ITUPublications

Union internationale des télécommunications
Secteur du développement

Rapport final sur la Question 4/2 de l'UIT-D

Équipements reposant sur les télécommunications/TIC: conformité et interopérabilité et lutte contre la contrefaçon et le vol de dispositifs mobiles

Période d'études 2022-2025

Rapport final sur la Question 4/2 de l'UIT-D

Équipements reposant sur les télécommunications/ TIC: conformité et interopérabilité et lutte contre la contrefaçon et le vol de dispositifs mobiles

Période d'études 2022-2025

Équipements reposant sur les télécommunications/TIC: conformité et interopérabilité et lutte contre la contrefaçon et le vol de dispositifs mobiles: Rapport final sur la Question 4/2 de l'UIT-D pour la période d'études 2022-2025

ISBN 978-92-61-41182-4 (version électronique)

ISBN 978-92-61-41192-3 (version EPUB)

Crédits photos de couverture: Adobe Stock

Remerciements

Les commissions d'études du Secteur du développement des télécommunications de l'UIT (UIT-D) offrent un cadre neutre où des experts des pouvoirs publics, du secteur privé, des organisations de télécommunication et des établissements universitaires du monde entier se réunissent pour élaborer des outils et des ressources pratiques permettant de traiter les questions de développement. À cette fin, les deux commissions d'études de l'UIT-D sont chargées d'élaborer des rapports, des lignes directrices et des recommandations sur la base des contributions soumises par les membres. Les Questions à étudier sont définies tous les quatre ans à la Conférence mondiale de développement des télécommunications (CMDT). Les membres de l'UIT, réunis à la CMDT-22 qui s'est tenue à Kigali en juin 2022, sont convenus que pour la période 2022-2025, la Commission d'études 1 examinerait sept Questions relevant du domaine de compétence général "Mise en place d'un environnement propice à une connectivité efficace".

Le présent rapport a été élaboré en réponse à la Question 4/2: **Équipements reposant sur les télécommunications/TIC: conformité et interopérabilité et lutte contre la contrefaçon et le vol de dispositifs mobiles**, sous la direction et la coordination générales de l'équipe de direction de la Commission d'études 2 de l'UIT-D dirigée par M. Fadel Digham (République arabe d'Égypte), Président, secondé par les Vice-Présidents suivants: M. Abdelaziz Alzarooni (Émirats arabes unis), Mme Zainab Ardo (République fédérale du Nigéria), M. Javokhir Aripov (République d'Ouzbékistan), Mme Carmen-Mădălina Clapon (Roumanie), M. Mushfig Guluyev (République d'Azerbaïdjan), M. Hideo Imanaka (Japon), Mme Mina Seonmin Jun (République de Corée), M. Mohamed Lamine Minthe (République de Guinée), M. Víctor Antonio Martínez Sánchez (République du Paraguay), Mme Alina Modan (Roumanie)[1], M. Diyor Rajabov (République d'Ouzbékistan)[1], M. Tongning Wu (République populaire de Chine) et M. Dominique Würges (France).

Le rapport a été rédigé sous la direction du Rapporteur pour la Question 4/2, M. Ibrahima Sylla (République de Guinée), auteur du Chapitre 1, avec la participation des auteurs suivants, pour les autres chapitres: les Vice-Rapporteurs Mme Tharalika Livera (République démocratique socialiste de Sri Lanka), auteur du Chapitre 2; M. Serigne Abdou Lahatt Sylla (République du Sénégal), auteur du Chapitre 3; M. Junzhi Yan (République populaire de Chine), auteur du Chapitre 4; Mme Awa Koko Valéry Nadège Traore épouse Goue (République de Côte d'Ivoire), auteur du Chapitre 5; et M. Sergei Melnik (International Telecommunication Academy), auteur du Chapitre 6. La contribution des participants actifs ci-dessous est également saluée: M. Gordon Gillerman (États-Unis d'Amérique) et M. Turhan Muluk (Intel Corporation).

Le présent rapport a été élaboré avec l'appui des Coordonnateurs pour la Question 4/2 de l'UIT-D, des éditeurs, de l'équipe chargée de la production des publications et du secrétariat de la Commission d'études 2 de l'UIT-D.

[1] A quitté ses fonctions au cours de la période d'études.

Table des matières

Liste des tableaux et figures

Tableaux

Figures

Résumé analytique

Les principes généraux qui ont guidé la rédaction du présent rapport ont consisté: 1) à tirer parti de la conformité et de l'interopérabilité (C&I) pour améliorer l'accès aux technologies de l'information et de la communication (TIC) pour les citoyens des pays en développement; 2) à éviter la création d'obstacles non nécessaires au commerce.

Le présent résumé met en relief les principales questions soulevées dans la Déclaration à la huitième Conférence mondiale de développement des télécommunications, qui s'est tenue à Kigali (République du Rwanda) du 6 au 16 juin 2022, sur le thème "**Connecter ceux qui ne le sont pas encore pour parvenir au développement durable**". Les principaux points soulevés étaient les suivants:

- **Importance des technologies de l'information et des télécommunications**: les dispositifs fondés sur les TIC jouent un rôle essentiel dans le monde numérique d'aujourd'hui.
- **Interopérabilité des réseaux**: la nécessité d'assurer l'interopérabilité entre les réseaux internationaux de télécommunication, qui fut la principale raison de la création de l'Union télégraphique internationale en 1865, reste aujourd'hui l'un des principaux objectifs du Plan stratégique de l'UIT.
- **Harmonisation des normes**: l'harmonisation des normes à l'échelle mondiale est essentielle pour assurer l'interopérabilité des réseaux et des dispositifs.
- **Programmes de conformité et d'interopérabilité (C&I)**: tous les pays mettent en œuvre des programmes de C&I, mais à des rythmes différents. Il est utile de mettre en valeur et de saluer les pratiques internationales existantes, comme celles établies aux États-Unis, dans l'Union européenne et ailleurs.
- **Assistance de l'UIT-D**: l'UIT-D aide les États Membres à résoudre les problèmes techniques et économiques liés à la conformité et à l'interopérabilité des dispositifs TIC.
- **Rôle des autorités de règlementation**: les autorités de règlementation jouent un rôle crucial dans la gestion des cadres de conformité et d'interopérabilité afin d'assurer la sécurité et le contrôle.
- **Évolutions futures**: l'émergence de nouvelles technologies, en particulier celles liées à l'Internet des objets (IoT), pose des difficultés supplémentaires pour la conformité et l'interopérabilité.
- **Nouvelles technologies de réseau**: il est nécessaire d'aider les États Membres, en particulier les pays en développement, à renforcer le niveau de compréhension et les connaissances en ce qui concerne les technologies de réseau désagrégées, ouvertes et interopérables, comme les réseaux d'accès radioélectrique ouvert (réseaux RAN ouverts), entre autres, en organisant des ateliers et d'autres activités de renforcement des capacités.
- **Fracture numérique**: il convient d'adopter des plans efficaces pour renforcer et améliorer les capacités et les compétences numériques nécessaires dans le monde en ligne, sans lesquelles les fractures numériques continueront de se creuser.
- **Bonnes pratiques**: le rapport porte sur les bonnes pratiques permettant de trouver des solutions optimales dans le domaine de la conformité et de l'interopérabilité.

En résumé, le rapport souligne qu'il importe d'aider les pays en développement dans le domaine de la conformité et de l'interopérabilité des TIC, ainsi que les obstacles à lever et les perspectives qui s'ouvrent dans ce domaine en évolution.

Abréviations et acronymes

Abréviations	Signification
3G	technologie mobile de troisième génération
3GPP	projet de partenariat de troisième génération
4G	technologie mobile de quatrième génération
5G	technologie mobile de cinquième génération
6G	technologie mobile de sixième génération[2]
AMNT	Assemblée mondiale de normalisation des télécommunications
ANSI	Institut national américain de normalisation
ANSSI	Agence nationale pour la sécurité des systèmes d'information de la Guinée
API	interface de programmation d'application
ARM	accord de reconnaissance mutuelle
C&I	conformité et interopérabilité
CAB	organe d'évaluation de la conformité
CEI	Commission électrotechnique internationale
CEM	compatibilité électromagnétique
CMDT	Conférence mondiale de développement des télécommunications
CNMN	consortium pour les normes de métrologie numérique
DMIS	norme d'interface de mesurage dimensionnelle
ETSI	Institut européen des normes de télécommunication
GSMA	Association du système mondial de communications mobiles
HPHC	dispositifs à haute capacité de traitement et à haute connectivité
IA	intelligence artificielle
IAF	forum international de l'accréditation

[2] Bien que toutes les précautions aient été prises, dans le présent document, pour employer correctement le terme des générations d'IMT selon leur définition officielle (voir la Résolution UIT-R 56 intitulée "Appellations pour les Télécommunications mobiles internationales, certaines parties du rapport contiennent des éléments fournis par les membres dans lesquels il est fait fréquemment référence à l'appellation commerciale des IMT, sous la forme "xG". Ces éléments ne peuvent pas nécessairement être mis en correspondance avec une génération particulière d'IMT, dans la mesure où les critères de catégorisation utilisés par les membres ne sont pas connus, mais, en règle générale, les concepts d'IMT-2000, IMT-évoluées, IMT-2020 et IMT-2030 sont respectivement désignés par les termes 3G, 4G, 5G et 6G.

(suite)

Abréviations	Signification
IECERS	système d'enregistrement intégré des équipements de communication électronique
IEEE	Institut des ingénieurs en électricité et en électronique
IETF	Groupe d'étude sur l'ingénierie Internet
ILAC	International Laboratory Accreditation Cooperation
IMEI	identité internationale d'équipement mobile
IMT	Télécommunications mobiles internationales
IoT	Internet des objets
ISO	Organisation internationale de normalisation
JTC	Comité technique mixte
KEBS	Bureau de normalisation du Kenya
LEO	orbite terrestre basse
LoRaWAN	réseau à couverture étendue de longue portée
LPHC	dispositif à faible capacité de traitement et à haute connectivité
LPLC	dispositif à faible capacité de traitement et à faible connectivité
LPWAN	réseau de faible puissance à couverture étendue
LTE	évolution à long terme
M2M	de machine à machine
NCA	Autorité nationale des communications du Ghana
OA	organismes d'accréditation
ODD	Objectifs de développement durable
OMC	Organisation mondiale du commerce
OTC	Obstacles techniques au commerce
PDCA	planifier, faire, vérifier, agir
PIB	produit intérieur brut
QIF	cadre d'information sur la qualité
RAN	réseau local d'accès
RF	radiofréquence
RGPD	Règlement général sur la protection des données
RNIS	réseau numérique à intégration de services
SIP	protocole d'ouverture de session

(suite)

Abréviations	Signification
SWG 5	Groupe de travail spécial 5
TIA	Association du secteur des télécommunications
TIC	Technologies de l'information et de la communication
TRCL	Commission de régulation des télécommunications de Sri Lanka
UIT	Union internationale des télécommunications
UIT-D	Secteur du développement des télécommunications de l'UIT
UIT-R	Secteur des radiocommunications de l'UIT
UIT-T	Secteur de la normalisation des télécommunications de l'UIT
W3C	World Wide Web Consortium
WSN	réseau de capteurs sans fil

Chapitre 1 – Les produits TIC pour atteindre les Objectifs de développement durable

1.1 Introduction

Les Objectifs de développement durable (ODD) sont au cœur des efforts mondiaux visant à résoudre les enjeux les plus pressants de notre époque, de la lutte contre la pauvreté à la durabilité environnementale. Les technologies de l'information et des communications (TIC) jouent un rôle crucial dans la réalisation de ces objectifs, offrant des outils et des solutions innovantes pour s'attaquer à ces difficultés de manière efficace et durable.

Les produits TIC peuvent contribuer à l'ensemble des ODD. Par exemple, les applications mobiles peuvent être utilisées pour améliorer l'accès à l'enseignement, les systèmes de surveillance fondés sur des capteurs peuvent aider à gérer les ressources en eau, et les plates-formes de commerce électronique peuvent stimuler une croissance économique inclusive.

De plus, les TIC peuvent encourager la collaboration et la sensibilisation en permettant aux individus et aux organisations d'échanger des informations, de coordonner leurs actions et de mobiliser des ressources à l'échelle mondiale. Cela favorise une approche holistique et intégrée de la réalisation des Objectifs de développement durable, en encourageant la coopération entre les autorités, le secteur privé, la société civile et les citoyens.

En investissant dans le développement et l'utilisation de produits TIC pour réaliser les Objectifs de développement durable, le potentiel de la technologie peut être exploité pour créer un avenir plus juste, plus durable et plus prospère pour tous.

Figure 1: Les Objectifs de développement durable

Source: ONU[3]

[3] https://www.un.org/fr/teach/SDGs

1.2 Intérêt des produits TIC pour la société

Les produits TIC jouent un rôle essentiel dans notre société moderne, offrant une multitude d'avantages et de possibilités. Leur intérêt pour la société s'observe à plusieurs niveaux:

- **Connectivité accrue**: les produits TIC, tels que les téléphones intelligents et les ordinateurs, facilitent la communication et la connectivité entre les individus, les peuples et les nations. Cela favorise l'échange d'informations et la collaboration, et renforce les liens sociaux.
- **Accès à l'information**: les TIC permettent un accès rapide et facile à une vaste quantité d'informations sur divers sujets, ce qui favorise l'apprentissage, la recherche, et la prise de décisions éclairées.
- **Amélioration des services publics**: les pouvoirs publics utilisent les produits TIC pour améliorer l'efficacité et l'accessibilité des services publics, tels que les services de santé en ligne, les systèmes d'enseignement à distance et les plates-formes de gestion des transports.
- **Innovation et développement économique**: les TIC stimulent l'innovation et le développement économique en facilitant la création d'entreprises, l'accès aux marchés mondiaux et l'automatisation des opérations commerciales.
- **Inclusion sociale**: les produits TIC peuvent contribuer à réduire la fracture numérique en fournissant un accès équitable à la technologie et en permettant aux groupes marginalisés d'accéder à de nouvelles perspectives sur le plan économique et social.
- **Aide à la réalisation des ODD**: les produits TIC peuvent jouer un rôle utile dans de nombreux domaines sociaux et environnementaux, tels que la lutte contre la pauvreté, la hausse de la scolarisation, la gestion des ressources naturelles et la réduction des inégalités.

Ainsi, les produits TIC sont importants pour la société car ils favorisent la connectivité, l'accès à l'information, l'efficacité des services publics, l'innovation économique, l'inclusion sociale et la réalisation des ODD.

1.3 Applications socio-économiques des TIC

Lorsque les objectifs sociaux d'une société sont bien intégrés et pris en compte au même titre que la viabilité économique, les dispositifs TIC peuvent aider à combiner les principes de l'entreprise sociale avec les possibilités offertes par la technologie pour obtenir des retombées positives et durables pour la société. Voici quelques façons dont les dispositifs TIC peuvent être utilisés dans ce contexte:

- **Accessibilité élargie**: grâce aux dispositifs TIC, les initiatives socioéconomiques peuvent produire des résultats plus marquants, en atteignant un public plus large. Les technologies telles que les téléphones intelligents ou les ordinateurs abordables peuvent rendre les services accessibles à un plus grand nombre de personnes, y compris celles des communautés marginalisées ou à faible revenu.
- **Innovation sociale**: les dispositifs TIC permettent d'élaborer et de mettre en œuvre des solutions innovantes pour résoudre des problèmes sociaux. Par exemple, les applications mobiles peuvent être conçues pour fournir des services de santé abordables dans les zones rurales ou pour faciliter l'accès à l'enseignement parmi les groupes défavorisés de la population.
- **Renforcement des capacités**: les équipements et dispositifs TIC peuvent être utilisés pour renforcer les capacités des organisations socioéconomiques en les dotant d'outils de gestion, de suivi et d'évaluation. Les logiciels de gestion de projet, les plates-formes

de collecte de données et les outils de communication en ligne peuvent aider ces organisations à optimiser leurs opérations et à en mesurer l'impact.

- **Inclusion numérique**: en offrant des formations sur l'utilisation des dispositifs TIC et les compétences numériques, les initiatives socioéconomiques peuvent favoriser l'inclusion numérique et réduire la fracture numérique au sein de la population.
- **Réduire la fracture entre les hommes et les femmes**: les TIC et produits TIC sont une voie essentielle vers l'égalité hommes-femmes et l'autonomisation de toutes les femmes et les jeunes filles.
- **Durabilité environnementale**: les dispositifs TIC peuvent également être utilisés de manière responsable sur le plan environnemental dans une société socioéconomique. Par exemple, les initiatives de recyclage des équipements électroniques peuvent contribuer à réduire les déchets électroniques et à renforcer la durabilité environnementale. En intégrant les dispositifs TIC dans une société socioéconomique, il est possible de créer des solutions innovantes, accessibles et durables pour répondre aux besoins sociaux, économiques et environnementaux de la population.

Les avantages liés à l'utilisation des produits TIC sont de plus en plus appréciés par les pays en développement, dont la plupart se lancent dans de vastes programmes de développement des TIC.

C'est dans ce contexte que la République centrafricaine[4] s'attaque à d'importantes lacunes règlementaires et institutionnelles afin de tirer pleinement profit du numérique en tant que moteur de croissance et outil d'aide à la réduction de la pauvreté. Les objectifs finaux consistent à résoudre les problèmes liés à la contrefaçon et à la falsification des équipements TIC et, surtout, à atteindre l'ODD relatif à l'industrie, à l'innovation et à l'infrastructure (ODD N° 9) à l'horizon 2030.

In fine, désireuse d'encourager la recherche, le développement et l'innovation technologique au niveau national et d'accroître de manière significative l'accès du public aux technologies et services large bande à un coût abordable, la République Centrafricaine a décidé de prendre les mesures suivantes:

a) améliorer le cadre juridique et règlementaire du secteur des télécommunications;

b) renforcer les capacités du Ministère de l'économie numérique, des postes et des télécommunications et de l'Autorité de régulation des télécommunications, qui est l'Autorité de régulation des communications électroniques et des postes;

c) établir un laboratoire accrédité approprié, chargé de tester ou de reconnaître les équipements TIC;

d) encourager le partage et le déploiement des infrastructures de télécommunications par l'autorité de régulation afin de réduire les coûts de déploiement.

1.4 Respect des normes TIC reconnues en matière de qualité et d'interopérabilité

Dans le contexte des TIC au service de la société, la conformité aux normes reconnues revêt une importance cruciale pour garantir la qualité, la sécurité et l'interopérabilité des produits

[4] Document SG2RGQ/17 de la CE 2 de l'UIT-D (République centrafricaine).

et des services. Parmi les normes reconnues auxquelles les produits TIC doivent se conformer, on peut citer:

- ISO 27001 – Sécurité de l'information: cette norme de l'Organisation internationale de normalisation (ISO) définit les exigences pour mettre en œuvre, tenir à jour et améliorer un système de gestion de la sécurité de l'information. Elle vise à protéger les informations sensibles contre les menaces telles que le piratage, la perte de données et les atteintes à la confidentialité.
- ISO 9001 – Qualité du management: la norme ISO 9001 établit les critères pour un système de gestion de la qualité efficace. Elle s'adresse aux fournisseurs de produits TIC afin de garantir la satisfaction des clients, l'amélioration continue et la conformité règlementaire.
- Le World Wide Web Consortium (W3C) établit des normes et des recommandations pour le développement des technologies web, telles que HTML, CSS et JavaScript. La conformité à ces normes assure que les produits TIC soient compatibles avec les navigateurs web modernes et accessibles à un large public.
- Règlement général sur la protection des données (RGPD): il est essentiel que les produits TIC traitant des données personnelles des utilisateurs se conforment aux dispositions du RGPD est pour garantir le respect de la vie privée et la protection des données.
- L'Institute of Electrical and Electronics Engineers (IEEE) établit des normes pour divers aspects des TIC, tels que les réseaux sans fil, les communications Ethernet et les normes de codage.
- Norme ISO/CEI 17025 "Prescriptions générales concernant la compétence des laboratoires d'étalonnages et d'essais". Cette norme de l'ISO et de la Commission électrotechnique internationale énonce les exigences générales relatives à la compétence, à l'impartialité et au bon fonctionnement des laboratoires. Il est employé par les clients des laboratoires, les autorités de règlementation, les organisations et les systèmes d'évaluation par les pairs, les organismes d'accréditation, etc. pour confirmer ou reconnaître la compétence des laboratoires. En faisant tester leurs produits TIC dans des laboratoires compétents (conformément à des normes telles que les recommandations du Secteur de la normalisation des télécommunications de l'UIT (UIT-T)) accrédités par des organismes signataires des Accords de reconnaissance mutuelle (ARM) de la Coopération internationale pour l'accréditation des laboratoires (ILAC), les fournisseurs de TIC gagnent la confiance de leurs clients en ce qui concerne la conformité et l'interopérabilité.
- Normes 5G (Télécommunications mobiles internationales (IMT) 2020) et 4G évolution à long terme (LTE) pour les communications mobiles à haut débit.
- ISO/CEI 17788 et ISO/CEI 17789 pour les normes relatives à l'architecture de référence de l'informatique en nuage.
- Norme ISO/CEI 22989 relative à la terminologie et aux concepts liés à l'intelligence artificielle (IA).

