ITU-D SG 2 - QUESTION 4/2
Workshop on Combating Counterfeit ICT devices

4th October, 2018

CONTROL SYSTEM IN COLOMBIA FOR STOLEN MOBILE DEVICES OR WITH ALTERED/DUPLICATE IMEI

Communications Regulation Commission

Hugo Romero

Adviser

AGENDA

- INTRODUCTION
- COMPREHENSIVE SET OF MEASURES
- IMEI BASED CONTROL SYSTEM
- DUPLICATED IMEI DETECTION AND CONTROL
- REGIONAL BLOCKING OF STOLEN IMEI
- RESULTS
- MAIN CHALLENGES

INTRODUCTION

¿WHY CONTROLLING HANDSET TEFTH ALSO CONTRIBUTES TO CONTROL COUNTERFEIT DEVICES?

STOLEN DEVICE ➔ IMEI BLOCKED ➔ IMEI **TAMPERED** ➔ RE-SOLD

COUNTERFEIT

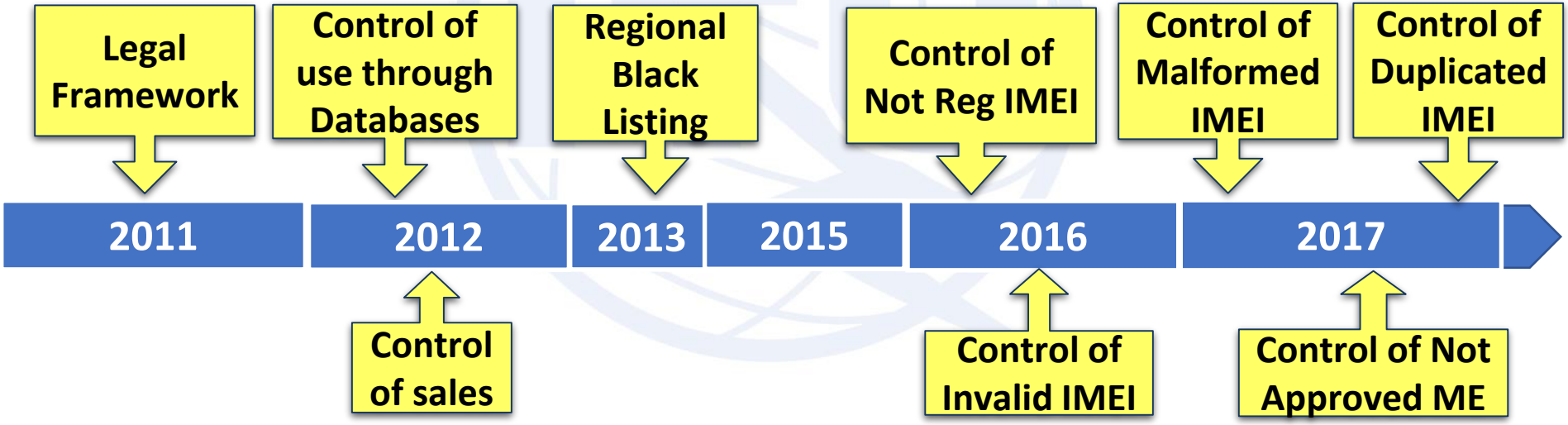
- COPY
- FAKE
- SUBSTANDAR
- NOT APPROVED

IMEI CHARACTERISTICS:

