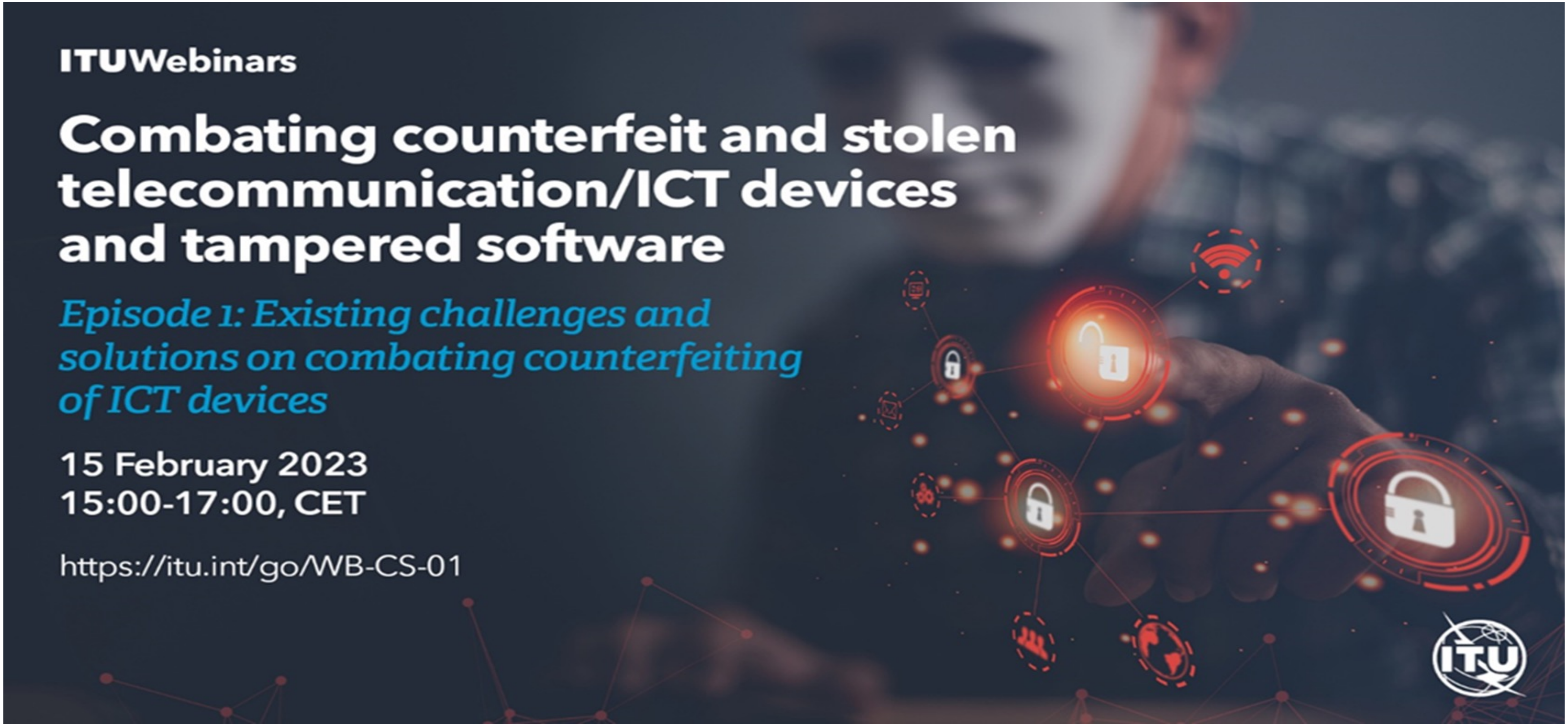
Overview of best practices/use cases and different measures on combating counterfeiting deployed in different countries.

Presented by: Engr. Olorundare, James Kunle, SMIEEE
Principal Manager, Nigerian Communications Commission, Abuja, Nigeria
Email: olorundarek@ncc.gov.ng



ITUWebinars

Combating counterfeit and stolen telecommunication/ICT devices and tampered software

Episode 1: Existing challenges and solutions on combating counterfeiting of ICT devices

15 February 2023
15:00-17:00, CET

https://itu.int/go/WB-CS-01

Synopsis

The presentation presents the overview of the activities of ITU-T Study Group 11 work on how to combat counterfeiting as presented in the approved Work Item current ITU-T Q Suppl.75 (12/2021) "Use cases on the combat of counterfeit ICT and stolen mobile devices".

