COMBAT TO THE USE OF STOLEN AND COUNTERFEIT ICT DEVICES

João Alexandre Zanon
National Telecommunication Agency – ANATEL – Brazil
ITU-T SG11 Vice Chairman
ITU-T Q15/11 Rapporteur

October 2018

ANATEL

Celular Legal Initiative - Summary

- **Objective:** Incentive the use of regular devices, orienting the population on the benefits of the initiative and combat the use of fraudulent devices in the country (stolen, tampered, with irregular unique identifiers and not certified).

  - **CEMI Module – "Cadastro de Estações Móveis Impedidas":** Block the use of stolen devices when requested by the user at the mobile operators or police.

  - **SIGA Module – "Sistema Integrado de Gestão de Aparelhos":** Identify and block other type of fraudulent devices, such as tampered, cloned or irregular unique identifiers and non-certified devices.

  - **Participants:** Coordinate by Anatel, with the participation of mobile operators, GSMA, ABR Telecom (Technical solution operator), manufactures and Polices.

Celular Legal Initiative – Legal Provisions:

- **All equipment's must be certified to be used on Brazil.**

  » Art. 162, §2º, of "Telecommunication General Law – LGT" (Law n.º 9.472/97).

  » Art. 20 of Anatel Certification Regulation (Res. n.º 242/00).

- **Operators must only activate certified equipment on their network.**

  » Art. 10º, V, of Mobile Service Regulation – RSMP (Res. n.º 477/07).

- **Users must only use certified equipment's and cannot tamper with then.**

  » Art. 4º, V, of Anatel Consumer General Regulation Regulation – RGC (Res. n.º 632/14).

- **Operators much combat fraudulent behavior on their networks.**

 » Art. 77 of RSMP (Res. n.º 477/07).

Celular Legal Initiative – Latest Actions :

- **Combat of Stolen devices:**

  – User can request the block of stolen devices direct with the Police.

  – Police can request the block of cargo and stores stolen devices (IMEI required).

  – It's not necessary to provide the IMEI when the user request the block.

- **Combat of Tampered, invalid unique identifiers and non-certified devices:**

  – **Awareness Campaign by Abinee:** From September-November 2016, about the importance of suing only certified devices.

  – **Celular Legal Hotsite -** http://www.anatel.gov.br/celularlegal: Collect all the information regarding the initiative, including the status tool.

  – **Status Tool:** A tool that allow the enduser to verify, thought the IMEI, if the terminal has any restriction (is stolen, has a tampered, cloned or invalid unique identifier).

- **Start of restrictive actions against fraudulent devices:**

  - February 2018: Start of restrictive actions, from feb/2018, against devices with tampered, cloned or invalid unique identifier.

  - September 2018: Start of restrictive actions on the provinces of phase 2.

