Combating counterfeit and stolen telecommunication/ICT devices and tampered software

Episode 1: Existing challenges and solutions on combating counterfeiting of ICT devices

Q&A Transcript

(15 February 2023, https://itu.int/go/WB-CS-01)

#	Question	Answer	Response provided by
Q1	How quickly a clone is detected after it appears?	*It's periodic. It depends on the MNO – how often they share the data*	**Biren Karmakar, C-DOT** biren[at]cdot.in
Q2	How many IMSIs could be allowed to be used with one IMEI in India?	*More than one IMSI on single IMEI is detected as duplicate, but SIM change is identified and allowed.*	**Biren Karmakar, C-DOT** biren[at]cdot.in
Q3	Is the CEIR hosted and administered by the regulator? Was it built in-house, or was it procured from an outside vendor?	*With regard to India case, CEIR is owned by Department of Telecommunication, Government of India. It's designed and developed in-house by C-DOT.*	**Biren Karmakar, C-DOT** biren[at]cdot.in
		Normally, it is hosted and administered by the regulator, but it can be offered as a managed service as well.	***Evgeny Zababurin, SC.Soft*** zababurin[at]soft.sc
Q4	So, in India, what are the challenges of allowing/authenticating/verifying/registering/maintaining existing clowned/duplicated IMEI on the CEIR while combating counterfeit and illegal ICT devices?	*It is highlighted in the presentation, see last slide.*	**Biren Karmakar, C-DOT** biren[at]cdot.in

#	Question	Answer	Response provided by
Q5	What are the most challenges that India has during the implementation of lost and stolen mobile devices blocking services?	*Kindly refer to the last slide of presentation. The details can be provided offline.*	**Biren Karmakar, C-DOT** biren[at]cdot.in
Q6	Does this mean that every time the user wants to change the SIM card, he needs to confirm it? By SMS?	*Yes, this is one of the options*	**Biren Karmakar, C-DOT** biren[at]cdot.in
Q7	If a counterfeit device is transferred to another country, is it possible to detect this device without the help of manufacturer?	*If the device is moved out from the country, as of now, it cannot be tracked until international-CEIR is deployed. It should be used for sharing the data among neighboring countries.* *In general, the international cooperation would be the way forward. It can be done through collaboration among neighboring countries or via implementing EIR/CEIR on different levels as defined in ITU-T Q.5052.*	**Biren Karmakar, C-DOT** biren[at]cdot.in
		There is a GSMA Blocked Devices Database, but we can't see that it is widely used. So, in general, if CEIR is implemented in one country - the counterfeit devices are expulsed, and start being used in the neighboring countries.	**Evgeny Zababurin, SC.Soft** zababurin[at]soft.sc

#	Question	Answer	Response provided by
		In general, the cooperation between multiple stakeholders and above the national level is required. There is a need global collaboration, on regional and international levels.	
		According to best practices highlighted in ITU-T Suppl.75, some countries consider implementation of CEIR in order to tracking the stolen or counterfeit mobile devices in the region (e.g. East Africa case). All ITU members are encouraged to contribute to ITU-T SG11 highlighting new initiatives on this matter deployed in different regions.	**James Kunle Olorundare, NCC** olorundarek[at]ncc.gov.ng
		Definitely, there is a need to build an international cooperation on this matter. Maybe, it can be the regulatory authority tasks of particular countries where they can form a consortium and try to tackle this issue.	**Venkatesh Gajendran, R&S** gajendran.venkatesh[at]rohde-schwarz.com

