International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

L.1034

(08/2022)

SERIES L: ENVIRONMENT AND ICTS, CLIMATE CHANGE, E-WASTE, ENERGY EFFICIENCY; CONSTRUCTION, INSTALLATION AND PROTECTION OF CABLES AND OTHER ELEMENTS OF OUTSIDE PLANT

E-waste and circular economy

Adequate assessment and sensitization on counterfeit information and communication technology products and their environmental impact

Recommendation ITU-T L.1034

ITU-T L-SERIES RECOMMENDATIONS

ENVIRONMENT AND ICTS, CLIMATE CHANGE, E-WASTE, ENERGY EFFICIENCY; CONSTRUCTION, INSTALLATION AND PROTECTION OF CABLES AND OTHER ELEMENTS OF OUTSIDE PLANT

OPTICAL FIBRE CABLES	
Cable structure and characteristics	L.100–L.124
Cable evaluation	L.125–L.149
Guidance and installation technique	L.150–L.199
OPTICAL INFRASTRUCTURES	
Infrastructure including node elements (except cables)	L.200–L.249
General aspects and network design	L.250–L.299
MAINTENANCE AND OPERATION	
Optical fibre cable maintenance	L.300–L.329
Infrastructure maintenance	L.330–L.349
Operation support and infrastructure management	L.350–L.379
Disaster management	L.380–L.399
PASSIVE OPTICAL DEVICES	L.400–L.429
MARINIZED TERRESTRIAL CABLES	L.430–L.449
E-WASTE AND CIRCULAR ECONOMY	**L.1000–L.1199**
POWER FEEDING AND ENERGY STORAGE	L.1200–L.1299
ENERGY EFFICIENCY, SMART ENERGY AND GREEN DATA CENTRES	L.1300–L.1399
ASSESSMENT METHODOLOGIES OF ICTS AND CO2 TRAJECTORIES	L.1400–L.1499
ADAPTATION TO CLIMATE CHANGE	L.1500–L.1599
CIRCULAR AND SUSTAINABLE CITIES AND COMMUNITIES	L.1600–L.1699
LOW COST SUSTAINABLE INFRASTRUCTURE	L.1700–L.1799

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T L.1034

Adequate assessment and sensitization on counterfeit information and communication technology products and their environmental impact

Summary

Recommendation ITU-T L.1034 provides awareness and guidance on the health and environmental impacts of counterfeit information and communication technology products. The intention is to create awareness and sensitization on human health and environmental risks, as well as measures implemented in different countries for risk mitigation.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T L.1034	2022-08-13	5	11.1002/1000/15023

Keywords

Counterfeit, environmental risks, health risks, ICT products.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

© ITU 2022

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

Introduction

Counterfeit information and communication technology (ICT) devices are commonly understood to mean "fake and substandard" [b-ITU-T QTR-CICT]. Counterfeit products can have an extremely short lifespan, quickly reach the end of their useful life and are discarded as e-waste.

Counterfeit ICT products can be found everywhere, but they are particularly prominent in developing economies. This can be attributed to diverse reasons, including low pricing, porous borders, grey and informal markets, insufficient regulatory surveillance (type approval/acceptance) and uncontrolled export-import business.

Among other ITU-related documents, the ITU-T SG11 focuses on signalling requirements, protocols, test specifications and combating counterfeit products. It is responsible for studies to combat counterfeiting products, including telecommunications/ICT and mobile device theft. [ITU-T Q.5050] provides a framework for solutions to combat counterfeit ICT devices. [b-ITU-T QTR-CICT] looks at counterfeit ICT devices in the African region. [b-ITU-D 2021] looks at assisting developing countries in implementing conformance and interoperability programmes and combating counterfeit ICT equipment and theft of mobile devices.

This Recommendation specifically describes and provides an assessment of the health and environmental risks and potential impacts of counterfeit ICT products (including separate parts and assembled components) and assesses their contribution to the generation of e-waste volumes to reduce their environmental impact and create awareness sensitization on the same.

Recommendation ITU-T L.1034

Adequate assessment and sensitization on counterfeit information and communication technology products and their environmental impact

1 Scope

This Recommendation provides awareness and guidance on what consumers and retailers should consider about counterfeit information and communication technology (ICT) products regarding environmental and health (EH) risks. The Recommendation describes counterfeit ICT products in this context to guide the assessment of the risks and potential adverse effects, sensitization of the public, and management of counterfeit goods in an environmentally sound manner. The main challenge in the management of counterfeit products is that they misrepresent legitimate ones, do not exist formally and therefore no assumptions about safety can be made. Consequently, counterfeit products can be considered to be potentially hazardous.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Q.5050] Recommendation ITU-T Q.5050 (2019), *Framework for solutions to combat counterfeit ICT devices*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 counterfeit [b-WTO glossary]: Unauthorized representation of a registered trademark carried on goods identical or similar to goods for which the trademark is registered, with a view to deceiving the purchaser into believing that he/she is buying the original goods.

3.1.2 counterfeit ICT device [ITU-T Q.5050]: An information and communication technology (ICT) device that explicitly infringes the trademark, copies hardware or software designs, or infringes brand or packaging rights of an original or authentic product and, in general, infringes applicable national and/or international technical standards, regulatory requirements or conformity processes, manufacturing licensing agreements, or other applicable legal requirements.

3.1.3 e-waste/WEEE [b-ITU-T L.1031]: Electrical or electronic equipment that is waste, including all components, sub-assemblies and consumables that are part of the equipment at the time the equipment becomes waste.

NOTE – For the purpose of this Recommendation, the term e-waste and waste electrical and electronic equipment (WEEE) are used interchangeably.

