Key challenges faced by India on circulation of counterfeit ICT devices and key measures to address this issue


Presenter: Biren Karmakar
Group Leader, C-DOT, India.
ITU SG11 Webinar, 15th Feb 2023.

Background

- Wireless communication started in August, 1995
- Current subscriber base is 1170 Million (as of 30th November 2022)
- With this subscriber-base, India is the World's second largest mobile market.
- The country is divided into multiple zones, called Telecom circles or Licensed Service Area – LSA (roughly along state boundaries).
- Calls within Service Area is local and call across Service Area is National Long Distance (NLD) or Subscriber Trunk Dial (STD) calls.
- Roaming applies for inter-Service Area calls.
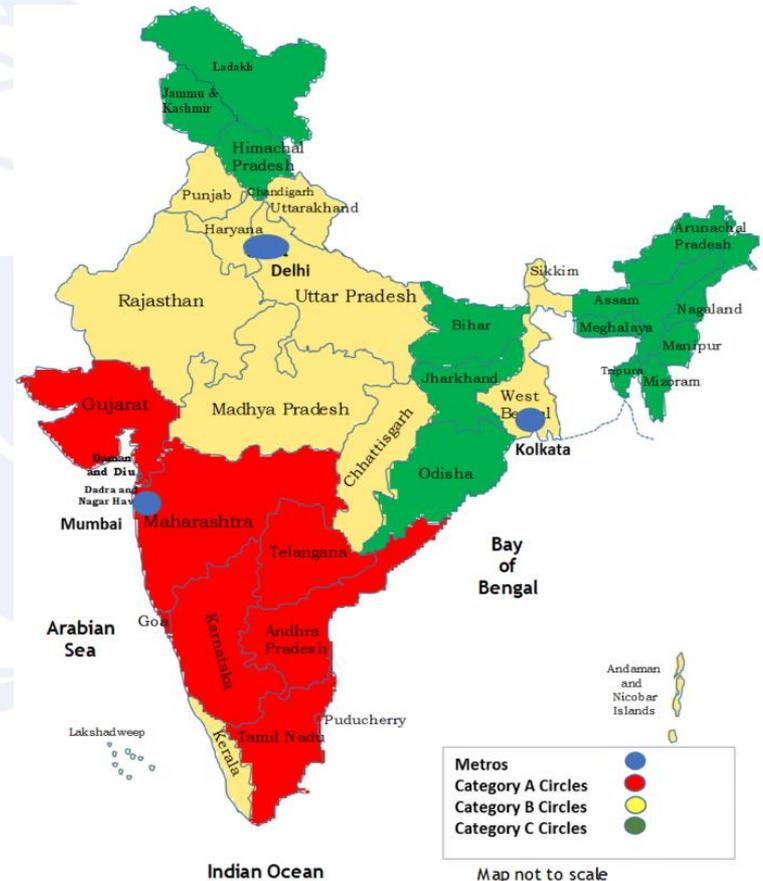
How the challenges found

- While tracking miscreants through IMEI and Lawful interception through IMEI, it was found that there are multiple mobile phones with same IMEI.
- After further observation it was found that there's a large number of mobile phones without IMEI numbers.
- Found huge number of mobile phones with all 0 in the IMEI numbers.
- It was found that Mobile Network Operator are not fully equipped with EIR for checking the IMEI of the mobile handsets.
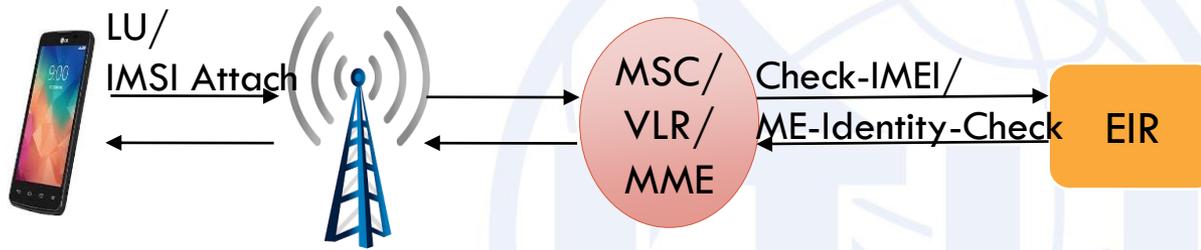
Preventive measures taken