Tableau 1: Organisations élaborant ou validant des normes internationales

N°	Organisation	Description	Lien
1	UIT	L'Union internationale des télécommunications élabore des normes mondiales pour les télécommunications et les TIC.	https://www.itu.int/ITU-T
2	ISO	L'Organisation internationale de normalisation publie des normes internationales pour divers secteurs, dont celui des TIC.	https://www.iso.org

Tableau 1: Organisations élaborant ou validant des normes internationales (suite)

N°	Organisation	Description	Lien
3	CEI	La Commission électrotechnique internationale planche sur les normes relatives aux technologies électriques, électroniques et connexes.	https://www.iec.ch
4	IEEE	L'Institute of Electrical and Electronics Engineers élabore des normes pour un large éventail de secteurs, dont les TIC et les réseaux.	https://www.ieee.org
5	ETSI	L'Institut européen des normes de télécommunication établit des normes pour les systèmes et services TIC en Europe et dans le monde.	https://www.etsi.org
6	ANSI	L'Institut national américain de normalisation supervise l'élaboration de normes faisant l'objet d'un consensus volontaire aux États-Unis.	https://www.ansi.org
7	W3C	Le World Wide Web Consortium (W3C) élabore des normes pour le web afin de garantir sa croissance et son interopérabilité à long terme.	https://www.w3.org

Principaux points:

- **Respect des normes**: veiller à ce que les produits et services TIC répondent aux normes mondiales en matière de qualité, de sécurité et d'interopérabilité.
- **Conformité**: veiller au respect des normes internationalement reconnues pour faciliter l'accès au marché et susciter la confiance des utilisateurs.
- **Interopérabilité**: veiller à la fluidité de l'intégration et de la communication entre différents systèmes et technologies.

Davantage de partenariats et d'échanges d'informations doivent être instaurés avec les principales organisations extérieures qui jouent un rôle déterminant dans l'élaboration des normes et l'accréditation internationale. Voici quelques mesures à prendre:

- **Créer des points de contact spécialisés** avec des organisations telles que l'IEEE, l'ISO, la CEI et le Groupe de travail sur l'ingénierie Internet (IETF) afin de favoriser un échange régulier d'informations.
- **Participer activement à des forums et à des groupes de travail** (Projet de partenariat de troisième génération (3GPP), IETF, IEEE, etc.) pour parvenir à une meilleure intégration des besoins locaux dans les normes internationales.
- **Mettre en place des mécanismes de suivi** pour recueillir des données d'intérêt dans ces budgets extérieurs et les intégrer dans les rapports futurs.
- **Renforcer les liens entre les institutions** par le biais d'accords de coopération ou de partenariat stratégiques afin de stimuler l'échange mutuel de compétences et de ressources.

Les programmes d'évaluation mondiaux doivent être adaptables et tournés vers l'avenir, à l'instar de ceux de la WiFi Alliance. Voici quelques mesures qui pourraient être prises:

- **Définir des programmes spécifiques**: par exemple, les certifications WiFi CERTIFIED® délivrées par la WiFi Alliance garantissent l'interopérabilité, la sécurité et les performances des produits[5].
- **Souligner leur importance**: décrire la manière dont ces programmes favorisent l'adoption de normes et assurent la compatibilité entre différents équipements et technologies.
- **Intégrer d'autres initiatives similaires**: mentionner des programmes tels que Bluetooth Special Interest Group (SIG), LoRa Alliance ou d'autres consortiums travaillant sur l'interopérabilité des technologies émergentes.
- **Analyser les retombées au niveau régional**: évaluer l'influence de ces programmes sur les marchés locaux et leur intérêt pour le développement technologique et économique de la région dans le rapport.

Pour exploiter le potentiel de transformation des plates-formes et des processus numériques, plusieurs pistes de développement devraient être envisagées:

- Définir les plates-formes numériques: expliquer ce qu'est une plate-forme numérique, comment elle facilite l'interconnexion des différents acteurs, produits et services (ex.: plates-formes de paiement, plates-formes de communication et commerce électronique).
- Présenter les avantages des plates-formes numériques:
    1) **Efficacité accrue**: optimisation des opérations commerciales et réduction des coûts d'exploitation.
    2) **Accessibilité accrue**: facilite l'accès aux services à distance, améliore l'inclusion et la connectivité.
    3) **Innovation continue**: permet le développement rapide de nouveaux produits et services grâce à l'intégration de technologies émergentes.
- Étudier les processus numériques:
    1) **Automatisation des processus**: intégration de technologies d'automatisation pour améliorer la productivité et réduire le risque d'erreur humaine.
    2) **Transformation des modèles économiques**: adoption d'outils numériques pour faciliter la gestion de l'information, la communication et la collaboration au sein des entreprises et des administrations publiques.
    3) **Numérisation des services publics**: étudier les incidences de la numérisation des services publics (ex.: administration en ligne, cybersanté, cyberenseignement).
- Exemples de plates-formes et de processus numériques efficaces:
    1) **Les plates-formes collaboratives**: telles que celles utilisées pour le cyberenseignement ou la télémédecine.
    2) **Processus numériques dans le secteur public**: déploiement de services publics numériques pour simplifier les démarches administratives.
    3) **Secteurs spécifiques**: applications dans les secteurs de la finance (Fintech), des transports (Mobility as a Service), etc.
- Enjeux et potentialités:

[5] https://www.wi-fi.org/certification

1) **Enjeux**: sécurité des données, cybersécurité, vie privée, exigences en matière d'infrastructure, inclusion numérique.
2) **Potentialités**: mise en place d'une économie numérique, amélioration de la compétitivité, stimulation de l'innovation.

1.5 Incidences de la pandémie de COVID-19 sur les procédures d'approbation

La pandémie de COVID-19 a eu d'importantes répercussions sur les procédures d'approbation dans de nombreux domaines, y compris dans le domaine des TIC. Voici quelques-unes des principales conséquences de la pandémie sur ces procédures:

- **Numérisation des procédures**: avec les restrictions de déplacement et les mesures de distanciation sociale, de nombreuses procédures d'autorisation ont été entièrement numérisées. Les autorités ont mis en place des plates-formes en ligne pour soumettre et traiter les demandes d'autorisation, réduisant ainsi la nécessité de documents physiques et de rencontres en personne.
- **Accélération des délais de traitement**: dans de nombreux cas, la pandémie a entraîné une accélération des délais de traitement des autorisations, car les autorités ont cherché à faciliter le déploiement rapide de solutions TIC pour répondre aux besoins urgents liés à la pandémie, tels que le télétravail, le cyberenseignement et la télémédecine.
- **Flexibilité accrue**: les autorités ont fait preuve d'une plus grande flexibilité dans l'évaluation des demandes d'autorisation, étant donnée les circonstances exceptionnelles découlant de la pandémie. Dans certains cas, cela a entraîné la simplification des procédures ou l'assouplissement des critères d'admissibilité pour encourager l'innovation et le déploiement rapide de solutions technologiques.
- **Renforcement de la sécurité**: malgré la tendance à la numérisation, les autorités ont également renforcé les mesures de sécurité pour protéger les données sensibles et prévenir les abus. Cela a entraîné la mise en place de protocoles de sécurité robustes pour veiller à l'intégrité et à la confidentialité des informations soumises dans le cadre des demandes d'autorisation.
- **Collaboration internationale**: la pandémie a suscité une plus grande collaboration internationale dans l'évaluation et la règlementation des technologies de l'information et des communications. Les autorités ont communiqué sur les bonnes pratiques, ont échangé des données et des ressources pour faire face aux difficultés communes posées par la pandémie et pour encourager une approche coordonnée à l'échelle mondiale.

Chapitre 2 – Conformité et interopérabilité

2.1 Introduction

Le secteur des télécommunications/TIC évolue rapidement, porté par l'innovation en matière de produits, de services et d'infrastructures. Au vu de l'interconnexion croissante de ces technologies, il est essentiel que les différents acteurs veillent à leur conformité et à leur interopérabilité. L'évaluation de la conformité permet de garantir que l'équipement TIC soit bien conforme aux normes et aux spécifications techniques, qui sont essentielles pour évaluer la qualité de fonctionnement et la compatibilité dans les environnements de réseaux. Les tests d'interopérabilité servent à s'assurer que plusieurs produits soient bien à même de s'intégrer et de communiquer sans heurts, en prenant en charge des protocoles de communication spécifiques. Ces tests sont conçus pour déterminer si deux ou plusieurs produits répondent aux spécifications techniques nécessaires à une intégration réussie en suivant des protocoles de communication spécifiques dans les secteurs des télécommunications et des TIC, en s'appuyant sur les connaissances d'organisations internationales telles que l'UIT et de groupes de travail régionaux. Cela met en lumière le paysage complexe dans lequel interviennent les initiatives en matière de conformité et d'interopérabilité: problèmes de signalisation dans les réseaux traditionnels, multiplication des téléphones mobiles de contrefaçon, etc. Ce chapitre traite également des arrangements et accords de reconnaissance mutuelle (ARM) relatifs à l'évaluation de la conformité, qui facilitent la reconnaissance transfrontière des résultats de tests et des certifications, et encouragent le commerce et la coopération internationaux. Il aborde également le rôle des tests de préconformité dans l'évaluation de la conformité des produits aux normes applicables, ainsi que l'importance de la surveillance du marché, de la sensibilisation des fournisseurs et des utilisateurs au respect des normes de qualité et de la lutte contre la contrefaçon des produits.

Les ARM peuvent être multilatéraux, passés entre des organismes d'accréditation dont l'équivalence est validée par des pairs afin d'évaluer la compétence des organismes d'évaluation de la conformité, tels que les laboratoires qui testent les produits TIC. Ces ARM contribuent à l'acceptation mutuelle des résultats des tests dans les pays représentés par les membres, ce qui peut aider à surmonter les obstacles techniques au commerce (OTC). Les ARM peuvent également être conclus entre des gouvernements pour renforcer le commerce, par l'acceptation mutuelle des produits et des rapports d'essai des laboratoires de ces pays respectifs accrédités par leur organisme d'accréditation national.

La vérification obligatoire de la conformité des équipements TIC est un outil essentiel pour garantir l'intégrité, la stabilité et la sécurité des réseaux de télécommunication. Cependant, il est essentiel de réduire le nombre de contrôles et de raccourcir le délai de mise sur le marché des équipements TIC. Si des ARM pour les résultats de tests provenant de laboratoires étrangers peuvent jouer un rôle utile, cette procédure est souvent coûteuse et longue en raison de la nécessité de faire traduire et apostiller les protocoles de test.

Une solution possible serait la création d'une expertise nationale en TIC, dans le cadre de laquelle une entité approuvée par les autorités assumerait la responsabilité de la vérification

de la conformité. Cette méthode réduit au minimum le temps et les coûts d'examen, car elle ne nécessite pas de tests complets de l'équipement. Le coût de tels examens est nettement inférieur à celui de la réalisation de tests complets des équipements TIC.

1) Conformité et interopérabilité:

- Les tests de conformité permettent de vérifier que les équipements TIC sont conformes aux normes et spécifications techniques.
- Les tests d'interopérabilité ont pour but de s'assurer que les produits peuvent s'intégrer correctement dans un réseau.
- Ces tests sont cruciaux pour détecter les équipements non conformes, qui pourraient compromettre la qualité du réseau.

2) Normes et spécifications techniques:

- Les normes sont fixées par les fournisseurs de services, les opérateurs et les régulateurs nationaux.
- Le respect de ces normes garantit l'interopérabilité, réduit la dépendance vis-à-vis d'un fournisseur en particulier et favorise la compétitivité sur le marché.
- Le Comité des obstacles techniques au commerce de l'Organisation mondiale du commerce (OMC) insiste sur la transparence, l'ouverture, l'impartialité et la cohérence dans l'élaboration des normes.

3) Accords de reconnaissance mutuelle (ARM):

- Les ARM facilitent la reconnaissance des résultats des tests de conformité entre les pays, en réduisant les coûts et la redondance des tests.
- Leur objectif est de se limiter à "un seul test, accepté partout". Cependant, les ARM se heurtent à des difficultés telles que des obstacles juridiques, un manque de réciprocité et l'insuffisance des ressources dans certains pays.

4) Savoir-faire national dans le domaine des TIC:

- Un système national de savoir-faire dans le domaine des TIC permet de maintenir la conformité aux normes nationales et internationales.
- Il établit les diverses responsabilités, décourage la contrefaçon des produits, et réduit les coûts en évitant la nécessité de mener des tests à grande échelle.
- Ce système exige un cadre règlementaire, des règles d'accréditation et des experts qualifiés.

5) Enjeux et solutions:

- Les différences dans la mise en œuvre des TIC entre les divers pays compliquent la reconnaissance mutuelle.
- Les systèmes nationaux de savoir-faire peuvent lever ces obstacles en vérifiant la conformité sur le plan local[6].

2.2 Examen de questions essentielles

Les problèmes d'interopérabilité dans la signalisation des réseaux intelligents existants peuvent être attribués à différents facteurs:

1) manque de conformité et d'interopérabilité entre les équipements de différents fournisseurs;

[6] Document 2/140 de la CE 2 de l'UIT-D (Académie internationale des télécommunications).

2) interfaces ou protocoles non normalisés; et

3) révisions logicielles provenant d'un unique fabricant.

Il peut en résulter une incompatibilité des protocoles d'ouverture de session (SIP). La capacité en vidéos, données et fichiers vocaux peut aussi souffrir de la surcharge du réseau. L'interopérabilité au sein de réseaux complexes peut être obtenue par l'intégration des réseaux et des dispositifs. Toutefois, il se peut que certains fournisseurs ne disposent pas de l'infrastructure et des équipes nécessaires à l'interopérabilité avec d'autres opérateurs. L'adoption de normes, la gestion des enregistrements détaillés des appels et la mise en œuvre de nouvelles fonctionnalités et de nouveaux services sur l'ensemble des plates-formes posent également des difficultés. Il y a en outre un manque de centres de test et de personnel formé, ainsi que des problèmes associés aux support du réseau numérique à intégration de services (RNIS), aux terminaux d'utilisateurs, à l'interopérabilité des services et des équipements terminaux utilisés par les clients.

De plus, certains problèmes ont été recensés aux niveaux régional et national, tels que:

- l'absence de collaboration régionale dans l'élaboration et la mise en œuvre de solutions au problème de contrefaçon de téléphones;
- le manque de données de référence permettant d'éclairer l'élaboration et la mise en œuvre des stratégies de lutte contre le commerce des dispositifs de contrefaçon au niveau régional;
- les problèmes persistants liés à l'accessibilité des téléphones portables sur le plan financier;
- la méconnaissance du problème de la contrefaçon de téléphones;
- la menace potentiellement posée par les dispositifs de contrefaçon pour les plans nationaux de transformation numérique des pays en développement;
- la baisse de la contribution du secteur des TIC au produit intérieur brut (PIB) du pays en raison du poids économique de la contrefaçon des dispositifs;
- la menace posée par les dispositifs de contrefaçon pour la sécurité, la performance des réseaux et la qualité de service, et mise en danger des populations en raison de multiples risques sanitaires.

La hausse de la demande de téléphones mobiles et du taux de possession permanent dépasse les facteurs géographiques tels que le clivage urbain/rural, et de facteurs sociétaux tels que la variabilité des revenus, le niveau d'analphabétisme, mais, pris ensemble, ils constituent un moteur potentiel d'afflux de téléphones de contrefaçon sur le marché[7].

2.3 Normes et spécifications techniques

2.3.1 Démonstration d'applications de C&I aux niveaux national et régional

La démonstration de la conformité et de l'interopérabilité des applications est cruciale pour comprendre les expériences réalisées aux niveaux national et régional et encourager l'adoption des bonnes pratiques. Il s'agit notamment de la désignation et de la reconnaissance des organismes d'accréditation et de certification, des normes et pratiques internationales et des laboratoires d'essais, de l'enregistrement et de la certification. Ces démonstrations peuvent

[7] Document SG2RGQ/37 de la CE 2 de l'UIT-D (Zambie).

fournir des informations précieuses sur les stratégies de mise en œuvre réussies, les difficultés rencontrées et les enseignements tirés.

L'un des prérequis pour la désignation ou la reconnaissance d'un organisme d'accréditation est la signature des ARM de l'ILAC et du Forum international de l'accréditation (IAF), attestant officiellement des méthodes et des critères utilisés pour évaluer si les organismes de certification et les laboratoires d'essais respectent les normes internationales.

En présentant des exemples d'organismes d'accréditation qui ont réussi à promouvoir les pratiques d'évaluation de la conformité et à faciliter l'accès aux marchés pour des produits et services conformes, on peut renforcer la confiance et réduire les obstacles au commerce. La désignation et la reconnaissance des organismes de certification vise à établir les procédures et les exigences permettant d'évaluer la conformité d'un produit aux normes et règlementations applicables.

La démonstration de la compétence, l'impartialité et la cohérence du fonctionnement des laboratoires de test peuvent renforcer la confiance dans leur capacité à produire des résultats de test valides. Lorsqu'il est difficile d'établir un programme national comprenant tous les différents éléments, les pays peuvent s'appuyer sur les bonnes pratiques, voire sur les certifications issues de programmes établis.

L'enregistrement et la certification désignent les procédures et critères d'enregistrement ou de certification de produits, de services ou de systèmes qui attestent de la conformité aux règlementations et normes applicables. La présentation de produits certifiés démontre que les marques d'enregistrement ou de certification sont des symboles de qualité, de sécurité et de fiabilité, permettant aux consommateurs de faire des achats éclairés. La reconnaissance de marques de certification issues de programmes établis, bien gérés et internationalement reconnus comme preuve de conformité peut réduire considérablement les coûts, les délais pour les consommateurs et les coûts pour l'administration nationale.

2.3.2 Bonnes pratiques

- **Délivrance de certificats de revendeur**: veiller à ce que les revendeurs de dispositifs TIC obtiennent des certificats officiellement reconnus afin de renforcer la transparence et la conformité.
- **Création d'un système intégré d'enregistrement**: mettre en place un système complet de référence et d'enregistrement des équipements de communications électroniques afin d'améliorer la traçabilité et le contrôle règlementaire.
- **Accès des consommateurs à la vérification des numéros d'identité internationale d'équipement mobile (IMEI)**: fournir aux consommateurs un moyen facilement accessible de vérifier les numéros IMEI au moyen d'un code court, améliorant ainsi l'authentification des dispositifs et la prévention de la fraude.
- **Rapports régionaux sur les tendances en matière de contrefaçon**: faciliter la mise à disposition de rapports régionaux sur les volumes et les tendances signalés (par exemple les modèles de téléphones les plus susceptibles d'être contrefaits) afin de sensibiliser les consommateurs.
- **Reconnaissance des normes internationales en matière d'essais et de certification**: veiller à ce que les résultats des tests et les certifications soient conformes aux normes et aux bonnes pratiques internationales pour renforcer l'interopérabilité et l'acceptation sur le marché.

2.3.3 Mécanismes de collaboration possibles en vue de l'établissement d'une C&I commune

Les fournisseurs de services et les opérateurs appliquent des normes et des spécifications harmonisées pour les équipements et les systèmes qu'ils utilisent pour servir leurs clients. Les régulateurs nationaux établissent des règlements pour harmoniser les normes et les spécifications des équipements et des systèmes déployés sur le territoire national. Les utilisateurs, les fournisseurs de services et les régulateurs nationaux doivent obtenir la preuve irréfutable que ces équipements et systèmes sont bien conformes aux normes, exigences et spécifications d'interopérabilité appropriées.

Afin de faciliter l'élaboration de normes, de guides et de recommandations internationaux, le Comité des obstacles techniques au commerce de l'OMC a établi les six principes suivants:

1) **Transparence**: en vertu de ce principe, toutes les informations essentielles concernant les travaux actuellement programmés, ainsi que les propositions de normes, de guides et de recommandations à l'examen et les résultats finaux, doivent être facilement accessibles à au moins toutes les parties intéressées, sur le territoire d'au moins tous les Membres de l'OMC. Elle encourage l'établissement de procédures qui laissent suffisamment de temps et de possibilités pour la soumission d'observations écrites. Les informations relatives à ces procédures devraient être diffusées comme il se doit.

   Afin de fournir des informations essentielles, les procédures de transparence devraient prévoir: l'octroi d'un délai suffisant pour permettre aux parties intéressées de soumettre leurs observations par écrit et d'en tenir compte lors de l'examen ultérieur de la norme; la publication rapide d'une norme après son adoption et la publication régulière d'un programme de travail contenant des informations sur les normes en cours d'élaboration et d'adoption.

2) **Ouverture**: en vertu de ce principe, la participation aux activités d'un organisme international de normalisation doit être ouverte, sans discrimination, aux organes compétents d'au moins tous les Membres de l'OMC, tant pour la participation à l'élaboration des politiques générales qu'à chaque étape de l'élaboration des normes.

