POLICY FRAMEWORK AND RECOMMENDATIONS TO MINIMIZE THE USAGE OF SUBSTANDARD, COUNTERFEIT AND STOLEN MOBILE COMMUNICATION DEVICES

Amila Prasanna Saputhanthri

(158486D)

Degree of Master of Science

Department of Electronic and Telecommunication Engineering

University of Moratuwa

Sri Lanka

December 2019

POLICY FRAMEWORK AND RECOMMENDATIONS TO MINIMIZE THE USAGE OF SUBSTANDARD, COUNTERFEIT AND STOLEN MOBILE COMMUNICATION DEVICES

Amila Prasanna Saputhanthri

(158486D)

Thesis submitted in partial fulfillment of the requirements for the degree Master of Science in Telecommunication

Department of Electronic and Telecommunication Engineering

University of Moratuwa

Sri Lanka

December 2019

DECLARATION

I declare that this is my own work and this thesis does not incorporate without acknowledgement any material previously submitted for a Degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant permission to University of Moratuwa, the non-exclusive right to reproduce and distribute my thesis, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

Signature: Date:

The above candidate has carried out research for the Masters Dissertation under my supervision.

Name of the supervisor: Eng. A.T.L.K. Samarasinghe

Signature of the supervisor: Date:

ABSTRACT

Telecommunication sector is one of the technologically advanced sectors, globally. The mobile device market is always growing and it is very competitive. Counterfeit and substandard devices are collectively known as black market devices. Availability of black market and stolen mobile devices is a global issue.

When buying a mobile device, most of the people focus on cost, brand and model. The important factors that represent the standard of mobile devices such as validity of International Mobile Equipment Identity (IMEI) and the Specific Absorption Rate (SAR) value are neglected.

It is important to adhere to a proper policy framework and introduce systems such as Equipment Identity Registers (EIRs) to minimize the usage of black market and stolen mobile communication devices. Mobile device blocking and regulation have become difficult tasks due to the unavailability of proper systems and policies. This has allowed stolen and black market mobile device usage.

As per the user survey conclusions, it was identified that user behavior patterns, limitations of existing EIR and prevailing policies should be changed to address the issue.

A policy framework that includes the steps of increasing user awareness, establishing a proper blocking mechanism and adding reforms to regulations is recommended as a solution.

ACKNOWLEDGEMENT

It is with great pleasure that I take this opportunity to convey my sincere thanks to the Department of Electronic and Telecommunication Engineering, University of Moratuwa, Sri Lanka for giving me the opportunity to participate in the Master of telecommunications course.

I would like to convey my special gratitude towards Eng. A.T.L.K. Samarasinghe (Senior Lecturer, Department of Electronic and Telecommunication Engineering) for providing me with valuable supervision and support throughout my research project. Further, I would like to thank Ms. Tharalika Livera, Deputy Director for Compliance (Surveillance & Quality of Service) of the Telecommunications Regulatory Commission of Sri Lanka (TRCSL) for providing information regarding the existing regulations and issues.

Finally, I would like to extend my gratitude towards all the lecturers, telecom service providers, my batch mates and all the others who helped me on this research project.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

Abbreviation	Description
GSMA	Global System for Mobile communications Association
SIM	Subscriber Identity Module
4G	4th Generations
5G	5th Generations
QoS	Quality of Service
OECD	Organization for Economic Co-operation and Development
MMF	Mobile Manufacturers' Forum
TRCSL	Telecommunication Regulatory Commission of Sri Lanka
ITU	International Telecommunication Union
IMEI	International Mobile Equipment Identity
SAR	Specific Absorption Rate
3GPP	3rd Generation Partnership Project
PTA	Pakistan Telecommunication Authority
CEIR	Central Equipment Identity Register
EIR	Equipment Identity Register
MSC	Mobile Switching Center
IMSI	International Mobile Subscriber Identity
DB	Data Base
GUI	Graphical User Interface
VIP	Very Important Person
DR	Disaster Recovery
OS	Operating System

CHAPTER 1: **INTRODUCTION**

1.1 Overview of mobile industry

The mobile industry worldwide is serving over 5 billion unique mobile subscribers, according to the data from the Global System for Mobile communications Association (GSMA) Intelligence [1]. So, the telecommunication ecosystem which includes the subscribers, operators and communication device manufacturers is critical to the world as it serves more than two third of the world's population.

When Sri Lankan context is considered, there are over 28 million mobile connections in the country and the population penetration of total SIM (Subscriber Identity Module) penetration is over 100%. The Table 1 provides the exact figures relevant to mobile device penetration.

Table 1: Telecommunication data summary of Sri Lanka as of May 2018

Topic	**Value**
Number of mobile connections	28.1 million
Population	20.9 million
SIM penetration	135%

Source: [1], [2]

As per Figure 1, the mobile subscriber growth in the country has now reached to a saturated level.

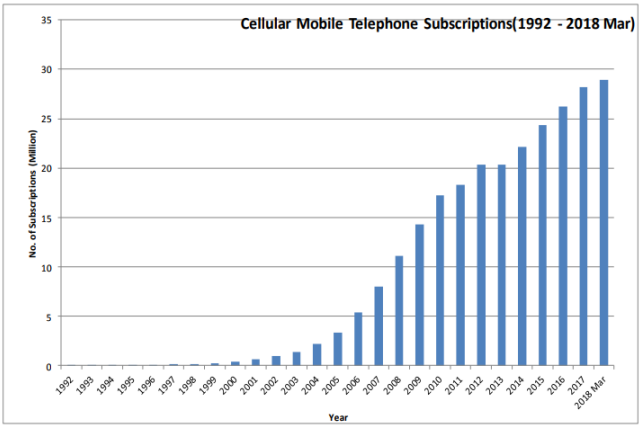

Figure 1: Mobile subscriber growth in Sri Lanka

Source: [2]

The statistics shown in Table 1 and Figure 1 indicate that there is very high demand for mobile devices in the country and almost every person is having a mobile device. The mobile device market is always growing and it is very competitive. The below given statistics show that the illegal or unlicensed devices have become a very serious issue worldwide. It's been identified that one out of every five cell phones sold in the world are illegal or unlicensed copycats – Nokia, 2011 [5] and shipments of grey-market China-made cell phones reached their peak in 2011 with a total of 250.4 million - IHS iSuppli, July 2013 [5]

The global mobile traffic growth predictions shown in Table 4 indicates a 60% worldwide mobile data traffic growth in between the 1st quarter of 2015 and 1stquarter of 2016. But the voice traffic is expected to be almost constant throughout the considered period.

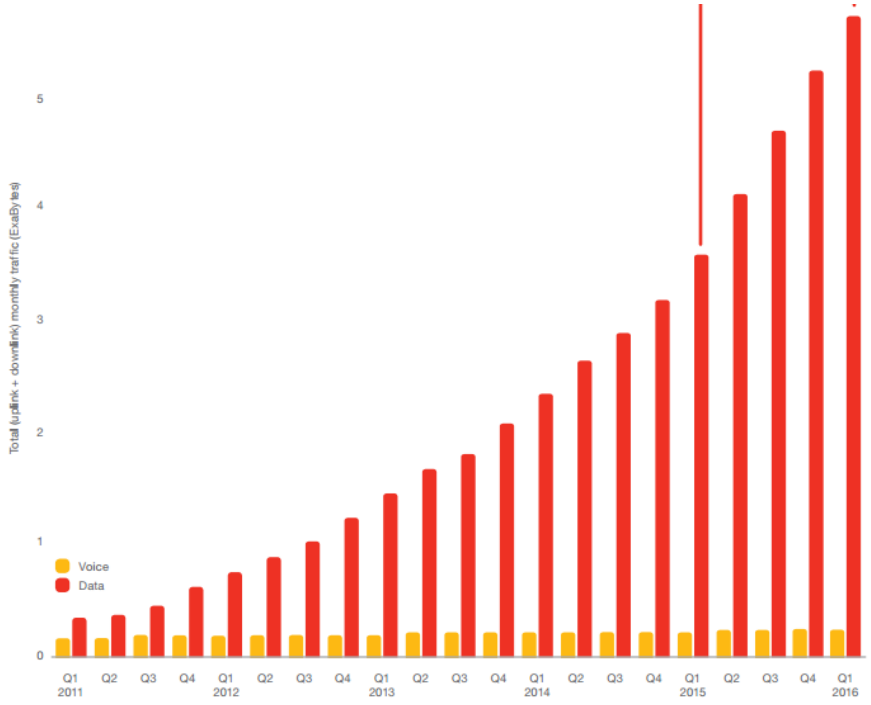

Figure 2: Global mobile traffic growth

Source: [6]

The capabilities of the mobile devices are at a very high level and to cope up with the highly advanced world, people will need to adapt to those new technologies. When compared with the global predictions of mobile traffic shown in Figure 2, Sri Lanka

also follows the same trend as per Figure 3. Therefore, the requirement for high end mobile devices with advanced technological capabilities is increasing.