3.1.4 grey market [b-Gartner]: The import and sale of devices outside regular commercial channels as defined by the original manufacturer or the relevant government, creating a parallel market to authorized distribution channels.

3.1.5 harm [ISO/IEC Guide 51]: Injury or damage to people's health, or damage to property, or the environment.

3.1.6 hazard [ISO/IEC Guide 51]: Potential source of harm.

3.1.7 risk [ISO/IEC Guide 51]: Combination of the probability of occurrence of harm and the severity of that harm.

NOTE – Limited for this recommendation to human health or safety of persons or to the environment.

3.1.8 tampered ICT device [ITU-T Q.5050]: An information and communication technology (ICT) device that had components, software, unique identifier, items protected by intellectual-protected rights or trademarks tentatively or effectively altered without the explicit consent of the manufacturer or its legal representative.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 counterfeit spare part: A false or misleading appearance copy, unauthorized copy, imitation, used part falsely claimed as new or modified part, that is deliberately misrepresented as a genuine part of a manufacturer and that misrepresents environmental and health compliance, and therefore constitutes hazards for people and the environment.

4 Abbreviation and acronyms

This Recommendation uses the following abbreviations and acronyms:

EH	Environmental and Health
EMC	Electromagnetic Compatibility
EPR	Extended Producer Responsibility
ICT	Information Communication Technology
IMEI	International Mobile Equipment Identity
MNO	Mobile Network Operator
WEEE	Waste Electrical and Electronic Equipment

5 Conventions

None.

6 Genuine versus counterfeit

The World Trade Organization (WTO) regards counterfeit products in terms of the closeness of the mark used to a registered product and applies to cases where the goods inappropriately bear a validly registered trademark [b-WTO ACTA]. In that sense of trade and market, counterfeit is considered equivalent to trademark violation, and generally, it means a fake and substandard device or part [b-ITU-T QTR-CICT].

Counterfeit electronics [b-Mattioli] have financial, privacy, security, quality, physical safety, and EH risks [b-Canon]. However, we focus on the last three in this Recommendation in terms of EH implications.

Absence of testing. Through design, testing, type approval, and other market surveillance mechanisms, genuine ICT products and their parts are tested before being sold on the market to ensure that they conform to quality and safety standards. Regarding safety, genuine ICT products are tested to ensure they meet the national and international standards for, among others, exposure to emissions;

therefore, they can provide guarantees to avoid or minimize known EH risks. In contrast, counterfeit and substandard ICT products may not be subject to such comprehensive testing to minimize the cost of production, and any certification may be false.

Absence of distinction. Counterfeit products may appear in any supply chain step, even including hardware manufacturers [b-DARPA] with counterfeit integrated circuit chips. Consumers may unknowingly purchase counterfeit electronics because they may be hard to distinguish from genuine articles [b-Mattioli].

Absence of EH guarantee. Intrinsic to misrepresentation in counterfeit products is the lack of guarantee of the protection of the health of people and the natural environment in any phase of the lifecycle of ICT products. Along with the forward and reverse supply chain, the most alarming are the risks resulting from the uncontrolled nature of counterfeit products, built to deceive. Any data may misrepresent reality due to a lack of verified compliance, including misleading certification labels. As a result, they may have non-compliant components, including substances of concern and hazardous materials not expected in legitimate products, which may go undetected. Therefore, they are intrinsically dangerous, with an unbounded risk to people and the environment.

Absence of physical safety guarantee. Counterfeit products such as charging devices or cables are likely not to have undergone stringent testing and certification as genuine products do. Other ICT products may not have gone through electromagnetic compatibility (EMC) verification. Therefore, users risk exposure to unknown electromagnetic radiation levels, interference or even electrical fires [b-Mattioli].

In terms of exposure to hazardous substances, the EH effects are accumulative, and the contribution of counterfeit is unexpected and unbound by their nature. Thus, although they could have a noticeable negative environmental impact in accumulation, they cannot be easily monitored or managed. These absences result in unexpected and unbound EH risks to avoid.

6.1 The relevance of counterfeit

The spread of the problem is hard to measure, but it is not small. East African countries have separately done studies to find quantities of counterfeit phones in their countries. For example, the Communications Authority of Kenya (CA) did a study (2012) that estimated 10% of all phones on the local market were counterfeit [b-Chebusiri] [b-Wangusi]. Using the International Mobile Equipment Identity (IMEI) database and an associated blocklist, the CA later ordered Kenyan operators to switch off counterfeit phones in October 2013. In Rwanda, the Rwanda Utilities Regulatory Agency estimated that 47.5% of phones used are counterfeit [b-ITWeb], while in Tanzania, the estimate was 22% [b-Athumani]. A study by the Uganda Communications Commission (UCC) in 2013 found that 29.5% of all phones used in Uganda were counterfeit [b-Telecompaper], updated to 6 million counterfeit phones in [b-Kazibwe].

Counterfeit mobile phones are ubiquitous and found to be owned by most farmers in research in rural areas of Zambia and Kenya [b-Wyche].

[b-OECD], on the trade in counterfeit ICT products, found that nearly one in five mobile phones and one in four video game consoles shipped internationally are fake. [b-OECD] further indicates that smartphone batteries, chargers, memory cards, magnetic stripe cards, solid-state drives and music players are also increasingly falling prey to counterfeiters. On average, 6.5% of global trade in ICT goods is in counterfeit products, according to the analysis of 2013 customs data. This is well above the 2.5% of overall traded goods found to be fake [b-OECD].

7 Environmental and health impact of counterfeit ICT products, separate parts and assembled components

Very little research has been conducted on the EH impacts of counterfeit ICT. While these studies are lacking, research on the EH impacts of WEEE (e-waste) recycling has grown over the past

10 years. ICT and its components and parts are included within e-waste streams when they reach end of life.