- In 2008, Mobile Network Operators were directed to make provision of EIR in their network so that calls from mobile with invalid IMEI, without IMEI or IMEI with all zero are rejected.
- Subsequent to this directive, all Mobile Network Operators across the country, implemented EIR in their local network.
- Although there were legal provisions to restrict IMEI re-programming in Indian Telegraph Act -1885 and Information Technology Act -2000, still a new rule has been enforced in 2017 specially to stop mobile unique number tempering by virtue of which change of IMEI numbers in any mobile handset is declared unlawful and punishable offence.

सी–डॉट
C-DOT
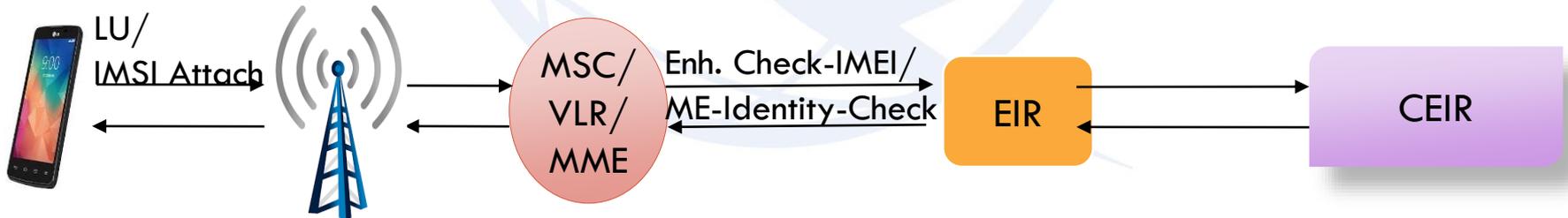
ITU

Further Challenges

- After EIR implementation by Mobile Network Operators, mobile IMEI checking, blocking became possible within same MNO and same Service Area.
- Any mobile blocked in one service area could be used in other service area. Again blocked mobile by one MNO could be used in other MNO network within same service area.
- So to check IMEI validity and common block-list across the country, Central EIR (CEIR) was required to be implemented.
- CEIR was launched in 2019.
- CEIR interfaces with all MNOs across the country.