The quality of the telecom service depends on the telecom ecosystem. Mobile devices are one of the major contributors for the quality of the service perceived by customers. If the devices are not made by following proper standards, then the efforts of the operators to provide a good service with the support of new technologies such as 4G (4th Generation) and 5G (5th Generation) will be in vain. As shown in Figure 3 below, the Sri Lankan mobile broadband penetration follows the same world trend. The users are focusing more on high end data services. Hence to provide them with the necessary QoS (Quality of Service), it is essential to regulate the mobile devices available in the market to guarantee the quality of those devices.

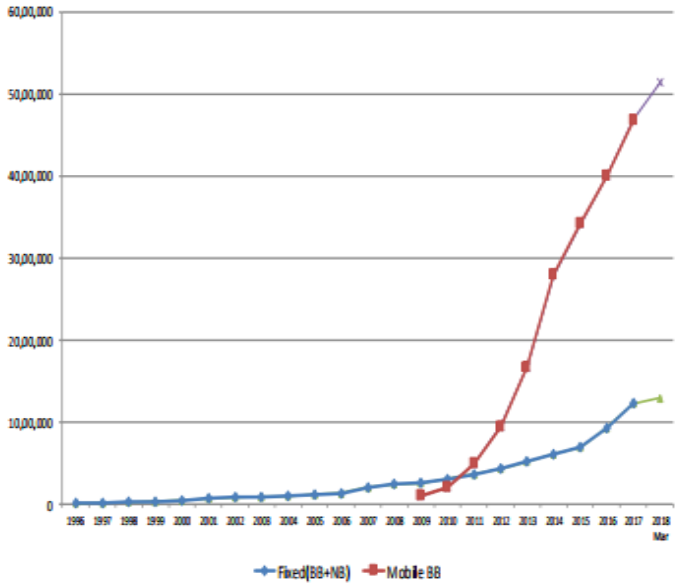

Figure 3: Broadband penetration in Sri Lanka

Source: [2]

1.2 Overview of stolen, counterfeit and substandard mobile devices

Mobile phones/handsets, dongles, tabs etc. are considered as mobile devices/mobile communication devices, as they are portable and used for communication purposes. The usage of counterfeit, substandard and stolen mobile communication devices is a worldwide issue. As the name suggests, stolen mobile devices are the mobile devices available in market but stolen from the real owner.

Counterfeit and substandard mobile devices are the two subsets of black market mobile devices. A counterfeit mobile device is an identical copy of the original brand or similar to the original brand where as a substandard mobile device resembles an original brand but different enough so it doesn't explicitly counterfeit a legitimate brand [3].

1.3 Motivation

The problem of manufacture, distribution and sale of black market mobile phones has created significant negative impacts to governments, industry, users and operators [2].Further, the usage of stolen mobile devices has been a societal problem in all countries of the world and it is ranked as one of the top five crimes committed in any given country [3]. Hence, it is essential to regulate the mobile devices available in the market and minimize the black market and stolen mobile communication device usage [4].

As per The Organization for Economic Co-operation and Development (OECD) nearly one in five mobile phones is fake [5]. Fig. 4 shows an analysis included in a report published by Mobile Manufacturers' Forum (MMF) which shows that Asia Pacific region is responsible for 50% of the proliferation of these handsets [3].

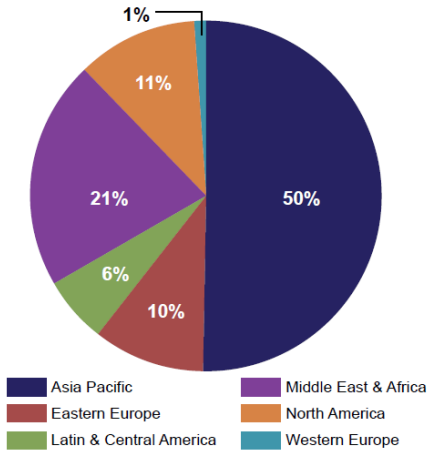

Figure 4: Proliferation of black market mobile devices
Source: [3]

Sri Lanka being in the Asia Pacific region makes it an ideal candidate to analyze the prevailing issues related to counterfeit, substandard and stolen mobile devices and identify suitable solutions.

Sri Lanka has signed the Trade Facilitation Agreement (TFA) of World Trade Organization. Therefore, the maximum number of containers that can be checked by customs is 50% of all arrivals. Anyhow, the current capacity of Sri Lanka customs is not capable of even handling that 50% of the containers that can be checked. Also, the people can easily smuggle a few mobile phones while coming from abroad as it's not practical to check each passenger unless they engage in a suspicious activity. Due to these facts, Sri Lanka has a considerable number of counterfeit, substandard and stolen mobile devices in the country.

1.4 Research Objectives

1. Conducting a literature survey to identify negative impacts

To identify the negative impacts faced by government, industry, users and operators due to black market and stolen device usage.

2. Conducting a literature survey to identify available solutions

To identify the solutions that have been implemented and suggested by various countries and organizations.

3. Conducting user surveys to identify the problems available in Sri Lanka

A user survey among consumers was conducted to identify the user behaviors related concerns which have allowed the usage of black market and stolen devices in the country and the issues faced by consumers due to the prevailing processes. A user survey among mobile operators was conducted to identify the existing processes followed to minimize the black market and stolen mobile device usage. A user survey with Telecommunication Regulatory Commission of Sri Lanka(TRCSL) was conducted to identify concerns and requirements of TRCSL

4. Providing a policy framework and recommendations

Final objective is to resolve the problems identified in objective 3 by providing a suitable policy framework and recommendations to minimize the usage of black market and stolen mobile device usage after analyzing suitable solutions that have already been followed and proposed by various countries and organizations.

1.5 Organization of the thesis

This thesis contains 6 chapters and 2 Annexes.

The chapter 1 provides a detailed introduction including background of the research, motivation and research objectives. The literature survey findings are summarized in chapter 2. This summarizes the negative impacts faced by government, industry, users and operators due to black market and stolen mobile device usage and the solutions that have been implemented and suggested by various countries and organizations.

Chapter 3 includes the problem formulation where the existing issues due to black market and stolen mobile devices is highlighted. Chapter 4 contains the details about the user surveys including questionnaire designing, sample selection and survey outcome.

Chapter 5 describes the suggested policy framework and recommendations to prevailing issues and Chapter 6 concludes the thesis while suggesting future improvements.

Annex-A contains the questionnaire used in consumer user survey and the Annex-B contains the questionnaire used in operator user survey.

CHAPTER 2: **LITERATURE SURVEY**

2.1 Negative impacts experienced by telecommunication eco system

2.1.1 Black market mobile devices

All parties involved in telecommunication eco system including the users, government, industry and operators are experiencing various negative impacts due to black market mobile devices. Below given is a summary of negative impacts as per an analysis done by International Telecommunication Union (ITU) and MMF [2], [3].

2.1.1.1 For government

The government loses a considerable amount of revenue as the illegal devices are imported and sold without paying relevant taxes. Every importer of mobile communication devices need to pay taxes to the government. But, these smuggled devices are sold without paying any taxes to the government which has resulted in a considerable revenue loss.

Additional measures are required to ensure the compliance with national regulations such as warranty requirement, environmental laws, intellectual property related laws etc. The relevant regulator of the country needs to regularly monitor the market and implement regulations and procedures to prevent the usage of illegal mobile devices. Therefore, this is an additional burden to the countries.

Black market devices tend to have invalid or cloned IMEI (International Mobile Equipment Identity) and they are potentially attractive for criminal activity and terrorism. The current procedure of identifying criminal and terrorist activities involve the tracing of mobile phones used for such activities. But, if the criminals use devices with cloned or incorrect IMEIs, it will not be possible to track such activities.

2.1.1.2 For industry

With the availability of turnkey solutions, it eliminated the research and development step in the development cycle and provided software solutions including the chipset. Hence, the black market device manufacturers are able to assemble and produce the devices at a very low cost compared to genuine products. Hence, it has created an unfair competition. The original equipment manufacturers have to spend a lot of money for research and development activities. But, since the black market device manufacturers copy the original devices, they can manufacture them for cheaper prices. This creates a very unfair competition for the original device manufacturers.

