Outcomes of the ITU Workshop

Global approaches on combating counterfeiting and stolen ICT devices

(23 July 2018, Geneva)

Appreciation

The workshop convener appreciated all speakers and moderators for their efforts and contributions in making this event successful.

The convener also expressed his appreciation for the two demos zones deployed by Rostelecom and SAP/DT/Camelot ITLab. These demos were used to visualize the DOA and Blockchain technologies to be used for combating counterfeiting and stolen ICT devices, which were presented at the workshop.

Council-17 and Council-18 decisions (1/2)

(C17/124, C18/107)

- **ITU Member States raised their concerns with regards to misuse of International Mobile Equipment Identity (IMEI) numbers**
- **Tampering with unique telecommunication device identifiers is a challenge faced by all members and an especially critical issue for developing countries**
- **Projects to build databases to store the IMEIs of mobile handsets and thereby prevent counterfeiting – would fail if the IMEI numbers changed or were duplicated**
- **Steps should be taken to guarantee that existing identifiers could be securely stored on devices and rendered tamper-proof, and to implement means of detecting clones and differentiating them from genuine devices**

Council-17 and Council-18 decisions (2/2)

(C17/124, C18/107)

- The problem needed to be tackled through a combination of country programmes and international cooperation initiatives, with the aim of at least ensuring that IMEI numbers were non-erasable and non-reprogrammable

- Resolution 97 (Hammamet, 2016) gave ITU-T a mandate to address tampering and non-reliability of unique identifiers

- Study Group 11, should therefore continue to develop Recommendations, technical reports and guidelines to address the problems posed by counterfeits, in accordance with Resolution 96 and Resolution 97 (Hammamet, 2016)

- Director of TSB to continue working on the issue with GSMA

Session 1. Current situation - Tampering of existing ICT identifiers

- **IMEI might be changed – there are plenty of tools** ***(India, Expresso, Rostelecom)***
- **Different stakeholders face some challenges to detect and control devices with altered/duplicated IMEI** ***(Colombia, Brazil, India).***
- **The tampering/Cloning of unique identifiers affect both the combat of counterfeit and stolen ICT (Brazil).**
- **Tampering and manipulation of ICT identifiers affect the functioning of operator's network** ***(Sudan).***
- **IMEI is not a universal identifier to be used in all ICT devices** ***(Rostelecom)***
- **India successfully showed Proof of Concept of CEIR system on one of it's telecom circle. Countrywide rollout is planned for next year. (India)*.***

Session 1. Actions, including potential new standardization activities to address tampering/duplication of existing ICT identifiers

- Vendors need to implement IMEI in non-erasable and non-reprogrammable ROM of mobile phones
- ITU Members are encouraged to submit contributions to ITU-T SG11 on different solutions to address tampering and cloning of existing ICT identifiers
- Blockchain-based approaches may increase the reliability of the existing identifiers, including IMEI
- Standardization for EIR - CEIR interface.

Session 2. Current situation – Combating stolen ICT devices

- **Tunis launched CEIR database for combating counterfeiting and stolen mobile devices *(Tunisia)***
- **No silver bullet, all stakeholders should be involved, at global level, engage law enforcement and custom, focusing on the source of the problem *(GSMA)***
- **There are several tools to be used to address mobile device theft across Latin America, including technical approaches (IMEI-blocking measures and kill switches) and policies *(TMG)***
- **Blockchain-based Global IMEI Storage could be open to accept other participants on top of mobile operators and in this way generate extra stimuli and incentives to deploy the solution globally *(SAP/DT/Camelot ITLab)***

Session 2. Actions, including potential new standardization activities to address combating stolen ICT devices

- Continue developing a global framework on combating stolen mobile devices

- Draw up a list of unique ICT identifiers to be used for combating mobile telecommunication device theft

- Identify approaches on how to increase reliability of unique ICT identifiers to be used for combating mobile telecommunication device theft.

- Study possible technologies as tools to combat the use of stolen mobile ICT.

- Study if the Demos during the workshop (on Blockchain and DOA) can assist in the combat of counterfeit and stolen ICT.

- Collaboration with other organization (SDOs, Police, Custom) is critical to the success of actions against stolen ICT.

Session 3 - Current situation – combating counterfeiting

- **The initiatives should be driven by regulatory agencies to combat the influx of counterfeit devices, including equipment audits, sales and installation licensing, factory audits based on ISO9001 and type approval process *(Nigeria)***

- **Along with the national regulatory framework, any proposed solution must be discussed with the appropriate participation and inclusion of all stakeholders such as governments, customs, enforcement, operators, device manufacturers, distributors, retailers, and the consumers *(Qualcomm, Nigeria)***

- **IMEI blocking system as a case study to combat counterfeit mobile phones. It might strengthen the argument for Governments to adopt similar schemes *(MWF)***

- **Counterfeit mobile devices usually have a lack of quality and performance and therefore, fail to comply with conformance requirements *(Rohde & Schwarz)***

Session 3 - Actions, including potential new standardization activities to address combating counterfeiting

ITU-T SG11 should focus on the following actions:

- develop methods of assessing and verifying identifiers used for purposes of combating counterfeit production

- develop mechanisms as appropriate for identifying counterfeit production

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

- develop regulatory framework for combating counterfeit (device registration, blocking, conformance assessment, etc.)

Conclusions - ITU-T SG11 is encouraged to:

- Study approaches on how to defend existing ICT identifiers against tampering/cloning of existing ICT identifiers.
- Draw up a list of unique ICT identifiers to be used for combating counterfeit and mobile device theft.
- Develop methods of assessing and verifying identifiers used for purposes of combating counterfeit and stolen devices.
- Continue to collaborate with other SDO on the combat of counterfeit and stolen ICT devices.
- Standardization for EIR - CEIR interface may be needed.
- Consider Blockchain-based technologies to address the tampering/cloning of existing ICT identifiers, combat counterfeiting and stolen ICT devices.
- Develop mechanisms as appropriate for identifying counterfeit production.
- identify a list of technologies/products, used for testing conformance with ITU Recommendations, in order to help efforts to combat counterfeit ICT production.
- Develop regulatory framework for combating counterfeit and device theft (device registration, blocking, conformance assessment, etc.)
- Incentivize collaboration between countries on combating counterfeiting and stolen devices
- Continue the collaboration with other relevant Study Groups in ITU-T and ITU-D in the combat of ICT and stolen devices.

All interested stakeholders (government, operators, device manufacturers, distributors, retailers) are encouraged to join ITU-T SG11 for discussions on the approach to address tampering, combat counterfeiting and stolen ICT.