4

CEMI Workflow – Stolen devices.
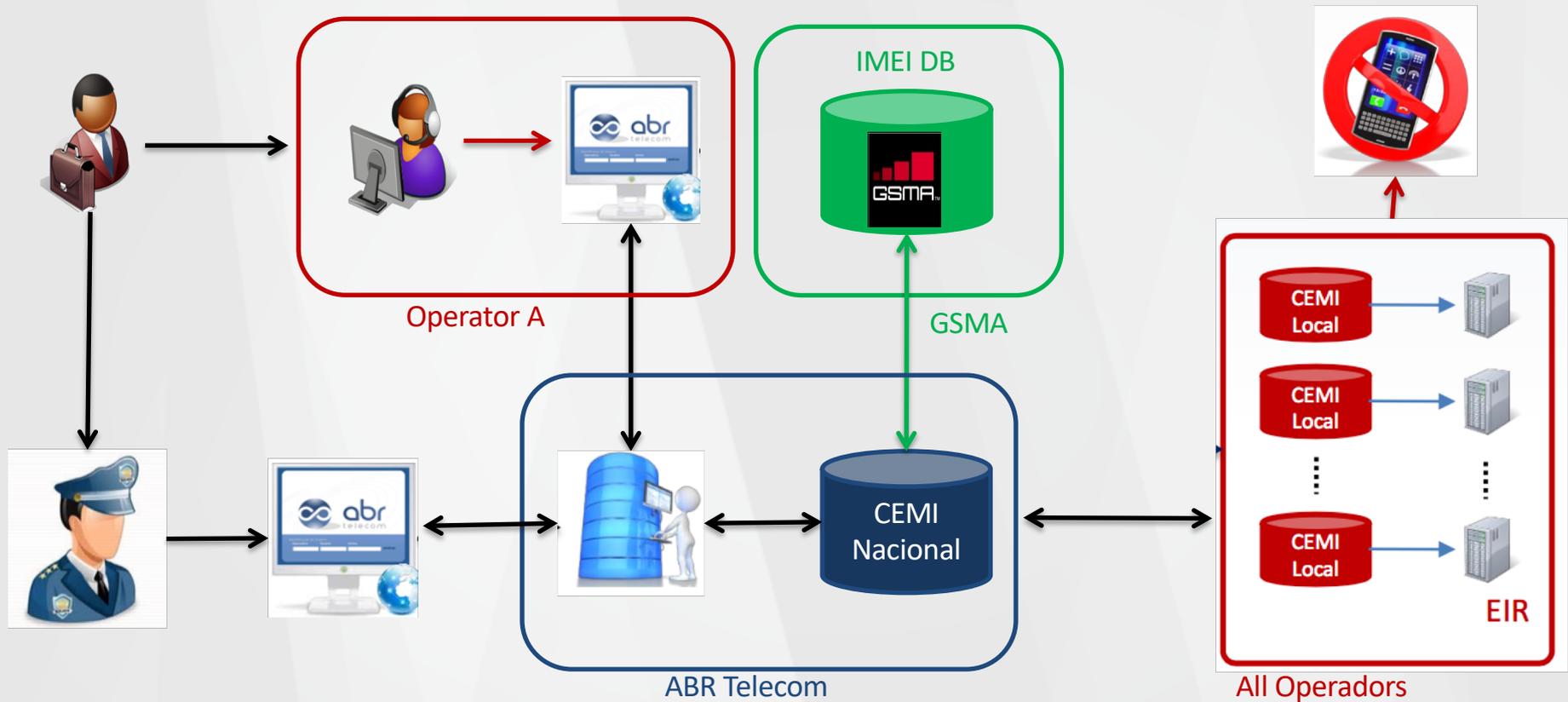
- User can request the block of stolen devices direct with the Police.
- Police can request the block of cargo and stores stolen devices (IMEI required).
- It's not necessary to provide the IMEI when the user request the block.

SIGA – Tampered, Cloned and invalid identifiers, non-certified devices.

- **Objetive :** Identify and block other type of fraudulent devices, such as tampered, cloned or irregular unique identifiers and non-certified devices.

  - Complement CEMI, since it's able to identify stolen devices that were included on the black list but were tampered to come back to the market.

  - Active since march 2014, collection information from all national operators.

  - Based on CDRs collected from all operators, able to identify in less than 24h and fraudulent devices connected to the network.

  - The hotsite "Celular Legal" has a tool that allow to check the status of a device based on IMEI. (www.anatel.gov.br/celularlegal).

- **Start of restrictive actions against fraudulent devices:**

  - Start of restrictive actions, from feb./2018, against devices with tampered, cloned or invalid unique identifier.

  - New irregular devices activated on the network are notified by SMS (in 24h, 25d 50d 75d) and after 75 days the terminal is blocked.

  - Pilot stated on feb./2018, with all country deployment until march 2019.