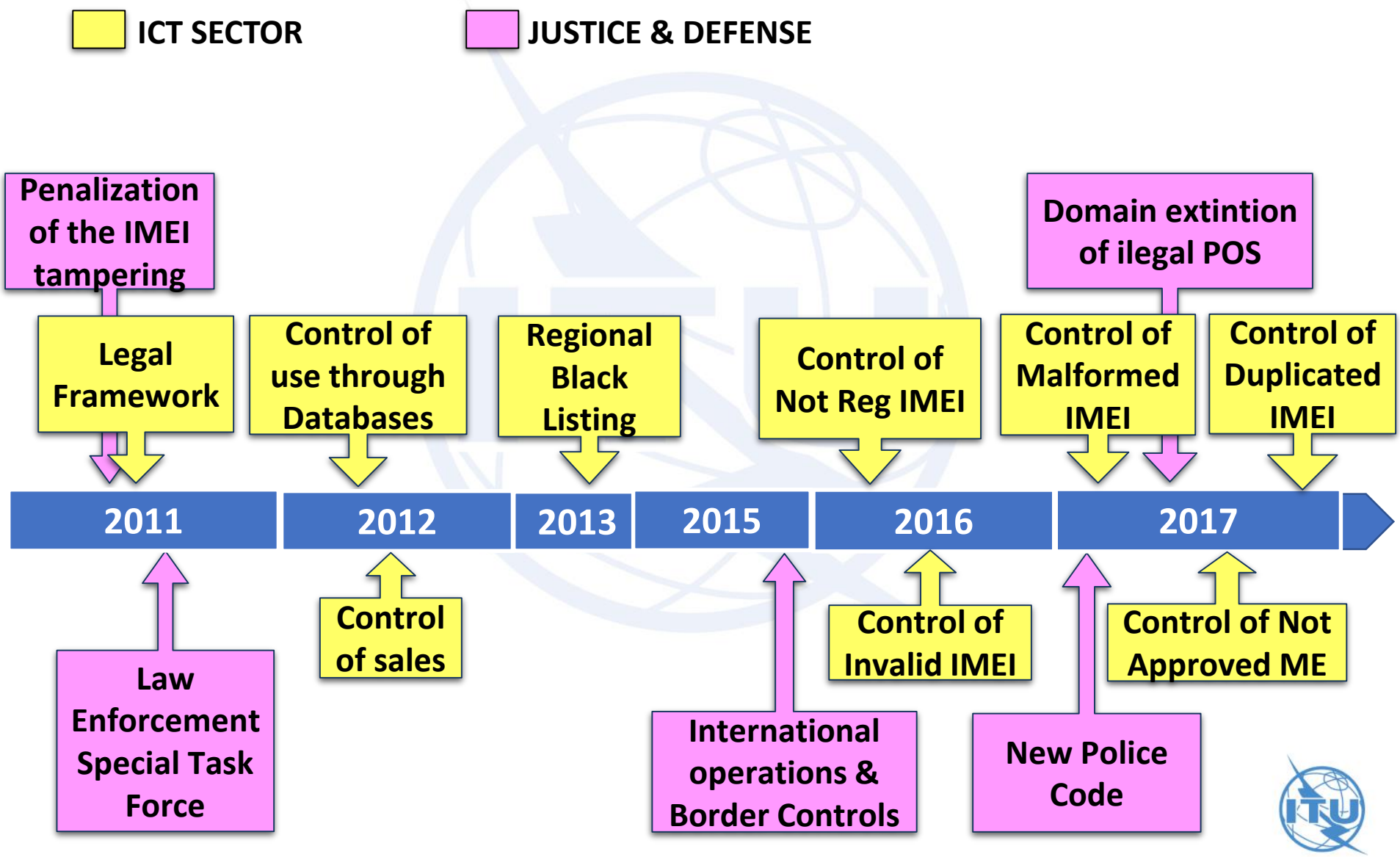
BLANK
UNFORMATTED
INVALID
NOT HOMOLOGATED
NOT REGISTERED
DUPLICATED

COMPREHENSIVE SET OF MEASURES

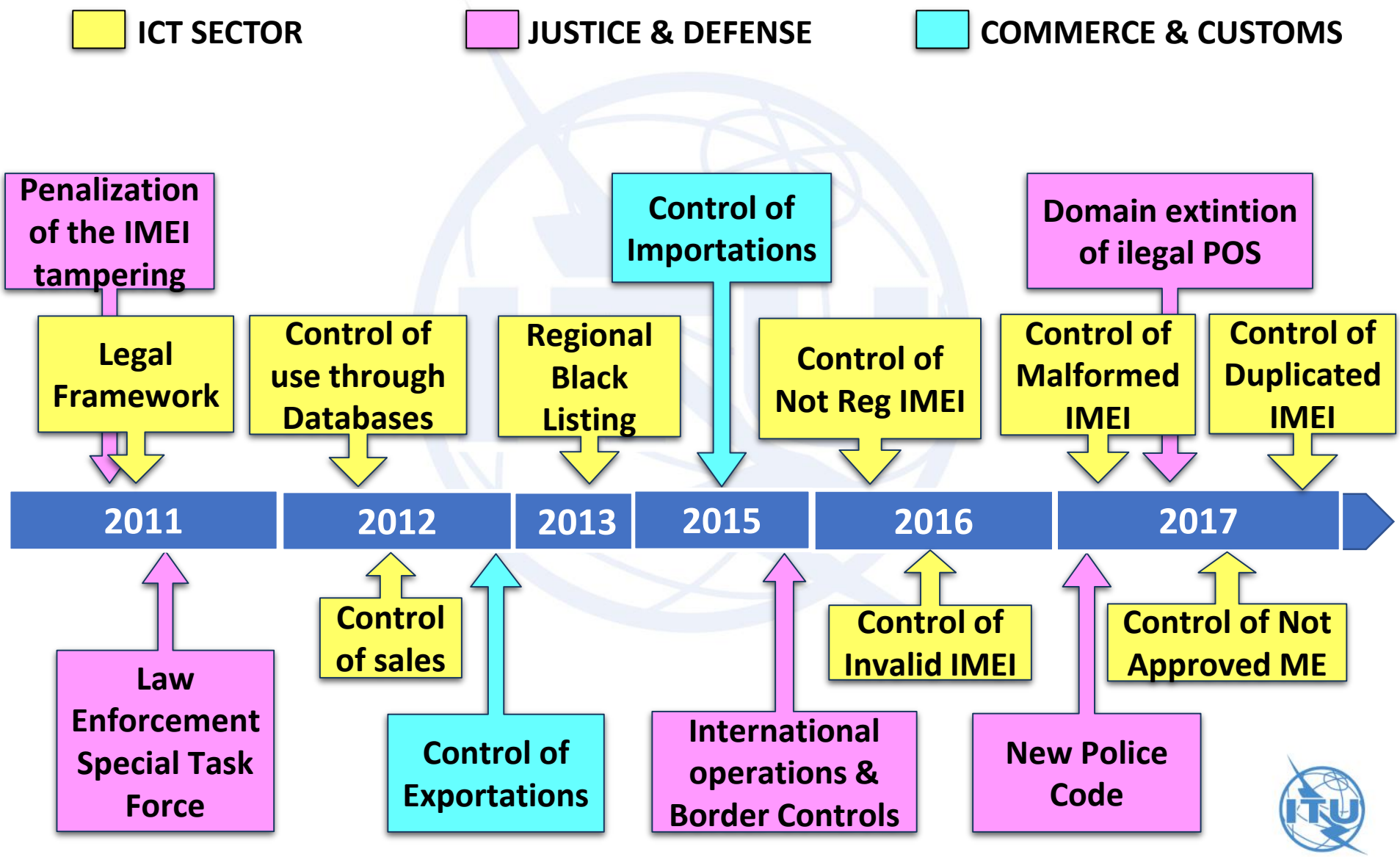
ICT SECTOR



COMPREHENSIVE SET OF MEASURES



COMPREHENSIVE SET OF MEASURES



ICT MEASURES FOCUS

Each user is responsable of his device procedence

Legal Device Registry

→ **POSITIVE DATA BASE**

Make lost/stolen device useless