Counterfeit ICT may have additional EH risks as items may:

- use unknown components, including chemicals and materials;
- contain poor quality or degraded chemicals or materials;
- contain materials that have been banned for use in ICT;
- LCA information cannot be applied or conducted, meaning unknown environmental impact;
- e-waste and industrial scrap may be a source of parts and materials for the production of counterfeit.

Given the EH risks, the discouragement and prevention are recommended of workers in the informal economy from manipulation e-waste more thoroughly, in greater detail, with inadequate protection, with the aim of extracting demanded elements for producing counterfeit devices, as that increases exposure and the harmful effects, described below, on the vulnerable population affected.

In summary, and among other impacts, counterfeit ICT represent a clear risk to public health [b-ITU-T QTR-CICT].

7.1 Specific risks to people and the environment

The risks across the lifespan of ICT devices result from the lack of safety guarantees provided by non-counterfeit products. These risks, grouped by elements and lifecycle phases, are described as follows.

Materials

The establishment of take-back and recycling systems for electronics, as well as controls on the use of materials in genuine products, is lacking for counterfeit goods. The European Restriction of Hazardous Substances Directive is the most well-known piece of materials legislation, restricting the use of six substances in many electronics applications: lead; mercury; cadmium; hexavalent chromium; polybrominated biphenyls (PBBs); and polybrominated diphenyl ether (PBDE) [b-Williams]. In contrast, it has also been observed that counterfeit equipment may contain dangerous elements such as lead and cadmium.

Compared to genuine products, counterfeit products that are not subject to comprehensive testing (i.e., health and safety, EMC, low voltage, type –approval) create a significant health safety risk to anyone involved and particularly consumers [b-ITU-T QTR-CICT].

Assembled components and separate parts

Consumers may even unknowingly purchase counterfeit electronics because, at a glance, they may be visually identical or similar and cheaper than their genuine counterparts. Examples are counterfeit:

- cables, with safety EH risks related to chemicals like flame retardants;
- chargers, with the risk of electric shocks for nearly all tested. [b-UL];
- phones with counterfeit batteries, with EH risks of burning, explosion, and corrosion.

Defective and substandard batteries can enter the market through either authorized manufacturers who did not conduct adequate quality checks or unauthorized retailers and suppliers who may be selling mislabelled or low-quality counterfeit batteries, in some cases including defective, substandard, degraded and damaged batteries that they purchased at low prices from other sources and then relabelled (re-wrapped) under a brand name. Counterfeit batteries are frequently made of poorer materials, have lower ratings than promised, and are of poor quality. Counterfeit lithium-ion batteries can be made through recycling, remarking, tampering and cloning, and have been found in

cell phones, computers, hoverboards and cameras. Counterfeit batteries have a more significant and unanticipated risk of battery fires and explosions than genuine lithium-ion batteries. [b-Saxena]

A thermal runaway is a condition in which the temperature of a battery rises unpredictably and quickly due to self-heating exothermic reactions and thermal degradation of battery components. Battery temperatures can reach 900°C during thermal runaway [b-Jhu], and the battery can produce flammable and poisonous gases such as CO, CO_2, CH_4, C_2H_4, C_2H_6, and H_2 [b-Golubkov].

Manufacturing

Counterfeit products and their manufacturing are rarely examined or approved by applicable regulatory criteria [b-ITU-T QTR-CICT]. Exposure to auxiliary chemicals used in high-tech processing is a critical risk for manufacturing [b-Williams]. Counterfeit ICT goods are not subject to control or limits on manufacturing.

In less formal or controlled environments related to counterfeit ICT, occupational poisoning in ICT manufacturing becomes more acute. At all levels of the supply chain, many of these operatives work with dangerous chemicals, including solvents, adhesives, resins and etchants that can cause disease and even death if not appropriately handled [b-EW]. There have been reports of ICT women employees being exposed to dangerous chemicals in poorly ventilated rooms without sufficient equipment or training, resulting in serious health problems like cancer and miscarriage [b-Björnsson].

Women and children comprise a large portion of the informal economy's workforce; some work in micro and small businesses, while others work independently. Their working conditions are frequently unregulated. Organizing and monitoring proper workplace safety and health procedures for informal businesses is still difficult [b-ILO 2019].

Use phase

The leading ICT counterfeit products that have hit the market include mobile phones and smart devices, cameras, monitors, drives, batteries, cables and networking equipment like structure cables and medical devices. These devices contain cheap substandard materials. Counterfeit mobile phones are widespread and found in a study [b-Wyche] to be owned by most farmers researched in Zambia and Kenya. They may also contain dangerous levels of metals (such as lead, mercury and cadmium) much higher than those permitted by industry standards. The main issue in the operation of ICT devices is exposure to brominated flame retardants (BFRs), which are added to casings and circuit boards in electronics to improve fire safety [b-Williams].

As a result, using counterfeit goods can be extremely dangerous to users. There have been reports of deaths caused by counterfeit batteries exploding, electrocution and fires caused by chargers, and recorded cases of these products containing high quantities of toxic compounds, including lead and cadmium [b-ITU-T QTR-CICT].

The use of counterfeit batteries in ICT has been highlighted as an item of particular concern due to health and safety risks due to leaching, malfunctioning or degraded batteries [b-OECD].