Counterfeit mobile devices are produced as copies of original products but, low in quality. Most of the time, the users are not able to segregate original device and the black market device. The black market devices don't function properly as an original device and the blame will be on original device manufacturers. Therefore, the brand value gets degraded.

Losses for right's holders as these black market device manufacturers don't pay intellectual property loyalties. When manufacturing a mobile phone, the manufacturer must pay loyalties for the parts and technologies used in the mobile phone. But, the illegal mobile phone manufacturers avoid paying such loyalties.

2.1.1.3 For users

Since, the black market devices are not tested in accredited labs, they are low in quality and reliability. As per a study done by GSMA, these devices are having low receiving sensitivity and transmit performance which result in performance degradation such as high percentage of dropped calls and handover problems [7].

Black market mobile devices contain hazardous substances such as Lead and Cadmium in excessive amounts and this leads to potential health hazards [8]. Mobile phones are very regularly used by people and they touch the device very often and keep them close to their skin. Therefore, the hazardous substances in the device can

harm people. Also, when such devices are thrown into garbage bins and not properly recycled, that can cause serious environmental pollution related issues.

These devices don't go through proper testing and compliance assessments such as adherence to national regulations including Specific Absorption Rate(SAR) value, audio safety, electromagnetic compatibility etc. Hence, the user safety is not guaranteed [8].

Unlike the genuine products which offer warranties of at least one year, users are not offered with any consumer warranty. The illegal mobile devices are low in quality. Therefore, the consumers will device functionality related issues. Since the device is not manufactured by an original device manufacturer, the consumers will not be able to claim their warranties.

The mobile phone contains very sensitive information of the users. The black market mobile devices can cause serious cyber security threats as they do not follow proper standards [8]. The hardware and software used in illegal mobile devices are not quality tested. They can contain various faults and such can easily be used by hackers and cyber criminals to hack or infect them with computer viruses.

2.1.1.4 For operators

The operators are also a victim to this issue. The Quality of Service (QoS) of the services perceived by the customers will be low and the operators will be held responsible. Due to the low quality of black market mobile devices, the users will face issues such as call drops. It will not be easy for the operators to troubleshoot such issues and convince the users regarding the manufacturing defects.

Due to poor performance of the devices, coverage will be significantly reduced and it will create a need of expensive and unnecessary technical measures such as more antenna installations, base stations etc. [7].As per a study done by GSMA, if such devices are used in large scale, the operators would suffer a 100% voice and 50% data capacity losses.

2.1.1.5 Stolen mobile devices

Mobile device theft is a societal problem in all countries of the world and as per MMF it is one of the top five crimes committed in any given country. Considering the sensitivity of the information available in mobile devices, governments have placed various regulations, policies and systems to discourage and minimize the usage of stolen mobile phones.

The black market mobile phones are a challenge to control the usage of stolen mobile phones via blacklists managed by operators and telecommunication regulators. Because, some of black market mobile phones don't have an IMEI or have cloned IMEIs.

2.1.2 Available solutions

The solutions that have been suggested and implemented by various organizations and countries to avoid the negative impacts mentioned above, are listed below.

2.1.2.1 MMF

MMF has issued a resource guide regarding counterfeit and substandard mobile phones. A mobile device needs to be connected to a mobile network before it's being used. Hence, this is the best occasion to block black market and stolen mobile devices to discourage usage and minimize the prevailing issues [3].

1. Network Blocking Solution

Black market and stolen mobile devices can have both invalid and valid IMEIs. Therefore, 'Counterfeit Identifier Platform' is the best option to block the devices. This platform cross checks the IMEIs of the mobile devices with their actual capabilities and identify the black market mobile devices. 3rd Generation Partnership Project (3GPP) has standardized the handset capabilities used by this platform [7].

2. IMEI Network Blocking Solution

This is a standard solution used by most of the countries to block devices based on IMEI. There are two approaches. One is maintaining a whitelist (allowed) of IMEIs by referring to GSMA IMEI database. In the case of identifying an invalid or cloned IMEI, they should be blocked. The other method is maintaining a whitelist as well asa black list (stolen devices and devices without regulatory approval etc.) of IMEIs. Then cross check in both the lists and block the devices accordingly [9].

3. Development of a Comprehensive Plan

Customer awareness regarding the negative impacts should be increased. Legislative and regulatory reforms are required and a comprehensive plan is required with increased enforcement of relevant authorities.

2.1.2.2 ITU

ITU proposes to implement a program to avoid illegal device import, cross check with GSMA IMEI database to check the validity of IMEIs during device approval process, maintain all legal device IMEIs in a central database and bar operators from providing services to black market or stolen mobile phones [2].

2.1.2.3 Australia

Customer can report to their service provider regarding a lost or stolen mobile device to bar the SIM card and block the handset from further use across all networks (emergency calls are allowed). Customer verification procedure to ensure that the correct handset is blocked and to prevent fraudulent blocking of other peoples' handsets is done by the service provider. Australian Mobile Telecommunications Association has allowed the customers to verify whether the IMEI number has been blocked through a website [10].

2.1.2.4 France

France regulator has reinforced anti-theft measures for improved effectiveness. A centralized database for identifying terminals that have been declared stolen is

available. Operators in metropolitan France were obliged to put the IMEI numbers in this and the terminals are blocked accordingly [10].

2.1.2.5 Pakistan

The Pakistan Telecommunication Authority (PTA) has placed a technical system to stop mobile phone theft. The system consists of cellular mobile operators, city police liaison committee, federal and provincial police departments and other government functionaries. EIRs have been installed by operators to block devices based on IMEI once the theft is reported by the customer. A standard operating procedure to be followed by all concerned parties including the mobile phone operators has been developed by PTA to streamline the reporting of stolen or snatched handsets [10].

Further, PTA has also launched awareness campaign to educate the users regarding the reporting of stolen mobile phones. Once the handset owner is verified, the system will block the handset by updating their database of stolen handsets which will be shared with all provinces.

2.1.2.6 Poland

Operators need to comply with the obligation to block IMEI numbers of stolen handsets by cooperation among themselves. The law imposes the following obligations on mobile operators [10].

1. Legitimacy of the blocking request of handsets should be thoroughly verified.
2. The use of stolen mobile handsets in their networks should be prevented.
3. The information identifying the stolen handsets should be transferred to other mobile operators to enable blocking.

2.1.2.7 Turkey

A Central Equipment Identity Register (CEIR) has been established to register the legally imported devices and disconnect the black market and stolen handsets from operator networks. The Information and Communication Technologies Authority in

Turkey has established a call center to obtain information regarding handsets related concerns and the processes have been automated to make them effective, accurate and quick [10].

2.1.2.8 United Kingdom

A database has been established by retailers and network providers to block stolen phones. Re-programming of IMEI is an offence punishable by law as per the legislation. Consumers can search online databases and verify the authenticity of mobile devices [10].

CHAPTER 3: **PROBLEM FORMULATION**

As per the introduction given in Chapter 1 and the literature survey done in Chapter 2, the usage of substandard, counterfeit and stolen mobile devices is a global issue. But being a developing country in the Asia Pacific region, Sri Lanka is an ideal candidate to analyze this global issue. This thesis mainly focuses on the issues faced by Sri Lanka and the possible solutions that can be adopted. But, the findings and solutions will be suitable for any country after doing slight modifications to the policy framework suggested in Chapter 5.

3.1 Counterfeit and substandard mobile devices

Even though there are regulations that are implemented by TRCSL to guarantee the quality of mobile devices, there is no proper blocking mechanism available in the country. There are mobile devices with invalid or fake IMEIs freely available in the country. So, this has created various issues to the society. These issues include:

3.1.1 Availability of hazardous substances

The parts such as memory card slot, SIM slot, camera etc. contains high proportion of hazardous substances such as lead (Pb). These parts physically touch with consumers fared and this has increased the risk. So, the Sri Lankans who are using black market mobile devices are at a high risk of exposing themselves to hazardous materials.

3.1.2 Other safety issues

The legitimate device manufacturers must go through rigorous testing and compliance assessments. But, the black market devices don’t go through any such procedures. Therefore, such mobile devices don’t comply with regulations that are implemented by TRCSL including electromagnetic compatibility requirements, audio safety requirements and low voltage device safety requirements. So, the Sri Lankans who are using black market mobile devices are facing safety issues discussed above.