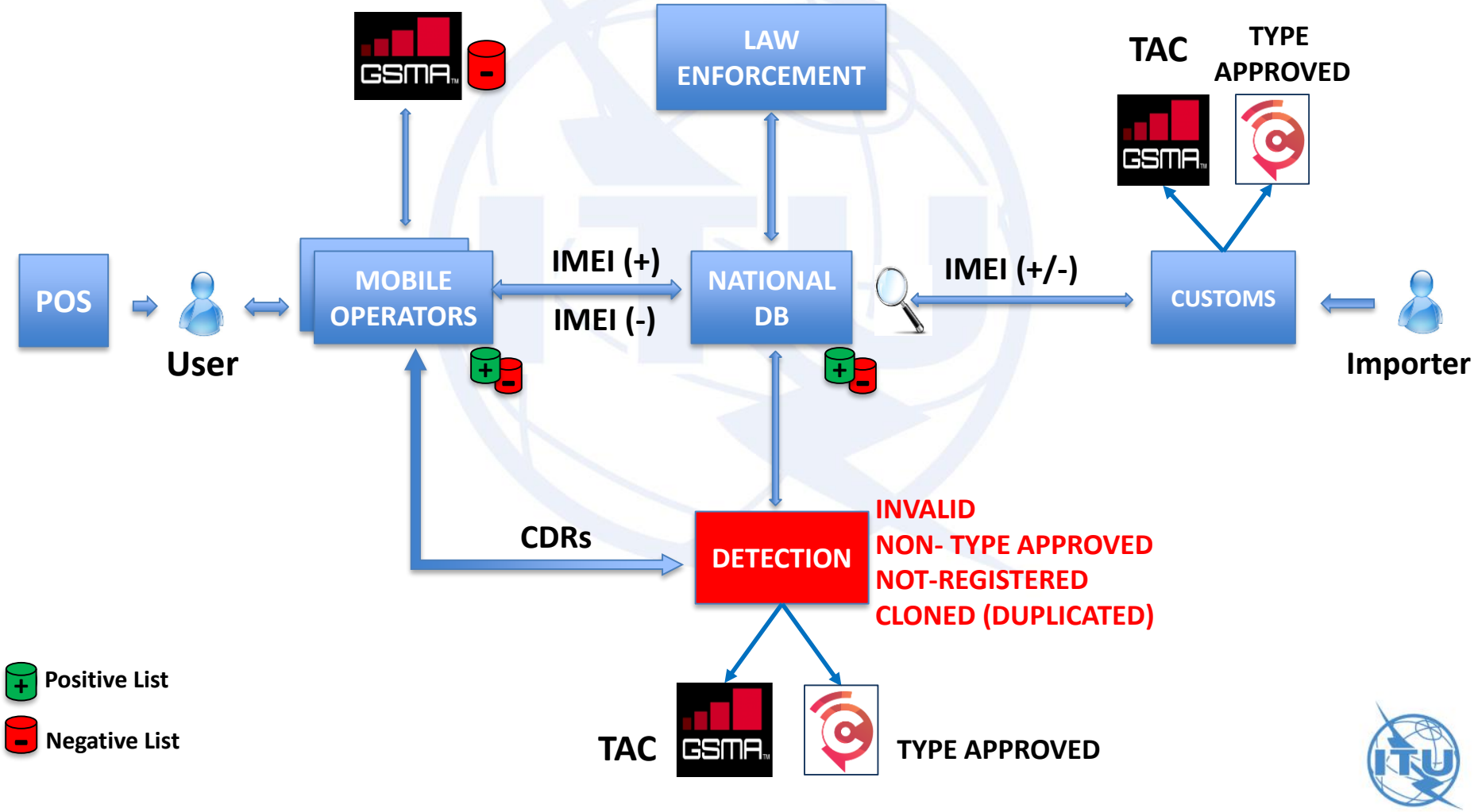
Blocking in mobile networks

→ **NEGATIVE DATA BASE**

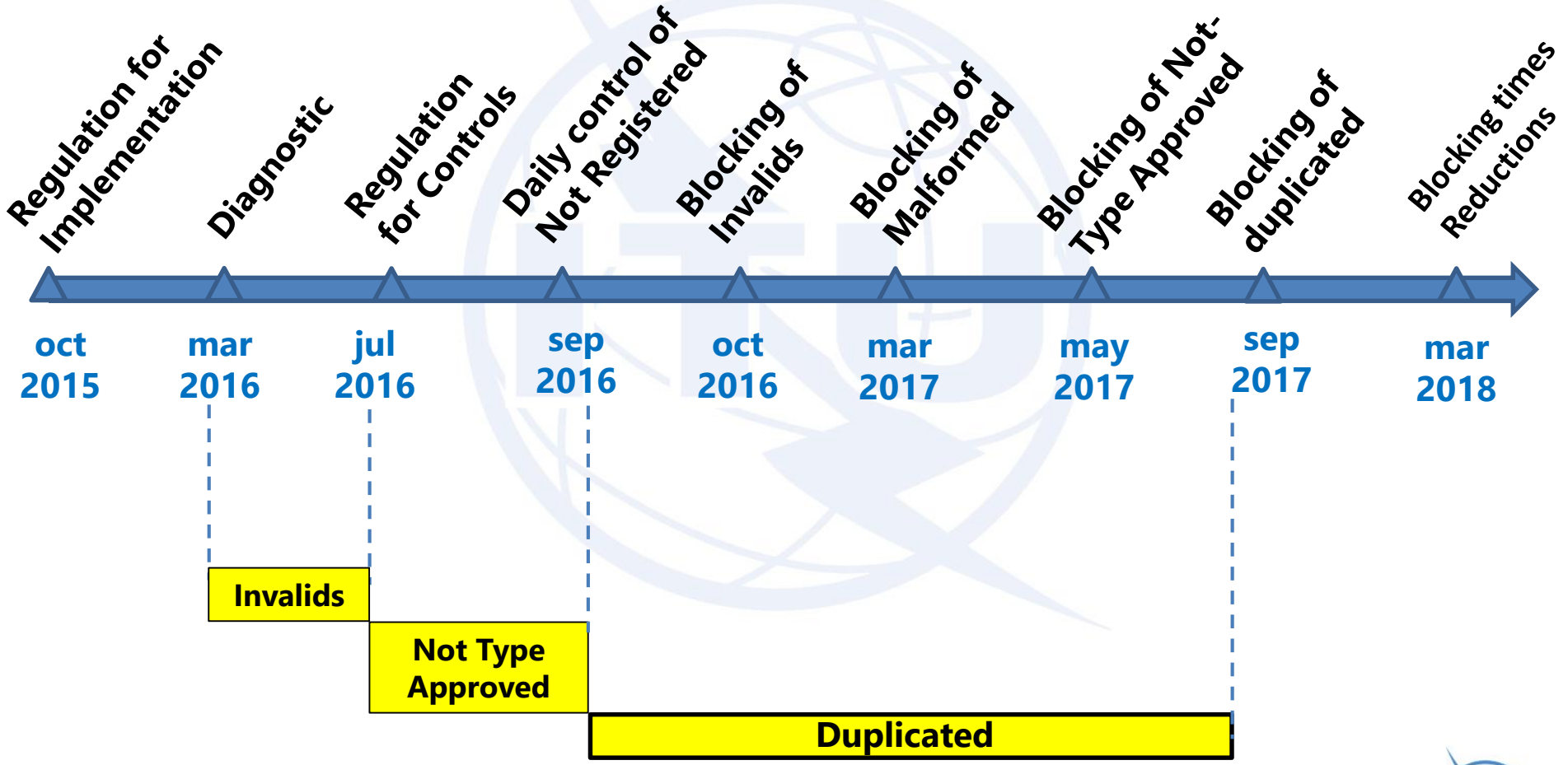
Detect and control Altered/duplicated devices

→ **DAILY CONTROL OF IMEIS WITH ACTIVITY IN MOBILE NETWORKS**

IMEI BASED CONTROL SYSTEM

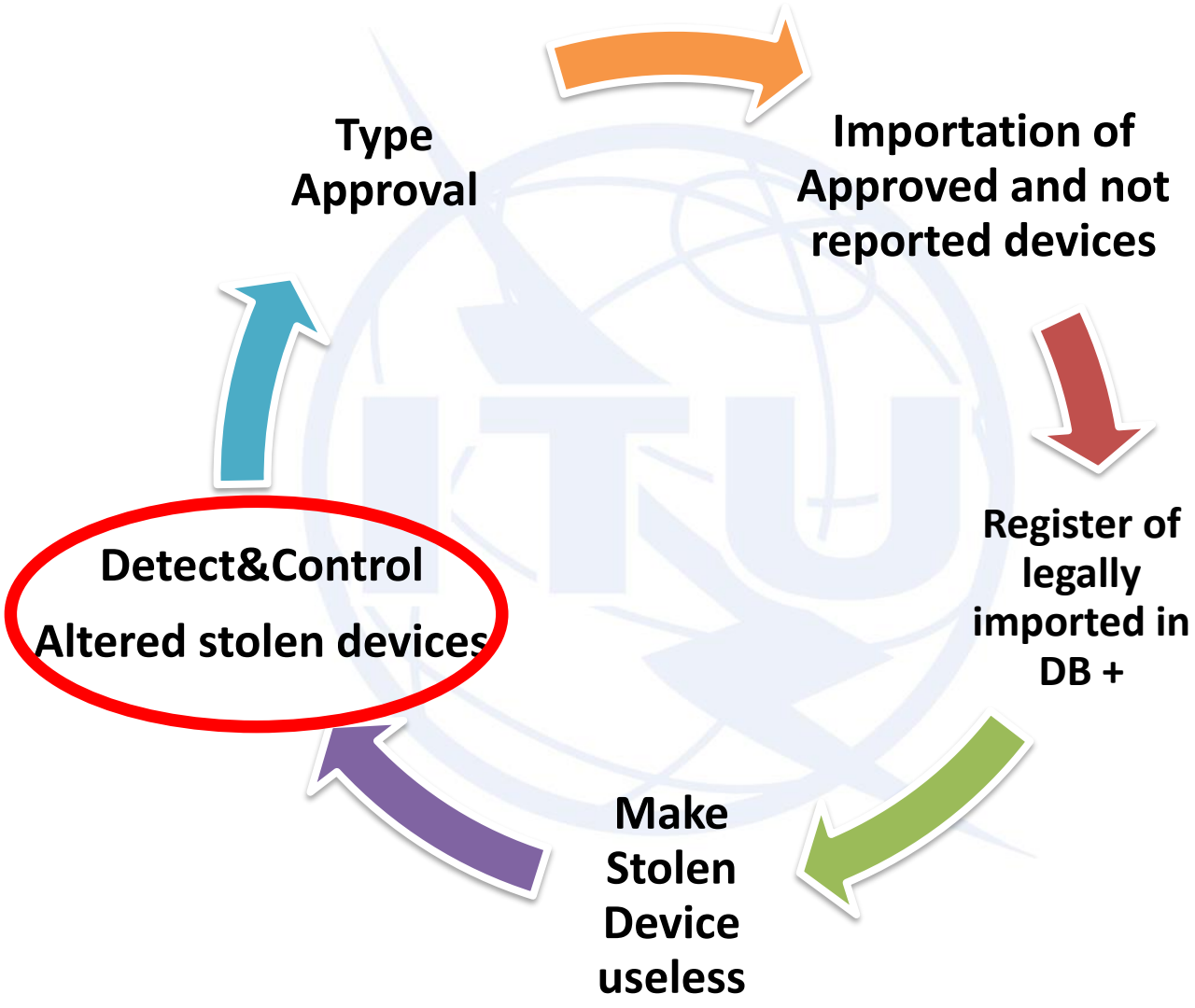


IMEI ACTIVITY CONTROL: DEPLOYMENT PROCESS



Transition periods (amnesties for existing devices)

