ITU Workshop on "Combating Counterfeit Using Conformance and Interoperability Solutions"
Geneva, Switzerland
28 June 2016

Overview of national initiatives and solutions to combat counterfeit mobile devices

Dmytro Protsenko

Deputy Director of Radio Service Directorate, Ukrainian State Centre of Radio Frequencies (UCRF)

protsenko@ucrf.gov.ua

Content

- Counterfeiting problem continues to grow

- Special concerns over mobile phones

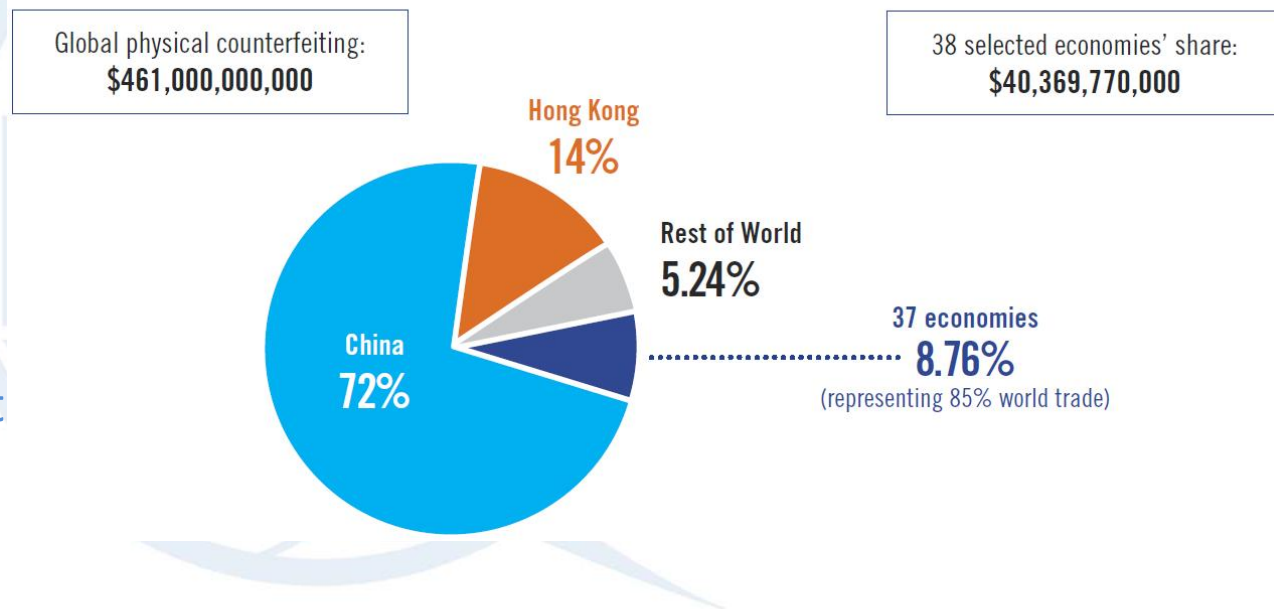- Measures of individual administrations and regulators

- Conclusions

Counterfeiting problem continues to grow

- The level of awareness and concern about counterfeiting among rights holders, trade organizations and government officials has risen, yet the problem continues to grow

- **OECD:** The share of counterfeit and pirated goods in world trade is estimated to have increased from 1.85% in 2000 (over USD 100 billion) to 1.95% in 2007 (USD 250 billion) and up to 2.5% in 2013 (USD 461 billion)

- In 2013, this was even higher in the EU context where counterfeit and pirated goods amounted to up to 5 % of imports (EUR 85 billion or USD 116 billion)

- **ICC/BASCAP:** The projected value of internationally traded counterfeit and pirated products was estimated up to USD 770 - 960 billion in 2015

86% of the world's counterfeit goods originate from China

- US Chamber of Commerce's Global IP Centre (GIPC) Report "Measuring the Magnitude of Global Counterfeiting" (2016) indicates that as much of 86% of the world's counterfeit goods originate from China

Figure 5: Selected economies' relative share in global physical counterfeiting

Global physical counterfeiting:
$461,000,000,000

38 selected economies' share:
$40,369,770,000

Hong Kong 14%

Rest of World 5.24%

China 72%

37 economies 8.76%
(representing 85% world trade)

Why is counterfeiting growing?