3.1.3 Low quality of service

As per the studies conducted by GSMA, both the users as well as network operators are impacted by the low quality of service due to the usage of black market mobile devices. The quality issues include transmit performance issues, call drops, loss in voice and data capacity, unnecessary coverage requirements, handover issues etc. So, due to the black market mobile devices available in Sri Lanka, both the consumers and network operators are facing quality of service issues.

3.1.4 Impact of counterfeit and substandard devices

As discussed further in Chapter 2, Sri Lankan government, consumers, network operators and industry as a whole are experiencing various negative impacts due to the black market device usage.

3.2 Stolen mobile devices

The availability of stolen mobile devices has created various security issues. The stolen mobile devices can be used for illegal activities including terrorism. But, the country is not following any proper mechanism to block the usage of such devices. Therefore, stolen mobile devices are freely available in Sri Lanka currently.

The existing policies and processes in the country to find a stolen mobile device is not user friendly. It involves a lot of manual procedures where the consumers need to make complaints at TRCSL and police. Once informed, the mobile operators act immediately to disconnect the SIM card in the stolen mobile device. But, the time consumed by the authorities to find a lost mobile device is not acceptable. Therefore, the consumers are severely affected and they tend to just disconnect the SIM and not to make any complaints regarding lost mobile devices.

3.3 Other issues

Sri Lanka doesn't have a CEIR. Therefore, TRCSL doesn't have a bird's eye view of the country's mobile device usage. If TRCSL has a CEIR, then they will know the details of all available mobile devices in the country. So, TRCSL can analyze and act promptly to prevent the usage of black market and stolen mobile devices in the country. Not having a CEIR has hindered the efforts of minimizing the usage of black market and stolen mobile device usage in Sri Lanka

The developed countries have adopted sophisticated and standardized procedures. But, those involves high capital requirements. Therefore, Sri Lanka needs a low cost but and effective solutions to minimize the usage of black market and stolen mobile devices. TRCSL needs to identify the existing issues and implement the best solution in terms of both functionality and cost.

3.4 Formulation of hypotheses

3.4.1 Identifying mobile phone usage related details

Table 2: Mobile phone usage related user behaviors

Hypothesis	**Variables**	**Indicator**	**Measure**	**Question**
Almost all the people use mobile phones	Types of the mobile devices used	Usage of mobile phones	Mobile phones, tabs, dongles, other	What type of mobile devices do you use?
People use different types of mobile phones	Type of the mobile phones used	Usage of different types of mobile phones	Feature phone, Android, IOS, other	What type of mobile phone do you use?
People use different brands of	Brand of the mobile phones used	Usage of different brands of	Samsung, Huawei, Apple, other	What is the brand of your mobile phone?

mobile phones		mobile phones		
Mobile phones without TRC approval are owned by people	The available options to purchase a mobile phone	Usage of mobile phones which don't have TRC approval	Authorized dealer, Bought from a friend, Bought from a foreign country, other	From where did you buy your mobile phone?
People don't consider the standard of the device	Selection criteria	Consideration level	Cost, Brand, OS, Network support, IMEI, SAR, other	What were the selection criteria?

3.4.2 Identifying details regarding loosing mobile phones

Table 3: Lost mobile phones related scenarios

Hypothesis	Variables	Indicator	Measure	Question
People loose mobile phones	Whether people have lost mobile phones	Whether people have lost mobile phones	Yes, No	Have you lost a mobile phone?
People are aware of the	Whether people will inform	Whether people are aware of the	I should disconnect SIM, Inform police,	If your mobile phone is lost, what should you do?

authorities that they should inform of a lost mobile device	Police, Operator and TRCSL	relevant authorities that they should inform	Inform TRCSL	
People don't inform the authorities about lost mobile phones	Whether people inform the authorities about lost mobile phones	The authorities which are informed by people	Operator, TRCSL, Police, All, None	To what authorities did you inform about the lost mobile phone?

3.4.3 Hypotheses to identify issues regarding finding a lost mobile phone

Table 4: Lost mobile phones related issues

Hypothesis	**Variables**	**Indicator**	**Measure**	**Question**
People can't find lost mobile phones through existing processes	Whether people have found the lost mobile phones	Whether people have found the lost mobile phones	Less than a week, less than a month, More than a month, never found	How long did it take you to find your lost mobile phone?
People are unhappy about the existing	How good is the process of handling lost mobile	Level of satisfaction	Good, Neutral , Bad	How satisfied are you regarding the process followed?

processes to find a lost mobile phone	phones			

Above hypotheses were tested during the consumer user survey. Refer 4.1.1 for questionnaire designing related details.

CHAPTER 4: **DATA COLLECTION AND DATA ANALYSIS**

4.1 User surveys

This chapter contains the details about the three user surveys conducted among mobile device users, mobile operators and TRCSL. Responses from total of 355 mobile device users, all five mobile operators in the country and TRCSL authorities were collected.

The sample selection for mobile device user survey to identify the common user behavior related issues was done based on "Random sampling" method. This survey was conducted using an online questionnaire and a printed questionnaire paper. It is included as Annex-A.

The user survey among mobile operators (Dialog, Mobitel, Hutch, Etisalat and Airtel) was carried out to identify the measures that have already been taken to minimize the usage of black market and stolen mobile devices. This user survey was conducted by interviewing the authorized personnel of each operator.

The user survey conducted with TRCSL was carried out by interviewing Ms. Tharalika Livera, Deputy Director for Compliance (Surveillance & Quality of Service). The existing issues faced by TRCSL and their requirements were captured during the user survey.

4.1.1 Questionnaire designing

A user survey was conducted among a selected sample of Sri Lankans to identify the common user behavior related issues and the prevailing issues due to the existing systems and processes.

The considered sample size calculation is as follows and the minimum sample size required as per (1) is 273 whereas 379 samples were collected during the user survey.

$$\text{Sample size} = \frac{\frac{z^2 \times p(1-p)}{e^2}}{1+\left(\frac{z^2 \times p(1-p)}{Ne^2}\right)} \qquad \text{----- (1)}$$

Where:

z = Z-score of the relevant confidence level = 1.65 (90% confidence)

p = expected response distribution = 0.5 (assumed normal distribution

e = percentage of margin error = 5%

N= Population size = 21 million (population of Sri Lanka)

4.2 User survey results

4.2.1 Demo graphic aspects

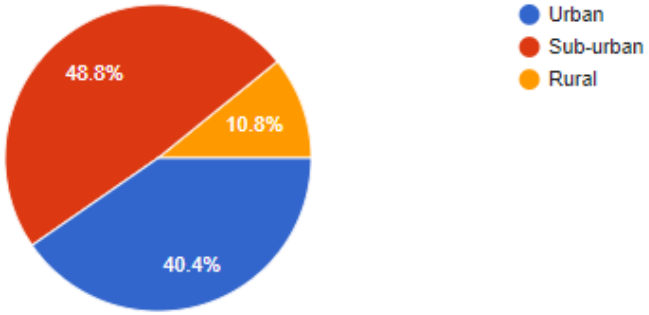

Figure 5: Living area

When the area wise distribution of participants is considered, 48.8%, 40.4% and 10.8% participants were sub-urban, urban and rural respectively.

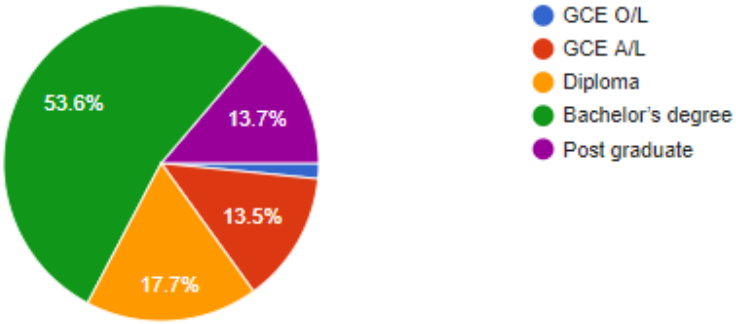

Figure 6: Education qualification

Significant percentage, i.e. 53.6% of the participants were having a bachelor's degree. So, most of the survey participants were from a good educational background.

4.2.2 Results of user survey conducted among mobile device users

Hypothesis 1 –"Almost all the people use a mobile phone" is proven as 99.7 % of the participants were using a mobile phone.

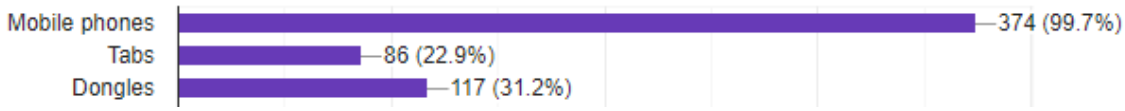

Figure 7: Mobile phone usage

Hypothesis 2 – "People use different types of mobile phones" is proven as 73.6 % were android, 21.1% were IOS and other 5.3% were feature, windows and different types of mobile phone users.