Medical devices are particularly critical for health as counterfeit elements can have detrimental or safety effects on other nearby medical devices from failure or incorrect operation. Some of the risks and consequences reported in [b-Webster], directly or indirectly related to health, can:

- affect patient care pathways due to a deterioration in diagnostic or treatment performance;
- provoke issues with performance or dependability;
- cause deterioration of equipment and infrastructure;
- disrupt service;
- give rise to potentially harmful or dangerous impacts on other nearby medical devices;
- incur additional costs, due to issues such as lost service or equipment replacement due to failure;

- damage reputation;
- cause patient or user injury or death;
- result in criminal proceedings, fines or imprisonment.

Counterfeiting affects ICT product reliability and durability, as reported in Kenya [b-Wyche]. Since counterfeit devices have a shorter lifespan, they generate electronic waste, causing environmental and disposal issues for central and local governments [b-ITU-T QTR-CICT].

These issues may endanger the user of counterfeit ICT because equipment may break down, leach or release chemicals while in use. This may expose recycling workers to new or unknown chemicals and materials incompatible with designated management techniques or infrastructure. [b-Mura] [b-OECD].

Post-use

E-waste includes old, end-of-life or discarded appliances using electricity or batteries. Counterfeit ICT with shorter lifespans at lower prices can contribute to the growth of e-waste. In addition, e-waste is the fastest growing waste stream, increasing three times faster than the world's population. It is particularly problematic due to its toxicity, heterogeneity and mass [b-ILO 2018] [b-Forti].

Studies of informal e-waste have found that as many as 1 000 different toxicants may be released through unsound e-waste recycling practices [b-WHO 2021]. Many of these are known or suspected to harm human health and the environment [b-Frazzoli]. Regarding their disposal, counterfeit ICT products, like others, are composed of hazardous and non-hazardous materials. The hazardous materials in ICT products are mainly the batteries comprising lead, nickel and cadmium, and sometimes lithium and mercury. These components are also listed as human carcinogens (i.e., substances capable of causing cancer in living tissue) as they damage the lungs, liver, neurodevelopment, birth outcomes, cardiovascular system, etc. when ingested, inhaled, in contact with skin or transferred via the placenta. However, mislabelling can hide the presence of dangerous toxicants.

Unsafe recycling

Unsatisfactory practices observed at e-waste sites include manual disassembly, open burning and heating, stripping and shredding, acid baths and leaching, dumping and landfilling. These practices can contaminate the air, soil, dust, water sources and groundwater. From the environment, toxicants released through e-waste recycling activities can find their way into the human body, food crops, livestock, fish, shellfish and eggs [b-WHO 2021].

As a result, the population may be exposed to potentially hazardous substances through inappropriate and unsafe e-waste management practices. Among the results in [b-Grant], there are undesirable changes in thyroid function, cellular expression and function, neonatal outcomes, temperament and behaviour and lung function that have all been linked to e-waste exposure in studies. Most studies found an increase in spontaneous abortions, stillbirths, premature births, and lower birthweights and birth lengths associated with e-waste exposure. People who lived in e-waste recycling towns or worked in e-waste recycling had more DNA damage than those in control towns. The relationship between informal workers and children is reported in more detail in [b-Bruné Drisse] [b-WHO 2021].

A study was carried out to identify which cell phones are the worst for toxic chemicals and to pressure phone manufacturers to reduce the toxic burden of their e-waste on the environment [b-ENS]. Researchers at the non-profit Ecology Center completely disassembled 36 legitimate phones from 10 manufacturers and determined the chemical composition of all interior and exterior components using x-ray fluorescence spectrometry. By overall ranking, six of the 36 phones were of low concern, while 24 were of medium concern. The newer phones on the market had fewer toxic substances. All tested phones conformed to the specified international standards and were therefore legitimate. Counterfeit phones can be much worse as they are not tested for conformity with specified standards. When unwanted cell phones are landfilled, these chemicals leach into groundwater; when incinerated, the

toxins contaminate the air. These substances can pollute throughout a cell phone's lifecycle, starting with the extraction of the minerals used in their manufacture.

Most e-waste systems in developing countries are dominated by the informal sector, which is struggling to deal with the negative environmental impacts of informal e-waste recycling, as research shows in India [b-Awasthi] or Ghana [b-Ackah]. Prolonged informal recycling of e-waste may cause high concentrations of heavy metals to accumulate in surface soils, plants and groundwater, a matter of concern for both environmental and occupational hazards [b-Pradhan].

Informal e-waste recycling is associated with severe EH impacts, the supply deficiency of formal recyclers, and the safety problems of remanufactured electronic products. Additionally, informal e-waste sites worldwide are considered major suppliers of essential parts, resources and materials to counterfeit ICT manufacturers [b-Zhou]. The development and effective implementation of e-waste import and export regulations at national, regional and international levels can help reduce the flow of materials, making counterfeit ICT possible. In addition, counterfeit ICT products end up as e-waste, and the unknown inclusion of more polluting materials increases the risk of EH effects such as unexpected poisoning and pollution. It can also deceive manufacturers and recyclers in extended producer responsibility (EPR) schemes and damage recycling and recovery processes. The effects may be more acute in informal recycling due to a lack of proper procedures and protection. Informal recycling practices are the most hazardous activities as they can indiscriminately release toxic chemicals, and create new ones that pollute the environment and are a health risk. Also, plastic shredding and pellets can pollute the environment. Probably the most dangerous element of counterfeit ICT is that its contents may be unknown and potentially hazardous. It is the recycling activity that is likely to release the hazardous material and cause harm to health and the environment.

Because counterfeit products have unknown components, they cannot be subject to standards for recycling. This situation may create a stream of inadequately treated recyclates, to which standard procedures cannot be applied due to lack of valid information. In addition, there is no accountability, without any cost contribution or cooperation by the producer of genuine products (EPR schemes), with EH impacts that are unknown or at least from products built from parts and products informally recovered from e-waste and industrial scrap.