  - **Irregular users activated before feb./2018 will no be blocked.**

SIGA – Tampered, Cloned and invalid identifiers, non-certified devices.
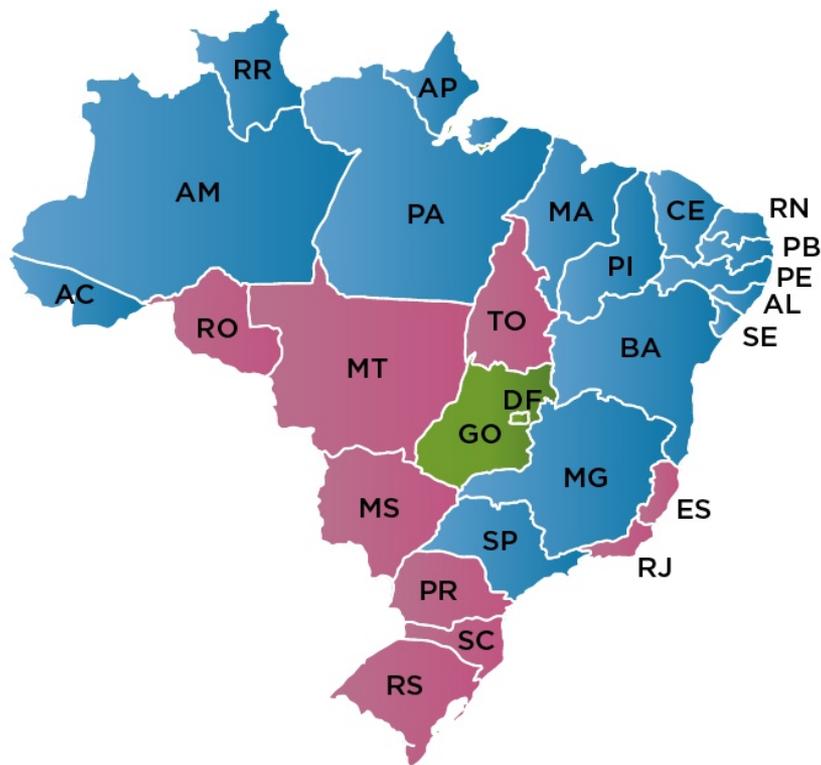
Pilot phase - Provinces in Green:
- **22/Feb/2018:** SMS to irregular devices.
- **9/May/2018:** Blocking of irregular devices.
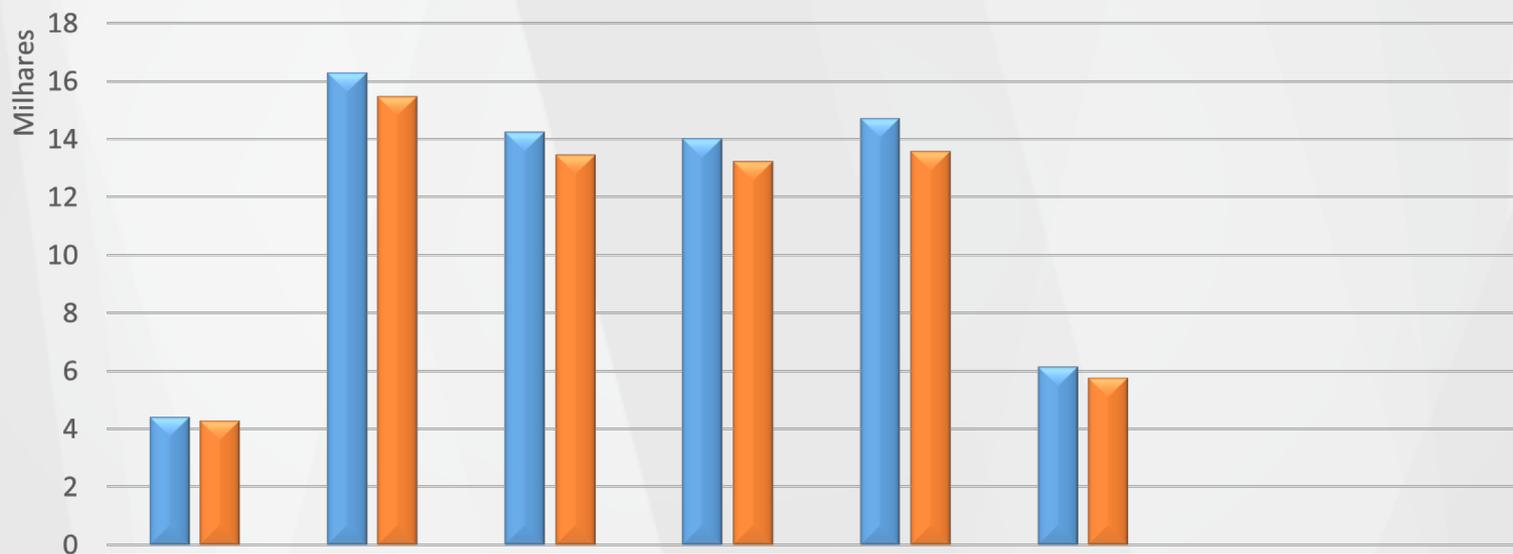
Phase 2 - Provinces in Pink:
- **23/Set/2018:** SMS to irregular devices.
- **8/Dec/2018:** Blocking of irregular devices.

