WSIS FORUM 2021
Starting from January
Final Week 17-21 May 2021

OUTCOMES

1) **Title of your session**

   Combating counterfeit telecommunication/ICT devices and software

2) **Name of Organisation(s) organising the session**

   ITU-T Study Group 11 "Signalling requirements, protocols, test specifications and combating counterfeit products"

3) **Relevance with the WSIS Action Lines – please specify the Action Lines C1 to C11**

   - Combating counterfeiting ICT devices is the way to prevent its negative impact on network infrastructure (C2).
   - Combating counterfeiting of ICT devices/software is one of the tools to be used for consumer protection (C5).
   - Combating counterfeiting software is linked with combatting illegal and harmful content in the media (C9).
   - Combating counterfeiting is an international issue where all stakeholders need to be involved (C11).

4) **Did your workshop highlight any issues related to COVID-19? If yes, please explain.**

   No

5) **Key achievements, announcements, launches, agreements, and commitments**

   I. Combating counterfeiting of ICT devices is very actual and well-known issue worldwide. Despite the intensive work that has been done by ITU-T SG11, there are still some gaps that are crucial for achieving success and resolving this important issue, such as device authentication, effective control of device with cloned and tampered identifiers and EIR and CEIR standardized interfaces.

   II. The piracy and multimedia data misappropriation is a new trend which affects most of the countries. There is a need to develop a global solution to combat such challenge and raise awareness among audiovisual industry, operators, governments and consumers.

   III. Panelists committed to continue this relevant discussion in ITU and encouraged all to join ITU-T SG11 meetings and all related events.

6) Main outcomes highlighting the following:

I. Debated Issues

a. Tampered or counterfeit software and consequent data misappropriation

Based on the experiences shared by members looking at tampered or counterfeit software, and consequent data misappropriation (such as TV Piracy), it appears that there is no "silver bullet" and various solutions should be implemented together. There was a discussion aimed to identify key actions that membership should put in place in order to solve this problem and how ITU standardization activities could assist on this.

- Uruguay and Brazil stated that piracy or cybercrime is a multi-million dollar problem that generates great economic losses for the audiovisual industry and provokes serious risk related to cyber security privacy, which is a big challenge for operators, governments and consumers.
- The legal framework that protects the industry and consumers is among the measures, which member states currently deploy. Among other instruments, this kind of legislation allows regulator to stop the import and block of unauthorized/illegal devices (e.g., tampered satellite receivers), block certain suppliers of illegal content and implement certification process. However, regulations have not kept paced with the new technologies, meaning that certain activities that affect the sector remain “in limbo”.
- The second measure is to build coordination and cooperation between the public and private sector in order to seek specific solutions that facilitate addressing the problem.
- In general, the customer gets the content without assessing the consequences they may face afterwards. The customer’s end-device might be affected by spyware, data theft, uncontrolled remote access, to name but a few. Therefore, the third measure that needs to be put in place is to educate people and raise awareness about the problem as it may help to stop promoting the illegal practice.
- It was noted that the illegal content provider is not located in one particular country and therefore, the international collaboration is important to achieve a success.
- It was highlighted that, based on the contribution proposed by Brazil in March 2021, ITU-T SG11 started a new work which aim is to collect use cases on the combat of multimedia content misappropriation.
- All Member States are encouraged to share their experience on fighting against multimedia content misappropriation, which will be further used for developing a global solution.

b. Combating counterfeit and stolen ICT devices

Tracking of ICT products becomes a problem on the national level. The discussion focused on the measures that members states and industry put in place to stop the circulation of counterfeit and/or stolen ICT devices.