Table 1 reports a summary of major EH risk.

Table 1 – Major environmental and health risks in different phases of the product lifecycle

Phase	Aspect	Genuine (controlled)	Counterfeit (EH risk)
Pre-use	Materials Components Manufacturing	Absence hazardous substances Minimized risks Workplace safety and health procedures	No verification Chemical exposure, electric shocks, burning, explosion Uncontrolled exposure, hard to monitor informal workers
Use	Safety Quality, reliability Durability	Controlled Predictable Predictable, product warranty, maintenance and repair	Uncontrolled exposure to unknown chemicals, electric shocks, burning, explosion Unreliable, deterioration Uncontrolled, much shorter, less predictable
Post-use	E-waste	Controllable, sustainability: EPR	Uncontrolled Source of counterfeit elements, higher e-waste exposure of informal workers

8 Recommendation

Combating the EH risks of counterfeit products requires mitigation of the problems leading to their existence. It can be achieved by enforcing the solutions proposed in [ITU-T Q.5050], discouraging the supply of and demand for counterfeit products that pose these risks.

[ITU-T Q.5050] has considerations when deploying solutions for combating counterfeit ICT devices that are beneficial to limiting EH risks:

- detection and identification of counterfeit ICT devices;
- tracking of counterfeit ICT device producers and traffickers;
- removal of counterfeit ICT devices already in use in the market;
- limitation of the import, circulation, and sale of new counterfeit ICT devices on the market;
- differentiation between genuine and counterfeit ICT devices;
- limitation of the impact on the authentic ICT device manufacturer;
- reduction of end-user impact when considering removing counterfeit ICT devices;
- consumer education;
- avoidance of technical barriers to trade.

[ITU-T Q.5050] establishes a set of requirements:

- identification and enforcement actions against producers and traffickers of counterfeit devices;
- consultation with industry and consumer groups;
- adoption of a reliable unique identifier;
- compilation of a centralized reference database;
- deployment of a conformity assessment regime;
- close collaboration with customs authorities and appropriate domestic agencies;
- sharing information with the end-user before any remedial action;
- support for applicable national and regional legal and regulatory frameworks;
- consideration for products already in use in the market.

[ITU-T Q.5050] describes counterfeit ICT solution approaches:

- prohibition of the use of invalid and non-genuine device identifiers;
- certification of ICT devices and market surveillance;
- device lifecycle management,

However, all solutions require action to implement additional formal control mechanisms to detect and prevent damage and offer alternatives and complements. The EH challenges should go together with actions to address them. Recommended action areas in the EH dimensions are outlined in Table 2.

Table 2 – Recommended action areas

Challenges	Recommended actions
Affordability	Promote the development and certification of lower-cost open hardware products with minimum features (but no major risks) developed and produced by and for emerging markets
Informal workers	Incentives for formalization, incentives to access legitimate market and the formal economy, support for the introduction of local circular business models for legitimate products
Reduction of counterfeit ICT	Incentives to remove counterfeit devices from the market: controls; incentives; voluntary take-back schemes
Verifiability, testing	Conformance and interoperability assistance to developing countries [b-ITU-D 2021] Introduction of digital product passports with self-verification software tools Voluntary ICT product certification schemes
Public awareness about risks	Training and public awareness campaigns about EH risks and protective measures: global; regional; local
Socio-economic development	Enabling consumers to access the legitimate market with economic incentives and protective measures to prevent risks, and bridge the digital divide
Control, public involvement	Involvement of public authorities, governments responsible for health and environmental topics

Counterfeit ICT products and parts, due to their intrinsic lack of control over the composition and operation, are dangerous products and have to be treated as such, under the principle of precaution, considering them dangerous for the health of people and the environment. Therefore, counterfeit ICT must be treated not like the products they represent, but as hazardous substances, parts and products, with risks for adverse effects on people and the planet.

Appendix I

Best practice

(This appendix does not form an integral part of this Recommendation.)

Uganda (2019) and Tanzania (2016) embarked on projects to eliminate the use and sale of counterfeit/fake/illegitimate mobile devices (phones) through the installation of the Central Equipment Identifier Register (CEIR). Counterfeit mobile devices are prominent in developing countries and are mainly attributed to low pricing, porous borders, insufficient regulatory surveillance (type approval/acceptance) and uncontrolled export-import business. Counterfeit products have an extremely short lifespan and easily reach the end of their useful life and are discarded as e-waste. The accumulation rate is too high, leading to volumes in designated and undesignated places.

In Uganda, the estimated number of counterfeit mobile devices is slightly more than 2 million, while in Tanzania, the estimate was around 2.2 million. Deregistering counterfeit mobile devices of the various networks renders them non-functional and therefore has a considerable impact implication on disposal. Uganda will gradually switch off counterfeit phones taking into account the social and awareness aspects.

See Table I.1.