It also speaks to best practices that can be used depending on the situation being face by a particular country.

a. Africa

i. Congo

To combat counterfeit ICT products, the Ministry of post, ttelecommunications and new information and communication technologies of the Democratic Republic of the Congo issued a ministerial order for the establishment of a CEIR system in 2020.

This system aims to limit the market for counterfeit mobile devices. Its introduction was accompanied by the creation of a central database of IMEI numbers.

By blocking counterfeit mobile devices, network operators make it difficult for consumers to recognize counterfeit devices. This procedure also does more harm than good as it leads to a greater number of legal complaints.

In that regard, Congo has chosen to have mobile network operators send a message or notification to consumers to inform them of the status of their device as part of the efforts to combat counterfeiting.

ii Republic of Botswana

The Communications Regulatory Authority Act of 2012, (CRA Act of 2012) is an act that provides all licensees manufacturers, distributors and suppliers shall type approve all their electronic communicating devices connecting to the public network. There is no testing lab for conformity. BOCRA has procured QoS/QoE emulation Monitoring system.

iii. Chad

ARCEP does not have control over importation. There is no test laboratory and type approval is based on documentation. The challenge of counterfeit is enormous.

Chad still does not have a testing laboratory and is similar to Botswana, the regulator relies on the documentation provided by the manufacturers and distributors/suppliers.

. Republic of Ghana

The NCA of Ghana is mandated by law to certify and test of communications equipment. To this end NCA has established the device type approval testing laboratories (RF and signalling for performance and protocol testing) and SAR (for safety) and aims at checking conformance and combating ICT device counterfeiting. Port inspection and market survey (for already type approved) are carried out. The labelling project is in top gear and Ghana is working on access to GSMA IMEI data base.

v. Guinea

The Ministry of posts, telecommunications and the digital economy, acting through the Direction Nationale des Télécommunications, initiated a study/survey to gather information on the difficulties encountered, different utilizations and the efforts that are in place for remedying the problem of counterfeit ICT devices.

indicates that the counterfeit products sold most on Guinean markets are the mobile phones (66.70 per cent according to those surveyed), chargers (67.36 per cent according to those surveyed) and earphone devices (66.91 per cent according to those surveyed). With the low incomes earned by Guineans – around USD 2 per inhabitant – most of the population prefer these counterfeit products as they can afford them.

Lastly, the report indicates that virtually all these counterfeit products flooding the Guinean markets come from Asia (92.76 per cent according to those surveyed).

vi. Republic of Kenya

Stolen Mobile Devices and then later counterfeiting came in. To solve this problem, CA developed, in 2005, together with the other regulators within east Africa, initiated a project to install equipment identification registers (EIR) through the

The aim was to ensure that no stolen device would have access to mobile services within east Africa. The challenge of this initiative, which still exists today, is that the authority cannot enforce denial of services outside its jurisdiction.

vii. Republic of Madagascar

Madagascar has taken a step in this direction with the publication of its ministerial decree 890/2018 of 17 January 2018, defining the restrictive measures relating to mobile phones that are counterfeit, stolen or non-compliant with international norms.

In the long term, this measure aims to ban the import and use of terminals with invalid IMEI numbers in Madagascar. The deadline set by the decree was 30 June 2019.

b. South America

viii. Federative Republic of Brazil

The SIGA solution, implemented since 2014, works in a way to complement CEMI's achieved goals, so that it can be possible to block tampered and uncertified devices. Unlike CEMI, SIGA's blockage is not done by request. The blockage occurs automatically after the user is informed about the irregularity several days before.

ix. Republic of Colombia

Since 2011, Colombia has been implementing a mechanism to combat counterfeit and stolen mobile devices, it is the result of the interaction and intervention between private agents (operators, the database administrators, manufacturers, sellers), public agents (MinTIC, CRC, police authorities) and the users; every one of them playing an active role in the reached results recently published; nevertheless, there are still some situations that are not entirely covered by the mentioned mechanism like the IMEI reprogramming and parts market, among others.

c. Asia

x. Federal Democratic Republic of Nepal

Type approval and the international mobile equipment identity (IMEI) registration mechanisms are the regulatory solutions to combat counterfeit and substandard mobile devices in the country. Nepal telecommunications authority (NTA) has been doing type approval of radio telecommunication customer premises equipment (CPEs) including mobile devices prior to importing and selling in Nepal since 2008

xi. Islamic Republic of Pakistan

The Pakistan telecommunication authority has launched, in collaboration with Qualcomm, an open-source technology platform called the device identification, registration and blocking system (DIRBS) (see Figure I.13) to ensure that only approved, legal devices can operate on mobile networks in the country.13 DIRBS allows the identification of all devices; captures an installed base of devices; monitors all new device activations; addresses illegal and counterfeit devices, including mobile thefts; and allows for exceptions/amnesties.

d. Europe

xii. Republic of Turkey

For the stolen and lost devices and for the devices that have been taken without the consent of the user; the legal user can notify ICTA via e-government portal or by calling the short number of ICTA's consumer communication centre in order to prevent the device to receive services from the electronic communication network.