- counterfeiting is a low-risk, high-reward crime
- counterfeits are considered as a safe revenue stream by criminal networks
- counterfeiting is seen as a low-level crime - long prison sentences are rarely imposed on counterfeiters, even in jurisdictions that have strong criminal penalties in place
- counterfeits can be sold for 10 times the amount of the manufacturing costs
- counterfeiting has proliferated with the rise of the Internet, which gives counterfeiters the reach to sell to consumers globally, outside the national limits of law enforcement
- growth of Internet banking and online payment services has also become vulnerable to misuse by counterfeiters

Special concerns over mobile phones

- The total mobile phone market is forecast to reach **1.9 billion** units in 2016 *(Gartner, March 2016)* – about **80%** of worldwide devices shipments

- Counterfeit mobile phones constitute an estimated 15-20% of the global market in terms of units sold and about $9 billion in revenue – *EC Study on internationalisation and fragmentation of value chains and security of supply (February 2012)*

Device Type	2015	2016	2017	2018
Traditional PCs (Desk-Based and Notebook)	244	228	223	216
Ultramobiles (Premium)	45	57	73	90
PC Market	289	284	296	306
Ultramobiles (Basic and Utility)	195	188	188	194
Computing Devices Market	484	473	485	500
Mobile Phones	**1,917**	**1,943**	**1,983**	**2,022**
Total Devices Market	**2,401**	**2,416**	**2,468**	**2,521**

1956 2016
CCITT / ITU-T

ITU

World Customs Organization (1)

- In 2014, smartphones was one of the commodities which drew Customs administrations' attention in terms of seizures. The issue is not unusual as mobile phones have comprised a big part of Customs counterfeit-related seizures for some time already:

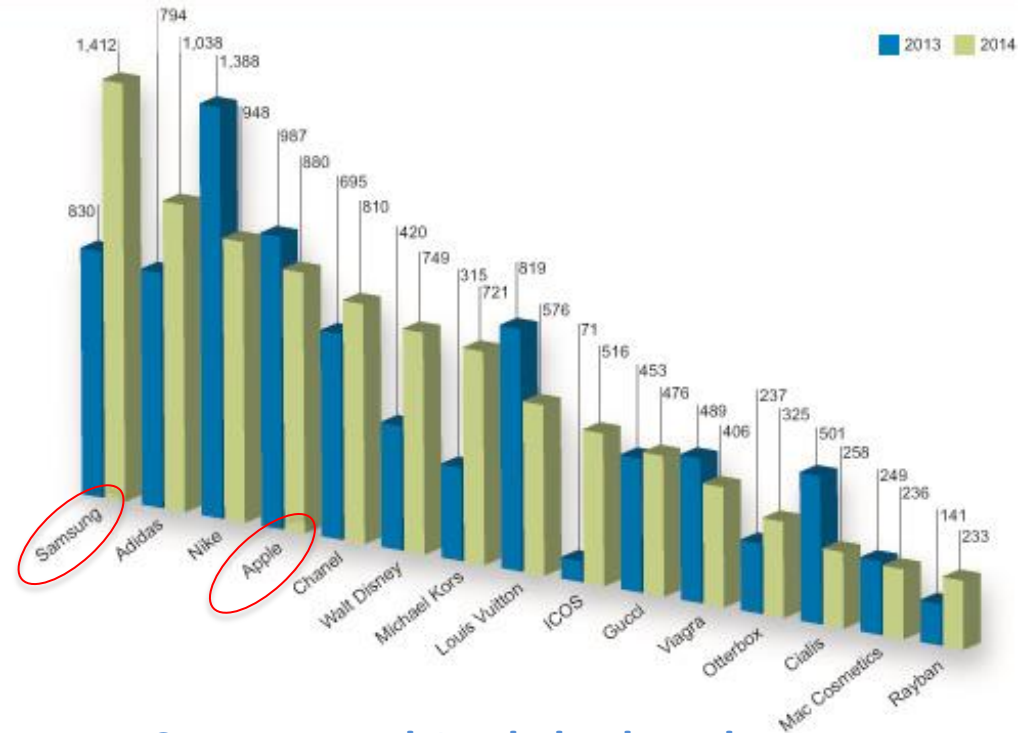| Commodity	Quantity (pieces) 2011	Quantity (pieces) 2012	Quantity (pieces) 2013	Quantity (pieces) 2014
Mobile phones and accessories	7,132,112	1,736,595	4,183,778	5,463,402

Source: WCO Illicit Trade Reports 2012-2014

- Numerous countries sent the WCO special reports on seizures of mobile phones, particularly smartphones: Finland, Greece, Japan, Montenegro, New Zealand, the Philippines and South Africa, to name but a few. **Some countries stated that imports of counterfeit mobile phones and accessories have overtaken the traditionally favoured items (e.g. clothing and caps**).