Table I.1 – Activity on counterfeit devices in Tanzania and Uganda

	Activity	Tanzania	Uganda
1	Develop an awareness campaign for collection of the counterfeit phones	The media (online and printed) is currently being used, which is crucial with respect to advocacy of the dangers of using counterfeit phones and creating awareness to the public on what needs to be done by the general public as well as key stakeholders in alleviating the situation. The Tanzania Communications Regulatory Authority (TCRA) coordinated with mobile network operators (MNOs) to remove counterfeit phones with fake IMEIs from operation. This was done under the CEIR project	Internal communications with the UCC CEIR project External – Awareness strategy under national initiatives (National Steering Committee on E-waste Management) UCC to coordinate the awareness campaign with key stakeholders
2	Establishment of collection points	TCRA coordinated with service providers to set up collection points. MNOs were encouraged to set up collection points at their shops. The collection of these were taken to zonal offices for collection by the licensed e-waste collector. The replacement of phones was left to the service providers so as to keep their customers	UCC to encourage service providers to set up collection points at their sale outlets or shops across the country in due cognizance of proximity, accessibility and intent of phone replacement. UCC to encourage service providers to set up collection points at their sale outlets or shops across the country in due cognizance of proximity, accessibility and intent of phone replacement

Table I.1 – Activity on counterfeit devices in Tanzania and Uganda

	Activity	Tanzania	Uganda
3	Disposal	TCRA coordinated the process by bringing together MNOs and the environment agency to manage disposal. Few collection points are available in the country, which makes collection of reasonable amounts of waste a challenging but doable task. Hence e-waste disposal was not 100%. Some companies have plans in place to set up phones manufacturing factory in the country, which in turn will result in having cheap/affordable genuine mobile Phones	Proposal to collect phones from the various collection points from the regions can then be collected at UCC regional offices for collection by the designated collector. UCC to coordinate and bring together the service providers, National Environment Management Authority (NEMA) and the designated e-waste collector. Further plans to leverage on the new phone manufacturing company in Uganda, and the consideration to facilitate or initiate collaboration or partnership with operators, so that these phones are at the sale points. Technical specification of collection point, to be determined by the designated e-waste collector and NEMA. UCC shall consider a collaborative approach to the disposal management of counterfeit ICT devices including: awareness, stakeholder engagement, compensation and redress, collection and disposal

Appendix II

Documents to assist in combating counterfeit and stolen ICT

(This appendix does not form an integral part of this Recommendation.)

During the 2017-2021 study period, ITU-T Study Group 11 (SG11), in accordance with World Telecommunication Standardization Assembly (WTSA) [b-WTSA Res. 96] [b-WTSA Res. 97], led activities on combating counterfeit telecommunication/ICT and mobile device theft.

Based on [b-WTSA Res. 96][b-WTSA Res. 97], Q15/11, *Combating counterfeit and stolen telecommunication/ICT devices*, experts managed to deliver various documents to assist ITU members to address this important problem, as listed in Table II.1.

Table II.1 – ITU-T documents aimed at combating counterfeit and stolen telecommunication/ICT devices

Topic	Reference
Use cases on the combat of counterfeit ICT and stolen mobile devices	[b-ITU-T Q-Suppl.75]
Guidelines for permissive versus restrictive system implementations to address counterfeit, stolen and illegal mobile devices	[b-ITU-T Q-Suppl.73]
Roadmap for the ITU-T Q.505x-series	[b-ITU-T Q-Suppl.74]
Mobile device access list audit interface	[b-ITU-T Q.5053]
Addressing mobile devices with duplicate unique identifier	[b-ITU-T Q.5052]
Combating the use of stolen mobile ICT device framework	[b-ITU-T Q.5051]
Solution framework to combat counterfeit ICT devices	[ITU-T Q.5050]
Reliability of International Mobile station Equipment Identity	[b-ITU-T QTR-RLB-IMEI]
Counterfeit ICT Devices in Africa	[b-ITU-T QTR-CICT]

The outcomes of related workshops and detailed information on combating counterfeiting and stolen telecommunication or ICT equipment and software can be found in [b-ITU-T SG11]

Bibliography

[b-ITU-T L.1031] Recommendation ITU-T L.1031 (2020), *Guideline for achieving the e-waste targets of the Connect 2030 Agenda*.

[b-ITU-T Q.5051] Recommendation ITU-T Q.5051 (2020), *Framework for combating the use of stolen mobile devices.*

[b-ITU-T Q.5052] Recommendation ITU-T Q.5052 (2020), *Addressing mobile devices with a duplicate unique identifier.*

[b-ITU-T Q.5053] Recommendation ITU-T Q.5053 (2021), *Mobile device access list audit interface.*

[b-ITU-T Q-Suppl.73] ITU-T Q-series Recommendations – Supplement 73 (2021), *Guidelines for permissive versus restrictive system implementations to address counterfeit, stolen and illegal mobile devices.*

[b-ITU-T Q-Suppl.74] ITU-T Q-series Recommendations – Supplement 74 (2021), *Roadmap for the ITU-T Q.5050-series - Combat of counterfeit ICT and stolen mobile devices.*

[b-ITU-T Q-Suppl.75] ITU-T Q-series Recommendations – Supplement 75 (2021), *Use cases on the combat of counterfeit ICT and stolen mobile devices.*

[b-ITU-T QTR-CICT] ITU-T Technical Report (2017), *QTR-CICT – Survey report on counterfeit ICT devices in Africa region.*

[b-ITU-T QTR-RLB-IMEI] ITU-T Technical Report (2020), *QTR-RLB-IMEI – Reliability of International Mobile station Equipment Identity (IMEI).*

[b-ITU-T SG11] ITU-T SG11 (2022). *Combating counterfeit and stolen telecommunication/ICT devices, software.* Geneva: International Telecommunication Union. Available [viewed 2022-09-12] at: https://www.itu.int/en/ITU-T/studygroups/com11/counterfeit/Pages/default.aspx

[b-WTSA Res. 96] WTSA Resolution 96 (Rev. Hammamet, 2016), *ITU Telecommunication Standardization Sector studies for combating counterfeit telecommunication/information and communication technology devices.*

[b-WTSA Res. 97] WTSA Resolution 97 (Rev. Hammamet, 2016), *Combating mobile telecommunication device theft.*