   À ce titre, tout membre d'un organisme international de normalisation (en particulier les pays en développement) intéressé par l'une ou l'autre activité de normalisation devrait se voir offrir de bonnes possibilités de participer à toutes les étapes de l'élaboration des normes.

3) **Impartialité et consensus**: ce principe fait ressortir la possibilité, pour tous les organes concernés des membres de l'OMC, de contribuer de bonne manière à l'élaboration d'une norme internationale, afin que la procédure d'élaboration de cette norme ne privilégie pas ou ne favorise pas les intérêts d'un ou de plusieurs fournisseurs, pays ou régions particuliers. Il souligne l'importance du consensus, pour tenir compte des points de vue de toutes les parties concernées et concilier les arguments divergents.

4) **Efficacité et pertinence**: les normes internationales doivent être pertinentes et répondre efficacement aux besoins de la règlementation et du marché, ainsi qu'aux progrès scientifiques et techniques dans les différents pays, afin de faciliter le commerce international et d'éviter des obstacles inutiles au commerce.

   Elles ne devraient pas fausser le marché mondial, nuire à une concurrence loyale, ni freiner l'innovation et le développement technologique. En outre, elles ne devraient pas privilégier les caractéristiques ou les besoins de certains pays ou de certaines régions lorsque des besoins ou des intérêts différents existent dans d'autres pays ou régions. Dans la mesure du possible, les normes internationales devraient avoir à cœur la qualité de fonctionnement plutôt que des caractéristiques nominales ou descriptives.

5) **Cohérence**: en vertu de ce principe, les organismes internationaux de normalisation doivent éviter les chevauchements ou les doubles emplois avec les travaux d'autres organismes internationaux de normalisation afin d'éviter l'instauration de normes internationales contradictoires. À cet égard, la coopération et la coordination avec d'autres organismes internationaux compétents sont essentielles.

6) **Dimension "développement"**: ce principe suggère que les contraintes auxquelles sont confrontés les pays en développement, en particulier celles qui les empêchent de participer efficacement à l'élaboration des normes, doivent être prises en compte lors de l'élaboration des normes. À ce titre, il encourage la recherche de moyens de faciliter la participation des pays en développement à l'élaboration de normes internationales (ex.: en recourant à l'assistance technique et au renforcement des capacités).

2.3.4 Coopération technique

- **Renforcement des capacités et formation**: élaborer des projets nationaux et régionaux, parallèlement à des activités de formation, pour aider les États à mettre en œuvre des mesures efficaces contre l'afflux de dispositifs de contrefaçon.
- **Appui politique et règlementaire**: contribuer à formuler et à renforcer les politiques, les règlementations et les mécanismes d'application afin de freiner la circulation des dispositifs TIC non conformes.
- **Collaboration transfrontière**: encourager la coopération entre les organismes de règlementation, les organismes chargés de l'application de la loi et les parties prenantes de l'industrie aux niveaux national et régional afin de renforcer la lutte contre la contrefaçon.
- **Amélioration de la technologie et de l'infrastructure**: encourager le déploiement de technologies avancées pour l'authentification, le suivi et la vérification des dispositifs afin d'améliorer l'intégrité du marché.

2.4 Arrangements et accords de reconnaissance multilatérale portant sur l'évaluation de la conformité

2.4.1 Qu'est-ce qu'un arrangement ou accord de reconnaissance mutuelle?

Un ARM est un accord contractuel (concernant les procédures et méthodes) conclu entre des parties (entités privées ou publiques) concernant la reconnaissance des résultats de l'évaluation de la conformité.

- **Confiance mutuelle**: renforcement de la coopération technique et de la confiance entre les autorités de régulation.

La Recommandation UIT-T Q.4068 présente un ensemble d'interfaces API ouvertes pour la fédération de bancs d'essai interopérables, capables de gérer non seulement l'interconnexion et l'interopérabilité des bancs d'essai dans une fédération, mais aussi la présentation, l'attribution et la fourniture des ressources. Des API sont conçues pour gérer les utilisateurs prenant part à la fédération, tels que les expérimentateurs, et pour attribuer des rôles aux utilisateurs. De même, l'utilisation des ressources est attribuée à un expérimentateur par le biais des interfaces API ouvertes pour la fédération de bancs d'essai interopérables. Un cas d'utilisation typique d'une expérience est une fédération de bancs d'essai et des exigences connexes. Des cas d'utilisation similaires peuvent être mis en œuvre dans une fédération de bancs d'essai comme Fed4FIRE.

2.4.2 Rôle des ARM dans la conformité et l'interopérabilité

Les ARM servent à:

- valider la compétence de tierces parties pour mener à bien les procédures nationales de règlementation ou d'octroi de licences;
- éviter les coûts découlant de la redondance des tests et favoriser la transparence;
- faciliter l'accès aux marchés étrangers;
- réduire les délais de mise sur le marché et les coûts de production;
- lutter contre les pratiques prédatrices et supprimer les obstacles à l'entrée sur le marché;
- rationaliser les procédures et les méthodes, en réduisant sensiblement les coûts pour les producteurs sur plusieurs marchés.

L'objectif ultime est de tester les produits une fois afin qu'ils soient acceptés partout.

2.4.3 Questions relatives aux ARM internationaux

Malheureusement, l'utilisation d'ARM est souvent émaillée de difficultés:

- De nombreux pays ne disposent pas d'un mécanisme juridique pour utiliser des documents établis dans un autre pays et ne disposent pas de traductions apostillées dans la langue du pays cible.
- Tous les pays ne disposent pas des ressources matérielles et humaines nécessaires pour effectuer leurs propres essais. Dans ce cas, la reconnaissance mutuelle des résultats d'essais et d'études ne peut pas avoir lieu, et la reconnaissance unilatérale ne serait pas acceptable. Dans ces cas, les pays peuvent reconnaître les résultats de tests et les certifications émanant d'administrations nationales ou internationales ayant une bonne réputation, ou de programmes nationaux ou régionaux bien établis et bien attestés. Cela permettra l'utilisation licite de tous les résultats d'essais et de recherches fondés sur l'avis de spécialistes d'une organisation autorisée par l'administration des communications du pays.
- Les TIC varient d'un pays à l'autre. L'administration des communications du pays fixe les objectifs de mise en œuvre des TIC. La conformité aux objectifs d'utilisation des TIC doit être contrôlée par un organisme agréé par l'administration des communications du pays.
- Dans le cas d'un différend, susceptible d'entraîner des préjudices en raison d'erreurs dans les résultats des tests et des études, il est très difficile de poursuivre une organisation dont le fonctionnement est conforme aux lois d'un autre pays.

Compte tenu de ce qui précède, il est nécessaire d'élaborer et d'appliquer universellement un mécanisme de savoir-faire national en matière de résultats et d'études d'essai. Dans le même temps, l'organisation qui formule un avis spécialisé conformément à la législation du pays dans lequel elle exerce ses activités est tenue pour responsable. Il importe également de tirer parti des bonnes pratiques et des expériences des pays qui mettent en œuvre des ARM avec succès.

2.5 Nécessité d'un cadre solide de conformité et d'interopérabilité

2.5.1 Infrastructure de base pour un cadre C&I de qualité: normes techniques et révisions législatives nécessaires

Un cadre C&I solide est essentiel pour parvenir à une intégration harmonieuse des systèmes TIC, encourager l'innovation et protéger les consommateurs. Les pays en développement

rencontrent souvent des difficultés pour établir un tel cadre en raison de lacunes dans les normes techniques, les exigences règlementaires et la législation. Pour une mise en œuvre efficace des programmes de C&I, il est essentiel d'établir une infrastructure bien structurée, intégrant les aspects techniques, législatifs et règlementaires.

Objectif

Le principal objectif de cette section est de décrire l'infrastructure fondamentale nécessaire à un cadre C&I de qualité. Cela comprend l'établissement des normes techniques, des mécanismes règlementaires et des révisions législatives nécessaires pour prendre en charge l'évaluation de la conformité et l'interopérabilité dans les pays en développement. Le renforcement de ces éléments permettra d'accroître la fiabilité, la sécurité et l'efficacité des écosystèmes TIC.

Retombées

Une infrastructure C&I bien définie procure d'importantes retombées sur le plan socioéconomiques et technologique. Elle garantit l'interopérabilité des solutions TIC, réduit les obstacles commerciaux, renforce la confiance des consommateurs et favorise une concurrence loyale. En outre, elle facilite le commerce international en harmonisant les normes nationales avec les bonnes pratiques ayant cours au niveau mondial, ce qui permet aux pays en développement de participer plus efficacement à l'économie numérique mondiale.

Rôle

En s'attaquant à ces domaines stratégiques, les pays en développement peuvent jeter des bases solides pour un cadre C&I de haute qualité et, à terme, stimuler la transformation numérique et la croissance économique.

2.5.2 Concept des tests fédérés

Les évolutions technologiques récentes concernant l'Internet sont devenues plus complexes à tester et à déployer dans le monde réel. Il faut tenir compte d'une plus grande diversité de conditions et évaluer la modularité. Il devient important de recourir à des bancs d'essai pour tester en conditions réelles les nouveaux cas d'utilisation. Cette évolution rend de plus en plus nécessaire et pratique l'utilisation et l'interconnexion de différents bancs d'essai. Toutefois, il n'existe pas dans ce domaine d'API clairement normalisées pour prendre en charge la fédération des bancs d'essai et ressources disponibles afin d'appuyer l'expérimentation, les essais et la validation de nouvelles technologies, de nouveaux services et de nouvelles solutions dans le but d'améliorer l'interopérabilité des bancs d'essai.

2.6 Surveillance du marché

2.6.1 Sensibilisation pour un meilleur suivi

La sensibilisation des vendeurs et des utilisateurs de terminaux est cruciale pour améliorer le suivi des normes dans le secteur des télécommunications. Cela améliore non seulement la qualité et la fiabilité des produits, mais favorise également l'interopérabilité, la conformité règlementaire et la confiance des consommateurs. Les fournisseurs peuvent encourager une culture de la qualité et de la fiabilité en comprenant bien les normes qui les concernent, ce

qui se traduit par une meilleure qualité des produits, moins de défauts et une hausse de la fiabilité. Les utilisateurs peuvent prendre des décisions d'achat éclairées et choisir les produits qui répondent à leurs besoins et à leurs attentes, ce qui augmente leur satisfaction et leur confiance dans la fiabilité et la performance des terminaux.

Les fournisseurs peuvent encourager l'interopérabilité en concevant des produits conformes aux normes et aux protocoles sectoriels, ce qui favorise une communication transparente et la compatibilité entre les différents systèmes et plates-formes. La connaissance des normes règlementaires avantage les utilisateurs, car elle contribue à garantir que leurs terminaux respectent les exigences en matière de sûreté, de sécurité et de confidentialité imposées par les organismes de régulation.

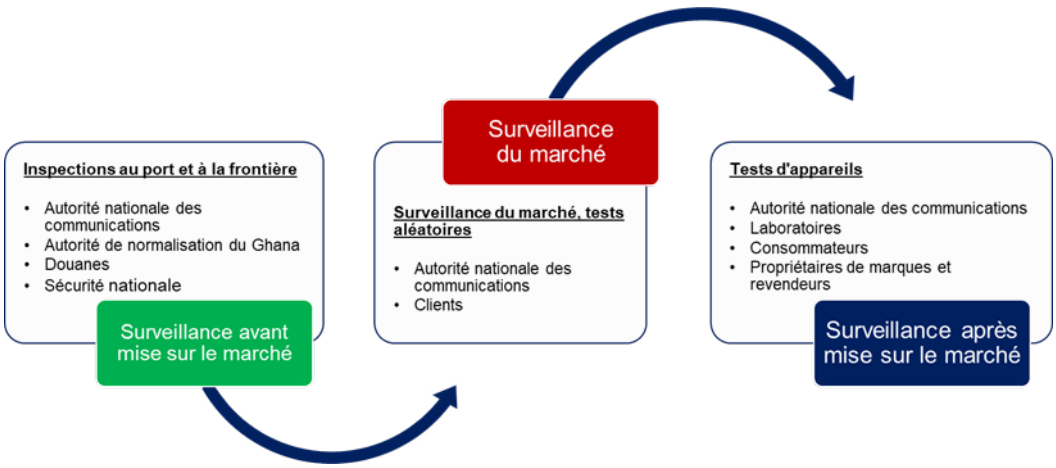
Pour les fournisseurs, il est essentiel de gagner la confiance des consommateurs, car cela démontre leur engagement envers la qualité, la fiabilité et la satisfaction de la clientèle. Les utilisateurs avertis sont plus susceptibles de faire confiance à des équipements conformes à des normes et des certifications reconnues, ce qui favorise la fidélité et une perception positive de la marque. La surveillance du marché est essentielle au bon fonctionnement du marché des télécommunications, car elle protège les consommateurs et les travailleurs contre les risques que présentent les produits non conformes, et protège les entreprises de la concurrence déloyale.

Surveillance du marché: cette procédure est suivie pour s'assurer que les équipements de communication électroniques utilisés ou mis sur le marché soient bien conformes aux normes approuvées avant leur mise sur le marché[8].

Approche en trois axes:

- Surveillance avant mise sur le marché, y compris les procédures d'autorisation d'entrée et les inspections physiques des points d'accès.
- Surveillance du marché, y compris les études de marché et les tests aléatoires.
- Surveillance après mise sur la marché.

Figure 2: Actions en faveur de la surveillance du marché au Ghana



[8] Roland Yaw Kudozia. Ghana. Combating counterfeit ICT devices through C&I testing and market surveillance. Atelier de l'UIT-D sur les enjeux de la conformité et de l'interopérabilité pour la transformation numérique, Genève, 2 juin 2023.

2.6.2 Surveillance et coopération

Les informations commerciales et l'expérience en matière de surveillance du marché sont essentielles pour garantir la conformité règlementaire, la concurrence loyale et les intérêts des consommateurs dans le secteur des télécommunications. Les régulateurs peuvent échanger des informations, se concerter avec d'autres pays et émettre des alertes précoces pour renforcer les efforts de surveillance du marché, rationaliser les activités de mise en application et encourager la collaboration entre les parties. L'échange de connaissances et la coopération régionale sont des atouts essentiels de ces consultations.

Les régulateurs peuvent tirer profit des échanges de bonnes pratiques, d'enseignements tirés et de connaissances d'autres pays en matière de règlementation. Cela peut mener à plus de coopération régionale et à une plus grande harmonisation des approches règlementaires, promouvoir une application cohérente et éviter la fragmentation règlementaire. Les consultations offrent également des possibilités de renforcement des capacités, permettant aux régulateurs de mieux comprendre les technologies, les tendances et les techniques d'application émergentes.

Des alertes précoces peuvent être envoyées aux partenaires afin d'atténuer les risques, d'optimiser l'allocation des ressources et de faciliter la conformité. Ces avertissements servent également d'outils éducatifs pour sensibiliser aux exigences règlementaires et encourager la conformité volontaire. En fournissant des indications claires et des informations en temps opportun, les régulateurs permettent aux parties de mettre leurs activités en conformité vis-à-vis des attentes règlementaires, atténuent les risques en matière de conformité et contribuent à uniformiser les règles du marché.

Principaux acteurs concernés:

- État et régulateurs.
- Organismes d'accréditation.
- Organismes d'évaluation de la conformité.
- Fabricants, importateurs, vendeurs et prestataires de services.

2.7 Évaluation de la conformité des nouvelles technologies

L'évaluation de la conformité est un outil essentiel pour s'assurer que les nouvelles technologies de télécommunication/TIC soient bien conformes aux normes du secteur, aux exigences légales et aux attentes des clients. À l'ère des dispositifs connectés et des réseaux, il est essentiel d'assurer la sécurité, la fiabilité et l'interopérabilité. Les décideurs, les entreprises et les consommateurs peuvent être rassurés sur la qualité et le bon fonctionnement des biens et services de télécommunications et TIC grâce à l'évaluation de la conformité.

L'évaluation de la conformité englobe plusieurs approches visant à évaluer diverses caractéristiques des TIC et des technologies de télécommunication. Ces méthodes comprennent l'accréditation, la certification, les tests et l'inspection. Afin de déterminer si un produit ou un système répond aux critères techniques établis, il est soumis à des tests, et notamment à un examen rigoureux dans des environnements contrôlés. Les principaux objectifs de l'inspection sont de confirmer la conformité au moyen d'une inspection visuelle, d'un examen de la documentation et d'évaluations sur place. La certification est la délivrance de licences ou de déclarations officielles attestant de la conformité à certaines règles ou lois. Les activités de test, d'inspection et de certification sont menées par des organismes d'évaluation de la conformité,

dont l'impartialité et la compétence ont été prouvées et qui sont reconnues comme faisant partie du processus d'accréditation.

Des normes internationalement reconnues et un cadre règlementaire solide sont des conditions préalables à l'efficacité de l'évaluation de la conformité. Les organismes de régulation établissent des normes et des directives pour assurer l'interopérabilité, la sécurité et la sûreté des systèmes de télécommunication et des TIC. Pour favoriser la compatibilité et l'harmonisation à l'échelle mondiale, des organismes de normalisation tels que: l'UIT, l'IEEE, l'IETF, la CEI, l'Institut européen des normes de télécommunication (ETSI) et l'ISO élaborent des spécifications techniques et des protocoles. Le respect de ces directives encourage l'innovation tout en assurant la cohérence et la responsabilisation dans l'ensemble du secteur des TIC et des télécommunications.

2.7.1 Nouveaux enjeux technologiques

Complexité des nouvelles technologies

La complexité des nouvelles technologies des TIC et des télécommunications est l'un des principaux obstacles à l'évaluation de la conformité. La diversité des composants, des protocoles et des capacités de technologies telles que l'IA et l'IoT pose des problèmes pour l'élaboration de techniques de test normalisées. L'évolution rapide et la diversité de ces technologies peuvent rendre difficile le maintien des techniques traditionnelles d'évaluation de la conformité, ce qui pourrait mener à des lacunes dans l'évaluation de la conformité de ces technologies aux normes établies. L'interconnexion des systèmes de télécommunication modernes engendre un degré de complexité supplémentaire. Par conséquent, il est nécessaire de disposer de cadres d'évaluation complets qui tiennent compte tant de l'interopérabilité que de facteurs au niveau du système.

Absence de normes harmonisées

L'absence de normes uniformes d'une juridiction à l'autre et d'une région à l'autre constitue un obstacle majeur. Les frontières internationales sont traversées par des produits et services disponibles sur les marchés mondiaux des TIC et des télécommunications. Toutefois, la diversité des cadres juridiques et des normes rend difficile la reconnaissance mutuelle et l'interopérabilité des résultats de l'évaluation de la conformité. Les différences entre normes peuvent entraîner une fragmentation du marché, une augmentation des coûts de conformité et la duplication des activités de test. Pour encourager l'interopérabilité, faciliter le commerce international et réduire les obstacles règlementaires dans les secteurs de la téléphonie et des TIC, il convient d'harmoniser les normes et les accords de reconnaissance mutuelle.

Obsolescence technologique rapide

L'obsolescence technique rapide constitue un obstacle évident à l'évaluation de la conformité dans les secteurs des TIC et de la téléphonie. Les normes et les procédures d'essai actuelles sont souvent rendues obsolètes par les nouvelles technologies, ce qui contraint à les actualiser et les ajuster en permanence. Pour conserver leur pertinence et leur efficacité, les organismes d'évaluation de la conformité doivent s'adapter rapidement aux nouvelles technologies et à l'évolution des exigences règlementaires. Mais ce besoin constant d'adaptation pourrait exercer une pression sur les connaissances et les ressources, en particulier pour les petites entreprises d'évaluation de la conformité. En outre, le fait que certaines technologies n'ont qu'une durée

de vie très courte pourrait limiter l'accessibilité des équipements de test et des matériaux de référence, ce qui rendrait encore plus difficiles les initiatives d'évaluation de la conformité.

Questions d'interopérabilité et de compatibilité

Les questions d'interopérabilité et de compatibilité constituent des obstacles importants à l'évaluation de la conformité des TIC et des technologies de télécommunication. Une interopérabilité transparente est essentielle pour fournir des services fiables et cohérents dans un écosystème interconnecté composé de dispositifs, de réseaux et de plates-formes divers. Toutefois, les tests d'interopérabilité peuvent s'avérer difficiles et nécessiter beaucoup de ressources, en particulier dans des environnements hétérogènes comportant des protocoles propriétaires et des systèmes obsolètes. Les efforts consentis en faveur de l'interopérabilité sont encore entravés par l'absence d'interfaces et de protocoles normalisés, entraînant des lacunes en matière d'interopérabilité et des interruptions de service. Pour surmonter ces obstacles, l'évaluation de la conformité doit faire intervenir des procédures de test fouillées, qui mettent l'accent sur l'interopérabilité entre les différents niveaux de la pile TIC et des télécommunications.

