Question 17/11 – Combating counterfeit or tampered telecommunication/ICT software

(Continuation of Question 17/11)

1 Motivation

ITU Resolution 188 (Rev. Dubai, 2018) of the Plenipotentiary Conference, recognizing the adverse impact of counterfeit telecommunication/ICT devices on governments, manufacturers, vendors and consumers and aware that tampering with telecommunication/ICT devices may diminish the effectiveness of solutions adopted by the countries to address counterfeiting, invites Member States to take all necessary measures to combat counterfeit telecommunication/ICT devices.

At the same time, Resolution 96 (Hammamet, 2016) of World Telecommunication Standardization Assembly recognizes that counterfeit and tampered telecommunication/ICT devices negatively impact on security and privacy for users and impose adverse impact on governments, manufacturers, vendors, operators and consumers such as the loss of revenues, erosion of brand value/intellectual property rights and reputation and network disruptions.

Moreover, ITU Resolution 189 (Rev. Dubai, 2018) of the Plenipotentiary Conference, on the combat of mobile devices theft, recognizing that device theft can have a negative impact on users' data and on their sense of security and confidence in the use of information and communication technologies (ICTs), resolves to explore and encourage the development of ways and means to continue to combat and deter mobile device theft, and invites Member States to adopt the necessary actions to prevent, discover and control tampering and replication of mobile ICT device identifiers.

Resolution 97 (Geneva, 2022) of World Telecommunication Standardization Assembly recognizes that the theft of user-owned mobile devices may lead to the criminal use of telecommunication/ICT services and applications, resulting in economic losses for the lawful owner and user; indicates the necessity to identify existing and future technological measures, both software and hardware, to mitigate the consequences of the use of stolen mobile devices.

ITU-T Study Group 11 received contributions from ITU Member States and Sector members that led to the approval of Recommendation ITU-T Q.5050 "Framework for solutions to combat counterfeit ICT devices" and Recommendation ITU-T Q.5051 "Framework for Combating the use of Stolen Mobile Devices". In addition, a number of new work items were agreed.

At the same time, some contributions suggested the need to address some new scenarios, such as:

(i) The tampering with stolen mobile device software in order to achieve unauthorized access to the user data with consequent impacts.

(ii) Counterfeit/tampered network devices (such as routers or switches) that has backdoors access to the user network, allowing data theft and consequent revenue loss.

(iii) Counterfeit/tampered Paid TV receivers with tampered software that allow unauthorized access to the content provider data by non-subscribers.

There is no simple solution for this topic, since in general the telecommunication/ICT user is unaware of the vulnerabilities that are included on counterfeit devices or can be present with the counterfeit or tampered ICT software. Therefore, is critical to raise the awareness of all stakeholders regarding this topic.

Therefore, this Question intends to explore appropriate possibilities to combat counterfeit or tampered ICT software. Cooperation among ITU-T study groups, between ITU-T and ITU-D as well as with external bodies outside the ITU (in particular with SDOs), will be required to gather a complete information and understanding on the subject including the organization of seminar/workshops in collaboration with stakeholders. Coordination among relevant organizations is also necessary to fulfil these tasks.

2 Question

Study items to be considered include, but are not limited to:

– What are the adverse impacts to the stakeholders due to the use of counterfeit telecommunications/ICT devices or devices with tampered or counterfeit software, and consequent data misappropriation?

– What kind of adverse impacts could counterfeit telecommunication/ICT and or regular devices with tampered telecommunication/ICT software impose on telecommunication/ICT stakeholders (such as the user and service provider), in particular with regard to data misappropriation?

– What Technical Reports and Guidelines are needed to raise awareness of the problem of telecommunication/ICT software tampering, telecommunication/ICT data misappropriation and the concerns they pose?

– What kind of Recommendations, Supplements, Technical Reports and Guidelines should be developed to assist ITU Members, in cooperation with ITU-D Sector, on combating counterfeit or tampered telecommunication/ICT software, theft misappropriation and the concerns they pose?

– What kind of Recommendations, Technical Reports and Guidelines should be developed to mitigate ICT data misappropriation, in special the user data contained on ICT devices and content delivered by ICT service providers?

– What technologies and solutions may be used for combating counterfeit or tampered telecommunications/ICT software and its adverse impacts?

– Can conformity assessment schemes be used to combat counterfeit or tampered ICT software?

3 Tasks

Tasks include, but are not limited to:

– study the adverse impacts to the stakeholders due to the use of counterfeit telecommunications/ICT devices or devices with tampered or counterfeit software, and consequent data misappropriation;

– study relevant and appropriate technologies and solutions that can be used to combat counterfeit or tampered ICT software, consequent data misappropriation and other adverse impacts;

– develop Recommendations, Supplements, Technical Reports and Guidelines to assist ITU Members, in cooperation with ITU-D Sector, on combating counterfeit or tampered ICT software and data misappropriation and its adverse impacts;

– organize workshops and events across ITU regions, in cooperation with the ITU-D Sector, to promote the work of ITU-T in this field and involve stakeholders;

– study possible conformity assessment schemes to combat counterfeit or tampered ICT software and data misappropriation, taking into account the activities of the ITU-T CASC;

– study results achieved by various international standardization bodies and develop technical specifications to feed the standardization work of the Question.

An up-to-date status of work under Q17/11 is contained in the SG11 work programme (https://www.itu.int/ITU-T/workprog/wp_search.aspx?sp=17&q=17/11).

4 Relationships

Resolutions:

– Resolution 188 of the Plenipotentiary Conference (Rev. Dubai, 2018) "Combating counterfeit telecommunication/information and communication technology devices";

– Resolution 189 of the Plenipotentiary Conference (Rev. Dubai, 2018) "Assisting Member States to combat and deter mobile device theft";

– Resolution 96 of the WTSA (Rev. Hammamet, 2016) "ITU Telecommunication Standardization Sector studies for combating counterfeit telecommunication/information and communication technology devices";

– Resolution 97 of the WTSA (Rev. Geneva, 2022) "Combating mobile telecommunication device theft".

Recommendations:

– ITU-T X.1127, ITU-T Q.5050, ITU-T Q.5051

Questions:

– All Questions of SG11, especially Questions relating to control, signalling architectures, protocols, conformance and interoperability testing, combating counterfeit and stolen ICT

Study Groups:

– ITU-T SG2

– ITU-T SG3

– ITU-T SG9

– ITU-T SG13

– ITU-T SG16

– ITU-T SG17

– ITU-T SG20

– ITU-D SG1 and SG2

Other bodies:

– ETSI

– IEC

– IEEE

– IETF

– ISO/IEC JTC 1

WSIS action lines:

– C2, C5, C9, C11

Sustainable Development Goals:

– 9