World Customs Organization (2)

- Between mid-2000 and now, mobile phones swept the WCO's chart rapidly. In 2014, the Customs Enforcement Network (CEN) database confirmed that where the first ranking counterfeit product in terms of number of cases was a smartphone brand

Chart 2. Top counterfeited brands by number of cases

Samsung and Apple both rank amongst the first of the 15 most counterfeited brands chart

Source: WCO Illicit Trade Report 2014

Negative impact of counterfeit mobile phones

GOVERNMENT

- loss of revenue due to non-payment of customs duties and sales taxes
- need of additional measures to ensure a compliance with national regulations *(import, sale, certification, changing the IMEI etc.)*
- danger to public security *(phones with invalid IMEI or "no IMEI" number are potentially attractive for criminal activity and terrorism; possible link to funding a terror activities)*
- lost workforce

INDUSTRY

- losses for right's holders *(unfair competition, loss of sales, price may be affected, copyright and trademark infringement, adverse effect on brand value and reputation)*

OPERATOR

- lowering QoS of mobile telecommunication services *(loss in voice and data capacities, data transmit speeds, reduced coverage)*
- potential interference and EMC problems
- need of expensive and unnecessary technical measures *(more antenna installations, base stations and the need of more spectrum)*

USER

- low quality *(performance degradation, high % of dropped calls, access failures, handover problems)*
- low reliability
- failed warranty and technical support
- potential hazard to health *(use of hazardous substances, higher SAR, batteries' explosion etc.)*
- security and privacy issues *(in cases of theft or stolen phone, it is difficult to track the phone with invalid IMEI or "no IMEI" number)*

Link between counterfeiting & terrorism – an increasing threat to Governments

- A growing body of evidence draws a clear link between physical counterfeiting and terrorist groups which exploit the easy-made money and high profit margin to fund terror activities around the world - *US Chamber of Commerce's GIPC Report "Measuring the Magnitude of Global Counterfeiting" (2016)*

- Counterfeit trade transit points include economies with very weak governance and having a strong presence of organised criminal or even terrorist networks (e.g. Afghanistan or Syria) - *OECD/EUIPO Report "Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact (2016)*

- Enforcement officials confirmed that the Charlie Hebdo assailants sold counterfeits to fund the January 2015 attacks, illustrating the link between counterfeiting and terrorist networks *(Anti-counterfeiting 2016 – A Global Guide, World Trademark Review)*
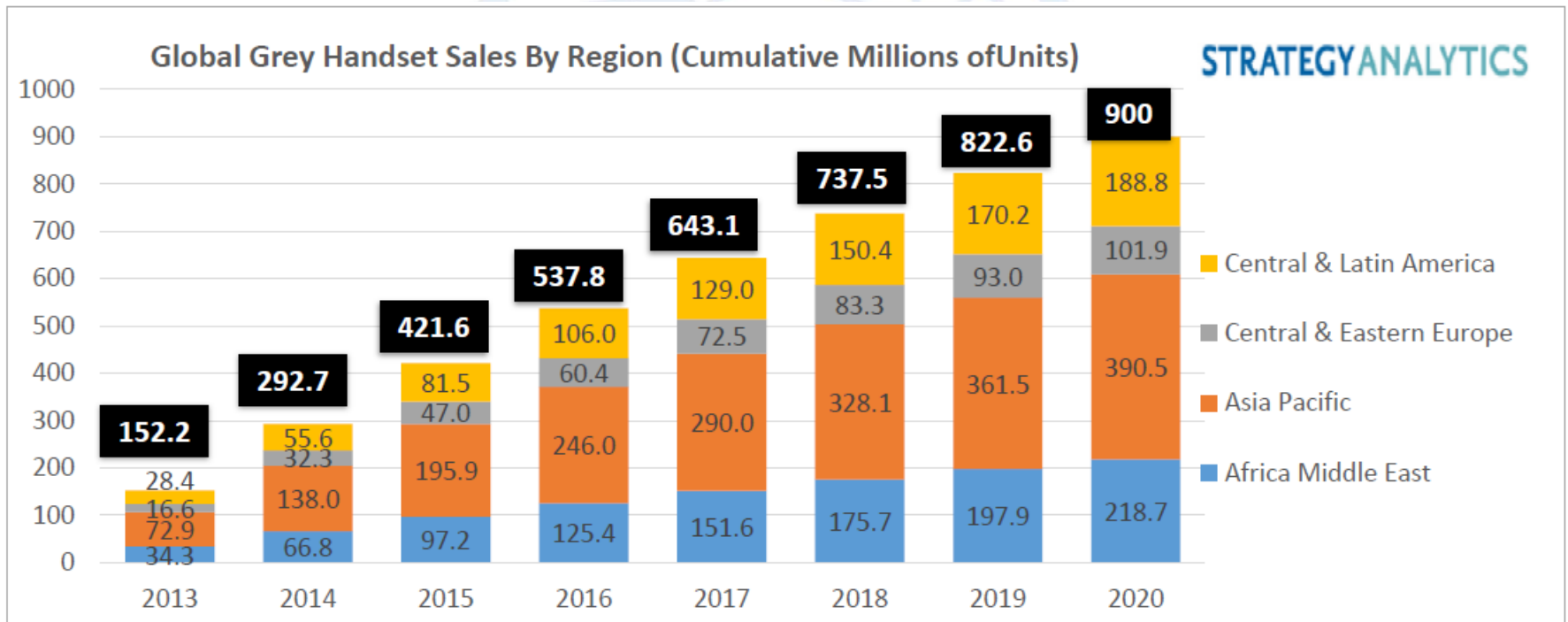
Optimistic forecast