2.7.2 Tests de conformité préalables

Les essais de conformité préalables sont une stratégie proactive utilisée par les fabricants pour évaluer la conformité de leurs produits par rapport aux normes et règlementations applicables avant de poursuivre la certification officielle. Grâce à ces essais, les fabricants peuvent détecter les problèmes de conformité potentiels dès le début du cycle de développement, y compris les retards de mise sur le marché et les reconceptions ou rappels qui reviennent fréquemment. De plus, les tests de conformité préalables permettent aux fabricants de se faire une meilleure idée des caractéristiques de performance de leurs produits, garantissant ainsi une fonctionnalité et une fiabilité optimales. Les tests de conformité préalables aident les fabricants à rester flexibles et adaptables dans des secteurs des télécommunications et des TIC en pleine mutation, caractérisés par une évolution constante des normes et une innovation rapide.

Les tests de conformité préalables sont cohérents avec la définition de normes et règlementations régissant un dispositif de télécommunication ou TIC en particulier. Un plan d'essai complet décrivant des essais et des évaluations spécifiques est élaboré à partir de ces normes. La configuration de l'essai joue un rôle primordial dans son exactitude et sa fiabilité. Les essais de conformité préalables comprennent les tests de compatibilité électromagnétique (CEM), les tests de sécurité électrique, les tests de performance en radiofréquence (RF) et les tests environnementaux. Les données sont enregistrées et analysées par rapport à des critères d'acceptation prédéfinis, ce qui permet de mettre en évidence les écarts par rapport à la norme et de déterminer l'état de conformité. Les fabricants peuvent corriger ces écarts en revoyant la conception des composants, en ajustant les paramètres ou en améliorant la protection. Une documentation complète est préparée tout au long de la procédure, décrivant les procédures de test, les résultats, les actions correctives et les écarts ou anomalies observés. Les tests itératifs sont souvent utilisés pour affiner les produits, résoudre les non-conformités restantes et optimiser les performances. Cette démarche aide les fabricants à affiner leurs produits et garantit la conformité aux normes et règlementations applicables.

Les tests de conformité préalables des dispositifs de télécommunication et TIC nécessitent le respect des bonnes pratiques et des normes du secteur. Il s'agit notamment de concertations

préalables avec des experts en règlementation, d'une couverture complète des tests, d'un étalonnage et d'une validation réguliers, de scénarios de tests réalistes, d'une collaboration entre diverses équipes interfonctionnelles, et d'une gestion et d'un suivi cohérents de la documentation. Des concertations à un stade précoce permettent une meilleure compréhension des exigences règlementaires et simplifient l'ensemble de la démarche. La couverture complète des tests assure l'exhaustivité de l'évaluation de la conformité des dispositifs. Un étalonnage et une validation réguliers garantissent l'exactitude et la fiabilité. Des scénarios d'essai réalistes simulent des conditions d'exploitation et des variables environnementales réelles. La collaboration favorise le partage des connaissances et la résolution de problèmes entre les équipes interfonctionnelles. L'amélioration continue s'appuie sur les retours d'information des tests de conformité préalables pour affiner la conception des produits et optimiser la conformité.

2.7.3 Résultats attendus

Dans le monde interconnecté d'aujourd'hui, la conformité et l'interopérabilité sont essentielles à la réussite des entreprises. Elles permettent aux entreprises de se doter d'un éventail de produits intelligents pour parvenir à une intégration et à une complémentarité sans faille des produits. Ainsi, on met en place un écosystème cohérent qui améliore l'expérience utilisateur et la satisfaction des clients. L'intégration précoce de la C&I dans l'élaboration des produits permet de résoudre les problèmes de compatibilité, de rationaliser les efforts d'intégration et d'accélérer la mise sur le marché. Cette approche réduit le risque de reconceptions ou de mises à niveau coûteuses plus tard dans le cycle de vie du produit.

Il est indispensable de comprendre les ressources humaines et matérielles nécessaires pour les tests C&I afin de pouvoir planifier et effectuer ces tests de manière efficace. On réduira les retards, diminuera les coûts et optimisera l'utilisation des ressources par une bonne allocation des spécialistes, de l'infrastructure et de l'appui.

Les régulateurs peuvent appuyer les produits et les industries émergents en préconisant la conclusion d'accords de reconnaissance mutuelle entre administrations qui simplifient la mise en conformité règlementaire, en reconnaissant les résultats des tests de conformité émanant de différentes juridictions ou secteurs. Cela facilite l'accès aux marchés pour des produits innovants et favorise la collaboration mondiale.

Les régulateurs peuvent également stimuler un dialogue éclairé avec les entrepreneurs en fournissant des conseils, des ressources, et en lançant des initiatives éducatives. Ce faisant, on renforcera la confiance, la transparence et la collaboration entre les régulateurs et les entrepreneurs, ce qui permettra d'obtenir de meilleurs résultats règlementaires et de créer un environnement propice à l'innovation et à la croissance des entreprises. Dans l'ensemble la conformité et l'interopérabilité sont essentielles à la réussite des entreprises dans le monde interconnecté d'aujourd'hui.

Chapitre 3 – Lutte contre l'utilisation illicite des terminaux: contrefaçon, défaut de qualité et vol de dispositifs portables

3.1 Le poids de la prolifération des dispositifs de contrefaçon

La prolifération des dispositifs de contrefaçon et de mauvaise qualité représente un problème croissant pour les consommateurs, les industries légales, les États et les organisations internationales. Les dispositifs de contrefaçon sont souvent fabriqués sans respect des normes de sécurité et de qualité et constituent une menace potentielle pour les programmes nationaux de transformation numérique des pays en développement du monde entier. En plus de compromettre la sécurité, les performances du réseau et la qualité de service, les dispositifs de contrefaçon font courir de multiples risques sanitaires et environnementaux à la population. Le poids économique de la contrefaçon d'équipements électroniques peut également réduire la contribution du secteur des TIC au PIB.

La lutte contre les dispositifs de contrefaçon exige des approches sur de multiples fronts, assorties de directives qui permettent aux États, aux entreprises et aux organisations internationales d'œuvrer ensemble pour réduire la prolifération de ces contrefaçons et améliorer la sécurité et la qualité des produits électroniques dans les pays.

Ce chapitre porte sur les définitions et lignes directrices pour lutter contre l'afflux des dispositifs de contrefaçon et de mauvaise qualité en mettant l'accent sur diverses expériences faites sur le plan national (études de cas).

L'objectif principal visé dans la combinaison des différentes approches abordées dans ce chapitre est de créer un environnement où les consommateurs ont accès à des produits électroniques authentiques et de bonne qualité, tout en réduisant les risques associés à la contrefaçon et à la fabrication de produits de mauvaise qualité.

La lutte contre la prolifération des dispositifs de contrefaçon et de mauvaise qualité:

- vise à protéger les consommateurs contre les dangers potentiels associés à l'utilisation de ces produits, tels que les risques liées à la santé, la sécurité et la performance, ainsi qu'à préserver l'intégrité des industries légales et la réputation des marques légitimes.

Les efforts pour lutter contre cette prolifération peuvent inclure:

- la promotion de la certification et de la traçabilité des produits électroniques;
- la coopération entre les États, les entreprises et les organisations internationales.

3.2 Directives

Des lignes directrices doivent être élaborées pour mieux lutter contre la prolifération des dispositifs de contrefaçon et de mauvaise qualité dans les pays en voie de développement, notamment:

- **Certification et traçabilité**: mise en place de programmes de certification et de traçabilité pour les produits électroniques légitimes afin rendre plus difficile la falsification et la distribution de contrefaçons.
- **Partenariats public-privé**: appui à la collaboration avec les fabricants autorisés, les associations professionnelles et les organisations internationales afin de repérer et d'éliminer les chaînes d'approvisionnement de produits de contrefaçon.
- **Collaboration régionale et internationale**: collaboration avec d'autres pays et organisations internationales pour échanger des informations et des bonnes pratiques dans la lutte contre la contrefaçon.
- **Formation et renforcement des capacités**: investissement dans la formation et le renforcement des capacités des organismes d'application de la loi pour améliorer leur efficacité dans la lutte contre la contrefaçon.
- **Mise en place de mécanismes de signalement**: instauration de mécanismes permettant aux consommateurs de signaler les produits de contrefaçon et d'encourager les autorités compétentes à enquêter et à prendre des mesures.
- **Responsabilité sociale des entreprises**: appui aux entreprises dans l'adoption de pratiques commerciales responsables, en s'engageant à ne pas utiliser de produits de contrefaçon dans leur chaîne d'approvisionnement et en contribuant à des programmes de sensibilisation et formation.

3.3 Vol de dispositifs mobiles

Le vol de dispositifs mobiles est un problème mondial qui touche tant les particuliers que les entreprises. Avec la prolifération des téléphones intelligents, des ordinateurs portables, des tablettes et autres dispositifs portables, leur attrait pour les criminels s'est considérablement accru. Ces dispositifs contiennent souvent des informations sensibles, telles que des données personnelles, bancaires et commerciales, ce qui en fait des cibles de choix non seulement pour le vol physique, mais aussi pour les attaques numériques. La lutte contre ce fléau nécessite une approche holistique, intégrant des mesures techniques, législatives, et des actions de sensibilisation du public.

Statistiques sur les vols de téléphones mobiles[9]

Le vol de téléphones mobiles est un phénomène mondial en constante augmentation, touchant tant les particuliers que les entreprises.

D'après différentes études et divers rapports:

- chaque année, quelque 70 millions de smartphones sont volés ou perdus dans le monde;
- près de 10% des utilisateurs d'un téléphone portable seront victimes de vol ou perdront leur téléphone pendant la durée de vie de leur dispositifs;
- dans certaines grandes villes, le vol de téléphones intelligents représente jusqu'à 50% des délits signalés;

[9] GSMA. Mobile Device Theft – State of Affairs Report. Février 2025.

- seuls 7 à 10% des dispositifs volés sont récupérés par leur propriétaire;
- près de 40% des vols de téléphones ont lieu dans les transports publics ou dans des lieux publics très fréquentés.

Ces chiffres montrent l'ampleur du problème, et soulignent l'importance des mesures de prévention et de protection.

Incidences sur la sécurité et la confidentialité

Le vol de téléphone portable est une préoccupation qui va au-delà du problème des pertes physiques: il constitue également une menace grave pour la sécurité et la confidentialité des données personnelles et professionnelles. Les voleurs peuvent exploiter les informations personnelles, bancaires et professionnelles conservées sur le dispositif.

Incidences sur la sécurité de l'accès non autorisé aux données sensibles:

- Risque de cyberattaques et de fraude: les criminels peuvent utiliser le téléphone pour accéder à des comptes en ligne, effectuer des achats frauduleux ou usurper l'identité du propriétaire.
- Exposition des données d'entreprise: dans un contexte professionnel, un téléphone volé peut donner accès à des données confidentielles, compromettant ainsi la cybersécurité d'une organisation.
- Utilisation à des fins criminelles: certains téléphones volés sont utilisés pour des activités illégales, telles que la fraude téléphonique ou la cybercriminalité.
- Divulgation d'informations personnelles: les photos, vidéos, messages et documents enregistrés dans le téléphone peuvent être exploités à des fins malveillantes.
- Atteinte à la vie privée: les applications de médias sociaux et de messagerie peuvent être compromises, entraînant le vol d'identité et la violation de la confidentialité des communications.
- Vente de données sur le marché noir: les informations contenues dans un téléphone peuvent être revendues sur le "dark web", mettant ainsi en péril la sécurité numérique de l'utilisateur.

Mesures d'atténuation

Plusieurs stratégies peuvent être mises en œuvre pour réduire les risques liés au vol de téléphone portable:

- Prévention et protection au moyen de l'utilisation des verrous de sécurité: activation de codes PIN, mots de passe forts et authentification biométrique (empreinte digitale, reconnaissance faciale).
- Chiffrement des données: protection des fichiers sensibles pour éviter leur exploitation en cas de vol.
- Sensibilisation des utilisateurs: formation aux bonnes pratiques de sécurité (comme éviter de sortir votre téléphone dans des endroits à risque).
- Surveillance accrue: ne jamais laisser son téléphone sans surveillance, en particulier dans les transports en commun et dans les espaces publics.
- Suivi et effacement à distance en cas de vol: utilisation de services tels que "Localiser mon iPhone" (Apple) ou "Localiser mon appareil" (Android) pour trouver, verrouiller ou effacer des données à distance.

- Blocage de l'IMEI: signaler le vol à l'opérateur mobile pour désactiver le dispositif et le rendre inutilisable sur le réseau.
- Dépôt de plainte: signalement du vol aux autorités pour tenter de récupérer le dispositif et prévenir une éventuelle utilisation frauduleuse.
- Modification immédiate du mot de passe: modification des identifiants de connexion des applications et services liés au téléphone pour empêcher tout accès non autorisé.
- Mesures règlementaires et technologiques de blocage des dispositifs volés par les opérateurs: mise en place de bases de données internationales pour prévenir l'activation de téléphones volés.
- Obligation pour les équipementiers d'intégrer des solutions antivol: mise en œuvre de fonctionnalités telles que l'effacement automatique des données après plusieurs tentatives infructueuses de connexion.
- Renforcement de la législation: adoption de lois réprimant la réception et la revente de dispositifs volés.

3.4 Problèmes et enjeux

- **Perte de données sensibles**: lorsque des dispositifs portables sont volés, les utilisateurs risquent de perdre des informations personnelles et professionnelles cruciales, ce qui peut entraîner des atteintes à la confidentialité.
- **Vol d'identité**: les données conservées sur un dispositif volé peuvent être exploitées à des fins frauduleuses ou d'usurpation d'identité.
- **Inaccessibilité des services**: le vol d'un dispositif peut priver l'utilisateur de l'accès aux services essentiels, perturbant ses activités quotidiennes.
- **Revente sur le marché noir**: les dispositifs volés sont souvent revendus sur un marché noir mondial qui échappe à la règlementation et exacerbe le problème de la criminalité.
- **Absence de normalisation des réponses législatives**: les lois et les sanctions varient d'un pays à l'autre, ce qui rend difficile la coordination de la riposte au niveau international.
- **Efforts de récupération des dispositifs**: les dispositifs de traçabilité actuels ne garantissent pas toujours la récupération des dispositifs volés.
- **Rôles des opérateurs de télécommunication**: les opérateurs ont un rôle clé à jouer dans le blocage de l'accès aux réseaux pour les dispositifs volés; cependant, les mesures appliquées diffèrent selon les régions.
- **Sensibilisation et éducation des utilisateurs**: il est primordial de mener des campagnes de sensibilisation du public aux risques de vol de dispositifs portables et aux bonnes pratiques en matière de sécurité numérique, telles que la mise en place de mécanismes de verrouillage et de traçabilité des dispositifs.
- **Renforcer la législation**: les pouvoirs publics doivent mettre en place des lois strictes pour décourager le vol de dispositifs portables, harmoniser les sanctions à l'échelle internationale et travailler avec les opérateurs et les fabricants pour empêcher l'utilisation de dispositifs volés.
- **Technologie de traçabilité**: adoption généralisée des technologies de suivi et de verrouillage à distance des dispositifs. Les fabricants devraient également intégrer des mesures antivol plus robustes dans leurs produits.
- **Participation des opérateurs de services de télécommunications**: les opérateurs doivent mettre en place des mécanismes pour bloquer rapidement les dispositifs volés et rendre plus difficile leur utilisation sur d'autres réseaux. Ils devraient aussi contribuer activement aux bases de données internationales des aéronefs volés.

- **Coordination internationale**: les efforts visant à lutter contre le vol de dispositifs portables doivent être renforcés au niveau international, avec la création de bases de données centralisées pour suivre les dispositifs volés et de mécanismes d'échange d'informations entre les pays.

En appliquant ces lignes directrices, les pouvoirs publics, les entreprises et les organisations internationales peuvent collaborer ensemble pour réduire la prolifération des dispositifs de contrefaçon et améliorer la sécurité et la qualité des produits électroniques dans différents pays, en particulier ceux en développement.

3.5 Études de cas au niveau des pays

Les contributions des États Membres et des parties prenantes ont joué un rôle fondamental dans l'élaboration du présent rapport. Se fondant sur l'expérience de chaque pays, les données disponibles et les pratiques existantes, ces contributions visent à lutter efficacement contre la prolifération des dispositifs de contrefaçon.

Tous les contributeurs s'accordent sur l'importance d'établir des cadres politiques, juridiques et règlementaires appropriés pour s'attaquer à ce problème.

En outre, certains suggèrent d'adopter des solutions techniques éprouvées, telles que la mise en œuvre de normes internationales, l'utilisation de techniques de surveillance du marché et la création de bases de données et de plates-formes centralisées pour bloquer les dispositifs de contrefaçon.

Un accent particulier est mis sur la nécessité d'aider les pays en développement à mettre en œuvre des programmes de C&I tout en renforçant les efforts pour lutter contre la contrefaçon des équipements TIC et le vol des dispositifs portables.

En outre, plusieurs contributeurs recommandent d'intensifier les efforts aux niveaux régional et sous-régional pour mutualiser les différentes approches et techniques permettant une lutte plus efficace contre la contrefaçon des dispositifs.

3.5.1 République de Zambie

La République de Zambie a présenté un document sur la prolifération de téléphones mobiles de contrefaçon et altérés, qui constitue une menace potentielle pour les programmes de transformation numérique des pays en développement, et de la Zambie en particulier. Ces dispositifs compromettent non seulement la sécurité, les performances du réseau et la qualité des services, mais exposent également les populations à des risques sanitaires et réduisent la contribution du secteur des TIC au PIB.

Difficultés relevées

- Absence de collaboration régionale dans la lutte contre la contrefaçon.
- Absence de données de référence pour orienter les stratégies nationales et régionales.
- Questions liées à l'accessibilité financière des téléphones portables authentiques.
- Sensibilisation insuffisante des consommateurs aux risques associés aux dispositifs de contrefaçon.

Cas de la Zambie

- La Zambie a huit pays voisins et fait face à une demande croissante de téléphones portables, ce qui la rend particulièrement vulnérable à l'afflux de dispositifs de contrefaçon.
- Les autorités y ont mis en place des mesures telles que:
  - l'adoption de lois sur les communications électroniques;
  - l'homologation des dispositifs TIC;
  - la collaboration entre les autorités des TIC, l'immigration, les douanes et le fisc;
  - la mise en place d'un système intégré d'enregistrement des équipements de communications électroniques (IECERS).

Initiatives en cours

- La Zambie étudie l'utilisation du service de vérification des IMEI de la GSM Association pour permettre aux consommateurs de vérifier l'authenticité des dispositifs avant de les acheter.
- Cette initiative vise à réduire la demande de dispositifs de contrefaçon et à sensibiliser davantage les consommateurs.

Recommandations

- Solutions régionales: encourager une approche collaborative entre les États Membres pour lutter contre le commerce des téléphones de contrefaçon.
- Formation et projets: élaborer des programmes nationaux et régionaux pour renforcer les capacités de l'administration.
- Rapports régionaux: publier des données sur les volumes et tendances de la contrefaçon pour mieux informer les consommateurs.
- Plate-forme régionale: créer un système de signalement rapide des dispositifs volés afin de protéger les consommateurs.

Conclusion

La lutte contre la contrefaçon de téléphones nécessite une approche globale, alliant solutions techniques, collaboration régionale et sensibilisation accrue des consommateurs. Grâce à ses initiatives et à l'adoption de technologies comme le service IMEI de la GSMA, la Zambie ouvre la voie à d'autres pays en développement[10].

3.5.2 Guinée

Introduction

Avec l'évolution rapide des technologies et l'apparition de nouveaux dispositifs, applications et services mobiles, les citoyens sont de plus en plus tributaires des TIC, souvent sans être conscients des risques encourus. Il est essentiel que les États établissent des politiques nationales cohérentes pour protéger leurs citoyens.

[10] Document SG2RGQ/37 de la CE 2 de l'UIT-D (Zambie).

Considérations générales

En Guinée, les citoyens sont fréquemment victimes de vols de dispositifs portables, de cyberattaques et d'activités frauduleuses. Les mesures prises par les autorités sont les suivantes:

- adoption de la Loi N° 2016\037\AN relative à la cybersécurité et la protection des données à caractère personnel;
- création de l'Agence nationale de la sécurité des systèmes d'information (ANSSI);
- étude de faisabilité en vue de la création d'une équipe d'intervention en cas d'incident informatique (CERT)/d'un centre des opérations de sécurité (SOC) au niveau national.

Cependant, les citoyens restent vulnérables en cas de perte ou de vol de leurs dispositifs, et sont confrontés à des difficultés pour récupérer leurs données ou restaurer leurs cartes SIM. Les dispositifs de contrefaçon inondent le marché, exacerbant les problèmes de fraude et de mauvaise qualité des services.