[b-ITU-D 2021] International Telecommunication Union Development Sector (2021), *Study Group 2 Question 4 – Assistance to developing countries for implementing conformance and interoperability programmes and combating counterfeit ICT equipment and theft of mobile devices – Study period 2018–2021*, Output Report on ITU-D Question 4/2. Geneva: International Telecommunication Union. 65 pp. Available [viewed 2022-09-10] from: https://www.itu.int/hub/publication/D-STG-SG02.04.2-2021/

[b-ILO 2018] ILO (2018), *The future of work in a changing natural environment: climate change, degradation and sustainability, ILO Future of Work Research Paper Series*, No.4. Geneva: International Labour Organization. 48 pp. Available [viewed 2022-09-11] at: https://www.ilo.org/wcmsp5/groups/public/---dgreports/---cabinet/documents/publication/wcms_644145.pdf

[b-ILO 2019] ILO (2019), *Safety and health at the heart of the future of work: Building on 100 years of experience*. Geneva: International Labour Organization. 82 pp. Available [viewed 2022-09-11] at: https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/documents/publication/wcms_686645.pdf

[b-ISO/IEC Guide 51] ISO/IEC Guide 51:2014, *Safety aspects – Guidelines for their inclusion in standards*.

[b-OECD] OECD (2017). *Trade in counterfeit ICT goods*. Paris: Organisation for Economic Cooperation and Development Publishing. 92 pp. Available [viewed 2022-09-10] from: https://www.oecd-ilibrary.org/governance/trade-in-counterfeit-ict-goods_9789264270848-en

[b-WHO] WHO (2021), *Children and digital dumpsites: E-waste exposure and child health.* Geneva: World Health Organization. 86 pp. Available [viewed 2022] at: Available [viewed 2022-09-10] from: https://apps.who.int/iris/handle/10665/341718

[b-WTO ACTA] WTO (2011). *Anti-counterfeiting trade agreement*. Geneva: World Trade Organization. 25 pp. Available [viewed 2022-09-11] at: https://www.mofa.go.jp/policy/economy/i_property/pdfs/acta1105_en.pdf

[b-WTO glossary] WTO (Internet). *Glossary*. Geneva: World Trade Organization. Available [viewed 2022-09-12] at: https://www.wto.org/english/thewto_e/glossary_e/glossary_e.htm

[b-Ackah] Ackah, M. (2017). Informal e-waste recycling in developing countries: Review of metal(loid)s pollution, environmental impacts and transport pathways. *Environ. Sci. Pollut. Res. Int.* **24**, 24092–24101. doi:10.1007/s11356-017-0273-y

[b-Athumani] Athumani, R. (2016). *Tanzania: Government blocks two million fake phones from market*. Cape Town: AllAfrica. Available [viewed 2022-10-13] at: https://allafrica.com/stories/201607270361.html

[b-Awasthi] Awasthi, A.K., Zeng, X., Li, J. (2016). Relationship between e-waste recycling and human health risk in India: A critical review. *Environ. Sci. Pollut. Res. Int.* **23,** 11509–11532. doi org/10.1007/s11356-016-6085-7

[b-Björnsson] Björnsson, O. (2021). *Hazardous chemicals in ICT manufacturing and the impacts on female workers in the Philippines*, Briefing. Stockholm: Swedwatch. 22 pp. Available [viewed 2022-09-11] at: https://swedwatch.org/wp-content/uploads/2021/03/mictfbriefing210120-fin.pdf

[b-Bruné Drisse] Bruné Drisse, M.-N. (2018), *Health effects of E-waste exposure on children*. Geneva: World Health Organization. 26 slides. Available [viewed 2022-09-10] at: https://www.itu.int/dms_pub/itu-d/oth/07/15/D07150000030001PDFE.pdf

[b-Canon] Canon (2022). *Counterfeit*. Tokyo: Canon. Available [viewed 2022-09-11] at: https://www.canon-europe.com/about_us/anti-counterfeit-awareness/

[b-Chebusiri] Chebusiri, W. wa (2012). *Kenya's battle to switch off fake phones.* London: British Broadcasting Corporation. Available [viewed 2022-10-13] at: https://www.bbc.com/news/world-africa-19819965?piano-modal

[b-DARPA] Leef, S. (2015). *Supply chain hardware integrity for electronics defense (shield)* [archived]. Arlington, VA: Defense Advanced Research Projects Agency. Available [viewed 2022-09-11] at: https://www.darpa.mil/program/supply-chain-hardware-integrity-for-electronics-defense

[b-ENS] ENS (2012). *Cell phones all contain toxics: Older ones the most.* Eugene, OR: Environment News Service. Available [viewed 2022-09-11] at: https://ens-newswire.com/cell-phones-all-contain-toxics-older-ones-the-most/

[b-EW] EW (2020). *How to protect workers from chemical hazards in electronics supply chains – Guidance for public buyers V.1.0*. Amsterdam: Electronics Watch. 37 pp. Available [viewed 2022-09-11] at: https://electronicswatch.org/how-to-protect-workers-from-chemical-hazards-in-electronics-supply-chains-guidance-for-public-buyers-v-1-0-november-2020_2582525.pdf

[b-Forti] Forti, V, Baldé, C.P., Kuehr, R., Bel, G. (2020). *The global e-waste monitor 2020: Quantities, flows, and the circular economy potential*. Bonn, Geneva, Rotterdam: United Nations University (UNU)/United Nations Institute for Training and Research (UNITAR) – co-hosted SCYCLE Programme, International Telecommunication Union (ITU) and International Solid Waste Association (ISWA). 120 pp. Available [viewed 2022-09-11] at: https://www.itu.int/en/ITU-D/Environment/Documents/Toolbox/GEM_2020_def.pdf