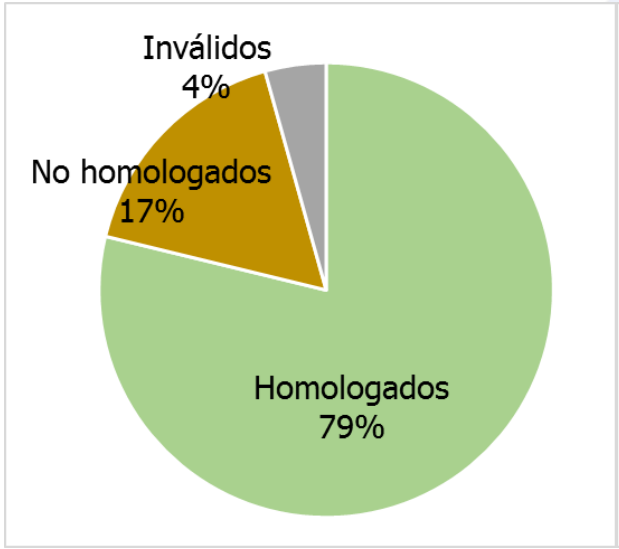
PURPOSE OF MEASURES & IMEI CONTROL PROCESS

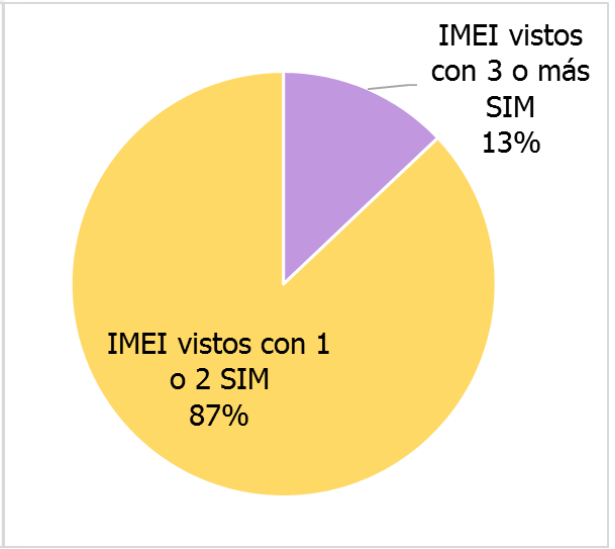


INITIAL DIAGNOSTIC MARCH 2016

47 M OF POPULATION WITH 57 M OF ACTIVE LINES

42 M OF IMEI WITH ACTIVITY IN MOBILE NETWORKS





- **7,1 M : Non Type Approved**
- **1,8 M : Invalids**

9,5 M : Not Registered

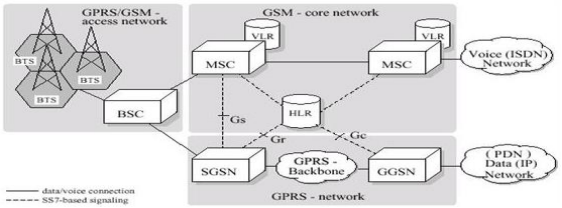
6,8 M Potential duplicated
(Same IMEI seen with 3+ SIMs)

March 2016

24% of Irregular IMEIs

DAILY DETECTION & CONTROL PROCESS

MOBILE NETWORK



24 H → CDR → IMEI → TAC → GSMA → DB CROSS CHECKS

GSMA

DB CROSS CHECKS RESULTS & ACTIONS

✗ ✗ ✗	→	SMS INVALID	48 HR →
✓ ✗ ✗	→	SMS NOT HOMOLOGATED	45 D →
✓ ✓ ✗	→	SMS NO REGISTERED	20 D →
✓ ✓ ✓	IMEI CELLID LAC FECHA/HORA → DUPLICATED SFW →	SMS DUPLICATED	30 D →

CONTROLS AND USER´s OPTIONS

IMEI TYPE	DEFINITION	CONTROL	USER´s OPTION
Malformed (with no standard format)	Less than 14 dígit or With alphabetic characters	No network access	Claim to vendor
Invalid	Not in GSMA TAC DB Not in CRC TAC DB	Blocked in 48 hr	Definitive blocking Claim to vendor
Non-type approved	Not in CRC TAC DB (Not homologated)	Blocked in 45 Days	Claim to vendor Or proceed to homologate in CRC
Not Registered	Not in Positive DB (Unknown user/origin)	Blocked in 20 Days	Proceed to register & Unblock
Duplicated	Same IMEI in different devices	Blocked in 30 Days Control IMSI-IMEI	Restricted use with one or more lines

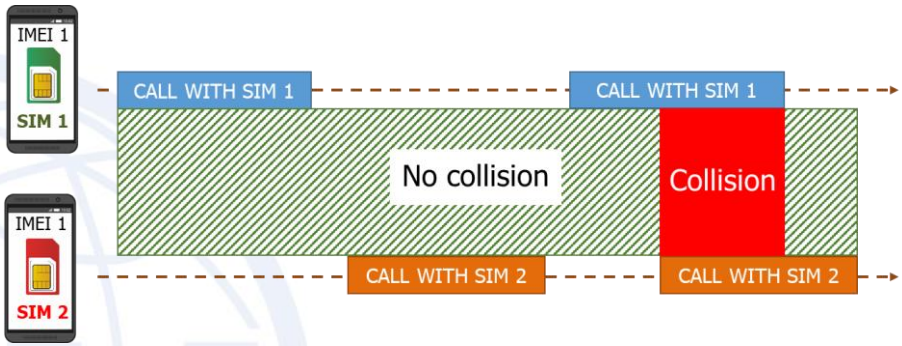
CONTROLS AND USER´s OPTIONS

IMEI TYPE	DEFINITION	CONTROL	USER´s OPTION
Malformed (with no standard format)	Less than 14 dígit or With alphabetic characters	No network access	Claim to vendor
Invalid	Not in GSMA TAC DB Not in CRC TAC DB	Blocked in 48 hr	Definitive blocking Claim to vendor
Non-type approved	Not in CRC TAC DB (Not homologated)	Blocked in 45 Days	Claim to vendor Or proceed to homologate in CRC
Not Registered	Not in Positive DB (Unknown user/origin)	Blocked in 20 Days	Proceed to register & Unblock
Duplicated	Same IMEI in different devices	Blocked in 30 Days Control IMSI-IMEI	Restricted use with one or more lines