- "Cellphone gray market goes legit, as sales continue to decline" - shipments reached their peak in 2011 with a total of 250.4 million gray-market cellphones, followed by decline to 133.9 million units in 2017 *(IHS, 2013)*

Global Gray Handset Shipment Forecast (Millions of Units)

Source: IHS Inc. July 2013

Pessimistic forecast

- Forecasts for future handset gray market vary but all estimates confirm that counterfeiting will remain a multi-billion dollar underground economy with hundreds of millions of counterfeit units being produced every year

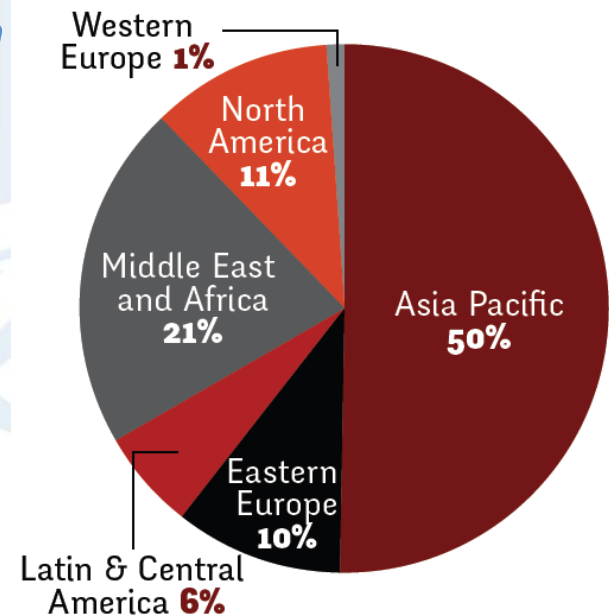Global Grey Handset Sales By Region (Cumulative Millions of Units) — STRATEGYANALYTICS

All regions, especially developing, are targeted

- Smartphones subscriptions are expected to grow from 2,600 million in 2014 to 6,100 million by 2020. This is due to greater affordability in developing markets such as Asia Pacific, the Middle East, and Africa

- Three quarters of global subscription growth came from Africa and Asia in Q1 2015 *(Ericsson Mobility Report, July 2015)*

*A significant **negative impact in all regions** can be illustrated by IHS iSuppli forecast for gray-handset markets for 2013:*   *Asia-Pacific - 103 million units,*

Middle East and Africa - 38.2 million units,

Central and Latin America - 37.3 million units,

countries in Eastern Europe also are major target markets.

Where is it happening?

- Western Europe 1%
- North America 11%
- Middle East and Africa 21%
- Asia Pacific 50%
- Eastern Europe 10%
- Latin & Central America 6%

Source: MMF

Anti-counterfeiting measures and strategies

- In general, the anti-counterfeiting measures and strategies, both locally and internationally, include the legislative frameworks that can operate on several levels:

- deterring domestic counterfeiting activity by imposing criminal liability,

- reducing import and smuggling of counterfeit products by strengthening customs authorities, and

- participating in international trade agreements and initiatives that harmonize global efforts against IP infringement.

- **In the mobile phone sector, there is an available identification and blocking mechanism based on use of the IMEI registration, that not exist in other sectors.**

National initiatives and solutions to combat counterfeit mobile devices

- Today, there are a number of solutions based on IMEI registration, which are implemented by individual administrations and regulatory authorities, based on:

- ✓ blocking the mobile phones with invalid IMEI numbers on their networks,

- ✓ blocking the use of equipment that is not type approved by the regulator,

- ✓ blocking the illegal import of these devices, or

- ✓ by performing other actions on consumer awareness, enforcement measures and appropriate legislation changes at the national level.