[b-Frazzoli] Frazzoli, C., Orisakwe, O.E., Dragone, R., Mantovani, A. (2010), Diagnostic health risk assessment of electronic waste on the general population in developing countries' scenarios. *Environ. Impact Assess. Rev*. **30**(1):388-99. doi: 10.1016/j.eiar.2009.12.004

[b-Gartner] Gartner (2022). *Gartner glossary*. Stamford, CT: Gartner. Available [viewed 2022-09-11] from: https://www.gartner.com/en/information-technology/glossary/gray-market

[b-Golubkov] Golubkov, A.W. Fuchs, D., Wagner, J., Wiltsche, H., Stangl, C., Fauler, G., Voitic, G., Thalera, A., Hacker, V. (2014). Thermal-runaway experiments on consumer Li-ion batteries with metal-oxide and olivin-type cathodes. *RSC Adv.*, **4**(7), pp. 3633–3642.Available [viewed 2022-09-11] from: https://pubs.rsc.org/en/content/articlelanding/2014/ra/c3ra45748f

[b-Grant] Grant. K., Goldizen, F.C., Sly, P.D., Bruné M.-N., Neira, M., van den Berg, M., Norman, R.E. (2013), Health consequences of exposure to e-waste: A systematic review. *Lancet Global Health*. **1**(6):350–61. Available [viewed 2022-09-11] from: https://www.thelancet.com/journals/langlo/article/PIIS2214-109X(13)70101-3/fulltext

[b-ITWeb] ITWeb (2012). *Rwanda plans fake phone switch off*. Johannesburg: ITWeb. Available [viewed 2022-09-11] at: https://itweb.africa/content/GxwQDM1ALWWMlPVo

[b-Jhu] Jhu, C.-Y., Wang, Y.-W., Shu, C.-M., Chang, J.-C. Wu, H.-C. (2011). Thermal explosion hazards on 18650 lithium-ion batteries with a VSP2 adiabatic calorimeter. *J. Hazard. Mater.* **192**(1), pp. 99-107.doi.org/10.1016/j.jhazmat.2011.04.097

[b-Kazibwe] Kazibwe, K. (2022). *Uganda: UCC to switch off six million fake phones in rejuvenated campaign*. Cape Town: AllAfrica. Available [viewed 2022-10-13] at: https://allafrica.com/stories/202208020402.html

[b-Mattioli] Mattioli, M. (2021). Consumer exposure to counterfeit hardware. *IEEE Consumer Electron. Mag.* **10**(5), pp. 29-32. doi: 10.1109/MCE.2020.3023873.

[b-Mura] Mura G, Murru R, Martine G. (2020). Analysis of counterfeit electronics. *Microelectron. Reliab.* **114**, pp. 1-7. doi: 10.1016/j.microrel.2020.113793

[b-Pradhan] Pradhan, J.K., Kumar, S. (2014), Informal e-waste recycling: Environmental risk assessment of heavy metal contamination in Mandoli industrial area, Delhi, India. *Environ. Sci. Pollut. Res.* **21**, pp. 7913–7928. doi.org/10.1007/s11356-014-2713-2

[b-Saxena] Saxena, S., Kong, L., Pecht M. G. (2018). Exploding e-cigarettes: A battery safety issue. *IEEE Access*, **6**, pp. 21442-21466. doi: 10.1109/ACCESS.2018.2821142.

[b-Telecompaper] Telecompaper (2012). *Study finds 30% of Ugandans have fake mobile handsets*. Houten: Telecompaper. Available [viewed 2022-10-13] at: https://www.telecompaper.com/news/study-finds-30-of-ugandans-have-fake-mobile-handsets--900588

[b-UL] Underwriters Laboratories (Internet). *Counterfeit iphone adapters: A UL technical investigation shows a 99 percent failure rate*.11 pp. Available [viewed 2022-09-10] at: https://code-authorities.ul.com/wp-content/uploads/sites/40/2016/09/10314-CounterfeitiPhone-WP-HighRes_FINAL.pdf

[b-Wangusi] Wangusi, F.W. (2012). *Press statement by Mr. Francis W. Wangusi, Director General, Communications Authority of Kenya (CA), on misleading media reports regarding the regulatory tool for curbing counterfeit devices on mobile networks.* Nairobi: Communications Authority of Kenya. Available [viewed 2022-10-13] at: https://www.ca.go.ke/wp-content/uploads/2018/01/Press-Statement-By-Mr.-Francis-W.-WangusiMBS-Director-General-CAK-On-Misleading-Media-Reports-on-The-Regulatory-Tool-for-Curbing-Counterfeit-Devices-on-Mobile-Networks-.pdf

[b-Webster] Webster, S. (2020), *Tackling the challenge of counterfeit medical devices across global healthcare settings*. NS Medical Devices. Available [viewed 2022-09-10] at: https://www.nsmedicaldevices.com/analysis/tackling-counterfeit-medical-devices/

[b-Williams] Williams, E. (2011). Environmental effects of information and communications technologies. *Nature* **479**, 354–358. doi.org/10.1038/nature10682

[b-Wyche] Wyche, S.P., Densmore, M., Geyer. B.S. (2015). Real mobiles: Kenyan and Zambian smallholder farmers' current attitudes towards mobile phones. In: *Proceedings of the Seventh International Conference on Information and Communication Technologies and Development* (ICTD '15), Article 9, 1–10. New York, NY: Association for Computing Machinery. doi.org/10.1145/2737856.2738013

[b-Zhou] Zhou Y. (2014). Electronic waste export regulations: How the responsible electronics recycling act can protect the defense supply chain from counterfeit electronic parts. *Publ. Contract Law J.* **43**(3), pp. 527-546.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	**Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant**
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2022