Lutte contre la fraude

Un comité de suivi, coordonné par l'Autorité de régulation des postes et télécommunications (ARPT) de la Guinée, a été mis en place pour lutter contre les dispositifs non autorisés et contrefaits. Exemples d'actions:

- Campagne de certification des dispositifs importés.
- Détection et déconnexion de 1 000 numéros frauduleux en 2023.
- Démantèlement de six sites SIMBOX à Conakry.

Lutte contre le vol de dispositifs

L'ANSSI et l'ARPT collaborent pour traquer les voleurs et les dispositifs volés. Une plate-forme centralisée d'identification des dispositifs mobiles et d'enregistrement des cartes SIM a été mise en place pour gérer les terminaux mobiles et repérer les dispositifs non conformes, clonés ou volés.

Conclusion

Pour lutter efficacement contre ce fléau, les actions suivantes sont proposées:

- Mise en place d'une stratégie nationale harmonisée de lutte contre le vol de dispositifs, la contrefaçon et les cyberattaques.
- Échange de données d'expérience et de bonnes pratiques entre les États Membres de l'UIT.
- Appui de l'UIT pour aider les pays en développement à élaborer des stratégies communes et à mettre en place leurs équipes nationales CERT.

Principaux points

- Les citoyens guinéens sont exposés aux risques liés au vol de dispositifs, à la contrefaçon et aux cyberattaques.
- Des mesures ont été prises, telles que la création de l'ANSSI et la mise en place de plates-formes de détection et de gestion des dispositifs.

- Une collaboration régionale et internationale est nécessaire pour renforcer la lutte contre ces problèmes[11].

3.5.3 République du Tchad

Au Tchad, la réduction de la fracture numérique a entraîné une augmentation significative du nombre d'utilisateurs de la téléphonie mobile et d'Internet. Cependant, cette expansion s'accompagne de soucis majeurs, tels que la prolifération des téléphones de contrefaçon ou falsifiés, ainsi qu'une augmentation du nombre de vols de dispositifs. Ces problèmes compromettent la sécurité des utilisateurs, la qualité des services de télécommunication et les performances du réseau.

Le Gouvernement tchadien, à travers le Ministère des télécommunications et de l'économie numérique, a mis en place des mesures de modernisation des infrastructures et de réduction de la fracture numérique. Cependant, le marché est inondé de dispositifs non vérifiés, souvent importés sans contrôles, ce qui expose les utilisateurs à des risques en matière de sécurité et de qualité. L'Autorité de régulation des communications électroniques et des postes (ARCEP) du Tchad, qui joue un rôle clé dans la régulation de ce secteur, ne dispose pas des moyens techniques pour vérifier efficacement les dispositifs et lutter contre le vol et la contrefaçon.

Pour résoudre ces difficultés, plusieurs recommandations sont proposées, notamment:

- la création d'un laboratoire de certification aux normes GSMA;
- le renforcement de la collaboration entre l'ARCEP, les douanes, les autorités et les opérateurs pour la vérification des dispositifs avant leur mise sur le marché;
- le lancement de campagnes de sensibilisation pour informer les consommateurs sur les risques associés aux dispositifs de contrefaçon ou volés;
- la conclusion d'accords régionaux pour faciliter la recherche des dispositifs volés et la coopération entre les pays.

En conclusion, bien que des efforts aient été réalisés, la lutte contre le vol et la contrefaçon de téléphones au Tchad est encore au stade initial. Une approche coordonnée, mêlant des mesures sur les plans technique, règlementaire et régional, est requise pour protéger les utilisateurs et améliorer la qualité des services de télécommunication[12].

3.5.4 Sri Lanka

La Commission de régulation des télécommunications de Sri Lanka (TRCSL) réglemente les importations de dispositifs mobiles en vertu de la Loi N° 25 de 1991 sur les télécommunications. Les opérateurs titulaires d'une licence doivent tenir à jour un registre des identités d'équipement (EIR) pour s'assurer que seuls les dispositifs importés légalement dotés d'un numéro IMEI sont activés. La TRCSL rend obligatoire l'homologation des dispositifs de télécommunication et tient à jour une base de données des IMEI des dispositifs importés légalement. Les amendes pour non-conformité ont récemment été considérablement augmentées. Un système en ligne permet désormais au public de signaler la perte ou le vol de téléphones, ce qui améliore l'efficacité et réduit les coûts. La TRCSL exploite également un système de vérification des IMEI

[11] Document SG2RGQ/115 de la CE 2 de l'UIT-D (Guinée).
[12] Document SG2RGQ/112 de la CE 2 de l'UIT-D (Tchad).

permettant aux clients d'authentifier les dispositifs par SMS, bien que la répression contre les importations illégales se heurte à des difficultés[13].

3.5.5 Rwanda

Au cours des deux dernières décennies, le secteur des TIC, y compris la technologie mobile, a considérablement progressé au Rwanda, ce qui a entraîné une expansion du marché des dispositifs mobiles. Cependant, cette croissance a également entraîné une prolifération importante de dispositifs mobiles de contrefaçon. Si le problème n'est pas correctement géré, il peut poser des menaces de sécurité, entraver la croissance économique, entraîner des risques opérationnels et nuire à la confiance des utilisateurs. Pour résoudre ces problèmes, le Rwanda a mis en place des outils, des cadres juridiques et des collaborations institutionnelles pour lutter contre la contrefaçon et le vol de dispositifs, conformément aux recommandations de l'UIT. Les principales parties prenantes, telles que les autorités douanières, les agences de protection des consommateurs, les opérateurs de télécommunication et les entités de sécurité, travaillent ensemble pour s'assurer que seuls des dispositifs légaux sont utilisés. La réticence du public et la faible sensibilisation à la protection des données restent des obstacles. Les campagnes conjointes de sensibilisation et la collaboration interinstitutions ont démontré un fort potentiel[14].

[13] Document 2/367 de la CE 2 de l'UIT-D (Sri Lanka).
[14] Document 2/352 de la CE 2 de l'UIT-D (Rwanda).

Chapitre 4 – Conformité et interopérabilité pour l'Internet des objets

4.1 Introduction

L'IoT est une infrastructure mondiale pour la société de l'information, qui permet de disposer de services perfectionnés en interconnectant des objets (physiques ou virtuels) grâce aux TIC interopérables existantes ou en évolution[15].

Les technologies IoT sont présentes dans de nombreux secteurs et influent sur la vie quotidienne des utilisateurs de l'IoT grâce à des plates-formes qui traitent les données de milliards de dispositifs connectés. Une étude d'IoT Analytics montre qu'il existe 16,7 milliards de points de terminaison IoT actifs; on prévoit que ce nombre passe à 29 milliards d'ici 2027[16].

4.2 Écosystème IoT et scénarios d'application

4.2.1 L'écosystème IoT

L'IoT est le réseau d'objets physiques ou de dispositifs équipés des composants électroniques, des logiciels, des capteurs et la connectivité des réseaux, qui permet de collecter et d'échanger des données. Les dispositifs collectent des données utiles à l'aide de diverses technologies et les font ensuite circuler de manière automatique entre d'autres dispositifs. Divers acteurs sont préoccupés par la sécurité et la fiabilité des connexions, des dispositifs et de la confidentialité des données stockées et en transit. L'écosystème IoT comprend les éléments suivants:

- **Dispositifs et capteurs**: ces éléments centraux sont des objets physiques équipés de capteurs et d'actionneurs qui recueillent des données de leur environnement ou effectuent des actions spécifiques en fonction des instructions reçues. Exemples: capteurs de température, détecteurs de mouvement, dispositifs à porter, compteurs intelligents.
- **Connectivité**: cette fonction permet aux dispositifs de communiquer entre eux, ainsi qu'avec des systèmes centraux ou fondés sur le nuage pour y subir des traitements supplémentaires. Les technologies utilisées sont notamment les technologies WiFi, Bluetooth, cellulaire (LTE, 5G), réseau de basse puissance à couverture étendue (LPWAN), réseau à couverture étendue de longue portée (LoRaWAN), Sigfox, etc.
- **Matériel de traitement des données**: traite les données collectées par les capteurs avant qu'elles ne soient envoyées vers le nuage ou les serveurs locaux pour un traitement plus intensif. Mise en œuvre: inclut des dispositifs informatiques en périphérie qui prétraitent les données pour réduire la latence et l'utilisation de la largeur de bande.
- **Plates-formes**: elles constituent l'épine dorsale du système IoT, intégrant différents dispositifs, gérant leurs communications et permettant la circulation des données entre eux. Les capacités comprennent la gestion des dispositifs, la collecte de données et l'activation des applications.

---

[15] Recommandation UIT-T Y.4000/Y.2060 (06/2012) – Présentation générale de l'Internet des objets.
[16] IoT Analytics. State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally. 3 septembre 2024.

- **Serveurs en nuage et centres de données**: ils fournissent l'infrastructure nécessaire au stockage de grandes quantités de données IoT et à l'exécution de modèles analytiques complexes pour extraire des informations exploitables. Ils sont fréquemment associés à l'IA et à l'apprentissage automatique pour réaliser des analyses prédictives pointues.
- **Interface utilisateur**: tableaux de bord, applications mobiles et autres interfaces humain machine permettant aux utilisateurs d'interagir avec le système IoT, de régler les paramètres et de visualiser les données sous une forme claire et intelligible. Ils peuvent être adaptés à des besoins spécifiques, fournir des informations et des contrôles pertinents à l'utilisateur.
- **Sécurité**: vise à protéger l'intégrité et la confidentialité des données et des systèmes IoT contre les cybermenaces. Les mesures comprennent le chiffrement, l'authentification à deux facteurs, le démarrage sécurisé et des mises à jour de sécurité régulières.
- **Normes et règlementation**: la normalisation assure l'interopérabilité et la compatibilité des dispositifs. Elle se conforme aux règlementations régionales et internationales régissant la protection des données, la confidentialité, la libre circulation des données au-delà des frontières et le fonctionnement des dispositifs entre différents secteurs.

4.2.2 Scénarios d'application

De nombreuses nouvelles applications de l'IoT ont vu le jour ces dernières années. Les scénarios d'application les plus pertinents et les plus actifs sont les suivants:

- Automatisation des environnements domestiques grâce à des dispositifs connectés, tels que des thermostats, des ampoules et des systèmes de sécurité, qui peuvent être contrôlés et surveillés à distance.
- Systèmes de télésurveillance des patients dans le domaine de la santé, dispositifs de santé à porter et solutions de télémédecine qui améliorent les soins aux patients et la gestion de la santé.
- Techniques agricoles de précision qui emploient des capteurs pour mesurer l'humidité du sol, les conditions météorologiques et la santé des cultures afin d'améliorer le rendement et l'efficacité des ressources.
- Usines intelligentes équipées de capteurs et de machines automatisées pour améliorer l'efficacité de leur production, prédire les besoins de maintenance et optimiser la chaîne d'approvisionnement.
- Les solutions de gestion de flotte logistique et de transport, suivi des véhicules en temps réel et systèmes intelligents de gestion du trafic pour optimiser la logistique et réduire les embouteillages.
- Systèmes de gestion intelligente des stocks, nouveaux dispositifs TIC en point de vente et marketing personnalisé permettant l'amélioration des services de détail et de l'expérience client.
- Villes intelligentes qui intègrent des systèmes de gestion des services urbains tels que la circulation, la gestion des déchets et la consommation d'énergie, qui contribuent à accroître la durabilité et la qualité de vie.
- Réseaux électriques intelligents et nouveaux dispositifs TIC améliorant l'efficacité énergétique et la gestion de l'énergie dans les maisons, les bâtiments et les villes.

4.2.3 Classification des dispositifs IoT

Les dispositifs IoT se divisent en trois catégories selon leur puissance de traitement et leurs capacités de communication[17]:

- Dispositif à faible capacité de traitement et à faible connectivité (Low Processing Low Connectivity device, LPLC).
- Dispositif à faible capacité de traitement et à haute connectivité (Low Processing High Connectivity device, LPHC).
- Dispositifs à haute capacité de traitement et à haute connectivité (High Processing High Connectivity device, HPHC).

La Recommandation UIT-T Y.4108 porte sur des dispositifs tels que les étiquettes sans puissance de traitement.

Entités fonctionnelles des dispositifs HPHC

Entité fonctionnelle de détection, d'actionnement et de saisie de données; entité fonctionnelle de messagerie; entité fonctionnelle d'accès à la passerelle; entité fonctionnelle de gestion des dispositifs; entité fonctionnelle assurant l'interface avec les applications et services de nuage; entité fonctionnelle de gestion de la connectivité; entité fonctionnelle de moteur d'exécution d'application; entité fonctionnelle de gestion des dispositifs; entité fonctionnelle de partage d'informations; entité fonctionnelle d'analyse des données; entité fonctionnelle de stockage des données.

Entités fonctionnelles de dispositifs LPHC

Entité fonctionnelle de détection, d'actionnement et de saisie de données; entité fonctionnelle de messagerie; entité fonctionnelle d'accès à la passerelle; entité fonctionnelle de gestion des dispositifs; entité fonctionnelle assurant l'interface avec les applications et services de nuage; entité fonctionnelle de gestion de la connectivité.

Entités fonctionnelles des dispositifs LPLC

Entité fonctionnelle de détection, d'actionnement et de saisie de données; entité fonctionnelle de messagerie LPLC; entité fonctionnelle d'accès à la passerelle; entité fonctionnelle de gestion des dispositifs.

Le Rapport du Comité technique mixte (JTC) 1 de l'ISO/CEI sur l'IoT donne des informations d'ordre général sur ce sujet ainsi que des exemples de moteurs, de règlementation, de sécurité, de confidentialité et de gouvernance des technologies IoT.

4.3 Enjeux de l'IoT en matière de C&I

Certains des problèmes et enjeux associés aux besoins particuliers de l'IoT, tels que la qualité, la fiabilité, la couverture et la faible consommation d'énergie, ont été abordés dans le Rapport

[17] Recommandation ITU-T Y.4460 (06/2019). Modèles architecturaux de référence des dispositifs pour les applications de l'Internet des objets.

final sur la Question 4/2 de l'UIT D (période d'études 2018-2021)[18]. Ces dernières années, de nouvelles tendances ont émergé et se sont développées, ce qui accroît la complexité des plates-formes et des protocoles IoT. Le système de certification IoT doit faire l'objet d'évaluations permanentes pour déterminer s'il est conforme aux évolutions les plus récentes. D'autres facteurs doivent être pris en compte lors de la sélection technique et du déploiement des dispositifs et systèmes IoT.

Augmentation de la part de la connectivité par satellite

Avec la baisse des coûts de lancement des satellites, la connectivité par satellite sur orbite terrestre basse devient de plus en plus prisée. La connectivité via un satellite en orbite basse présente un affaiblissement de trajet plus faible, et nécessite donc moins de puissance du terminal et moins de directivité d'antenne, ce qui rend la conception et le déploiement de dispositifs IoT plus simples et moins coûteux. Les recherches montrent que le marché de l'IoT satellitaire continuera à devenir de plus en plus compétitif et que la taille de marché devrait atteindre 1 milliard de dollars. Toutefois, le point idéal pour la connectivité IoT par satellite reste le déploiement de cette technologie dans les zones éloignées et isolées. La taille totale du marché de l'IoT par satellite ne demeurera qu'une fraction du marché de l'IoT total dans un avenir prévisible.

Convergence de l'IA et de l'IoT

On estime que près de la moitié de toutes les applications IoT seront fondées sur l'IA d'ici à 2027[19]. L'intégration de l'intelligence artificielle dans les applications IoT connaîtra une forte croissance et devrait s'accroître fortement dans les années à venir.

La convergence de l'IA et de l'IoT, dite "AIoT", se développe rapidement avec l'application à grande échelle de la technologie de l'IA. La technologie de l'IA peut fournir des capacités d'analyse et de traitement des données plus précises pour les applications IoT, ce qui aidera les utilisateurs à mieux gérer et contrôler leurs dispositifs IoT. Les dispositifs IoT fournissent à l'IA davantage de sources de données et d'applications, ce qui lui permet de mieux comprendre l'environnement, de détecter des tendances et d'améliorer la prise de décisions dans divers domaines.

Par exemple, la convergence de l'intelligence artificielle et de l'Internet des objets ouvre davantage de possibilités pour les maisons intelligentes. L'IA peut surveiller l'environnement domestique en temps réel et se réguler intelligemment en connectant différents dispositifs domestiques. Dans les scénarios de ville intelligente, l'IA peut collecter des informations en temps réel sur la ville et appuyer la planification et la prise de décisions intelligentes en connectant diverses infrastructures et divers dispositifs de la ville. Le système de transport peut ajuster les feux de circulation en temps réel et optimiser la circulation grâce à des algorithmes d'IA.

---

[18] UIT-D. Rapport final sur la Question 4/2 de la Commission d'études 2 de l'UIT-D pour la période d'études 2018-2021. Assistance aux pays en développement pour la mise en œuvre de programmes de conformité et d'interopérabilité et pour lutter contre la contrefaçon d'équipements TIC et le vol de dispositifs mobiles. UIT, 2021.

[19] https://iot-analytics.com/how-enterprise-iot-market-is-evolving.

4.4 Règlementation et politiques relatives aux produits IoT

L'IoT, de par sa nature même, nécessite une adaptation des cadres règlementaires et des politiques de gouvernance afin de gérer les nouvelles dynamiques qu'il introduit dans le secteur des TIC. Voici quelques aspects clés à prendre en compte:

- **Normes d'interopérabilité internationales**: plusieurs organisations, dont l'UIT, l'ISO et l'IEEE, s'emploient à élaborer des normes mondiales régissant l'interopérabilité des dispositifs IoT. Ces normes visent à assurer l'harmonisation technique et à faciliter le déploiement à grande échelle de solutions IoT.
- **Règlementation de la sécurité concernant l'IoT**: face à la multiplication des objets connectés, l'harmonisation des règlementations est nécessaire pour assurer la sécurité de ces dispositifs. Les pays mettent en place des lois obligeant les fabricants à respecter des protocoles de sécurité minimaux afin de protéger les réseaux TIC contre des intrusions malveillantes.
- **Politiques de protection des données**: avec l'augmentation du nombre de données générées par l'IoT, les autorités de régulation imposent des obligations strictes de protection des données, comme le RGPD en Europe. Ces lois exigent des entreprises IoT qu'elles garantissent la confidentialité et la sécurité des informations personnelles collectées par le biais de leurs dispositifs.
- **Initiatives de certification**: afin de veiller à ce que les produits IoT soient conformes aux normes C&I, certaines juridictions encouragent ou exigent des procédures de certification. Ces certifications peuvent porter à la fois sur la compatibilité technique et sur des aspects liés à la protection des consommateurs et à la durabilité de l'environnement.

Le cadre règlementaire de l'IoT est l'ensemble de politiques, de normes et de lignes directrices conçues pour régir le développement, le déploiement et la gestion des technologies IoT. Un cadre règlementaire efficace est indispensable pour garantir la sécurité, la confidentialité, l'interopérabilité et l'utilisation éthique des dispositifs et des données IoT.

Le cadre règlementaire des nouvelles TIC doit prendre en compte:

- l'élaboration de normes internationales;
- la protection de la vie privée;
- la définition d'exigences en matière d'interopérabilité;
- l'élaboration de normes de qualité de service et de fiabilité;
- les lois sur la protection des consommateurs;
- la conformité aux normes internationales;
- l'élaboration de lignes directrices respectant la déontologie.

Avant tout chose, le régulateur local doit offrir les prestations suivantes:

- la certification des dispositifs et du réseau;
- la gestion du spectre;
- la gouvernance et la souveraineté des données.

La certification des dispositifs permet de s'assurer que les dispositifs sont conformes aux règlementations avant leur mise sur le marché. Les certifications de réseau sont obligatoires pour veiller à ce que les dispositifs IoT fonctionnent en toute sécurité au sein de l'infrastructure de réseau.

Gestion du spectre: encadre l'utilisation des fréquences radio afin d'éviter les brouillages et de garantir la fiabilité des communications pour les dispositifs IoT.

La gouvernance des données établit des règles régissant la propriété, le partage et le transfert des données, en particulier dans les opérations transfrontalières. Des normes de souveraineté des données déterminent la manière dont les données sont stockées, traitées et protégées.

4.5 Normes de conformité applicables aux nouveaux dispositifs IoT

Les organisations de normalisation du monde entier sont résolues à établir des cadres exhaustifs pour les nouveaux dispositifs TIC afin d'en garantir la sécurité, l'interopérabilité et l'efficacité. Ces normes s'inscrivent dans le cadre d'un effort concerté mené par ces organisations pour fournir des orientations claires sur le développement et la mise en œuvre de nouvelles TIC. Elles portent sur divers aspects, y compris les exigences relatives aux couches physique, réseau, session et application, ainsi que sur des considérations relatives à la sécurité et à la confidentialité. Les organisations de normalisation telles que l'UIT, l'IEEE et l'ISO travaillent activement à élaborer et à tenir à jour des normes pour assurer la conformité des nouveaux dispositifs TIC.