ITU-T Technical Report "Counterfeit ICT equipment" & ITU Event on "Combating Counterfeit and Substandard ICT Devices" (17-18.11.14)

Information about national initiatives and solutions to limit the spread of counterfeit mobile devices was presented for:

- Azerbaijan
- Brazil
- Colombia
- Egypt
- Ghana
- India
- Indonesia

- Kenya
- Rwanda
- Sri Lanka
- Turkey
- UAE
- Uganda
- Ukraine

There is a number of new developments and updates

Bangladesh

- According to the Bangladesh Mobile Phone Importers Association (BMPIA) survey - one out of every three handsets available in the market is fake or illegal

- Currently, the Bangladesh Telecommunication Regulatory Commission (BTRC):

- takes necessary steps to insure the correct IMEI number and standard mobile phone handset import and usage;

- initiated the "Type Approval for Mobile Phone Handset Import" process;

- in order to prevent the intrusion of mobile phone sets with duplicate or fake IMEI into the market, implementation of Equipment Identity Register (EIR) in the operators' network is also **in process**.

Cameroon

- Prime Ministerial decree of September 3, 2015 sets out the guidelines for the identification of telephone subscribers and terminal equipment of electronic telecommunication networks

- The operation has been launched by mobile telephone operators under the auspices of the Ministry of Posts and Telecommunications with the Telecommunications Regulatory Board

- Among others, subscribers have to submit the IMEIs of the equipment terminals for identification

- Identification deadline is 10 June 2016

India (1)

- Government of India banned services on mobile handsets without IMEI number after 30.11.2009. Up to **25 million mobile handsets** were estimated to become ineffective

- **Revenue loss to government from sale of mobile phones in grey market in 2014** *(FICCI CASCADE)*

Loss to the exchequer (INR billion)		
Direct tax loss	Indirect tax loss	Total Loss
10.4	56.6	67

India (2)

Director General of Foreign Trade Notification No. 107/(RE-2013)/2009-2014 dated 16.01.2015:

- Import of 'GSM mobile handsets' without IMEI No., with all zeroes IMEI, duplicate IMEI or fake IMEI is **'Prohibited'**

- Import of 'CDMA mobile handsets' without ESN/MEID, with all Zeroes as ESN/MEID, duplicate ESN/MEID or fake ESN/MEID is **'Prohibited'**

- 'GSM mobile handsets' with duplicate IMEI or fake IMEI & 'CDMA mobile handsets' with duplicate ESN/MEID or fake ESN/MEID are **added to the list of 'Prohibited' items for import**

Kenya

- All mobile handsets must be type approved by the Communications Commission of Kenya (CCK) before they are imported

- Collaboration was established between CCK and the Anti-Counterfeit Agency (ACA), Kenya Revenue Authority (KRA), Kenya Bureau of Standards (KEBS), Security Agencies, GSMA, Handset manufacturers, Mobile operators and the Consumer organizations

- ACA inspects the traders of handsets, KRA and KEBS check entry of devices at border points, Security agencies enforce laws on counterfeits, GSMA provides the IMEI database, handset manufacturers pay for the SMS service, mobile operators switch off counterfeit handsets as advised by the CCK and the Consumer organizations ensure the consumer rights' protection

- **Switch off of 1.4 million devices with null or no IMEIs on 5 October 2012**

Kenya - Post Implementation Challenges

Table 4.8: IMEI Verification Requests		2013/14	2014/15	Total Requests
Number of Requests Where the IMEI Was Not Found*		1,500,739	13,658	**1,514,397**
Number of Requests Where the IMEI Was Less Than the required 15 Digits*		3,736,097	42,989	**3,779,086**
Number of Requests Where the IMEI Was Found		10,999,730	82,660	**11,082,390**
Total Number of Requests		**16,236,566**	**139,307**	**16,375,873**
*These are instances where the device was a counterfeit				

Source: Communications Authority of Kenya

- Discovery of numerous devices operating on GSM networks with duplicate/ cloned IMEIs. This makes it difficult to identify the counterfeited terminal

- Genuine IMEIs have also been embedded on counterfeit handsets resulting in counterfeit handsets being sold to the public as genuine handsets

- Slow contributions by handset manufacturers to finance the SMS service

In November 2015, the Communications Authority of Kenya (CA) informed that it started the process of switching off fake mobile phones by inviting suppliers of **automated systems that can authenticate serial numbers of handsets** (for example, identify IMEIs that are invalid, duplicated or cloned, or counterfeit)

Malaysia

- The Malaysian Communications and Multimedia Commission (MCMC) implemented the Public Cellular Blocking Service (PCBS) in February 2014

- A system called MCEIR is implemented with a purpose to handle the lost/stolen devices by maintaining a central repository for the reported devices. MCEIR is connected to EIR for transmission of blocking/unblocking requests

- The active end user's information stored in the MCEIR shall be used for purposes of the PCBS and for such other lawful purposes as deemed necessary by the MCMC

ITU

Nepal

- Importers should register IMEI, ESN or MEID of every mobile handset with the Nepal Telecommunications Authority (NTA) from April 2016

- NTA introduced 'Interim Directives for the Implementation of National Equipment Identity Registry (NEIR)-2072' to implement Equipment Identity Register (EIR) system in Nepal

- Objectives:

  a. To meet the requirements for the national and consumer security

  b. To identify the genuine mobile handsets and make the fake and non-genuine handsets inoperable in Nepal

  c. To enable tracking/blocking of mobile handset that is lost/ stolen

  d. To encourage to import and sell genuine mobile handsets

  e. To minimize the possible grey market and encourage mobile handsets import through the custom office(s).