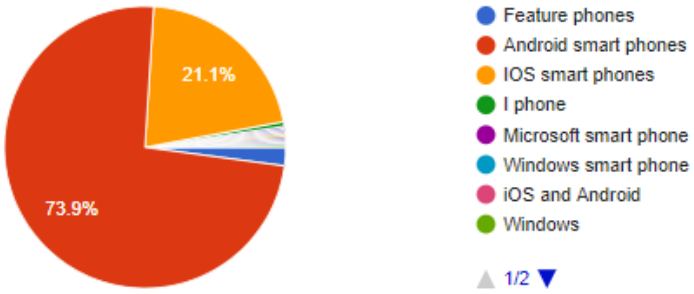

Figure 8: The types of mobile phones used

Hypothesis 3 – "People use different brands of mobile phones" is proven as 27.4% were Samsung, 26.9% were Huawei, 21.9% were Apple and other 23.8% were HTC, Nokia, Oppo, Sony, etc. users.

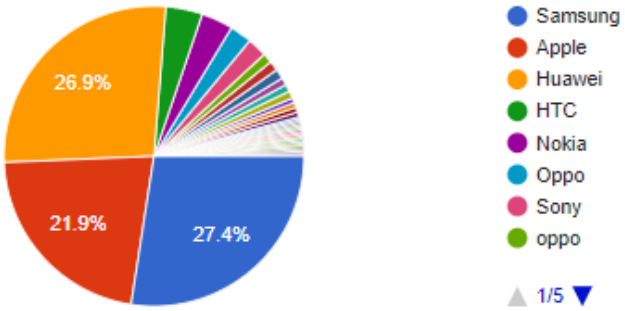

Figure 9: The brands of mobile phones used

Hypothesis 4 – "Mobile phones without TRC approval are owned by people" is proven as 15.6% of the participants were using mobile phones bought from a foreign country.

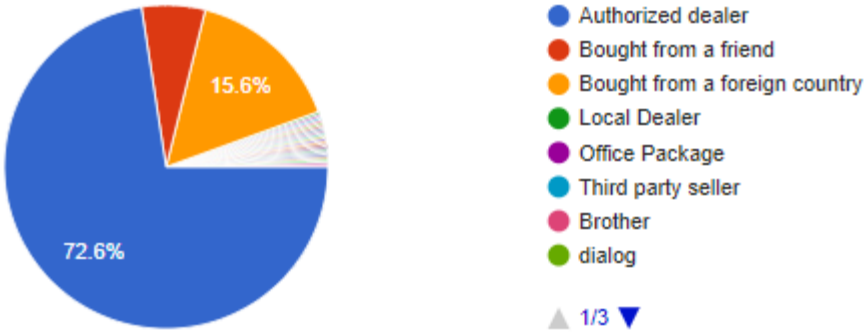

Figure 10: The ways of purchasing a mobile phone

Hypothesis 5 – "People don't consider the standard of the device when buying" is proven as the factors such as cost, brand, operating system and the supported network technology were considered by the majority (i.e. 77.9%, 76.3% and 57.9% respectively). But the validity of IMEI is considered by 18.7% and the SAR value is considered by only 7.2%.

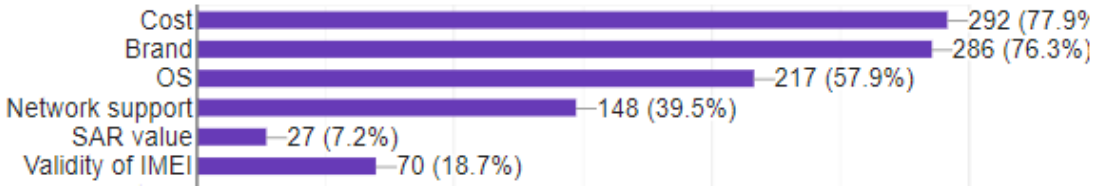

Figure 11: The selection criteria of users

Hypothesis 7 – "People loose mobile phones" is proven as 25.9% of the participants had lost one of their mobile phones.

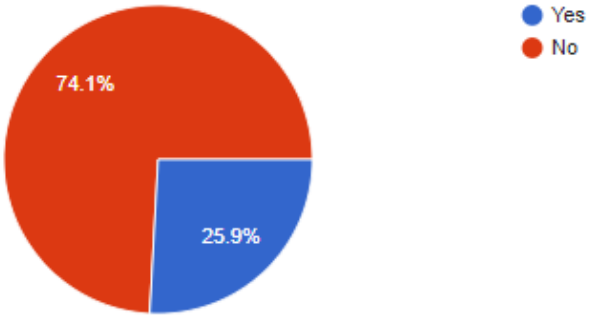

Figure 12: Lost mobile phones

Hypothesis 7– "People are aware of the authorities that they should inform of a lost mobile device" is not proved as expected. Nearly 75% of the people are aware of the requirement to inform mobile operator to disconnect the SIM. But, only 68.1% and 55.1% are aware of informing Police and TRCSL respectively.

Figure 13: Awareness of people

Hypothesis 8 –"People don't inform the authorities about lost mobile phones" is proven as only 45% of the victims had informed police and 34% had informed Telecommunication Regulatory Commission and another 34% of the victims have not informed any of the authorities.

Figure 14: Informing relevant authorities after losing a mobile phone

Hypothesis – 9 "People can't find lost mobile phones through existing processes" is proven as a clear majority of 82.7% had not found their mobile devices. Hence, there is a possibility for those devices to be available in a cellular network of one of the operators currently.

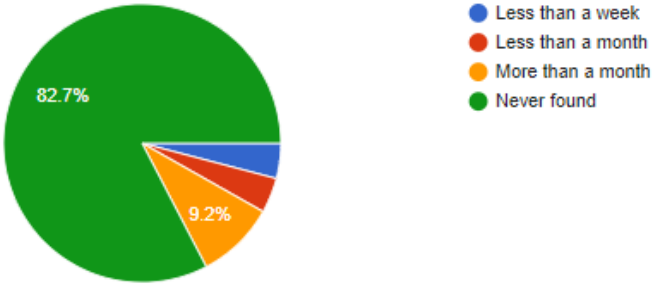

Figure 15: Finding a lost mobile phone

Hypothesis – 10 "People are unhappy about the existing processes to find a lost mobile phone" is proven as 53.1% people have mentioned that the existing processes is bad while only 5.1% have stated that the existing processes is good.

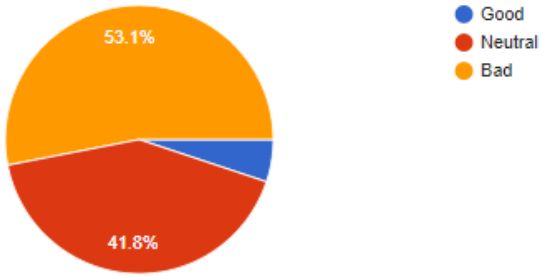

Figure 16: Satisfaction of people regarding the existing proses

As per the user survey conducted among consumers and the results discussed above, following conclusions can be made:

99.7% of the people use mobile phones and some are using various types of mobile devices including tabs and dongles. Therefore, mobile phones are used by almost all the people.

Cost of the mobile device, brand, operating system and the supported network technology are the four main factors considered by people when buying a mobile device and the important factors to minimize the usage of black market and stolen devices such as validity of IMEI and SAR value are neglected by the majority. Therefore, this user behavior has allowed the availability of black market and stolen mobile devices in the country.

Once a mobile device is lost, even though the authorities were informed, a clear majority of 82.7% had not found their mobile devices. Therefore, it is very clear that the current procedure of finding lost mobile phones is not effective and people are not able to find lost mobile devices easily.

As per the user responses, 53.1% of the people are unhappy about the existing process to find a lost mobile device. Therefore, the existing processes to find a lost mobile device should be changed to suit the needs of people.

Due to the time consuming and inefficient processes placed, people are not interested in even complaining to the authorities to find stolen mobile devices and even though they inform, the probability of finding them back is very low.

4.2.3 Results of user survey conducted among mobile operators

Another user survey was conducted among mobile operators in Sri Lanka (Dialog, Mobitel, Hutch, Etisalat and Airtel) to identify the measures that have already been taken to minimize the usage of black market and stolen mobile devices.