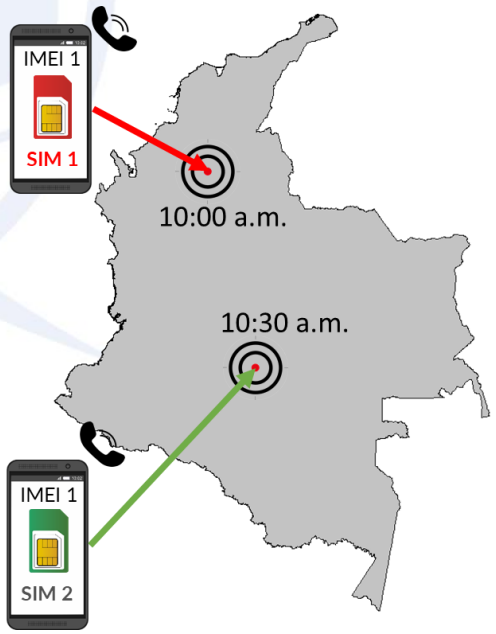
SOURCES OF ALTERED DEVICES

DUPLICATED IMEI DETECTION

1. **Same IMEI with different SIM making calls at the same time**

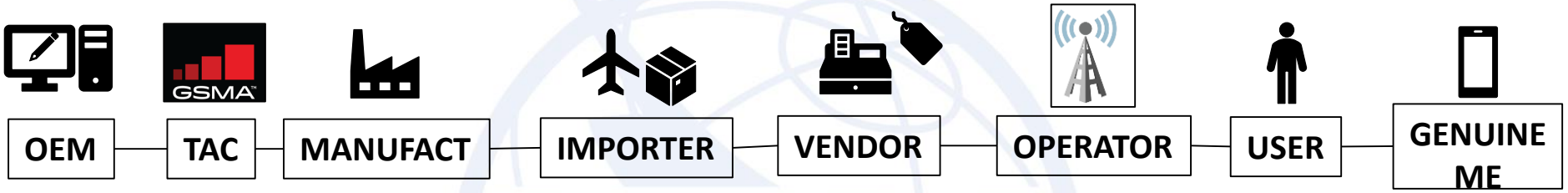


2. **Or within not posible time and distance frames**

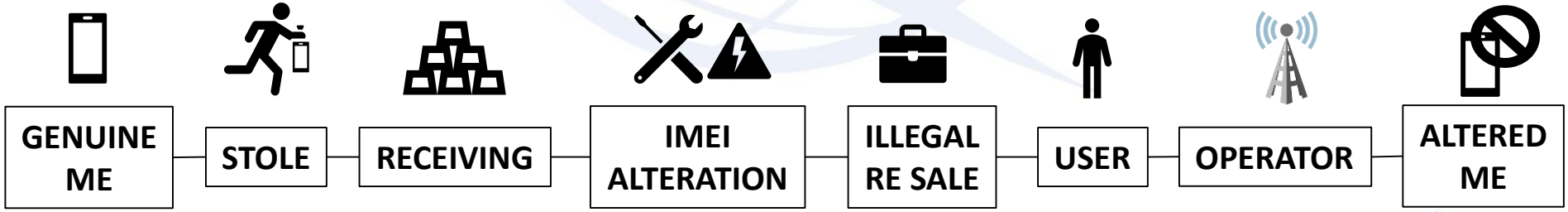


GENUINE VS ALTERED MEs

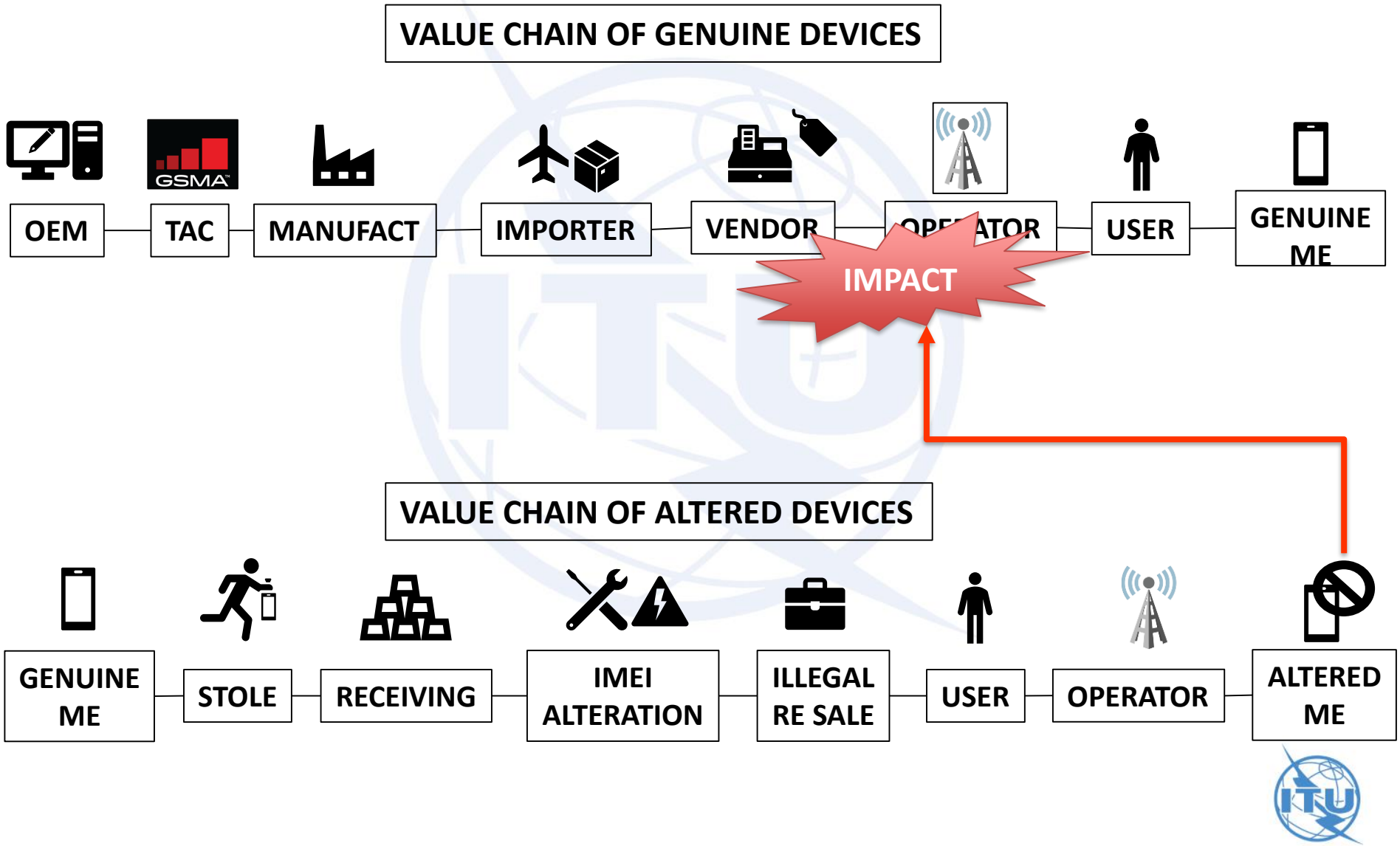
VALUE CHAIN OF GENUINE DEVICES



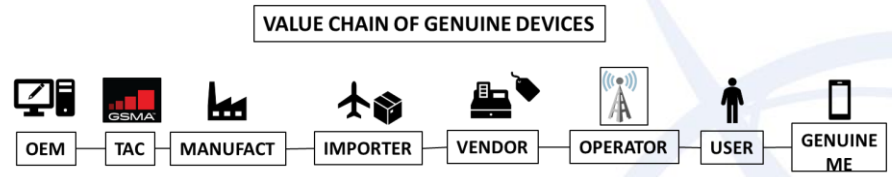
VALUE CHAIN OF ALTERED DEVICES



GENUINE VS ALTERED MEs

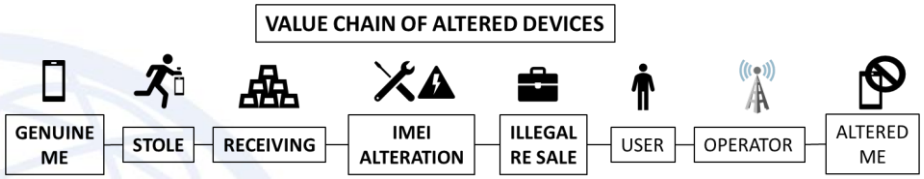


GENUINE VS ALTERED MEs



- Match of TAC, Brand and Model
- Internal IMEI = external IMEI
- Original Label
- Importation papers
- Authorized vendors (Big surfaces/operator)
- Invoice consistency (value, IMEI, etc)
- IMEI history associated with a subscription data