Phase 3 - Provinces in Blue:
- **7/Jan/2019:** SMS to irregular devices.
- **25/Mar/2019:** Blocking of irregular devices.

SIGA – Statistics

- Total number of irregular devices blocked on the pilot phase until September 2018: **68.894**

	fev/18	mar/18	abr/18	mai/18	jun/18	jul/18	ago/18	set/18
CASOS	4.418	16.311	14.266	14.036	14.718	6.145		
Nº ACESSOS (MSISDN)	4.279	15.470	13.471	13.245	13.592	5.772		

Celular Legal Initiative – SIGA Pilot – Key Points:

- It's necessary to have a daily up-to-date reference database.

- Most of the cases are related to MSISDN that change the IMEI various times (ex. Some MSISDN have changed 1000 times in a month).

  - Possible fraud indication (simboxes) -> action is to block the MSISDN.

- Until now, Anatel have received low user complains.

  - Information campaigns are important to achieve this.

- Until now, cloned devices are identified but are not blocked.

  - Definition of a procedure to reduce the impact on the victim (the user that had it's devices unique identifier copied).

  Until now, its not possible to 100% sure diferentiate the victim from the cloner without physical verification of the device.

ITU-T SG11 Discussions – High Level Decisions:

- **PP-14 Decision:**
  - **PP-14 Resolution 188 (BUSAN, 2014):** "Combating counterfeit telecommunication/information and communication technology devices".
  - **PP-14 Resolution 189 (BUSAN, 2014):** Assisting Member States to combat and deter mobile device theft.
- **WTSA-16 Decisions:**
  - **WTSA-16 Resolution 96 (Hammamet, 2016):** "Studies for combating counterfeit telecommunication/information and communication technology devices".
  - **WTSA-16 Resolution 97 (Hammamet, 2016):** Combating mobile telecommunication device theft.
  - **Revision of ITU-T Resolution 2 (Hammamet, 2016):** ITU-T study group responsibility and mandates.

  ITU-T SG11 became the Lead study group on combating counterfeiting and the use of stolen ICT device.

- **Other Related SGs: ITU-T SG 5, 12, 17, 20 – ITU-D SG2 (Q4/2).**

ITU-T SG11 Discussions – Key challenges extracted from Resolutions:

- Developing Recommendations, technical reports and guidelines on combating the use for Counterfeit and Stolen Devices.

- Study existing as well as new reliable, unique, persistent and secure identifiers to assist on the combat of counterfeit and stolen.

- Methods of assessing and verifying identifiers used for purposes of combating counterfeit production.

- List of technologies/products, used for testing conformance with ITU-T Recommendations, in order to help in efforts to combat counterfeit ICT production

- Solutions to address the problem of tampering and duplication of unique identifiers.
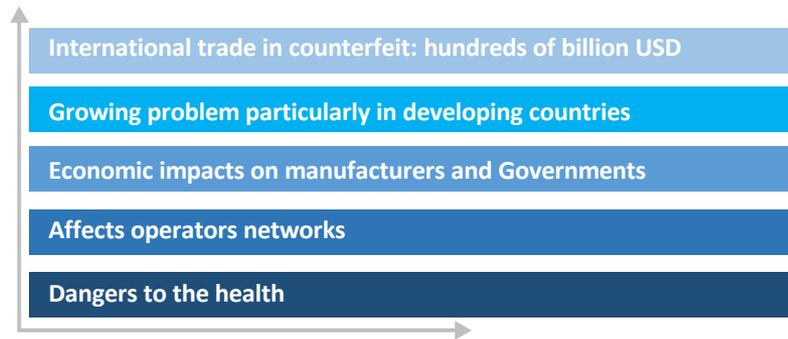
Combating Counterfeiting ICT Equipment