L'UIT publie les normes suivantes: UIT-T Y.4000/Y.2060 (06/2012) – Présentation générale de l'Internet des objets (IoT)[20] et UIT-T Y.4100/Y.2066 (06/2014) – Exigences communes relatives à l'Internet des objets[21].

L'ISO et la CEI ont élaboré les normes suivantes: ISO/CEI 30141 (2024) – Architecture de référence de l'IoT[22] et ISO/CEI 27400 (2022) – Cybersécurité – Sécurité et protection de la vie privée pour l'IoT – Lignes directrices[23].

L'ETSI publie les spécifications techniques suivantes: ETSI TS 103 645 (01/2024) – La cybersécurité au service de l'Internet des objets pour les consommateurs: exigences de base, qui fournit un guide de haut niveau sur la sécurité de l'IoT pour le grand public[24], et la norme européenne ETSI EN 303 645 (09/2024) – La cybersécurité au service de l'Internet des objets pour les consommateurs: exigences de base, qui établit des normes de cybersécurité pour les dispositifs IoT grand public pour protéger la vie privée et les données personnelles des utilisateurs[25].

L'Institut national américain de normalisation (ANSI) et la Telecommunications Industry Association (TIA) ont élaboré les normes suivantes: ANSI/TIA-942C (07/2024) – Normes relatives à l'infrastructure des télécommunications pour les centres de données, qui définit les normes concernant l'infrastructure des télécommunications pour les centres de données, ainsi que des spécifications pour les déploiements IoT[26] et ANSI/TIA-1179-B (06/2023) – Normes pour l'infrastructure de télécommunications dans les établissements de santé, qui définit des normes

---

20 Recommandation UIT-T Y.4000/Y.2060 (06/2012) – Présentation générale de l'Internet des objets.
21 Recommandation UIT-T Y.4100/Y.2066 (06/2014) – Exigences communes relatives à l'Internet des objets.
22 ISO/CEI 30141 (2024) – Internet des objets (IoT) – Architecture de référence.
23 ISO/CEI 27400 (2022) – Cybersécurité – Sécurité et protection de la vie privée pour l'IoT – Lignes directrices.
24 ETSI TS 103 645 – La cybersécurité au service de l'Internet des objets pour les consommateurs: exigences de base.
25 ETSI EN 303 645 – La cybersécurité au service de l'Internet des objets pour les consommateurs: exigences de base.
26 ANSI/TIA-942-C – Normes relatives à l'infrastructure des télécommunications pour les centres de données.

pour l'infrastructure de télécommunications dans les établissements de santé prenant en charge les dispositifs IoT[27].

Le 3GPP fournit les normes suivantes: 3GPP TS 22.368 (04/2025) – Exigences de service pour les communications de type machine, y compris les aspects liés à l'IoT[28] et 3GPP TS 23.682 – Améliorations à apporter aux architectures pour faciliter les communications faciliter les communications avec les réseaux et applications de transmission de données à commutation de paquets, qui décrit les améliorations à apporter aux architectures pour faciliter les communications IoT et machine à machine (M2M)[29].

L'Initiative oneM2M fournit les spécifications techniques pour une couche de services M2M commune qui peut être incorporée dans le matériel et les logiciels pour connecter les dispositifs. OneM2M fournit également la norme TS-0004 – Spécification du protocole central de couche service, qui définit le protocole de communication pour les systèmes compatibles oneM2M, les applications M2M et d'autres systèmes M2M[30].

Le Groupe de travail spécial 5 (SWG 5) du JTC 1 de l'ISO/CEI était chargé de d'étudier l'IoT et les technologies connexes, y compris les réseaux électriques intelligents et d'échanger des informations pour faciliter la coordination. Il a été dissout en 2014 et ses travaux ont été poursuivis par le Groupe de travail 10 du JTC 1 de l'ISO/CEI jusqu'en 2016, puis le Sous-comité 41 du JTC 1 de l'ISO/CEI a hérité du programme de travail de ce groupe.

Les rapports et activités techniques spécifiques ont élaboré les normes suivantes: efforts visant à garantir la conformité des dispositifs IoT aux normes X73 existantes dans le domaine de la santé, en particulier les dispositifs de santé individuels (normes IEEE 11073). Analyses comparatives des normes ISO/CEI et IEEE dans le domaine de l'IoT afin de garantir la C&I entre les dispositifs et systèmes de différents fabricants.

Un cas d'utilisation est l'expérimentation d'un réseau de capteurs sans fil (WSN) composé de dispositifs IoT communiquant entre eux au moyen d'un protocole sans fil. L'objectif de cette expérimentation est d'évaluer la performance de ces dispositifs IoT dans des conditions réelles et dans différents environnements. Plusieurs bancs d'essai devraient être utilisés pour représenter pour chacun d'eux un environnement d'installation particulier pour les dispositifs IoT. Fondamentalement, l'expérimentateur accède à distance à l'infrastructure du banc d'essai pour préparer et contrôler l'expérience IoT sans fil. Les paramètres types à mesurer dans un tel réseau hertzien sont la fiabilité, la latence, le facteur d'utilisation radioélectrique, le nombre de bonds, la synchronisation et la largeur de bande. Cette expérience mène aux conditions suivantes:

- Pertinence: les tests et paramètres à mesurer doivent correspondre aux conditions réelles rencontrées dans un déploiement professionnel.
- Reproductibilité: l'expérience doit être renouvelée sur différents bancs d'essai et dans différentes conditions.
- Répétabilité: l'expérience doit être répétée dans les mêmes conditions.

---

27 ANSI/TIA-1179-B – Normes pour l'infrastructure de télécommunications dans les établissements de santé prenant en charge les dispositifs IoT.
28 3GPP 22.368 – Exigences de service pour les communications de type machine, y compris les aspects liés à l'Internet des objets.
29 3GPP 23.682 – Améliorations à apporter aux architectures pour faciliter les communications avec les réseaux et applications de transmission de données à commutation de paquets.
30 OneM2M TS-0004 – Spécification du protocole central de couche service.

– Expérience automatisée: une expérience doit être exécutée automatiquement.

Une fédération de bancs d'essai telle que Fed4FIRE+ fournit tous les outils et services répondant aux exigences, permettant d'exécuter et de répéter l'expérience dans les conditions prédéfinies.

Chapitre 5 – Transfert de connaissances

5.1 Introduction

Pour transférer avec succès les connaissances et le savoir-faire en matière de C&I, il est fondamental d'évaluer les compétences existantes, de recenser les lacunes en matière d'apprentissage et, surtout, de dispenser une formation appropriée.

5.2 Besoins et possibilités en matière de formation C&I

Le Plan d'action de Dubaï (CMDT-14) rappelle que la généralisation de la conformité et de l'interopérabilité des équipements et des systèmes de télécommunication/TIC multiplie les opportunités commerciales, renforce la fiabilité et simplifie l'intégration et le commerce à l'échelle internationale.

Cependant cette généralisation met en lumière des disparités et des problèmes d'acquisition et d'appropriation des processus ou procédés de conformité qu'il convient de bien évaluer afin d'atteindre les objectifs visés.

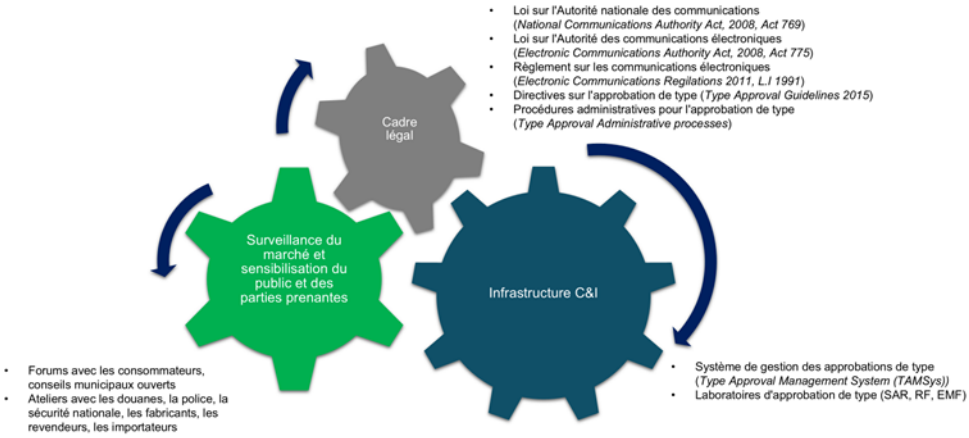
L'impact des problèmes liés à la conformité, à l'interopérabilité ou à la contrefaçon des équipements TIC est multidimensionnel. La sécurité des utilisateurs, la certification des techniciens et la normalisation des processus de conception au niveau des fabricants, l'accompagnement à la prise de décisions par les autorités et la qualité des services réseaux sont à prendre en compte pour la mise en place d'un cadre efficient de transfert des connaissances.

Les innovations et les évolutions constantes observées autour des technologies numériques révèlent la nécessité de former et d'éduquer, les parties prenantes, à la conformité afin de garantir le respect des exigences règlementaires et de prévenir les risques liés à la non-conformité.

Outre les enjeux liés à la maîtrise des équipements technologiques innovants, la compréhension et la formulation du cadre légal, l'acquisition et la mise en place des infrastructures de conformité et d'interopérabilité ainsi que la surveillance des contrats, il demeure d'autres difficultés qui pourraient être résolues par un programme spécifique de formation et de transfert des connaissances.

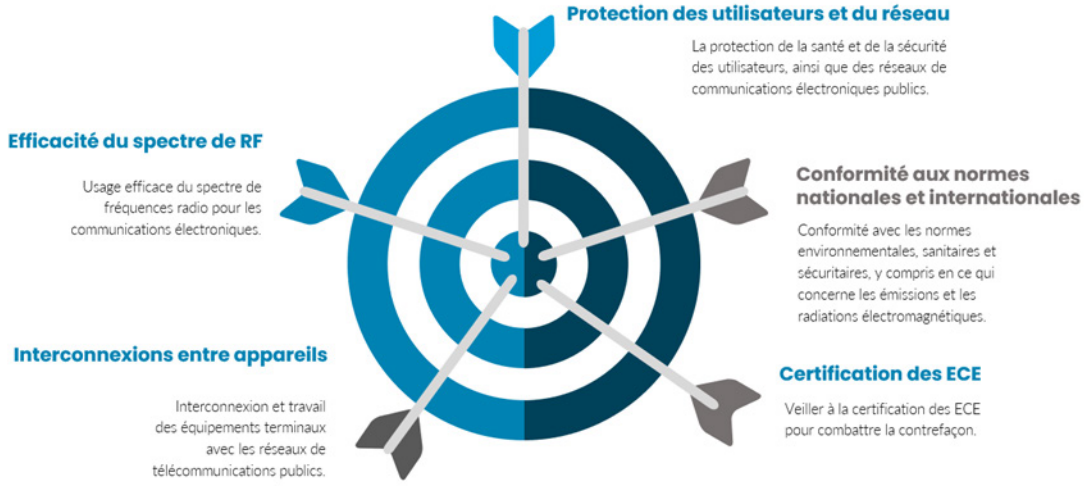
L'Autorité nationale des communications (NCA) du Ghana décrit l'objectif, les difficultés, les indicateurs, les composantes, les normes, spécifications et prescriptions techniques, les prescriptions règlementaires et l'infrastructure d'essai de son régime C&I pour la lutte contre les dispositifs TIC de contrefaçon au moyen d'essais C&I et de la surveillance du marché.

Figure 3: Composition du régime C&I au Ghana



Source: Ghana[31]

Figure 4: Objectifs du régime C&I au Ghana



Source: Ghana[32]

Dans le prolongement de cette étude de cas du Ghana, la République du Kenya, en collaboration avec la Fondation Diplo, a fourni un exemple de cadre règlementaire pour les activités d'évaluation de la conformité en Afrique.

Ce cadre s'appuie sur les activités du Bureau kenyan des normes (KEBS), organisme national de normalisation responsable de l'élaboration et de la mise en œuvre des normes, ainsi que de l'exécution des procédures d'évaluation de la conformité dans le pays et ceux du régulateur des TIC au Kenya, l'Autorité des communications.

---

31 Roland Yaw Kudozia. Ghana. Combating counterfeit ICT devices through C&I testing and market surveillance. Atelier de l'UIT-D sur les enjeux de la conformité et de l'interopérabilité pour la transformation numérique, Genève, 2 juin 2023.

32 *Ibid*.

Figure 5: Objectifs du régime C&I au Kenya

Source: DiploFoundation[33]

5.3 Réponses aux besoins d'acquisition et de rétention des connaissances

Conformément à la Déclaration de Buenos Aires adoptée par la CMDT-17, la conformité et l'interopérabilité généralisées des équipements et systèmes de télécommunication/TIC, à travers la mise en œuvre de programmes, politiques et décisions pertinents, peuvent élargir les débouchés commerciaux, renforcer la fiabilité et encourager l'intégration et le commerce à l'échelle mondiale.

C'est pourquoi les États Membres et les Membres du Secteur de l'UIT-D sont encouragés à se prêter assistance et se conseiller mutuellement en menant à bien des études, en recherchant des moyens de réduire l'écart en matière de normalisation et en examinant les sujets se rapportant aux questions abordées dans la Résolution 47 (Rév. Kigali, 2022) de la CMDT, des Résolutions 44 et 76 (Rév. New Delhi, 2024) de l'Assemblée mondiale de normalisation des télécommunications (AMNT) et de la Résolution 177 (Rév. Bucarest, 2022) de la Conférence de plénipotentiaires.

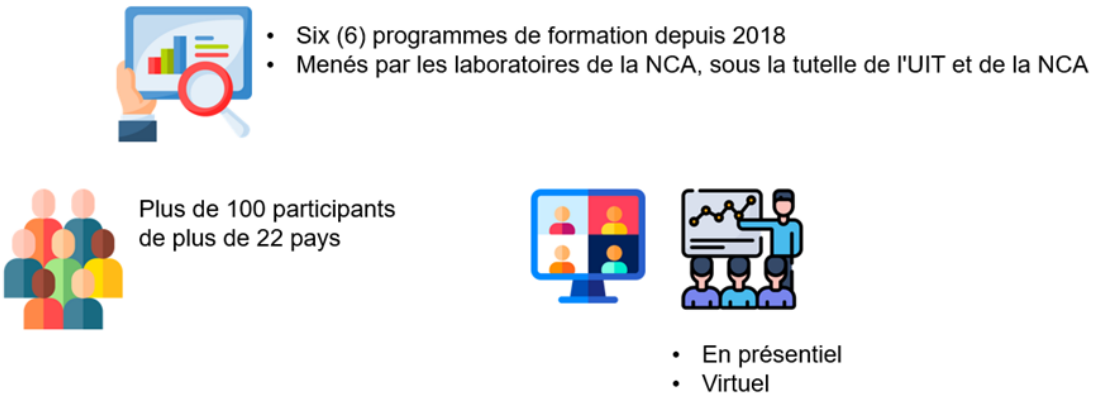
Répondant à cette nécessité de collaborer et afin d'aider la communauté internationale à atteindre les ODD définis par les Nations Unies, plusieurs initiatives ont été prises en faveur du renforcement des compétences de conformité et d'interopérabilité. Ces initiatives menées en collaboration avec l'UIT ont été rapportées par le BDT.

Ces contributions présentent des données d'expérience sur le renforcement des capacités dans la région Afrique, et informent les membres de l'UIT sur les futurs réseaux et infrastructures numériques (y compris les activités, actions, manifestations et/ou ressources telles que les formations et les lignes directrices) qui ont été élaborés.

Depuis 2018, six programmes de formation C&I ont été réalisés pour l'Afrique par le laboratoire du Ghana et ont été sponsorisés par l'UIT via l'Académie de l'UIT et la NCA.

[33] Mwende Njiraini. DiploFoundation. Conformance and interoperability assessment in Africa: case study of Kenya. Atelier de l'UIT-D sur les enjeux de la conformité et de l'interopérabilité pour la transformation numérique, Genève, 2 juin 2023.

Figure 6: Formation UIT-NCA pour l'Afrique



Source: Ghana[34]

Ce partage d'expérience a permis d'aborder des obstacles à la conformité en lien avec:

- les aspects règlementaires et juridiques, dont les ARM et la CEM;
- les problèmes d'acquisition d'une infrastructure C&I de base pour faciliter l'approbation de type et la surveillance du marché;
- la nécessité d'une coopération technique entre les participants;
- les difficultés d'interprétation des rapports de test de divers équipements de télécommunication, etc.

Le Centre égyptien de formation à la règlementation des télécommunications (EG-ATRC), inauguré par l'Égypte en juillet 2021, vise à renforcer les compétences des professionnels africains du secteur des TIC afin d'aller vers une Afrique numérique. Ce centre accrédité par l'UIT dispense une formation théorique et pratique par le biais de sessions en présentiel et en ligne. Les cours de formation portent notamment sur la cybersécurité, les villes intelligentes et les procédures de certification des équipements de communication afin de garantir la conformité aux normes internationales. À ce jour, 381 personnes originaires de plus de 50 pays y ont été formées. Les programmes du centre facilitent le transfert de connaissances aux régulateurs africains et contribuent à l'élaboration de stratégies numériques et de cadres règlementaires à travers le continent[35].

Outre les initiatives nationales lancées par les États Membres, qui constituent de véritables leviers de transfert d'expérience et de connaissances, l'UIT informe ses membres sur les travaux du Bureau de développement des télécommunications (BDT) dans le domaine de l'infrastructure des TIC et sur les ressources élaborées ou en cours d'élaboration pour faciliter l'adoption de politiques et de stratégies en matière d'infrastructures TIC dans les différents pays et les différentes régions.

Cet appui de l'UIT aux États Membres accélère la connectivité, tire parti des connaissances locales, nationales et régionales, et contribue à la réalisation de l'objectif commun consistant à édifier des sociétés numériques inclusives dans le monde entier. Ces ressources couvrent différents thèmes tels que les réseaux TIC (cartographie des infrastructures TIC et analyse géospatiale, kit de planification des activités en matière de TIC, IMT-2020/5G), les technologies

[34] Roland Yaw Kudozia. Ghana. Combating counterfeit ICT devices through C&I testing and market surveillance. ITU-D Workshop on conformance and interoperability challenges for digital transformation, Geneva, 2 June 2023.
[35] Document 2/329 de la CE 2 de l'UIT-D (Égypte).

émergentes, l'assistance technique aux États membres, les possibilités de formation (IPV6, IoT, 5G, points d'échanges, etc.), la conformité et l'interopérabilité, la connectivité au dernier kilomètre et l'exposition aux champs électromagnétiques[36].

En ce qui concerne la C&I, l'Académie de l'UIT a organisé un cours de formation pour la région Afrique sur la conformité et l'interopérabilité des rapports de test, l'analyse et les aspects règlementaires des tests de CEM.

5.4 Lignes directrices pour l'élaboration de programmes de conformité et d'interopérabilité

En définitive, les différents objectifs de développement peuvent être atteints grâce à la mise en œuvre de programmes visant la généralisation de la conformité et de l'interopérabilité des équipements et systèmes de télécommunication/TIC et qui allient les besoins réels et les capacités des pays en développement et les pays les moins avancés.

Cependant, pour élaborer ces programmes, il convient de suivre les lignes directrices suivantes:

- Faire un état de lieux de l'existant, en matière de C&I, dans les pays en développement et les pays les moins avancés, afin de s'attaquer aux difficultés comme il se doit et d'intervenir d'une façon qui corresponde effectivement aux besoins réels.
- Mettre les informations pertinentes détenues par l'UIT et d'autres organisations de normalisation à la disposition des États Membres afin de les sensibiliser aux avantages de la conformité.
- Améliorer la classification et la segmentation des cours de formation afin de mieux adresser les besoins des débutants et de ceux des spécialistes.
- Concevoir des modules de formations pour une meilleure acquisition des compétences par chaque individu, et améliorer ceux qui ont déjà été créés.

[36] Documents 2/48, 2/189, 2/253, SG2RGQ/49 et SG2RGQ/194 de la CE 2 de l'UIT-D (BDT, UIT).

Chapitre 6 – Problèmes liés à la conformité et à l'interopérabilité: enjeux, solutions et perspectives

6.1 Les nouvelles technologies, au-delà des procédures règlementaires et de test

Le développement au-delà des procédures règlementaires et des tests nécessite un mécanisme unique pour obtenir les meilleurs résultats dans les plus brefs délais.

Le cycle "Planifier, Faire, Vérifier, Agir" (PDCA, Plan, Do, Check, Act) est un cycle d'amélioration continue, également appelé "cycle de Deming" ou "roue de Deming". Il s'agit d'une méthode structurée pour résoudre des problèmes, améliorer les procédés ou optimiser les projets. Une telle approche permettra d'unifier les procédures de développement au-delà des procédures règlementaires et des procédures de test et de garantir leur efficacité, leur intégrité et leur adéquation.