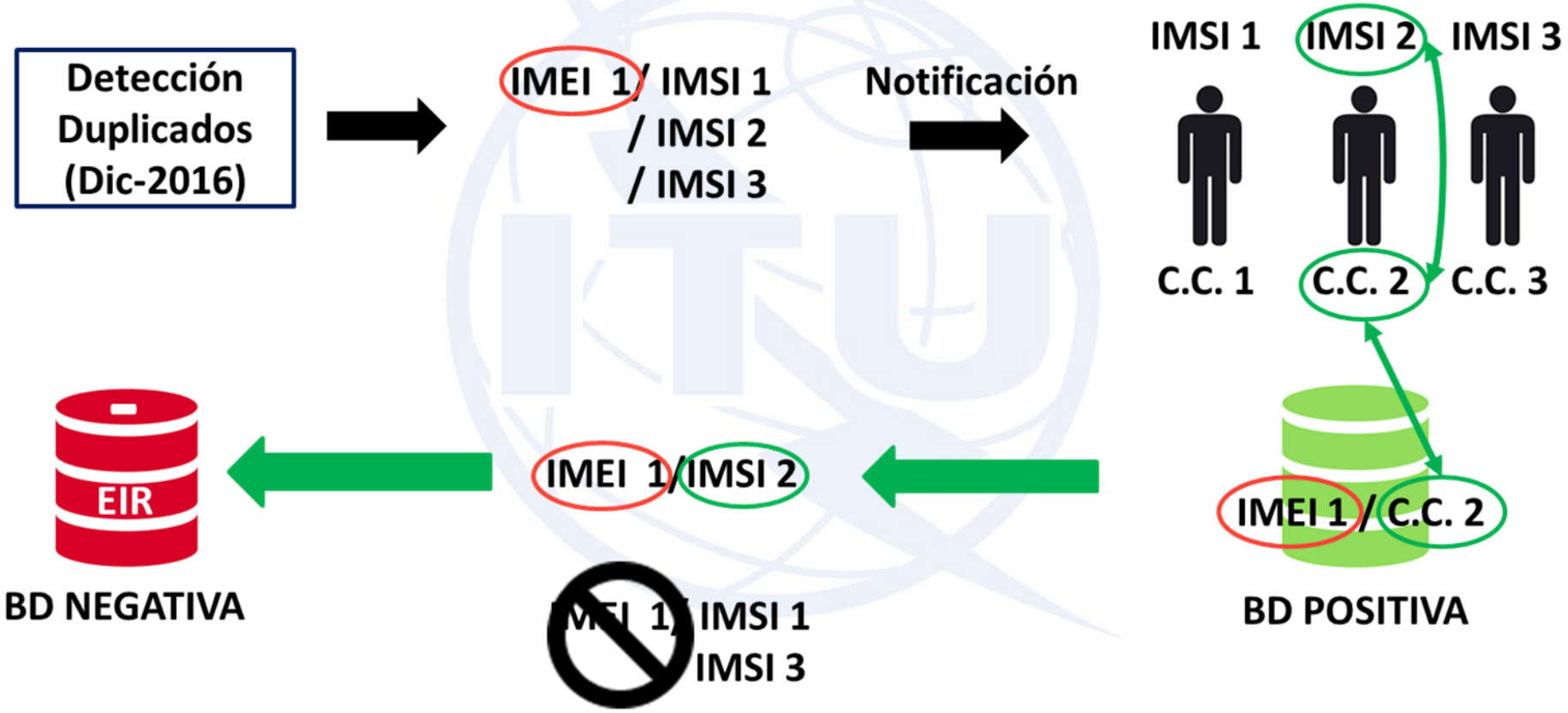
STAKEHOLDERS DON´T HAVE CHANCE TO PREVENT DUPLICATION IN OTHER ME



- TAC, Brand, Model don´t Match
- Internal IMEI different from external IMEI
- Fake label
- Case Brand and Model are different from the TAC
- No importation papers
- Invoice inconsistencys (value, IMEI, etc.)
- No IMEI history associated to a subscription
- IMEI technical diagnostic required (Case manufacturer)

ME ALLOWS IMEI TAMPERING TO USE OTHER´s GENUINE ME IMEI

Duplicated IMEI Control

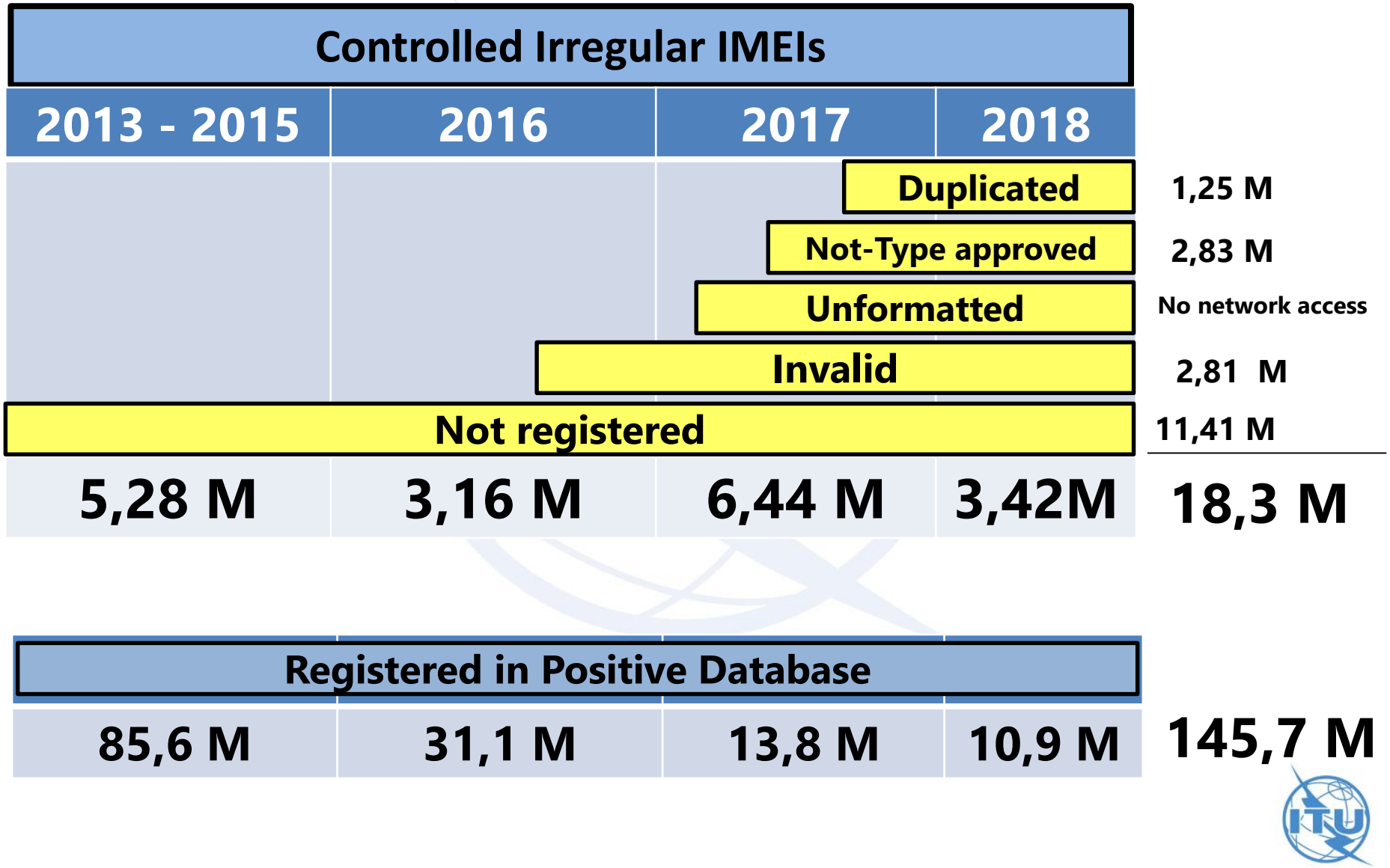


REGIONAL BLOCKING OF STOLEN IMEI

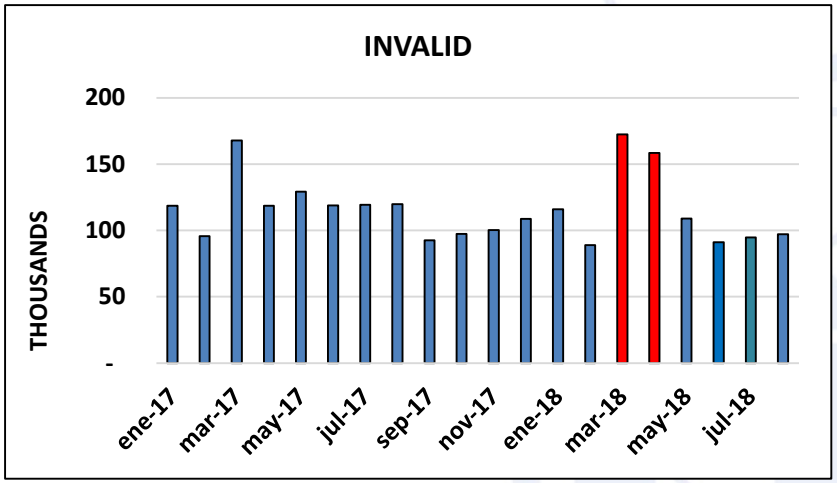
OTHER REGIONS CONNECTIONS TO GSMA IMEI DB (# of Countries)