- Colombia and Mauritania highlighted their experience on combating counterfeiting and stolen ICT devices. It was noted that countries loss the revenue of the smartphones sales due to counterfeit. For example, it was indicated that the European market lost around 45.3 billion Euro over 2015.
- It was highlighted that the system implemented in Colombia blocks stolen ICT devices checking the IMEIs on different criteria. As of today, the subscriber database in Colombia contains 62 million entries for 8 million population. The positive list contains 116 million IMEIs with relevant owner's ID while negative list contains 25 million of blocked IMEIs (60% non-registered, 16% invalid and 7% duplicated). However, there is a problem with the registration of new devices in the positive list for devices which were bought in Internet or brought from abroad. Moreover, this problem also applies for devices connected to different networks in one or more countries. IMEI alteration is another issue as there is a wide margin of error caused to identification which equipment is genuine or original and which one has been altered or tampered. In this regard, Colombia highlighted the importance of the standardization of measures and tools, which would help to stop IMEI alteration.
- Mauritania pointed out that sometimes the counterfeit and tampered devices may be more affordable than the genuine one. However, the counterfeit devices bring some negative impact on human health, the security issues, consumer privacy issues, the quality of networks and services, revenue loss and so on. Therefore, from this perspective, it is important to establish regulatory and technical framework to combat proliferation of counterfeit products. Mauritania suggested to establish a legal framework, C&I regime and establish a solid cooperation between all stakeholders at the regional level.
- Also, all panellists highlighted the importance of raising awareness about this challenge. There is a need of global cooperation in order to exchange information among all countries on stolen mobile devices.
- Svyazcom (Russian Federation) highlighted the importance of having standardized interface between EIR and CEIR, as it may help to save 40-50% of time and resources as well as 20-30% of costs for building and deploying the solution.

- The Global Voice Group (Cape Town) highlighted that it is estimated that between 10 to 20% of the mobile devices connected to the African telecom networks are counterfeit and the number continues to grow. The Global Voice Group also proposed using digital certificates for identification of the terminals and the blockchain technology may become one of the solutions to identify devices on the network.
- The Moderator highlighted that ITU Conformity Product Database might become a tool to facilitate combating counterfeiting.
- Qualcomm (United States) pointed out that illegal devices are other forms of fraud and therefore the mechanisms to commit that crime is essentially similar to the one applied for counterfeit and stolen devices. The regulatory framework is obviously very important. Along with other measures such as type approval or device certification the regulation should also require mandatory device registration at the national level. The registration system should allow regulator or the government to be able to access and analyse the data from mobile networks.
- The technical framework should be in place as well. It should grant amnesty to existing devices which were already in place. However, for the time being, there is no device authentication and currently, all we have is subscriber authentication.
- Also, it was noted that Open-Source projects should be encouraged for implementing such solutions.
- As kind of measures, it was proposed to study within SG11 the potential approach on creation of device authentication mechanisms and its implementation on the networks.
- ITU-T SG11 developed and continue working on several standards which define frameworks on combating counterfeiting and stolen ICT devices. All members are encouraged to contribute to the following SG11 meeting on the topics and proposals highlighted at this session.

II. Quotes

- **Mrs Mercedes Aramendía (President of the Uruguayan Regulatory Unit of Communication Services (URSEC), Uruguay):**
  "The piracy or cybercrime practice can be carried out from anywhere globally. So, collaborating at regional and international level is essential to share information, techniques and seek global solution is increasingly relevant."

- **Mr Cheikh Tidjani Oudaa (Head of technical department of Autorité de Régulation, Mauritania)**
  "In order to combat counterfeiting, it is important to conclude the mutual recognition agreement between countries for conformity assessment and market surveillance."
- **Mr Mohammad Raheel Kamal (Senior Director of Qualcomm, United States)**
  "There is a need a public consultation among the ministries, the governments, the customs, the importers, the manufacturers and consumers implementing a system on combating counterfeiting and stolen ICT devices."

III. Overall outcomes of the session highlighting

- According to the discussion, it is proposed that ITU-T SG11 should:
  i. start new work items on: device authentication; EIR-CEIR standardized interface;
  ii. conduct open discussion among different stakeholders on implementing system standardized by ITU on combating counterfeiting and stolen ICT devices/software;
  iii. collect use cases on the combat of multimedia content misappropriation and further develop standards and technical report to address this problem.

7) Main linkages with the Sustainable Development Goals (please specify the SDGs)

Vendors lose their revenues due to large market of counterfeit devices, while network operators face the challenges on growth of connected counterfeit devices which decrease QoS on their networks (SDG9).

8) Emerging Trends related to WSIS Action Lines identified during the meeting

The implementation of systems combating counterfeit and stolen ICT devices all over the world will mitigate the number of counterfeit or illegal devices connected to the network which will definitely reduce the negative impact of such devices on the network infrastructure.

9) Suggestions for Thematic Aspects that might be included in the WSIS Forum 2022

Authentication of ICT devices aiming to facilitate combating counterfeit and stolen ICT devices