The Problem

- **PP-14 Resolution 188** (BUSAN, 2014): "Combating counterfeit telecommunication/information and communication technology devices"
- **WTSA-16 Resolution 96 (Hammamet, 2016):** "Studies for combating counterfeit telecommunication/information and communication technology devices"

International trade in counterfeit: hundreds of billion USD

Growing problem particularly in developing countries

Economic impacts on manufacturers and Governments

Affects operators networks

Dangers to the health

Past Events

Workshop on Combating counterfeit and substandard ICT devices *(November 2014)*

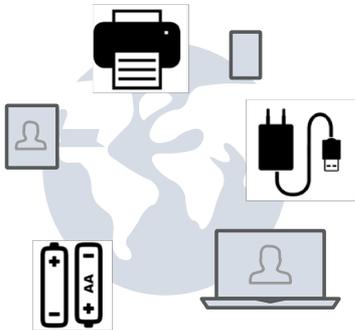Demo on a solution to combat Counterfeiting of ICT products based on the Digital Object Architecture *(April 2015)*

Workshop on Combating counterfeit using conformance and interoperability solutions *(June 2016)*

Regional Workshop on Africa - "Counterfeit ICT Devices, Conformance and Interoperability Testing Challenges in Africa". *(April 2017)*

2nd Regional Workshop on Africa - "Counterfeit ICT Devices, Conformance and Interoperability Testing Challenges in Africa". *(April 2018)*

COMPLETED WORK

Technical Report on "Counterfeit ICT Equipment" *(2014, rev. 2015)*

QTR-CICT:
Survey report on counterfeit ICT devices in Africa region *(02-2017)*

ON-GOING WORK

Q.5050 (ex. Q.FW_CCF) – Q.5050:

"Framework for solution to combat counterfeit ICT Device"

Draft TR-CF_BP:

"Technical Report - Guidelines on Best Practice and Solutions for Combating Counterfeit ICT Devices"

ITU-T SG11 Discussions – Combating Stolen Devices:

The Problem:
- **PP-14 Resolution 189 (BUSAN, 2014):** Assisting Member States to combat and deter mobile device theft.
- **WTSA-16 Resolution 97 (Hammamet, 2016):** Combating mobile telecommunication device theft.

Completed Work:
- **ITU-T X.1127 (2017):** Functional security requirements and architecture for mobile phone anti-theft measures (aka. Killswitch).

On-going Work:
- **Draft Recommendation Q.FW_CSM:** Framework for Combating the use of Stolen Mobile ICT Devices.

Events Related:
- ITU Workshop on Global approaches on combating counterfeiting and stolen ICT devices, 23 July 2018 (during next ITU-T SG11 meeting).
- Past Counterfeit workshop have also touched the combat of stolen ICT since the solutions to address both problems are related.

ITU-T SG11 Discussions – Q15/11 Strategic plan (2017-2020):

- Action plan for Implementation of WTSA-16 Res. 96 (Counterfeit) and 97 (stolen Devices) - (SG11-TD115R2/GEN):

  - **Division of the work in <u>four major blocks</u>, based on the Res. 2, Res. 96 and Res. 97:**

    1. Raise the awareness and promote the discussion;

    2. Coordinate the actions and collect information, within and outside ITU;

    3. Produce deliverable, such as Technical Reports and Recommendation;

    4. <u>Assist ITU members implement the deliverables and combat the use of counterfeit and stolen devices;</u>

- **Next actions regarding the combat of Counterfeit and Stolen ICT devices:**

  - Begin the determination process of Q.FW_CCF (July/2018).

  - Q.FW_CSM scheduled to be approved on Q1/2019.

  - Continuation of the Technical Reports on the Combat of Counterfeit ICT.

  - Creation of new work-items related (e.g the tampering/cloning of unique identifiers).

THANK YOU!

João Alexandre ZANON
zanon@anatel.gov.br

National Telecommunication Agency – ANATEL – Brazil
ITU-T SG11 Vice Chairman
ITU-T Q15/11 Rapporteur

ANATEL