#	Question	Answer	Response provided by
		This was a topic of discussion on PP-22 and for sure the CEIR is a key issue. Probably, we should look at its implementation on regional and international levels.	**João Alexandre Moncaio Zanon, ANTEL** zanon[at]anatel.gov.br
Q8	How can we detect the right IMEI especially when the clone device IMEI registered in network first?	*Yes, it can be detected through device authentication.*	**Biren Karmakar, C-DOT** biren[at]cdot.in
		There is a number of techniques available. One of them is device authentication, another - is device "normal" usage, and one more - usage of legitimate triplets, or injection of an extra level of verification like National ID linked to the IMSI.	**Evgeny Zababurin, SC.Soft** zababurin[at]soft.sc
Q9	What is the mechanism of IMSI change detection for an authentic device?	*IMSI changes are allowed, no limit imposed. But identified with big data analysis of the system.*	**Biren Karmakar, C-DOT** biren[at]cdot.in

#	Question	Answer	Response provided by
	Is the deployed system restricted with few exceptions for an authentic device or any other method used to allow only authentic devices?	*It is an excellent question and a very requested feature. It can be a revenue generator for regulators and the MNOs. Especially in the context of 2-factor authentication or/and confirmation of an authentic device in use.*	**Evgeny Zababurin, SC.Soft** zababurin[at]soft.sc
Q10	But if I want to use my phone with many SIM cards and/or share it with my relatives? Do I always need to confirm?	*It depends on the policy of the national regulator. You can lock the triplet (IMEI-IMSI-MSISDN) or duplet (IMEI-IMSI) and allow only the usage of one pair/triplet. You can limit the use of one IMSI with a predefined number of IMEI (predefined number or number of IMEIs per certain period of time (month, year, etc.) You can notify all new bindings (USSD, SMS) and request them for an action (you to define).*	**Evgeny Zababurin, SC.Soft** zababurin[at]soft.sc
Q11	Why other departments, a part of Telecommunication Authority India, want to access the CEIR, if CEIR is accessible to	*Yes - by Law Enforcement Agencies.*	**Biren Karmakar, C-DOT** biren[at]cdot.in

#	Question	Answer	Response provided by
	other departments may be the security breaching issues will be faced by the country?	*There are many stakeholders and many interests. You can design the CEIR so everyone can have their own level of access to the data (via API) and contribution to the database(s).*	**Evgeny Zababurin, SC.Soft** zababurin[at]soft.sc
Q12	Can you elaborate on the IMSI change mediums available for the general public. Either it is a USSD service or web portal, or does a person need to request regulator?	*USSD, Portal and SMS.*	**Biren Karmakar, C-DOT** biren[at]cdot.in
		IVR menu, offline offices (post offices), white retailers, etc. It depends on the national legislation and policies created by the regulator.	**Evgeny Zababurin, SC.Soft** zababurin[at]soft.sc
Q13	Why is GSMA charging the regulators the use of the IMEI database? With the prices they have, it is impossible for a regulator to implement an IMEI Check page for the consumer	*I can't speak on behalf of GSMA being not a part of it but yes, you can build the national IMEI Check page. Please see an example of it: https://uzimei.uz/.*	**Evgeny Zababurin, SC.Soft** zababurin[at]soft.sc

#	Question	Answer	Response provided by
		If I'm not mistaken the whitelist and blacklist can be made available to regulators without cost. Colombia manages to get like this and the same in Brazil. The base that they charge is the extended whitelist (DEVICEMAP). But maybe they have changed.	**João Alexandre Moncaio Zanon, ANTEL** zanon[at]anatel.gov.br
Q14	Can the CEIR access only to LEA?	*LEA including police and regulator. Stakeholders are highlighted in the presentation.*	**Biren Karmakar, C-DOT** biren[at]cdot.in
Q15	Is there a charge for using the Device Verification by any entity either the Mobile Operators or the regular public?	*Subscribers need to get their duplicate device verified.*	**Biren Karmakar, C-DOT** biren[at]cdot.in
Q16	I am interested in the type of approval test kit. Can it be used to test ICT devices and equipment apart from mobile phones?	*Yes, ICT devices, cellular & non-cellular devices can be tested.*	**Venkatesh Gajendran, R&S** gajendran.venkatesh[at]rohde-schwarz.com

Combating counterfeit and stolen telecommunication/ICT devices and tampered software