4.2.3.1 EIR system architecture of operators

The general EIR system architecture used by mobile operators to identify and block black market and stolen mobile devices is given in Fig. 5 below.

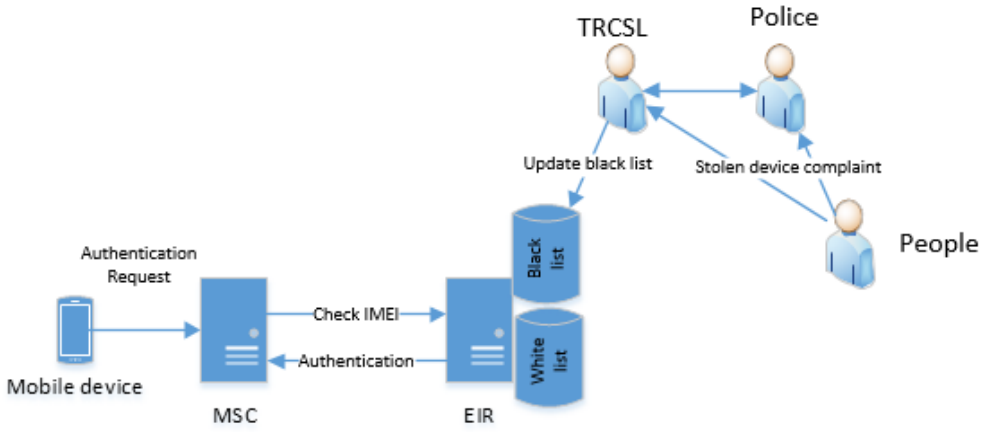

Figure 17: EIR system architecture of operators

The methodology used by operators to acquire device details for EIR functionality is to obtain check IMEI requests from the Mobile Switching Center (MSC). A check IMEI is generated from MSC during International Mobile Subscriber Identity (IMSI) attached process. IMSI attach process includes following scenarios

1. Turn off and on a mobile device

2. Turning on a new device for the first time (new device detection)

3. Changing the mobile device that has been used.

This check IMEI is sent to EIR platform and the EIR Data Base (EIR DB) parameters are updated. The EIR DB update parameters are Mobile Station International Subscriber Directory Number (MSISDN), International Mobile Equipment Identity (IMEI) [11], and International Mobile Subscriber Identity (IMSI).

After receiving the check IMEI request from MSC, EIR cross checks the IMEI of mobile device in its white (allowed), grey (suspicious), and black list (not allowed). Then the EIR gives response to MSC depending upon the result of the search. Based

on the status provided in the response by EIR, MSC either continues the registration procedure or block the device from using the network [12].

As per the user survey conducted among operators to identify the EIR procedure used by operators, following issues were identified.

1. Availability of black market mobile devices

Due to the unavailability of a proper process to block black market mobile devices from using the networks, such devices are freely available.

2. Availability of stolen mobile devices

Even though the operators have individual EIRs, there is no central EIR in the country. Since, the stolen mobile device IMEIs are not maintained in a central database and monitored, such devices can be easily used in networks.

4.2.4 Results of user survey with TRCSL

As per the user survey conducted with TRCSL, following issues were identified,

1. Operator dependency to identify the availability of a Device

Once operators are informed of a lost device, they check the availability of the device in the network once. But, the device might not be available in the network at that moment. Hence, continuous monitoring of the IMEI should be done. The existing process is time and resource consuming for the operators and it's done as a free of charge service. There should be a convenient methodology to identify the availability of a given IMEI without depending on operator feedback.

2. Manual process of acquiring information regarding lost devices

If a mobile device is lost, the user must go to police and TRCSL to lodge a complaint. Then, the operators are informed to check the availability of lost mobile device in their networks. If the lost device is available in an operator network, the police will be informed by TRCSL. This is a time-consuming process.

Hence, we can conclude that, the existing EIR model only deals with the IMEI numbers in the EIR database of a given network. According to the existing model, if a mobile device is lost, the service provider can block the IMEI of that device in its own network. But if the SIM card is changed, the mobile device will be latched to a different network. There is no proper process to block stolen and black market mobile devices. TRCSL requires a more efficient and centralized system to minimize the usage of black market and stolen mobile devices.

CHAPTER 5: **POLICY FRAMEWORK AND RECOMMENDATIONS**

5.1 Available solutions for Sri Lanka

As per the problems identified in Section III and the literature survey done in Section II above, a suitable solution should be identified. As per the consumer user survey, user behavior related concerns have created a demand for black market and stolen mobile devices and the existing processes to find a lost device is inefficient. As per the operator user survey, black market and stolen devices are available in operator networks and there is no central system and adequate policies to block black market and stolen devices. Also, as per the survey done with TRCSL, the operator dependency to implement a proper blocking mechanism, unavailability of an automated and centralized system, and manual process of acquiring information regarding lost devices are the problems that should be addressed.

Based on above, the policy framework components that should be included in the final policy framework is mentioned in the Table 5.

Table 5: User survey findings that should be addressed in policy framework

User survey finding	**Policy framework component that should be included**
1. Consumer - user behavior related concerns have created a demand for black market and stolen mobile devices and the existing processes to find a lost device is inefficient	A mechanism to increase user awareness should be implemented and the existing processes to find a lost mobile device should be made more efficient.
2. Operators - unavailability of a central system and lack of policies to block black market and stolen devices.	A central system should be implemented to track all mobile devices in the country and block the black market and stolen devices.

3. TRCSL - the operator dependency to implement a proper blocking mechanism and the unavailability of an automated and centralized system.	Existing regulations and policies should be reformed.

5.2 Comparison of alternatives

5.2.1 Alternative methods of increasing user awareness

As per the user survey results obtained in Section III, cost of mobile device, brand, operating system and supported network technologies are the four main factors considered by people when buying a mobile device. The important factors such as validity of IMEI and SAR value are neglected by the majority. The main reason for black market and stolen device availability is the demand for such devices.

The main consideration of the consumers when buying a handset is, its cost. The black market and stolen devices are always less costly. The other two considerations namely brand and OS can prevent substandard device usage, but it will not minimize counterfeit or stolen device usage.

Therefore, TRCSL should do an island wide awareness campaign to make the consumers aware of the serious issues that black market and stolen devices can create. If it's a black market device, it'll cause health threats, poor performance of the devices, lack of warranty coverage and security threats in the domains of cyber security and privacy. If it's a stolen device, the consumer will have to face legal proceedings for keeping stolen devices with themselves.

1. TV advertisement

TRCSL can summarize the above facts and prepare a TV commercial to be broadcasted during peak hours. Since, this is a national initiative which will benefit

the whole country, it will be possible to convince the TV broadcasters to broadcast the advertisement for a nominal fee.

2. Social media campaign

Most of the youth in Sri Lanka are using social media. Therefore, Facebook and YouTube can be considered as two main mediums to conduct an effective awareness campaign. If it's done correctly, a Facebook post or a YouTube video can be made viral. Since, TRCSL doesn't have the expertise in doing a social media campaign, some of the famous social media stars can be requested to do the campaign, on behalf of TRCSL. Since, this is a national initiative, public figures such as singers, cricketers, professionals, doctors can be requested to join in with the campaign free of charge.

3. Newspaper advertisement

It is a common practice to use newspaper advertisements during awareness sessions due to its wider reachability. Since, the advertisement needs to be eye catching, one-page newspaper advertisement is a suitable option. Like the TV advertisements, the newspaper publishers can be convinced the importance of the awareness session as a national initiative and request for a reduced price.

4. Distribution of leaflets

This again is a common method of doing awareness campaigns. A leaflet highlighting the negative impacts of using black market and stolen mobile devices should be designed. Then, it should be distributed among people at public places such as bus stands and train stations.

5. One to one awareness sessions

A team should be formed and sent to individual households to make them aware of the negative impacts of using black market and stolen mobile devices. It is a common practice to carry a leaflet and educate the household regarding the content.

5.2.2 Alternative methods of establishing a centralized database and blocking mechanism

The problem of not having a centralized system and proper blocking mechanism should be addressed after carefully analyzing the available options. Mobile devices must be activated in respective operator network to utilize the services. This is the main advantage where we can capitalize on providing a blocking solution. When implementing the solution, as described in Section II, the guidelines given by ITU and MMF should be considered [2], [3].

5.2.2.1 Implementing a centralized database and IMEI blocking solution

A centralized database and IMEI blocking solution can be implemented by referring the architecture suggested by MMF and ITU. TRCSL should obtain GSMA IMEI database and maintain that as a whitelist database to identify valid IMEIs [17]. The IMEIs in the central database should be cross checked for invalid IMEIs.