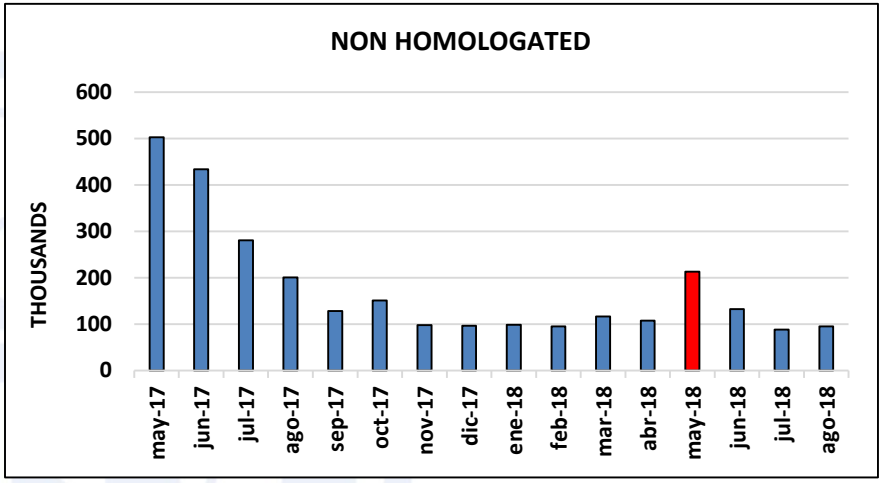
EUROPE: 39% **ASIA: 5%** **AFRICA: 4%** **OCEANIA: 7%**

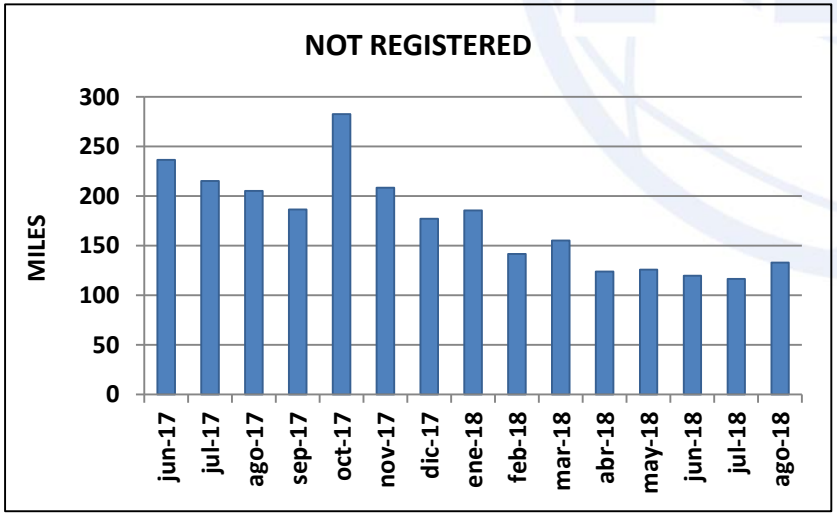
RESULTS

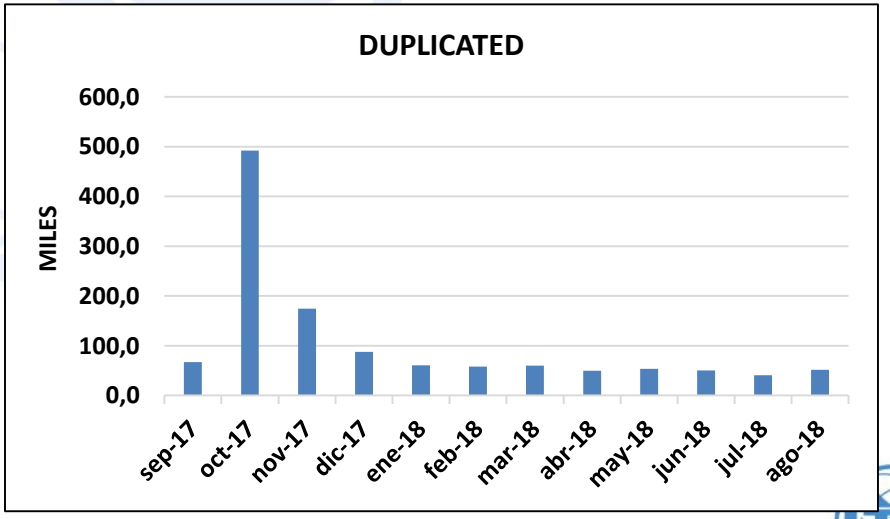

Controlled Irregular IMEIs
2013 - 2015
2016
2017
2018
Duplicated
1,25 M
Not-Type approved
2,83 M
Unformatted
No network access
Invalid
2,81 M
Not registered
11,41 M
5,28 M
3,16 M
6,44 M
3,42M
18,3 M
Registered in Positive Database
85,6 M
31,1 M
13,8 M
10,9 M
145,7 M