Nigeria

- **In August 2014**, the Standards Organisation of Nigeria (SON) announced that the Federal Government would order telecom companies in the country to effect a nationwide switch-off of **over 12.6 million** counterfeit phones (**10%** of subscribers) from networks by using the IMEI number

- The aim is the consumer rights protection, increased revenue for the government via taxes; increase revenue for the genuine mobile phone manufacturers as well as improved GSM networks in the country.

- **In May 2016**, the NOC informed that **about 20%** of mobile phones imported into the country classified as sub-standard

- The Nigerian Communications Commission (NCC) confirmed that it works with agencies and international organisation to pick up all the genuine handsets with IMEI numbers to be registered on its database

Oman

- April 2016, the Telecommunications Regulatory Authority (TRA) launched a service that helps consumer to find whether the mobile or a tablet that they plan to purchase is authentic or fake within minutes through a SMS

- This service launched as part of a campaign to educate consumers on the health risks associated with using counterfeit phones

- The campaign also aims at protecting consumers from the potential risks faced in using fake devices due to their poor quality and low efficiency, which also undermine the communications networks in Oman

- Mobile equipment/devices must be marked with the 'TRA' name stamp

- Customers can report about fake mobile to TRA through an email, following which necessary action will be initiated

- TRA anticipates the financial penalties under the appropriate Act for those selling counterfeit mobiles and started the talks with Customs authorities to stop the entry of fake phones into the country at various border points
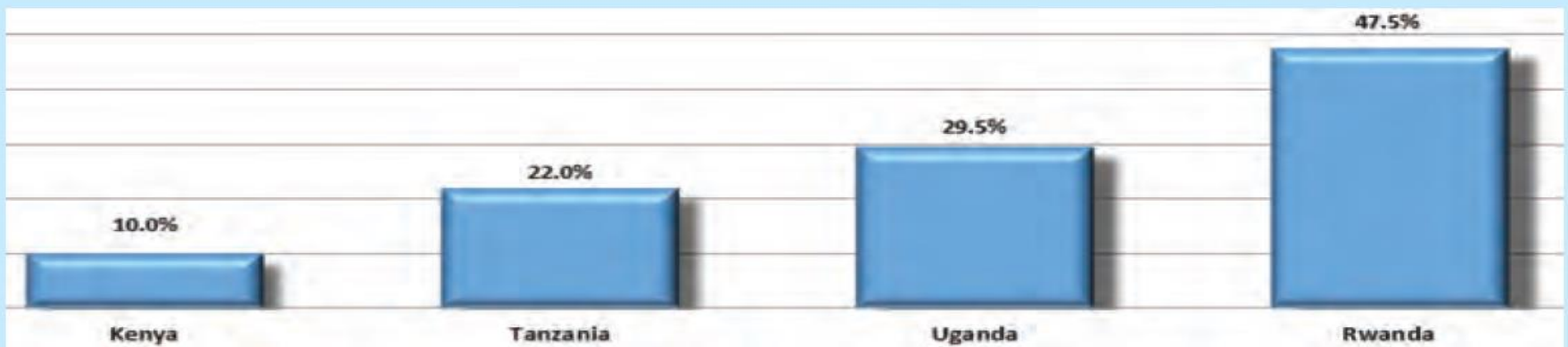
Pakistan

- In 2011, the Pakistan Telecommunication Authority (PTA) estimated 30-35% of the mobile handsets as having non-standard equipment identity number

- Currently, the PTA is **in process of developing Device Identification, Registration and Blocking System (DIRBS)** that will operate as a Centralized Equipment Identity Register to achieve following key objectives:

- terminal equipment with SIM functionality must have a valid and unique IMEI or equivalent identifier

- all parties wishing to import such equipment commercially must have a valid GSMA Type Access Code (TAC)

- mobile operators will disallow registration of new terminal equipment with un-authenticated DIRBS IMEI/invalid identifiers on their networks