Episode 1: Existing challenges and solutions on combating counterfeiting of ICT devices

#	Question	Answer	Response provided by
Q17	Kindly provide some more details on the IMEI Testing and verification?	*Details will be shared offline.*	**Venkatesh Gajendran, R&S** gajendran.venkatesh[at]rohde-schwarz.com
Q18	Device registration is an interesting concept for CEIR implementation but is also device owner registration necessary to counterfeit stolen devise?	*It depends on the policies implemented by the regulator. Either applied to end-users or to bulk-importers, retailers, and MNOs.*	**Evgeny Zababurin, SC.Soft** zababurin[at]soft.sc
Q19	Whether implementation of CEIR in India helped to reduce circulation of counterfeit and stolen devices? Any statistic/numbers?	*Initially, there were plenty of stolen devices but after CEIR deployment in 2019 this number got reduced. There is public awareness on this issue and public knows that if it is reported as stolen it will be blocked and will not be used on mobile network all over the country.*	**Biren Karmakar, C-DOT** biren[at]cdot.in

#	Question	Answer	Response provided by
		There is another case on deployment CEIR in Uzbekistan in 2019. The initial statistics was about 98.5% of the imported devices has been illegal and were not declared. After one-year term it was totally opposite – 98.5% became legal while 1.5% remains illegal. It was done due to amnesty which regulator put in place and some awareness programmes setup in Uzbekistan.	**Evgeny Zababurin, SC.Soft** zababurin[at]soft.sc
		In Brazil, the deployment of system detecting counterfeit/stolen mobile phones in 2018 is very effective. Since then, the percentage of circulating counterfeit devices in Brazil is getting 65% down.	**João Alexandre Moncaio Zanon, ANTEL** zanon[at]anatel.gov.br
Q20	Whether EIR/CEIR can be a solution for different ICT devices but not for mobile phones only?	*Yes, indeed, EIR/CEIR can be used for tracking any type of ICT devices.*	**Evgeny Zababurin, SC.Soft** zababurin[at]soft.sc

#	Question	Answer	Response provided by
Q21	How India achieved its goal without impacting operator revenue?	*I don't think there is a loss of revenue of the operators as the devices being replaced, not the subscribers.*	**Biren Karmakar, C-DOT** biren[at]cdot.in
Q22	Is GMSA CEIR (IMEI DB) solution and device check API most effective?	*According to our experience, it is global and effective database.* *But, it is populated by the manufacturers which are GSMA members only. So, non-members are not represented there. It is good, except that it might be a bit slow and some information is missing.*	**Evgeny Zababurin, SC.Soft** zababurin[at]soft.sc
		GSMA allocates TAC to particular manufactures which may not produce one million number of handsets, so chance are there that un-used IMEIs could be misused. So, it cannot give the actual picture and therefore, from this database the actual counterfeit cannot be detected. *Other issue is that GSMA has Global blocklist, till now it is not shared/participated by all the countries.* *Therefore, when all countries will participate in Global*	**Biren Karmakar, C-DOT** biren[at]cdot.in

#	Question	Answer	Response provided by
		Block list, it may be effective for combating counterfeiting.	
		It is not the only solution that is available on the market. There are other solutions that maybe deployed. A very good example is a digital object architecture which also might be used for solving counterfeiting issues. Therefore, we need to look through other solutions as well.	**James Kunle Olorundare, NCC** olorundarek[at]ncc.gov.ng
Q23	Could the GSMA IMEI be used in type approval process, like it is used in UAE?	GSMA does not store complete IMEI, but yes, GSMA TAC is included for type approval.	**Biren Karmakar, C-DOT** biren[at]cdot.in
		It is advisable to add conformity assessment procedure in which laboratory tests such as Specific Absorption Rate, RF Tests, EMC tests are conducted for the purpose of type approval.	**James Kunle Olorundare, NCC** olorundarek[at]ncc.gov.ng