Invalid and fake IMEIs should be maintained in a black list database. The cloned IMEIs should be updated in the same black list. TRCSL should add the IMEIs of stolen handsets to the same black list. This blacklist database should be pushed to individual operators. Then, the operators can use this database to cross check the IMEIs of the mobile devices and identify the blacklisted devices via the EIR systems that the operators have already established.

As per the literature survey done in Section II, mobile operators in a country should have EIRs. A Central EIR (CEIR) managed by the regulator can be implemented by connecting the operator owned EIRs [13-16]. Similar implementations have been done in France and Turkey [10].

5.2.2.1.1 Implementing a real time updating CEIR

Initially, all operator IMEI databases should be pushed to a central database managed at the regulator. Then the mobile device changes detected by EIRs should be updated in CEIR and this should happen in real time.

TRCSL had called for a tender to deploy a real time updating CEIR in 2012 and it was not proceeded mainly due to the cost and technical complexities. Therefore, identifying the CEIR proposal and the tender responses received by TRCSL will be helpful to identify a suitable solution for Sri Lanka.

CEIR should be completely installed by the vendor and TRCSL staff should be trained by the vendor to maintain the CEIR. Also, the vendor should maintain the system once deployed.

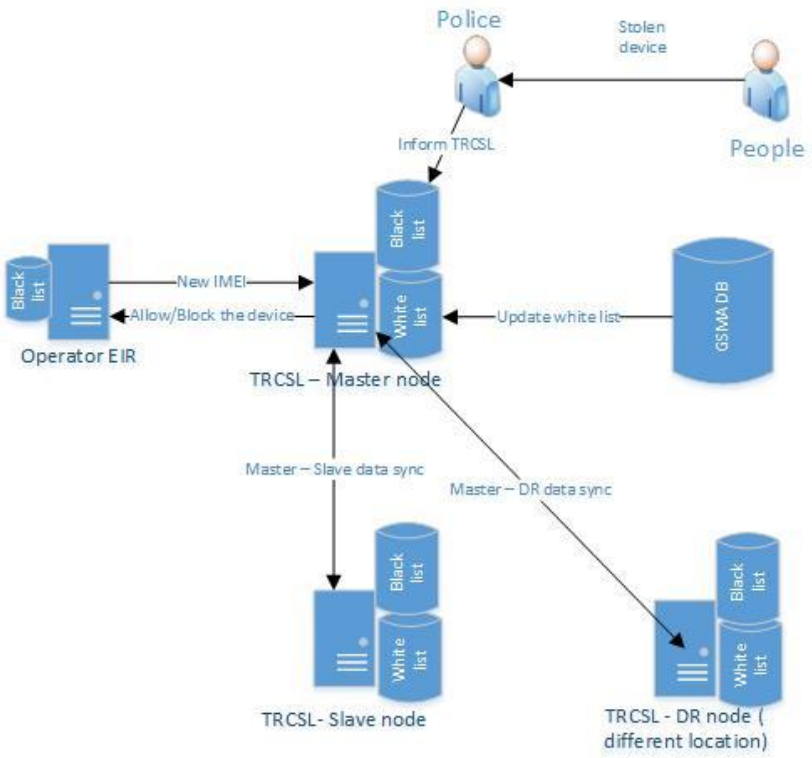

Figure 18 : The proposed real time CEIR system architecture

The EIRs of individual operators should be connected to CEIR and IMEI, IMSI and MSISDN changes should be updated in real time. Then the decision of allowing or not allowing the device to be connected to the mobile operator network should be informed to the EIR in real time by the CEIR. The proposed CEIR architecture by TRCSL is given in Figure 18.

The system should be able to store 300 million IMEI data and it should be scalable. A graphical user interface should be provided to view and perform necessary

functionalities such as blocking an IMEI. The system availability should be 99% and 24*7 support should be provided by the system provider.

IMEI, IMSI and MSISDN should be stored in CEIR. When an IMEI is blocked from CEIR, it should be blocked in operator EIR in real time. A white list, black list and grey lists should be available to monitor mobile devices. When black market or stolen devices are detected, the authorities should be notified. A Very Important Person (VIP) list of IMEI data should be able to be configured to avoid tracking of sensitive data of high profile people in the country. A reporting tool should be available to download white, black or grey list device details.

The hardware for the CEIR should be provided by the vendor who is responding to the tender. Three servers with each having 2 or 4 Central Processing Units (CPUs) and 256 GB Random Access Memory (RAM) each should be provided. Two servers should be deployed as Master-Slave live nodes and one server should be deployed as a Disaster Recovery (DR) node at a different location provided by TRCSL. The required switches and firewalls should also be deployed.

The costing of the tender proposals was in the range of 20 million Sri Lankan Rupees. The technical complexities of deploying required hardware resources, establishing a real-time system by integrating to EIRs of mobile operators and the high cost of the proposed solutions, hindered any progress of the tender.

5.2.2.1.2 Implementing a non-real time updating CEIR with onsite hardware

Initially, all operator IMEI databases should be pushed to a central database managed at the regulator. Then the mobile device changes detected by EIRs should be updated in CEIR and this need not to happen in real time. When a black listed device is added to the CEIR or a black listed device is detected in the details received from operator, the operator EIRs should be informed to update their black lists and block such devices.

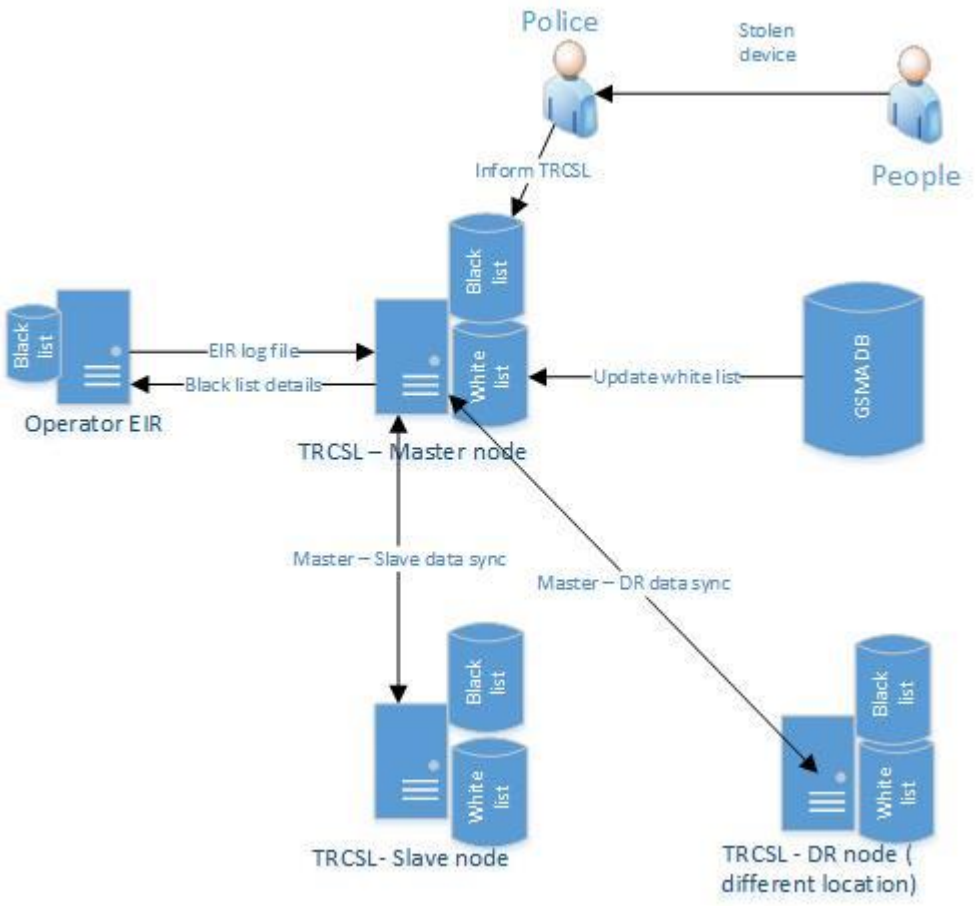

Figure 19 : Then on-real time CEIR system architecture with onsite hardware

Figure 19 shows the proposed system architecture of a non-real time updating CEIR that can be deployed at TRCSL premises. This way, the requirement of complex integrations with operator EIRs can be avoided. The EIRs of mobile operators can pass log file based on a defined period to CEIR. Then CEIR can process the logs to identify any mobile device changes and update its database.