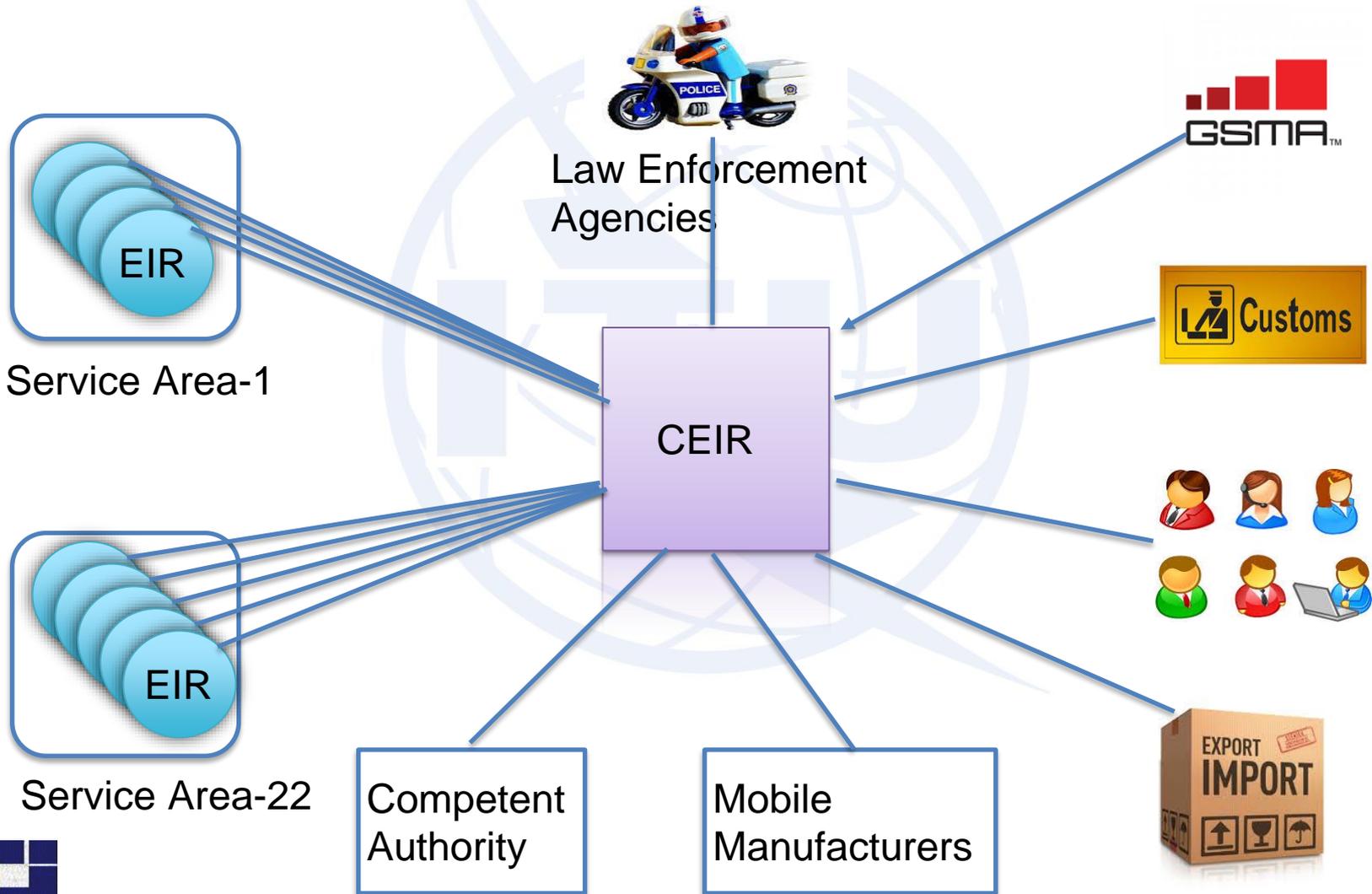# Local EIR to CEIR interface

Earlier Information Flow

LU/
IMSI Attach

MSC/
VLR/
MME

Check-IMEI/
ME-Identity-Check

EIR

Current Information Flow

LU/
IMSI Attach

MSC/
VLR/
MME

Enh. Check-IMEI/
ME-Identity-Check

EIR

CEIR

सी–डॉट
C-DOT

ITU

CEIR Stakeholders

Law Enforcement Agencies

GSMA™

Customs

CEIR

Service Area-1

EIR

Service Area-22

EIR

Competent Authority

Mobile Manufacturers

EXPORT IMPORT

सी–डॉट
C-DOT

ITU

Major CEIR features

- Detection of fresh cloned/ duplicate mobile and permit the use of existing mobile phones.
- Block stolen/lost mobile devices all over India
- Maintain Device Registry for
  - ✣ Local Mobile Manufacturers
  - ✣ Imported Devices
- Enhance mechanism to report stolen/lost mobiles
- Verification of cloned/duplicate/ blocked mobiles - even before buying handset through Web-portal, Mobile App and SMS.
- Cloned/duplicate device authentication by competent authorities/ mobile manufacturers.

IMEI tampering detection

- IMEI tampering could be detected if Re-programmed IMEI is -

  – invalid.

  – non-allocated by GSMA.

  – allocated by GSMA and not used by Manufacturers.

  – already in use with in country (duplicate).

Current Challenges

- IMEI numbers are still re-programmable, however some mobile manufacturers have confirmed that their IMEI can not be modified.

- Only GSMA TAC data is stored in MNO EIR.

- Existing cloned mobile devices can not be discarded from the network.

- Current EIR capacity is not sufficient to store the IMEI-IMSI of its own active subscriber. Therefore MNO need to increase capacity of their EIR.

- Real-time interface implementation from MNO is still pending. When implemented, it will restrict entry of any duplicate/cloned IMEI.

- Device Authentication : When any subscriber's mobile device is detected as cloned and gets notification message for the same, if the subscriber has a valid device, he/she should have an option to get the device authenticated. This issue is addressed in collaboration with mobile manufacturer, but may not be easily accessible for the rural customers.