Réduction des délais de mise sur le marché et mise en œuvre progressive des règles et procédures applicables aux nouvelles technologies

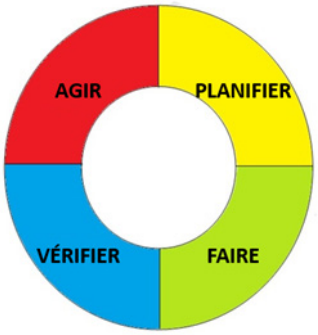
- Étape 1 – Utilisation des protocoles de test disponibles auprès des équipementiers, en lien avec la procédure d'analyse.
- Étape 2 – Déploiement de la zone d'essai pour les essais de compatibilité.
- Étape 3 – Élaboration des exigences établies et réalisation de tests dans un laboratoire accrédité Les nouvelles technologies vont au-delà de la règlementation et des procédures d'essai.

Le développement d'une nouvelle technologie et l'adoption d'une nouvelle norme TIC prennent toujours du temps, dans la mesure où de nouvelles exigences règlementaires doivent être établies et des procédures de test doivent être organisées.

Pour résoudre ce problème, on peut appliquer une approche étape par étape, comme décrit dans la norme ISO 9001.

Le modèle de cycle PDCA est illustré à la Figure 7.

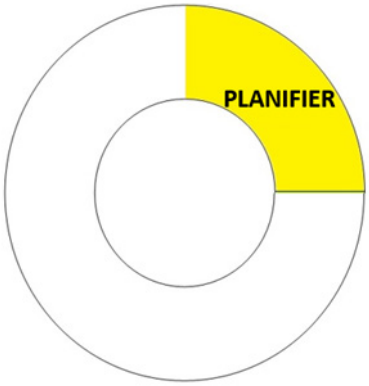
Figure 7: Cycle PDCA



Étape 1 – Planifier

Dans un premier temps, il est nécessaire de déterminer quelles sont les nouvelles normes TIC qui seront mises en œuvre dans un proche avenir. Fort des résultats de cette analyse, un rapport peut être produit, contenant une liste des documents nécessaires pour mettre à jour le cadre règlementaire actuel, définir de nouvelles exigences et élaborer des méthodes de test dans le contexte de l'évaluation obligatoire de la conformité et des tests de compatibilité des nouveaux équipements.

Figure 8: Étape "planifier" du cycle PDCA



Description de la première étape

Un ensemble de documents devrait être élaboré au stade de la planification.

Ces documents doivent décrire:

1) la procédure d'importation d'équipements dans un pays;
2) les spécifications des équipements nécessaires pour assurer la sécurité des personnes, des animaux et de l'environnement;
3) les équipements nécessaires pour assurer l'intégrité, la durabilité et la sécurité du réseau de communication;
4) les licences requises pour les nouvelles TIC (si nécessaire);
5) la procédure de mise en service d'équipements commerciaux;
6) les méthodes d'essai des nouvelles TIC dans le cadre de l'évaluation obligatoire de la conformité et des essais de compatibilité des nouveaux équipements avec les équipements existants des réseaux de communication;
7) les spécifications des équipements de laboratoire d'essai.
8) les travaux nécessaires pour l'accréditation et la validation des laboratoires pour le début des tests et l'utilisation des nouvelles méthodes;
9) le niveau de formation et de certification nécessaire de la part du personnel chargé de concevoir et de tester de nouvelles TIC;
10) l'élaboration et adjonction de mesures de contrôle et de contrôle, tout en veillant au respect des exigences établies.

Toutes ces mesures exigent du temps et des moyens matériels. Ce travail peut prendre de un à deux ans. Pour ne pas ralentir le développement des TIC pendant cette période, le mécanisme d'examen devrait être utilisé.

L'autorité de communication donne l'autorisation à l'entreprise locale qui vérifie que l'équipement est conforme aux prescriptions en analysant les documents du fabricant. Lorsque l'évaluation est réalisée avec succès, l'équipement est importé, installé et mis en service. Cela éliminera les obstacles au déploiement des zones pilotes et réduira le temps nécessaire à la mise en place commerciale des équipements.

Étape 2 – Faire

Dans un deuxième temps, le travail est fait, conformément aux documents règlementaires préparés, qui portent sur l'importation, les essais, l'installation et la maintenance des nouvelles TIC. Des activités de suivi et de surveillance sont prévues pour veiller au respect des exigences établies. La formation et la certification du personnel ont lieu conformément aux programmes élaborés.

Figure 9: Étape "faire" du cycle PDCA

Description de la deuxième étape

Durant l'étape d'action, les procédures qui ont été planifiées et élaborées à l'étape précédente doivent être mises en œuvre. Cela implique de:

1) certifier que les équipements sont conformes aux exigences garantissant la sécurité des personnes, des animaux et de l'environnement;
2) certifier que l'équipement est conforme aux exigences visant à garantir l'intégrité, la durabilité et la sécurité du réseau de communication;
3) veiller à ce que les nouveaux équipements TIC soient importés conformément aux exigences d'importation pertinentes;
4) vérifier la disponibilité des licences nécessaires à l'utilisation des nouvelles TIC (si nécessaire);
5) veiller à ce que l'équipement soit commercialisé conformément aux besoins définis;
6) veiller à ce que les laboratoires d'essais travaillent sur les nouvelles méthodes;
7) former et certifier le personnel participant à la mise au point et à la mise à l'essai de nouvelles TIC;
8) planifier et mettre en œuvre des mesures de supervision et de contrôle pour veiller au respect des exigences établies.

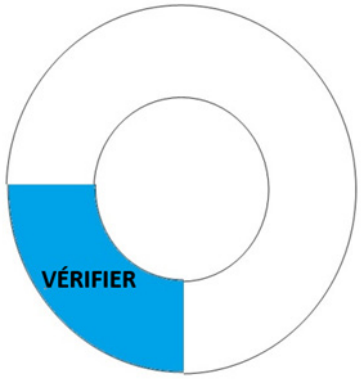
Toutes les activités et statistiques relatives aux TIC, y compris les retours d'informations des utilisateurs finaux sont recueillies. Au cours de la deuxième étape, l'utilisation d'équipements obligatoires et de mécanismes d'examen des projets est également autorisée lorsque les

paramètres ne présentent pas de risques critiques pour la sécurité humaine, animale ou environnementale.

Étape 3 – Vérifier

Après analyse des statistiques relatives à l'utilisation des nouvelles TIC, ainsi que des plaintes et souhaits des utilisateurs finals, un plan de modification du cadre règlementaire actuel peut être élaboré. Des changements sont introduits et de nouvelles TIC sont importées, testées, installées et exploitées en conséquence. Des activités de surveillance et de contrôle sont prévues, afin de veiller au respect des nouvelles exigences après ajustement. Des modifications sont apportées aux programmes de certification et de formation du personnel, si nécessaire.

Figure 10: Étape "vérifier" du cycle PDCA



Description de la troisième étape

Dans la phase d'action corrective, les statistiques et les retours d'information des utilisateurs finaux sont analysés. Sur la base de cette analyse, des modifications des procédés existants suivants sont planifiées et mises en œuvre:

1) La certification obligatoire des équipements conformes aux exigences de sécurité pour les personnes, les animaux et l'environnement.
2) La certification obligatoire des équipements pour vérifier leur conformité aux exigences visant à garantir l'intégrité, la durabilité et la sécurité du réseau de communication.
3) La procédure d'importation de nouveaux équipements TIC.
4) La formation et la certification du personnel chargé de concevoir et de tester de nouvelles TIC.
5) Les mesures de suivi et de contrôle, tout en veillant au respect des exigences établies.

À partir des résultats des actions correctives, des rapports sont établis et des données statistiques sont recueillies.

Étape 4 – Agir

L'impact des mesures correctives élaborées au cours de la troisième phase est examiné, et l'utilisation future des TIC correspondantes est relevée.

Figure 11: Étape "agir" du cycle PDCA

Le cycle se poursuit jusqu'à ce qu'aucune décision n'ait été prise sur l'arrêt de l'utilisation de ces TIC et le démantèlement des équipements. Il est nécessaire d'élaborer des exigences relatives à la sécurité du démontage et de l'enlèvement des équipements, ainsi qu'à la formation des employés qui les utilisent.

Description de la quatrième étape

Dans la phase d'action ou de prise de décisions, les rapports et les statistiques de l'étape précédente sont analysés.

Sur la base de cette analyse, des modifications des procédés existants suivants sont planifiées et mises en œuvre:

1) La formation et la certification du personnel chargé de concevoir et de tester de nouvelles TIC.
2) Les mesures de suivi et de contrôle visant à garantir le respect des exigences établies.

Après une analyse complète des données tirées de l'ensemble du processus, la décision d'arrêter ou non l'utilisation des TIC peut être prise.

6.2 C&I pour la 5G

6.2.1 Accréditation des laboratoires et des organismes de certification pour l'utilisation des technologies 5G

Les évaluations programmées des laboratoires et des organismes de certification (utilisant des technologies liées à la 5G) doivent être réalisées par les organismes d'accréditation en tenant compte de la législation nationale et des exigences règlementaires en vigueur. L'organisme public chargé de faire respecter les exigences et règlementations doit travailler en étroite collaboration avec l'organisme d'accréditation de l'économie, les laboratoires et les organismes de certification. Cela facilitera le contrôle et le suivi des aspects liés à la qualité et à l'interopérabilité des produits 5G. Les pouvoirs publics pourraient envisager de tirer parti des bonnes pratiques et de l'harmonisation de la technologie 5G. La période de transition nécessaire pour acquérir les équipements requis et pour former le personnel spécialisé doit être prise en considération. Pendant cette période, il est souhaitable d'employer un mécanisme d'examen obligatoire. Il importe également de tirer parti des bonnes pratiques et des expériences d'autres pays.

Une des particularités de la 5G est le grand nombre d'objets IoT qu'elle permet de gérer. Des mécanismes de test à distance devraient être établis pour ces équipements. Contrairement aux utilisateurs humains, ils ne peuvent pas signaler eux-mêmes les problèmes potentiels.

Étant donné que les équipements de test des installations et services de communication employant les technologies 5G sont coûteux et nécessitent l'intervention de spécialistes hautement qualifiés, il est souhaitable de créer des centres régionaux permettant une centralisation des ressources requises.

Le mécanisme d'examen obligatoire est prometteur et économiquement approprié.

6.2.2 Mise en place de mécanismes de tests à distance fondés sur la métrologie numérique

Le Digital Metrology Standards Consortium (DMSC™) élabore les normes régissant le Cadre d'informations sur la qualité (QIF).

En 2018, l'ANSI a adopté la norme QIF 3.0, qui a ensuite été soumise à l'ISO par un comité technique au début de l'année 2019.

Se fondant sur la méthodologie QIF, l'ANSI et l'ISO ont élaboré et adopté la norme ISO 23952:2020[37].

Pour appliquer cette norme, une "norme d'interface de mesurage dimensionnelle" (DMIS) a été élaborée. Elle assure la transmission bidirectionnelle de données de commande entre les systèmes informatiques et l'équipement de contrôle. Elle peut servir de base à un langage de programmation commun pour les systèmes de commande. La norme DMIS établit une syntaxe de programmation permettant de transmettre les instructions de commande aux dispositifs de mesure et de recevoir les données de mesure et de traitement des systèmes d'analyse, de collecte ou d'archivage. Le format défini par la norme est neutre. Il a été conçu afin que l'échange de données soit facilement contrôlable par l'être humain.

Tous ces mécanismes, à leur tour, nécessitent des canaux de communication calibrés pour une utilisation sur des sites distants. Par exemple, la métrologie numérique fait partie des TIC.

L'introduction de mécanismes de métrologie numérique repose technologiquement sur la mise en place d'un cadre pour l'évaluation des sondeurs. Les sondes sont installées aux frontières des domaines et fournissent une analyse complète du trafic de transit, y compris l'origine (l'adresse réelle du dispositif ayant constitué le paquet), ainsi que tous les autres paramètres (lors de l'interaction avec des dispositifs de mesure pour générer et analyser le trafic de référence).

Il est aujourd'hui inconcevable de préserver la souveraineté numérique sans disposer de la métrologie numérique. En effet, en l'absence de preuves juridiquement recevables sur l'origine des paquets, il sera impossible d'appliquer les règles actuelles du droit international.

[37] ISO 23952:2020 – Systèmes d'automatisation et intégration – Cadre d'information sur la qualité (QIF) – Modèle intégré pour les informations sur la qualité de production.

6.3 Modifications des logiciels des dispositifs TIC après certification et leur influence sur les cadres C&I existants

Les modifications apportées aux logiciels des dispositifs TIC après leur certification peuvent avoir d'importantes répercussions sur les cadres de C&I existants. Ces cadres sont conçus pour garantir que les dispositifs respectent des normes spécifiques en matière de sûreté, de sécurité, d'interopérabilité et de performance. Voici quelques points clés à prendre en compte concernant les enjeux liés aux modifications des logiciels:

Conformité aux normes de certification

- **Certification initiale**: lorsqu'un dispositif TIC est certifié, il est évalué par rapport à des normes et règlementations bien définies. Toute modification apportée au logiciel après sa certification est susceptible d'altérer la conformité du dispositif à ces normes.
- **Recertification**: selon la nature de la modification, il peut être nécessaire de recertifier le dispositif pour s'assurer qu'il est bien toujours conforme aux normes requises. Cela peut demander beaucoup de temps et d'argent.

L'Académie internationale des télécommunications a proposé un nouveau projet de recommandation UIT-T visant à améliorer les tests de conformité des équipements TIC aux normes de l'UIT. Cette proposition s'appuie sur la Recommandation UIT-T Q.4068, qui décrit la procédure de test, mais se heurte à des problèmes d'application pratique. L'objectif est d'élaborer une nouvelle recommandation visant à clarifier et à normaliser les mécanismes de certification[38].

Principaux points

1) Organisation actuelle du système de test

- Le système d'essai se fonde sur la Recommandation UIT-T Q.4068, qui définit des interfaces API ouvertes pour la fédération interopérable de bancs d'essai.
- Les avancées technologiques rendent les tests plus complexes et nécessitent l'interconnexion de bancs d'essai pour simuler des conditions réelles; c'est particulièrement le cas dans le domaine de l'IoT.
- Les API ouvertes permettent de gérer l'interconnexion, l'interopérabilité, l'annonce, les bancs d'essai dans une fédération, l'annonce, l'attribution et la mise à disposition de ressources, ainsi que les rôles des utilisateurs (expérimentateurs).

2) Cas d'utilisation: expérimentation dans une fédération de bancs d'essai

- Un exemple concret est l'expérimentation d'un réseau de capteurs sans fil (WSN) composé de dispositifs IoT.
- Les bancs d'essai permettent de tester la qualité de fonctionnement des dispositifs IoT dans divers environnements en mesurant des paramètres tels que la fiabilité, la latence et l'utilisation du spectre radioélectrique.
- Les critères portent notamment sur la pertinence, la reproductibilité, la répétabilité et l'automatisation de l'expérience.
- Les fédérations de bancs d'essai, telles que Fed4FIRE+, fournissent les outils nécessaires pour répondre à ces exigences.

3) Cas d'utilisation: système de certification

[38] Document 2/79 de la CE 2 de l'UIT-D (Académie internationale des télécommunications).

- Le système actuel présente des lacunes, telles que des conflits d'intérêts lorsque les laboratoires d'essais appartiennent à la société exploitante.
- Les résultats des tests ont un caractère informatif plutôt que juridique, ce qui limite leur utilisation en cas de différend.
- La proposition préconise la participation d'organismes de certification accrédités, indépendants et indépendants afin de garantir:
  - la transparence du financement (via l'autorité de certification);
  - l'absence de conflit d'intérêts;
  - la validité juridique des résultats d'essai.

4) Propositions et solutions

Nouvelle recommandation: élaborer une recommandation UIT-T visant à clarifier les mécanismes de certification et à normaliser les interfaces API pour les bancs d'essai fédérés.

Organismes de certification indépendants

- Travailler avec les organisations accréditées pour garantir l'impartialité, la transparence et la validité juridique des tests.
- L'accréditation devrait se faire en se fondant de la législation nationale, en tant compte des bonnes pratiques internationales existantes.

Amélioration de l'interopérabilité: normaliser les interfaces API pour faciliter l'interconnexion des bancs d'essai et mener des expériences reproductibles et automatisées.

La solution proposée vise à moderniser et à normaliser les procédures de test et de certification des équipements TIC. S'appuyant sur la Recommandation UIT-T Q.4068, elle propose des solutions pour résoudre les difficultés actuelles, telles que la complexité des tests IoT, les conflits d'intérêts et l'absence de validité juridique des résultats des tests. L'adoption d'une nouvelle recommandation et la participation d'organismes de certification indépendants permettraient d'accroître la fiabilité, la transparence et l'interopérabilité des tests de conformité[39].

Incidences sur la sécurité

- **Vulnérabilités**: les mises à jour ou les modifications logicielles peuvent introduire de nouvelles vulnérabilités ou révéler des vulnérabilités existantes, ce qui peut compromettre la sécurité du dispositif.
- **Gestion des correctifs**: il est essentiel de procéder à des mises à jour et à des correctifs réguliers pour corriger les failles de sécurité. Cependant, ces actualisations doivent être soigneusement gérées pour veiller à ce qu'elles n'introduisent pas par inadvertance de nouveaux risques ou problèmes de non-conformité.

Interopérabilité

- **Compatibilité**: les modifications logicielles peuvent affecter la capacité du dispositif à interopérer avec d'autres dispositifs et systèmes. Ceci est particulièrement critique dans les environnements où plusieurs dispositifs de différents fabricants doivent fonctionner ensemble de manière transparente.

[39] *Ibid.*

- **Respect des normes**: les modifications doivent être conformes aux normes sectorielles afin de maintenir l'interopérabilité. Toute dérogation à ces normes peut entraîner des problèmes de compatibilité et perturber les cadres C&I existants.

Performances et fiabilité

- **Fonctionnalité**: les modifications logicielles peuvent se répercuter sur les performances et la fiabilité du dispositif. Les modifications qui influent sur la fonctionnalité du dispositif peuvent entraîner des défaillances ou une réduction des performances, qui peuvent ne pas correspondre aux critères de certification d'origine.
- **Tests et validation**: des tests post-modification sont essentiels pour s'assurer que le dispositif continue de fonctionner comme prévu et réponde bien aux critères de performance nécessaires.

Bonnes pratiques pour la gestion des modifications logicielles

- **Gestion du changement**: mise en œuvre d'un mécanisme éprouvé de gestion du changement pour évaluer et tester les modifications apportées au logiciel et en garder une trace.
- **Surveillance continue**: mise en place de mécanismes de surveillance continue pour détecter et résoudre rapidement tout problème découlant des modifications logicielles.
- **Mobilisation des parties prenantes**: dialogue avec les parties prenantes pour comprendre les répercussions des modifications apportées au logiciel et en assurer leur conformité avec les cadres C&I.

En résumé, les modifications apportées aux logiciels des dispositifs TIC après leur certification peuvent avoir de profondes répercussions sur les cadres C&I existants. Il est essentiel de gérer ces changements avec soin pour préserver la conformité, la sécurité, l'interopérabilité et les performances, tout en adaptant les cadres C&I pour tenir compte de la nature dynamique des mises à jour logicielles.

6.4 Harmonisation efficace des procédures et collaboration technique

Une collaboration technique et une harmonisation efficace des procédures sont essentielles pour garantir la fluidité des opérations, favoriser l'innovation et atteindre les objectifs communs de toute organisation ou de tout partenariat. Voici les principales stratégies pour y parvenir:

Définir des objectifs et des normes clairs

- **Définir les objectifs**: énoncer clairement l'objectif de l'harmonisation et de la collaboration, en veillant à la conformité aux objectifs de l'organisation ou du projet.
- **Standardiser les procédures**: élaborer des protocoles, des flux de travail et une documentation standardisés pour assurer la cohérence entre les équipes ou les partenaires.
- **Adopter les meilleures pratiques**: tirer parti des normes et des meilleures pratiques sectorielles pour créer un cadre commun de collaboration.

Favoriser une communication ouverte

- **Réunions régulières**: planifier des vérifications, des mises à jour et des séances de retours régulières pour maintenir la transparence et résoudre les problèmes rapidement.

- **Plates-formes unifiées**: utiliser des outils collaboratifs (ex.: Slack, Microsoft Teams ou un logiciel de gestion de projets) pour centraliser la communication et le partage d'informations.
- **Équipes interfonctionnelles**: encourager la collaboration entre les départements ou les partenaires pour briser les silos et favoriser l'échange de connaissances.

Tirer parti de la technologie

- **Systèmes intégrés**: mettre en œuvre des outils et des plates-formes interopérables pour rationaliser le partage des données et l'intégration des flux de travail.
- **Automatisation**: recourir à l'automatisation pour réduire les erreurs manuelles et améliorer l'efficacité des tâches répétitives.
- **Analyse des données**: utiliser les informations fondées sur les données pour repérer les goulots d'étranglement, optimiser les processus et mesurer les retombées des efforts d'harmonisation.