- end users and retailers should verify IMEI validity

- imported terminal equipment must be type approved by PTA

Rwanda

- The Rwanda Utilities Regulatory Agency (RURA) implemented type approval as a measure of minimizing importation of counterfeit/ substandard terminals *(instead of switching off the existing ones on the networks as announced in 2012)*

- The law forbids to import, supply, connect, or allow to remain connected to a telecommunications network, or put into service any item of terminal equipment which does not comply with RURA type approval requirements, however these devices are being connected to operators' network through unofficial means

COUNTERFEIT PHONE USAGE IN EAST AFRICA

	47.5%
10.0%	22.0%	29.5%	
Kenya	Tanzania	Uganda	Rwanda

Source: Communications Journal (Uganda) 27.06.14

CCITT / ITU-T

Sri Lanka

- Cabinet of Ministers' Decision (30.01.2014) on setting-up of National Equipment Identity Register (NEIR) at Telecommunications Regulatory Commission of Sri Lanka (TRCSL) with the aim of curtailing the counterfeit mobile phone market and to discourage mobile phone theft so as to protect the consumers . NEIR acts as a central system to ensure the blocking of blacklisted mobile terminals in all networks

- Mobile Phones/Devices Importation procedure:

- must have a valid Vendors License issued by TRCSL

TRCSL APPROVED
Ref No : TRCxx/xxxxxx/xxxxxxxxxx

- only the Type Approved Mobile Phones/ Devices are allowed to import

- IMEI Numbers of mobile phones/ devices should be e-mailed to TRCSL

- TRCSL issues a Reference Number which would be pasted on the box of the mobile phone/ device, in a form of a sticker for Customer's Reference

Tanzania

- All electronic communications equipment used to connect or access the public operating electronic communication networks and all wireless communications equipment to be type approved by the Tanzania Communications Regulatory Authority (TCRA) before they are imported
- **In 2015, about 40% of mobile phones were estimated as counterfeits**
- In December 2015, the TCRA launched the CEIR
- awareness campaign and switch-off deadline (16.06.16) were announced
- IMEI Validation is ensured (TCRA's web-site shows Model, Manufacturer and Frequency Bands to verify if a mobile device is genuine or not)
- CEIR helps users to report stolen phones
- 10-year jail term, 30m/- fine or both for attempt to change the IMEI No.
- **On 17.06.2016 the TCRA switched off 603,000 fake mobile phones**
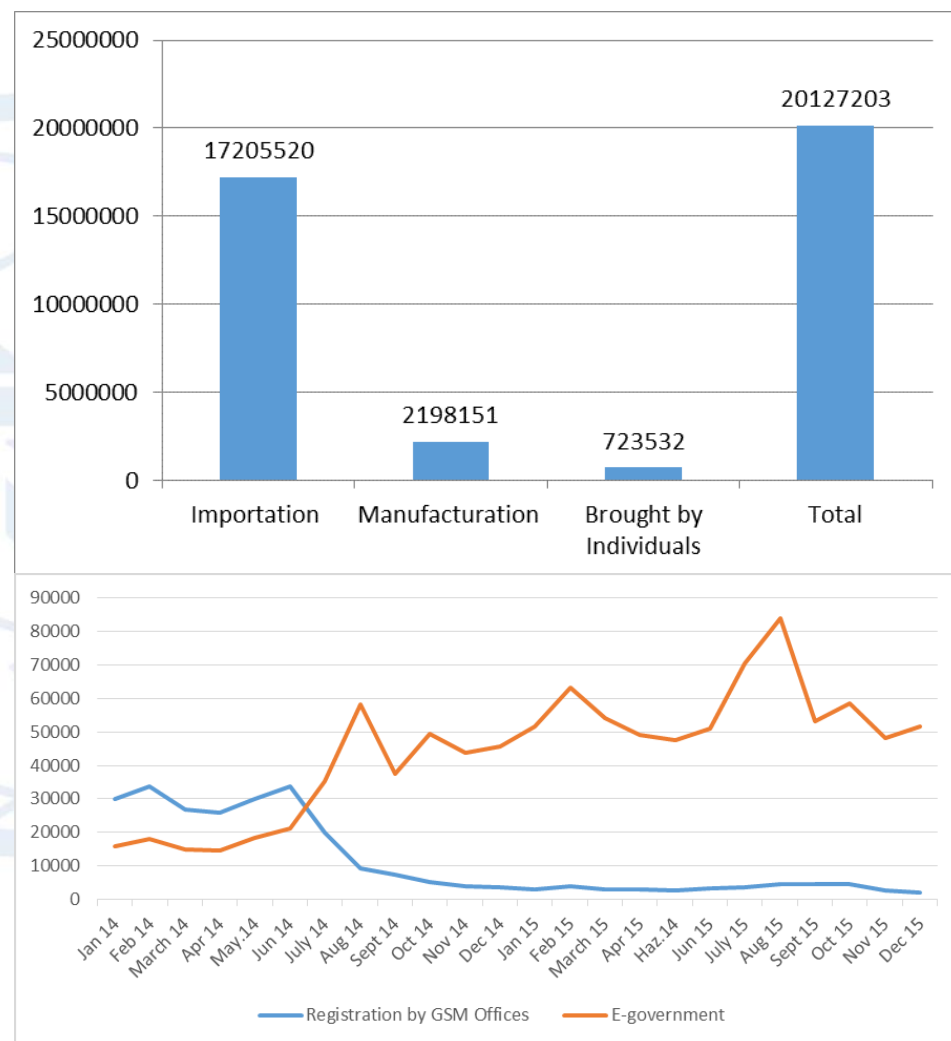
Turkey (1)