MCKS is a multi-interface system in which close online/offline interactions with various ministries/public authorities take place. These parties include but are not limited to the Ministry of Trade, Ministry of Justice, Ministry of Interior, Ministry of Treasury and Finance (Revenue administration) and mobile operators in Turkey. Operators feed the system with up-to-date usage information of the devices from their own network separately and these separate pieces of information flows to MCKS. This information is used for detecting clone devices as well as unregistered devices. For devices brought from abroad, a cross-check is fulfilled by the Ministry of Interior's law enforcement agency units if the passport meets the criteria, and by the revenue administration, if the fee is paid.

xiii. Ukraine

The current procedure for importing from abroad and the sale of electronic means and radiating devices in Ukraine stipulates that importers including citizens, have the right to apply to the UCRF with a corresponding application (notification) for registration of international terminals of IMEI after completion of customs procedures, which are imported into Ukraine as per the requirements of the customs code. Currently, data entry is carried out on a voluntary (optional) basis, which leads to a lack of relevant and complete information in the database. The existing system needs to be replaced or significantly modernized due to changes in the legal, technological, and technical requirements.

Private sector and NGO initiatives

xiv. The GSM association

The GSM association (GSMA) manages the international mobile equipment identity database, a global central database containing basic information on the serial number (IMEI) ranges of millions of mobile devices.17

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

GSMA seeks to connect as many mobile network operators as possible to the IMEI database.

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

Best practices, measures and standardization activities on combating counterfeiting

RECOMMENDATIONS

There are several best practices and measures that countries have deployed to combat counterfeiting, including:

- Legal frameworks: From Supplementary 75, many countries have enacted laws and regulations to criminalize counterfeiting and provide legal remedies for intellectual property rights holders. This can include laws that criminalize the production, distribution, and sale of counterfeit goods, as well as laws that provide for civil remedies such as injunctions and damages. ITU-T can also work on a more robust recommendations in that regard.

- Border measures: From some use cases discussed, customs and other border control agencies have been given powers to seize and detain counterfeit goods, and to provide information to rights holders about suspected counterfeit goods. This measure can be advanced to include measures such as the establishment of special IP rights-related enforcement teams, and the use of electronic databases and other tools to identify and track suspected counterfeit goods. Standardised recommendations can be proposed in that regard at the level of the ITU-T.

- Collaboration with industry and civil society: Many countries have established partnerships between government agencies and industry groups, as well as civil society organizations, to combat counterfeiting. This can include the sharing of information and resources, as well as joint enforcement efforts.

- Public awareness campaigns: Many countries have launched public awareness campaigns to educate consumers about the dangers of counterfeiting, and to encourage them to purchase only genuine goods. These campaigns can include print and television advertisements, as well as educational materials distributed in schools and other community settings under consumer education scheme. ITU-T can work on Standardised recommendation on Consumer education scheme for the sole aim of counterfeiting.

- Internet enforcement: A lot of the counterfeiting activities are done online, it is important to create online marketplaces, and e-commerce platforms to identify and remove counterfeit products. Digital tools and software can be used to detect and track counterfeit products online. Such recommendations can we worked on.

International cooperation: it is also important to bring international organizations, such as the World Intellectual Property Organization (WIPO) and the World Trade Organization (WTO) on board, to combat counterfeiting on a global scale. This can include participating in international agreements and conventions, as well as collaborating with other countries on law enforcement and other anti-counterfeiting efforts. Regional and global strategic solutions should be encouraged.

These are some of the main practices and measures that can be deployed deployed to combat counterfeiting, but it's important to note that the specific measures used will vary depending on the country and the specific challenges it faces.

Bibliography

INTERNATIONAL TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

SERIES Q: SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

Supplement 75 (12/202, Unique ID: 11.1002/1000/14885), Use cases on the combat of counterfeit ICT and stolen mobile devices

Published by ITU-T (approved on 10-12-2021) Edition 1 [Source: Online, Available at: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14885

About the Presenter

My Google Scholar Link: https://scholar.google.com/citations?user=T_MCVeAAAAJ&hl=en

My Linkedin Page:
https://www.linkedin.com/in/james-kunle-olorundare-smieee-coren-regd-engr-2b223666/?originalSubdomain=ng