RESULTS
Trends of Irregular IMEI presence

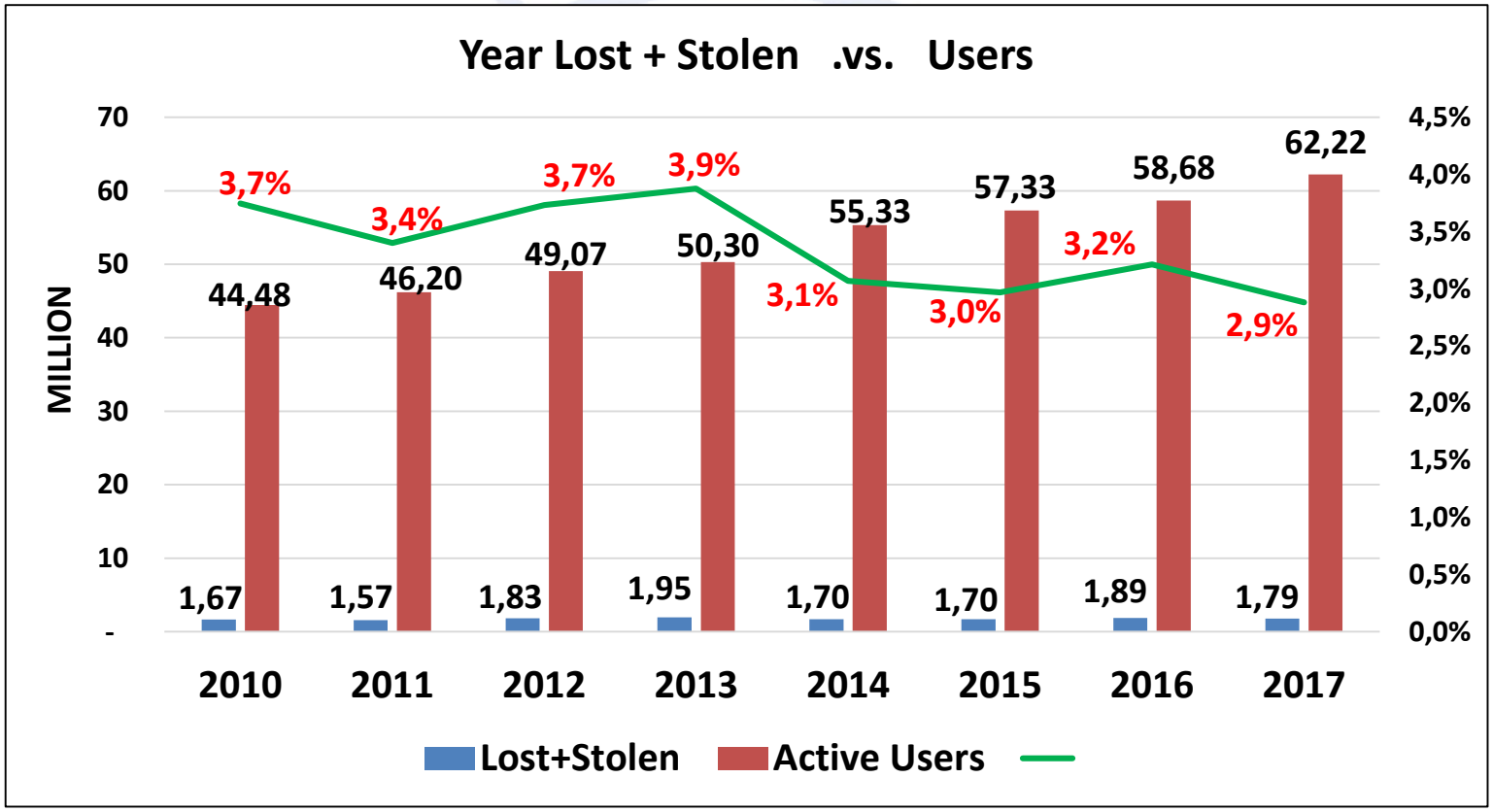








RESULTS


Year Lost + Stolen .vs. Users
MILLION
70
60
50
40
30
20
10
-
4,5%
4,0%
3,5%
3,0%
2,5%
2,0%
1,5%
1,0%
0,5%
0,0%
3,7%
3,4%
3,7%
3,9%
3,1%
3,0%
3,2%
2,9%
44,48
46,20
49,07
50,30
55,33
57,33
58,68
62,22
1,67
1,57
1,83
1,95
1,70
1,70
1,89
1,79
2010
2011
2012
2013
2014
2015
2016
2017
Lost+Stolen
Active Users

MAIN CHALLENGES - GOVERNMENT

Challenge	Treatment
Active role by different goverment entities	Leadership from the top of the government
Attack criminal economy	Legal framework & revisions All law enforcement involvement International scope
Follow up of the problem trends	Police findings & statistics Multisector f.U. Meetings
Impacts on stakeholders	Dialog focused on solving public safety issue
How to built the positive and negative data bases	By law, is a financial/operational responsabiltiy of operators
Enforcement of ICT measures	Per law is ict ministry function
Device repair technicians	Educate them in ethics in front of alteration
Black market of device parts	Police controls on points of sale

MAIN CHALLENGES -REGULATOR

Challenge	Treatment
Empowerment to regulate	Law issued by congress Decree issued by ict ministry
Know how of the problem	Experienced team profile Exchange of experiences with other countries
Dynamics of the problem	Technical follow up commitees Continuos regulation adjustments
Volume and types of IMEI to control	pashed deployment priorization per imei type transition periods for each type of existing imeis
Not registered devices	gov&operators public campaigns start blocking of not registered imeis
Blocking of not homologated devices	Re engineering of homologation process (on-line, for any person)
Control of duplicated IMEIs	Search of technology to control duplicates Adoption of 2 criteria to define genuine devices: 1. The ones owned by registered user in db+ 2. The one who proves having genuine device

MAIN CHALLENGES - OPERATORS

CHALLENGE	TREATMENT
Operate national DBs	Centralized + Distributed DBs Protocols Automatization
Consistency & Concilliation of DBs	Daily treatment of error messaging
Block rigth IMEI of stolen devices	Take IMEI from netowork activity
Volumes of IMEI to block	Upgrade EIR Keep entries on EIR for a limit of time Add new IMEIs to blacklists deleting earliest entries
Control of malformed IMEIs	Apply changes on Radio acces and core networks
Control of not homologated devices	Daily CRC homologated TAC list
Detection of duplicated IMEI	Agree on duplicated IMEI definition Agree on criteria and algorithms to detect duplicates Given time to develop, test and opérate algotihms

MAIN CHALLENGES - OPERATORS

CHALLENGE	TREATMENT
Detect both intra network and inter network duplicates (with activity in different mobile operators)	Split processes, one for intranetwork detection and other for inter network detection by a third party thac collects information and apply defined criteria and algorithms
Volume of data to analyze in the process of duplicates detection	Only Voice CDR is taken to analysis Use of minimun fields of CDRs to analyze in the detection For inter network detection, use only data related to those IMEI with activity in more than one network for a month period.
Protection of personal data contained in CDRs	Only using fields that are not personal data by itself (or alone) Sending only fields required for analysis to the third party in charge of inter network detection of duplicates.
Control of duplicated IMEIs	Upgrading EIR to IMSI-IMEI check functionality Updating of CRM to EIR provisioning process Establishing customer care processes
Identify genuine devices from several with same IMEI	Agree on criteria of genuine devices with the regulator. Using general criteria to let the operator take decision based in each case, proves and the devices involved.
Rotation of devices with irregular IMEIs	Reduction on bllocking times

MAIN CHALLENGES – LAW ENFORCEMENT

CHALLENGE	TREATMENT
Better and on line information of stolen devices	Access to centralized DB
Low technical know how on mobile theft	ICT Ministry and Regulator training
Increase Street surveillance	Georeference of hot spots with centralized DB info
Control to Points of Sale of mobile devices	Device Sale Authorization Regime by ICT Ministry On line information system of authorized POS Legal framework (closings + Domain extintion)
Judicialization of people that alter IMEI	Proposal for law revision to pass in the congress New Police Code (mobile device contraventions)
Impact all links in to the criminal chain	Legal framework & revisions Create several interinstitutional groups (intelligence/operations) Actions with international scope
Very low denounce levels of stolen devices from users	Change presencial process to virtual denounces Public campaings

Findings and Recommendations

- Reach global exchange and blocking of IMEI reported as stolen/lost
- Complement black lists with national detection / control of altered devices
- Detect and control all IMEI types that identify posible altered devices:
  - Malformed (Unformatted)
  - Invalid
  - Not homologated (Not-Type approved)
  - No Registered in positive/white data bases
  - Duplicated
- Thieves act and adapt rapidly. Continuos follow up of the application of measures.
- Key success factor: Reference Data Base with unique regular identifiers of legally imported and acquired devices
- Mid – Term process (~3 year). Phased deployment recommended: Diagnostic – Design – Implementation – Operation – Transition (amnesty) periods to existing devices – User processes

REFERENCES

1. **GSMA and ETSI standards (ETSI 3GPP TS 122.016 v13.0.0 (2016-02), 3GPP TS 123.003)**

2. **GSMA TS.06 – IMEI Allocation and Approval Process**

3. **GSMA Latin America quarterly reports of GSMA IMEI DB to CITEL Permanent Consultive Committee I**

4. **IDC Consulting Latin America: "*Using IMEI Control Systems to combat stolen, fraudulent and counterfeit mobile phones: A Colombia case study*". March, 2018.**

   English:

   http://www.idclatin.com/qualcomm/index.html

   Español:

   http://www.idclatin.com/qualcomm/index-esp.html

ITU-D SG 2 - QUESTION 4/2
Workshop on Combating Counterfeit ICT devices

THANKS

HUGO ROMERO

hugo.romero@crcom.gov.co

+57 310 2101716

4th October, 2018