Instaurer une culture de la collaboration

- **Vision partagée**: veiller à ce que toutes les parties prenantes comprennent la vision et les objectifs communs et s'y engagent.
- **Confiance et respect**: favoriser un environnement de confiance, de respect et d'inclusion pour encourager un dialogue ouvert et la coopération.
- **Reconnaissance et récompenses**: saluer et récompenser les efforts de collaboration pour motiver les équipes et renforcer les comportements positifs.

Fournir des formations et une assistance

- **Développement des compétences**: proposer des programmes de formation pour faire en sorte que tous les membres de l'équipe maîtrisent les outils, les technologies et les procédures utilisés.
- **Gestion du changement**: soutenir les équipes tout au long des transitions en leur fournissant des ressources, des conseils et en répondant à leurs préoccupations.
- **Mentorat**: coupler des membres expérimentés de l'équipe avec de nouveaux arrivants pour faciliter le transfert des connaissances et le renforcement des compétences.

Suivre et évaluer les progrès

- **Indicateurs clés de performance et mesures**: établir des indicateurs fondamentaux de performance pour suivre la réussite des efforts d'harmonisation et de collaboration.
- **Boucles de rétroaction**: recueillir en continu les commentaires des parties prenantes pour prendre note des points à améliorer.
- **Capacité d'adaptation**: être prêt à adapter les procédures et les stratégies en fonction de l'évolution des besoins et des difficultés rencontrées.

Assurer la gouvernance et la responsabilisation

- **Définir clairement les rôles et les responsabilités**: définir les rôles et les responsabilités afin d'éviter les chevauchements d'activités et d'assurer la responsabilisation.
- **Conformité**: faire en sorte que toutes les procédures et collaborations respectent les exigences règlementaires et les politiques de l'organisation.

- **Résolution des conflits**: mettre en place des mécanismes pour résoudre les conflits ou les désaccords de manière constructive.

Encourager l'innovation et l'amélioration continue

- **Encourager l'expérimentation**: aménager un espace sécurisé où les équipes peuvent essayer de nouvelles idées et approches.
- **Processus itératifs**: examiner et affiner régulièrement les procédures pour intégrer les enseignements tirés et les tendances émergentes.
- **Partage des connaissances**: garder une trace des réussites et des échecs, et communiquer à leur sujet afin d'instaurer une culture de l'apprentissage continu.

En mettant en œuvre ces stratégies, les organisations peuvent parvenir à une harmonisation efficace des procédures et à une plus grande collaboration technique, ce qui améliore l'efficacité, l'innovation et la réussite globale.

6.5 Comment hiérarchiser les modèles de dispositifs et d'homologation tout en conciliant la confiance des utilisateurs et les mesures règlementaires applicables?

Pour trouver le bon équilibre entre la confiance des utilisateurs (ex.: par le biais de l'homologation) et la conformité aux mesures règlementaires, les éléments suivants sont d'importance:

- Collaborer avec le personnel qualifié, afin d'assurer la qualité et l'efficacité des tests d'homologation.
- Garantir l'indépendance des tests d'homologation.
- Veiller au marquage neutre des échantillons d'essai.
- Mener à bien des procédures d'essai comparatives dans différents laboratoires.

Toutes les procédures d'homologation doivent être établies par les administrations locales ou régionales.

Ces administrations établissent et maintiennent un système d'accréditation et de vérification des activités des entreprises qui réalisent les tests d'homologation.

6.6 Difficultés et possibilités en matière de C&I pendant la pandémie de COVID-19

La pandémie de COVID-19 a montré que, dans une situation de pandémie, la C&I peut offrir les éléments suivants:

- Systèmes d'alerte.
- Systèmes de contrôle d'accès extérieur.
- Systèmes de contrôle d'accès intérieur.
- Systèmes de suivi hors site.
- Systèmes de collecte, de stockage et d'analyse des informations sur les paramètres de la pandémie.
- Systèmes de collecte, de stockage et d'analyse des informations sur les soins aux patients.

- Systèmes de collecte, de stockage et d'analyse des informations sur le travail du personnel médical.
- Systèmes de collecte, de stockage et d'analyse de l'équipement médical.
- Systèmes de collecte, de stockage et d'analyse des informations pour la vaccination et la prévention des infections.
- Systèmes logistique pour le transport et l'hospitalisation des patients.
- Systèmes de gestion des médias.
- Systèmes d'interaction international et interrégional.

6.7 Comment les nouvelles technologies peuvent-elles contribuer à améliorer le cadre international de C&I ainsi que le commerce et l'utilisation des dispositifs TIC?

On trouvera ci-dessous certaines des manières dont les nouvelles technologies peuvent contribuer à améliorer le cadre international de C&I ainsi que le commerce et l'utilisation de dispositifs TIC:

- Établissement de registres électroniques internationaux et interrégionaux des équipements autorisés.
- Mise en place de systèmes d'enregistrement électronique des documents.
- Essais et mesures à distance, mise en œuvre de mécanismes de métrologie numérique.
- Mise en place de registres électroniques communs pour les services frontaliers et douaniers.
- Harmonisation des lois internationales sur la protection des données et les informations personnelles
- Création de systèmes d'information internationaux et interrégionaux.
- Garantie de la sécurité et de la protection de l'information des citoyens, des entreprises et des organes de l'État.
- Tenue à jour de registres internationaux et interrégionaux unifiés des produits de contrefaçon.
- Mise en œuvre de mécanismes de télémédecine pour aider les populations dans tous les pays.
- Mise en œuvre de systèmes internationaux et interrégionaux d'alerte en cas de catastrophe.

Annexes

Annex 1: Conformance and interoperability frameworks: data by country

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

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

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

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

Key findings (2022-2025)

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

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

Visual representation: histogram

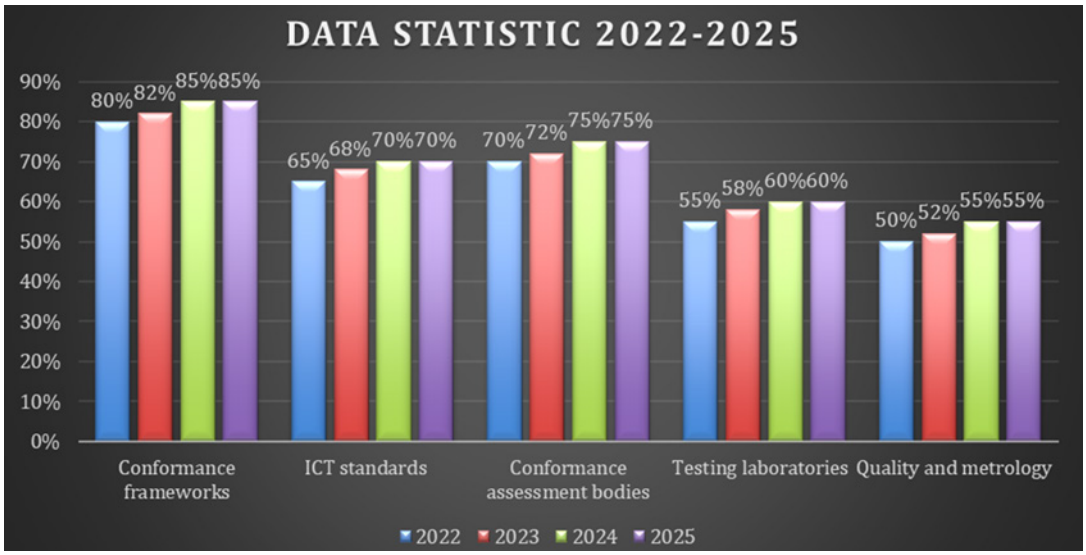
Below is a conceptual representation of the data using a bar diagram and spiral diagram to highlight trends and comparisons.

Bar diagram

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

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

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



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

Recommendations for 2025 and beyond

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

Conclusion

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

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

Friday, 2 June 2023, 0900 – 1200 hours

Workshop programme: link

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

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

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

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

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

Co-moderators:

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

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

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

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

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

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

In the report, Mr Melnik noted that in the Russian Federation and the CIS region, an approach similar to the one presented in the Brazilian report was applied to confirming the conformity of communications. Algorithms for the operation of declaration and certification were given. It was noted that cyber security problems were also proposed to be solved through voluntary certification. The need to introduce digital metrology mechanisms for remote testing was especially worth noting.

SESSION 2: C&I infrastructure and applications

This session focused on**:**

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

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

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

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

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

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

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

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

Achieving these objectives necessarily required the establishment of an effective and harmonized C&I system that could assess the compliance of ICT equipment with standards

and the interoperability between competing systems, in order to build a high-quality, reliable, durable and resilient ICT infrastructure, to serve and achieve the objectives of the policy declaration for the telecommunications sector in Mauritania.

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

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

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

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

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

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

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

Friday, 10 May 2024, 1430 - 1730 hours

Workshop programme: see link

Background information

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

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

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

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

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

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

Ms Mwende Njiraini (DiploFoundation)

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

Q&A session:

Questions were raised regarding the operational aspects of the Device Management System, the establishment of a laboratory for counterfeit management and the verification of

documents supplied during the type-approval process. Ms Njiraini responded by explaining the collaboration with various regulatory organizations, the proposed laboratory's role, and the current operational challenges, including trusting the authenticity of documents in the absence of a local laboratory.

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

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

Q&A session:

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

Mobile Device Registration System

Ms Zeynep Nehir Sarıgöl (Dekob Technology)

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

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

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

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

Q&A session:

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

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

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

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

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

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

Mr Roland Yaw Kudozia (Ghana)

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

Q&A session:

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

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

Conclusion

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

Overall, the workshop served as a crucial platform for exchanging knowledge, experiences and good practices among various stakeholders in the ICT sector. The discussions reinforced the necessity of developing robust and adaptable regulatory frameworks that could keep pace

with technological advancements. The workshop's outcomes pointed towards the need for ongoing dialogue, research and collaboration to create a more harmonized and global ICT environment, which was particularly vital for the sustainable growth and development of ICT infrastructure in developing countries.

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

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

Contributions on Question 4/2

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

(suite)

Web	Received	Source	Title
RGQ2/203	2024-04-16	Côte d'Ivoire	Draft text for the Q4/2 Final Report, Chapter 6 ("Review of information transfer, know-how and training")
RGQ2/194	2024-04-16	BDT Focal Points for Questions 1/1, 2/1, 4/2, 5/1 and 7/2	BDT report on the implementation of ICT Infrastructure work since the last ITU-D Study Group meeting
RGQ2/186	2024-04-15	International Telecommunication Academy	Proposed text for Q4/2 Final Report, Section 7.1 ("New technologies beyond regulatory/testing procedures")
RGQ2/115	2024-02-27	Guinea	Combating counterfeiting and theft of mobile devices in Guinea
RGQ2/112	2024-02-21	Chad	Combating mobile phone theft in Chad
2/193	2023-10-16	Telecommunications Management Group, Inc.	Frameworks of conformance and interoperability to support wireless power transmission via radiofrequency beam (beam WPT)
2/189	2023-10-16	BDT Focal Points for Questions 1/1, 2/1, 4/2, 5/1 and 7/2	BDT report on the implementation of ICT Infrastructure work since the last ITU-D Study Group meeting
2/140	2023-10-03	International Telecommunication Academy	National expertise for the compliance of the ICT devices and services with the ITU standards
2/124	2023-09-14	Rapporteur for Question 4/2; Vice-Rapporteurs for Question 4/2	Annual progress report for Question 4/2 for October-November 2023 meeting
2/114	2023-09-05	Sri Lanka	Registration of legitimate mobile devices and combating counterfeiting and theft of mobile devices
2/99	2023-08-04	Liberia	Public policy challenge to combat mobile crime in Liberia
RGQ2/49	2023-04-25	BDT Focal Points for Questions 1/1, 2/1, 4/2, 5/1 and 7/2	BDT report on Future Network and Digital Infrastructure work including activities, and resources since the last ITU-D Study Group meetings
RGQ2/37	2023-04-07	Zambia	Combating the influx of counterfeit phones
RGQ2/22	2023-03-23	Madagascar	Importance of awareness-building among suppliers and users of terminal equipment in the context of improved monitoring of equipment and compliance of equipment in use
RGQ2/17	2023-03-20	Central African Republic	SDG 9 in relation to impact of counterfeit and fake telecommunications/ICTs and devices trafficked to developing countries

(suite)

Web	Received	Source	Title
2/TD/5	2022-12-06	Rapporteur for Question 4/2	Proposed workplan and table of contents for Question 4/2
2/79	2022-11-24	International Telecommunication Academy	Certification system for ICT devices and services compliance with ITU standards
2/48	2022-10-18	BDT Focal Points for Questions 1/1, 2/1, 4/2, 5/1 and 7/2	BDT report on the implementation of ICT Infrastructure work since the last ITU-D Study Group meeting
2/46	2022-10-17	Inter-Sector Coordination Group	Mapping of ITU-D Questions to ITU-T Questions and ITU-R Working Parties

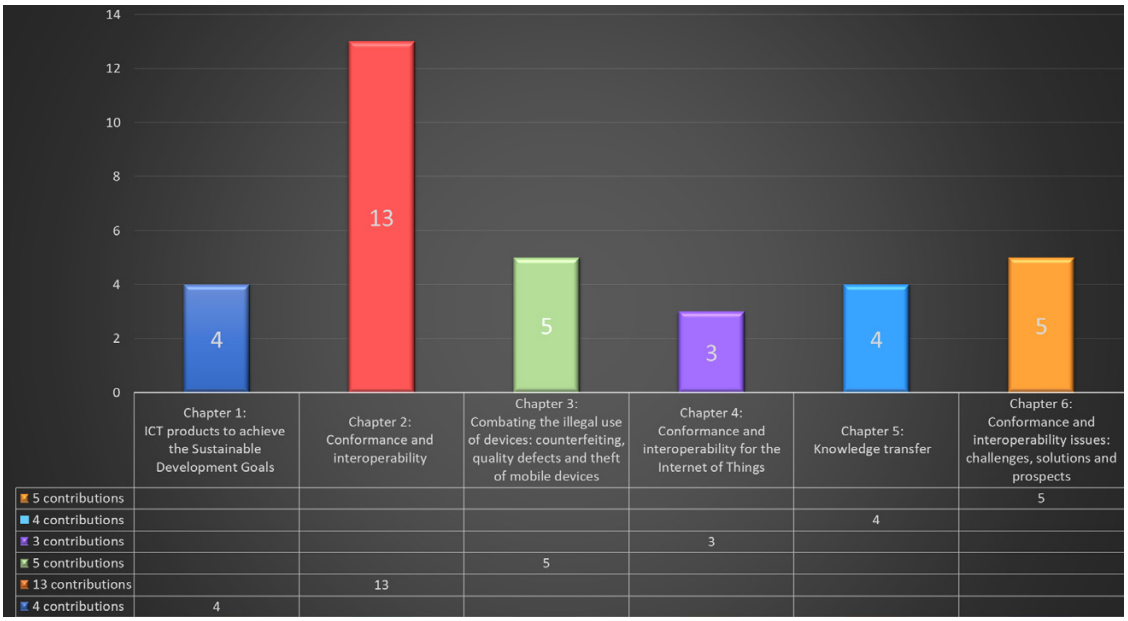
Incoming liaison statements for Question 4/2

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

(suite)

Web	Received	Source	Title
2/206	2023-10-26	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Group 2 Question 4/2 on ITU Workshop "Episode 2: "Global approaches on combating counterfeiting of telecommunication/ICT devices and mobile device theft"
2/203	2023-10-24	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Group 2 Question 4/2 on ITU Tutorial on Testing Laboratories Recognition Procedure
2/93	2023-06-05	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Group 2 Question 4/2 on telecommunication/ICT equipment
RGQ2/59	2023-05-03	ITU-T Study Group 15	Liaison statement from ITU-T Study Group 15 to ITU-D Study Groups 1 and 2, Question 1/1 and Question 4/2 on contributions from developing countries
2/25 +Ann.1-4	2022-07-18	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Group 2 Question 4/2 on ITU recognition of testing laboratories
2/21 +Ann.1	2022-06-16	ITU-T Focus Group on Testbeds Federations for IMT-2020 and beyond	Liaison statement from ITU-T Focus Group on Testbeds Federations for IMT-2020 and beyond (FG-TBFxG) to ITU-D Study Groups 1 and 2 on call for use cases on testbeds federation
2/15 +Ann.1-2	2022-04-14	ITU-T Focus Group on Testbeds Federations for IMT-2020 and beyond	Liaison statement from ITU-T Focus Group on Testbed Federations for IMT-2020 and beyond (FG-TBFxG) to ITU-D Study Groups 1 and 2 on the outcomes of the first meeting of the Focus Group
2/10 +Ann.1	2021-12-21	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Groups 1 and 2 on establishment of a new ITU-T Focus Group on Testbeds Federations for IMT-2020 and beyond (FG-TBFxG) and first meeting (virtual, 4-7 April 2022)
2/8	2021-12-16	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Group 2 Question 4/2 on the progress on the combat of counterfeit and stolen ICT
2/6 +Ann.1-3	2021-12-10	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Group 2 Question 4/2 on ITU Testing Laboratory Recognition Procedure

Figure 13: Mapping distribution to chapters



Union internationale des télécommunications (UIT)
Bureau de développement des télécommunications (BDT)
Bureau du Directeur
Place des Nations
CH-1211 Genève 20
Suisse

Courriel: bdtdirector@itu.int
Tél.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Adjoint au directeur et Chef du Département de l'administration et de la coordination des opérations (DDR)
Place des Nations
CH-1211 Genève 20
Suisse

Courriel: bdtdeputydir@itu.int
Tél.: +41 22 730 5131
Fax: +41 22 730 5484

Département des réseaux et de la société numériques (DNS)
Courriel:: bdt-dns@itu.int
Tél.: +41 22 730 5421
Fax: +41 22 730 5484

Département du pôle de connaissances numériques (DKH)
Courriel: bdt-dkh@itu.int
Tél.: +41 22 730 5900
Fax: +41 22 730 5484

Département des partenariats pour le développement numérique (PDD)
Courriel: bdt-pdd@itu.int
Tél.: +41 22 730 5447
Fax: +41 22 730 5484

Afrique

Ethiopie

International Telecommunication Union (ITU) Bureau régional
Gambia Road
Leghar Ethio Telecom Bldg. 3rd floor
P.O. Box 60 005
Addis Ababa
Ethiopie

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

Cameroun

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

Courriel: itu-yaounde@itu.int
Tél.: + 237 22 22 9292
Tél.: + 237 22 22 9291
Fax: + 237 22 22 9297

Sénégal

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

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

Zimbabwe

International Telecommunication Union (ITU) Bureau de zone
USAF POTRAZ Building
877 Endeavour Crescent
Mount Pleasant Business Park
Harare
Zimbabwe

Courriel: itu-harare@itu.int
Tél.: +263 242 369015
Tél.: +263 242 369016

Amériques

Brésil

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

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

La Barbade

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

Courriel: itubridgetown@itu.int
Tél.: +1 246 431 0343
Fax: +1 246 437 7403

Chili

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

Courriel: itusantiago@itu.int
Tél.: +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

Courriel: ituteguciglapa@itu.int
Tél.: +504 2235 5470
Fax: +504 2235 5471

Etats arabes

Egypte

International Telecommunication Union (ITU) Bureau régional
Smart Village, Building B 147,
3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
Cairo
Egypte

Courriel: itu-ro-arabstates@itu.int
Tél.: +202 3537 1777
Fax: +202 3537 1888

Asie-Pacifique

Thaïlande

International Telecommunication Union (ITU) Bureau régional
4th floor NBTC Region 1 Building
101 Chaengwattana Road
Laksi,
Bangkok 10210,
Thailande

Courriel: itu-ro-asiapacific@itu.int
Tél.: +66 2 574 9326 – 8
+66 2 575 0055

Indonésie

International Telecommunication Union (ITU) Bureau de zone
Gedung Sapta Pesona
13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10110
Indonésie

Courriel: bdt-ao-jakarta@itu.int
Tél.: +62 21 380 2322

Inde

International Telecommunication Union (ITU) Area Office and Innovation Centre
C-DOT Campus
Mandi Road
Chhatarpur, Mehrauli
New Delhi 110030
Inde

Courriel:
Bureau régional: itu-ao-southasia@itu.int
Centre d'innovation: itu-ic-southasia@itu.int
Site web: ITU Innovation Centre in New Delhi, India

Pays de la CEI

Fédération de Russie

International Telecommunication Union (ITU) Bureau régional
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Fédération de Russie
Courriel: itu-ro-cis@itu.int
Tél.: +7 495 926 6070

Europe

Suisse

Union internationale des télécommunications (UIT)
Bureau pour l'Europe
Place des Nations
CH-1211 Genève 20
Suisse
Courriel: eurregion@itu.int
Tél.: +41 22 730 5467
Fax +41 22 730 5484

Union internationale des télécommunications
Bureau de développement des télécommunications
Place des Nations
CH-1211 Genève 20
Suisse

ISBN: 978-92-61-41182-4

Publié en Suisse
Genève, 2025

Photo credits: Adobe Stock