FORCES
STRIVE TO STRIKE A BALANCE
BETWEEN
ACCESS TO FEATURES
ICT
&
THE CONFIDENCE EQUIPMENT WILL NOT HARM PUBLIC TELECOMS SYSTEMS
THE EXPECTATION OF ALL THINGS CONNECTED...
PUSHES FORWARD THE NEED FOR
C&I
HOW DO WE ACHIEVE
CONFORMITY
NOW A
HIGH PRIORITY
IN THE AGENDA FOR PRIVATE & PUBLIC AGENTS
WARNING
THERE'S A NEED FOR
ENHANCED SAFETY
AND
INTERFERENCE FREE SPACE
POLICIES FOR ROBUST
C&I FRAMEWORK
ESTABLISHMENT OF MECHANISMS
SUPPLIER DECLARATION
MUTUAL RECOGNITION AGREEMENTS
PROMOTING COLLABORATION
DEVELOPING COUNTRIES...
ARE LOOKING AT INNOVATIVE WAYS...
TO COPE WITH ISSUES SUCH AS...
ESTABLISHING COMMON TECHNICAL REQUIREMENTS
IDENTIFYING THE
MAIN TECHNICAL REFERENCE
AT AN INTERNATIONAL LEVEL

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)

(continued)

Web	Received	Source	Title
2/257	2019-12-20	Mauritania	Proposed draft text for Chapter 2 of the Final Report for Question 4/2
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

(continued)

Web	Received	Source	Title
2/90	2018-04-24	Mauritania	Draft work plan for ITU-D Study Group 2 Question 4/2
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
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

(continued)

Web	Received	Source	Title
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

Office of the Director
International Telecommunication Union (ITU)
Telecommunication Development Bureau (BDT)
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Office of Deputy Director and Regional Presence
Field Operations Coordination Department (DDR)
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdeputydir@itu.int
Tel.: +41 22 730 5131
Fax: +41 22 730 5484

Digital Networks and Society (DNS)

Email: bdt-dns@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

Digital Knowledge Hub Department (DKH)

Email: bdt-dkh@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

Partnerships for Digital Development Department (PDD)

Email: bdt-pdd@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

Africa

Ethiopia

International Telecommunication
Union (ITU) Regional Office
Gambia Road
Leghar Ethio Telecom Bldg. 3rd floor
P.O. Box 60 005
Addis Ababa
Ethiopia

Email: itu-ro-africa@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

Cameroon

Union internationale des
télécommunications (UIT)
Bureau de zone
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé
Cameroon

Email: itu-yaounde@itu.int
Tel.: + 237 22 22 9292
Tel.: + 237 22 22 9291
Fax: + 237 22 22 9297

Senegal

Union internationale des
télécommunications (UIT)
Bureau de zone
8, Route des Almadies
Immeuble Rokhaya, 3e étage
Boîte postale 29471
Dakar - Yoff
Senegal

Email: itu-dakar@itu.int
Tel.: +221 33 859 7010
Tel.: +221 33 859 7021
Fax: +221 33 868 6386

Zimbabwe

International Telecommunication
Union (ITU) Area Office
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792
Belvedere Harare
Zimbabwe

Email: itu-harare@itu.int
Tel.: +263 4 77 5939
Tel.: +263 4 77 5941
Fax: +263 4 77 1257

Americas

Brazil

União Internacional de
Telecomunicações (UIT)
Escritório Regional
SAUS Quadra 6 Ed. Luis Eduardo
Magalhães,
Bloco "E", 10º andar, Ala Sul
(Anatel)
CEP 70070-940 Brasilia - DF
Brazil

Email: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

Barbados

International Telecommunication
Union (ITU) Area Office
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown
Barbados

Email: itubridgetown@itu.int
Tel.: +1 246 431 0343
Fax: +1 246 437 7403

Chile

Unión Internacional de
Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Santiago de Chile
Chile

Email: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras

Unión Internacional de
Telecomunicaciones (UIT)
Oficina de Representación de
Área
Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cía
Apartado Postal 976
Tegucigalpa
Honduras

Email: itutegucigalpa@itu.int
Tel.: +504 2235 5470
Fax: +504 2235 5471

Arab States

Egypt

International Telecommunication
Union (ITU) Regional Office
Smart Village, Building B 147,
3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
Cairo
Egypt

Email: itu-ro-arabstates@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

Asia-Pacific

Thailand

International Telecommunication
Union (ITU) Regional Office
Thailand Post Training Center
5th floor
111 Chaengwattana Road
Laksi
Bangkok 10210
Thailand

Mailing address:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210, Thailand

Email: ituasiapacificregion@itu.int
Tel.: +66 2 575 0055
Fax: +66 2 575 3507

Indonesia

International Telecommunication
Union (ITU) Area Office
Sapta Pesona Building
13th floor
JI. Merdan Merdeka Barat No. 17
Jakarta 10110
Indonesia

Mailing address:
c/o UNDP – P.O. Box 2338
Jakarta 10110, Indonesia

Email: ituasiapacificregion@itu.int
Tel.: +62 21 381 3572
Tel.: +62 21 380 2322/2324
Fax: +62 21 389 5521

CIS

Russian Federation

International Telecommunication
Union (ITU) Regional Office
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

Email: itumoscow@itu.int
Tel.: +7 495 926 6070

Europe

Switzerland

International Telecommunication
Union (ITU) Office for Europe
Place des Nations
CH-1211 Geneva 20
Switzerland
Email: eurregion@itu.int
Tel.: +41 22 730 5467
Fax: +41 22 730 5484

International Telecommunication Union
Telecommunication Development Bureau
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN 978-92-61-34131-2

9 789261 341312

Published in Switzerland
Geneva, 2021
Photo credits: Shutterstock