- In 2006, the Information and Communication Technologies Authority of Turkey (ICTA) established the Central Equipment Identity Register in line with the provisions of Law 5809

- Main aim - to prevent the use of smuggled, cloned or stolen mobile devices and tax loss and to protect the mobile business environment against illegal and unfair competition

- Mobile Device Registration System (MDRS) stores the IMEI numbers of all mobile equipment used in mobile networks in Turkey. Registered legal devices are stored in a list known as the white list, while other devices are stored in the black list. These lists are generated and updated by the ICTA and are shared with operators several times a day

- All devices whose IMEI numbers appear in the black list are blocked
  (Source: WSIS Stocktaking Report 2015)

Turkey (2)

- In 2015, 20.127.203 IMEIs belonging to 17.958.467 equipments were registered to MDRS. This consists of imported and manufactured devices or devices brought by individuals while returning from abroad

- After the change of secondary legislation regarding the registration of mobile equipment in July 12th, 2014, to a great extent, registration of mobile equipment to MDRS has been transferred to e-government platform. Registrations by ICTA personnel was terminated

(Source: ICTA 2015 Annual Report

Uganda

- The Uganda Communications Commission (UCC) estimated that about 30% of Uganda's mobile phones were counterfeits

- The government loses constitute about Shs15 billion (approx. USD 5 million) in tax revenue annually

- UCC has established a system capable of identifying and denying devices with fake and/or cloned IMEI's access to all operator networks

- UCC operates a tool for verification of IMEI Number by consumers by sending an SMS or through its website

- UCC's campaign to crackdown on counterfeits had started in 2012, but a decision to switch off all counterfeit phones in 2013 was put on hold

- **Once the law to this effect is approved, the system will be operational**

Ukraine

- General Database of mobile phone IMEI codes has been operated by the Ukrainian State Centre of Radio Frequencies (UCRF) since 01.07.2009

- Implementation effect:

- grey import of mobile terminals decreased from 93-95% in 2008 to 5-7% in 2010

- the revenue from customs duties on import of mobile terminals to the State Budget of Ukraine increased to USD 200 million in 2010 (20 times, compared with year 2008) and remained stable by mid of 2014

- After the change of legislation in April 2014 that cancelled a mandatory IMEI registration, it is continued on voluntary basis (the UCRF registers about 1.5 million IMEI codes annually)

- To renew a positive effect of the IMEI database implementation, there is a need in approval of the law for mandatory IMEI registration and blocking of the mobile phones with invalid IMEI numbers on operators' networks

Zambia

- In September 2014, the Zambia Information and Communication Technology Authority (ZICTA) informed about its plans on registration of IMEI codes to rid the country of counterfeit handsets that have flooded its telecom market, as well as combat against theft of handsets in Zambia

- According to *the ICT Survey Report "Households and individuals" (2015)* , 64% of individuals that own more than one mobile phone indicated that they have at least one mobile phone without an IMEI number, and 5% of the individuals that own only one mobile phone indicated that their phones do not have IMEI numbers

Conclusions

- Counterfeit mobile phones constitute an estimated 15-20% of the global market and the problem continues to grow

- In some countries the imports of counterfeit mobile phones and accessories have overtaken the traditionally favoured items (e.g. clothing)

- In the mobile phone sector, there is an available identification and blocking mechanism based on use of the IMEI registration, that not exist in other sectors and has been widely and successfully deployed by individual administrations and regulators in different regions of the world in response to the problem of counterfeit mobile devices

- The lack of knowledge or expertise to deploy a suitable solution, need of considerable investment for implementation of IMEI database, operation of devices with duplicate/ cloned IMEIs, and lack of national regulations for mandatory blocking of the mobile phones with invalid IMEIs on operators' networks are still among the main challenges for various governments around the world

Thank you!

Any questions?

60

1956 2016

CCITT / ITU-T