The hardware for the CEIR should be provided by the vendor who is responding to the tender. Three servers with each having 4 Central Processing Units (CPUs) and 16 GB Random Access Memory (RAM) should be provided. Two servers should be deployed as two Master-Slave live nodes at TRCSL and one server should be deployed as a Disaster Recovery (DR) node at a different location provided by TRCSL. The required switches and firewalls should also be deployed.

The cost of this type of a solution will be high, considering the requirement of deploying onsite hardware. This is like establishing a data center at TRCSL and continuing its maintenance.

5.2.2.1.3 Implementing a non-real time updating CEIR without onsite hardware

Initially, all operator IMEI databases should be pushed to a central database established at mobile operator data centers. Then the mobile device changes detected by EIRs should be updated in CEIR and this need not to happen in real time. When a black listed device is added to the CEIR or a black listed device is detected in the details received from operator, the operator EIRs should be informed to update their black lists and block such devices.

This way, the requirement of complex integrations with operator EIRs can be avoided. The EIRs of mobile operators can pass log files based on a defined period to CEIR. Then CEIR can process the logs to identify any mobile device changes and update its database.

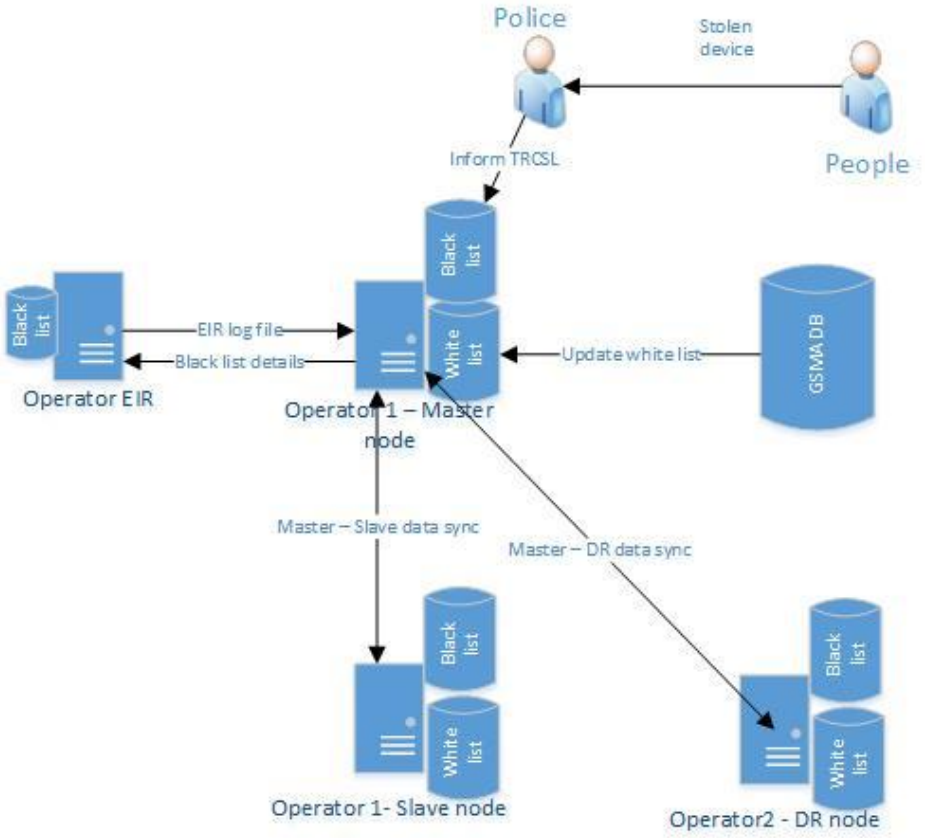

Figure 20: Then on-real time CEIR system architecture without onsite hardware

Considering this as an important national initiative which will benefit the operators also, the hardware for the CEIR can be obtained from operator premises at a reduced annual fee. TRCSL and operators can have a discussion to identify two suitable operator datacenters to deploy two live DB nodes and one DR node. It is also possible to deploy the two live DB nodes at two operator data centers (Master at operator 1 and Slave at operator 2) and DR node at another operator data center. But, this will add more complexities and master-slave sync issues can also arise.

A collaboration of TRCSL and operators should be formed to distribute the cost and resources appropriately. If an operator is providing data center resources, other operators should compensate the selected operator to avoid any unfair situation.

Three servers with each having 4 Central Processing Units (CPUs) and 16 GB Random Access Memory (RAM) should be obtained from two operator owned data centers. Two servers should be deployed as two Master-Slave live nodes at one of the operator data centers and one server should be deployed as a Disaster Recovery (DR) node at another operator data center.

5.2.2.2 Implementing a centralized database and Counterfeit Identifier Platform blocking solution

The black market devices probably have invalid IMEI, no IMEI, and a valid IMEI but cloned from an original mobile device. Therefore, the approach of blocking the devices purely based on IMEI is not an ideal solution as it might not be possible to distinguish the devices with valid IMEIs.

Therefore, 'Counterfeit Identifier Platform' is the best option to block the devices. This platform cross checks the IMEIs of the mobile devices with their actual capabilities and identify the black market mobile devices. Mobile phone capabilities used by this platform relate to information already standardized by 3GPP.

The system has a database containing the capabilities of the mobile phones. This database is created based on information provided by original device manufacturers relating to the IMEIs and capabilities. Then the system compares the actual

capabilities of the mobile phone with capabilities stored in the capability database of the system. If the capability cross check fails then the system sends a blocking request to Home Location Register (HLR) based on subscriber's IMSI. Then the operator can notify the user regarding the illegal mobile device and then block the device accordingly.

5.2.3 Alternative methods of adding reforms to existing regulations and policies

When implementing reforms, similar implementations done in other countries should be considered. Section II in this research paper describes the current practices of different countries which Sri Lanka can follow.

5.2.3.1 Improving the manual processes

It's the common practice of the world to move into digitized mechanisms to avoid any delays and inconveniences to the public. Therefore, stolen devices related complaint handling process needs to be digitized. An online Graphical User Interface (GUI) should be established to make lost devices related complaints and once validated the complaint should be automatically lodged at a police station.

Sri Lanka needs to establish a central data base to store person identification related information including the thumb print, photographs of face, information in National Identity Card (NIC), birth certificate and driving license. Then, very accurate person identification methods such as facial recognition and thumb print recognition can be included into the proposed GUI. This is a major requirement prevailing in the country to prevent frauds and criminal activities. Establishing a central person identification system for the country should be a national initiative.

The stolen device details should be updated in the central database suggested in 5.2.2 above. Then the black listed device details should be sent to mobile operators to update their black lists and the availability of the stolen device in mobile operator networks should be monitored.

When a stolen device is detected, police should be informed automatically and necessary actions should be taken to find the lost device. If it's found the user should be informed and the physical intervention of the person who made the complaint is required only at this final step.

5.2.3.2 Blocking black market and stolen mobile devices

Once a black market or a stolen mobile device is detected, an appropriate action should be taken to avoid the usage of such devices. The regulator can use mediums such as Short Message Service (SMS) or voice calls to inform the users regarding the illegal devices. A concession period should be provided to the users initially. If the illegal mobile device users continue to use the devices even after the concession period, those devices should be permanently blocked.

5.3 Proposed policy framework for Sri Lanka

A policy framework will be proposed after referring the literature survey done in Section II to identify negative impacts and solutions that have been implemented and available solutions discussed in Section 5.2.

Consumers' user survey highlighted the user behavior related concerns which has created a demand for black market and stolen mobile devices and inefficient processes in the country. Operator user survey finding confirmed the negative impacts that the telecommunication industry is facing, unavailability of a central system and lack of policies to block black market and stolen devices. TRCSL user survey confirmed that the operator dependency to implement a proper blocking mechanism and the unavailability of an automated and centralized system are major draw backs in minimizing the usage of black market and stolen mobile devices

As per the user survey findings summarized in Table 5, the three main steps that should be included in the policy framework are as follows.

1. Increasing user awareness
2. Establishing a central database and a blocking mechanism
3. Adding reforms to existing regulations and policies

Sri Lanka is still a developing country which is facing various budget concerns due to high debts. Therefore, the investment that the country can afford for implementing a policy framework for minimizing the usage of black market and stolen mobile devices is limited.

The order of implementing the three steps mentioned above, should be step 1 – increasing user awareness, step 2 – establishing a central database and a proper blocking mechanism and finally step 3 – adding reforms to existing regulations and policies. The order is decided after considering the least difficult task as per the current context of Sri Lanka. The step 1 is the least cost and easiest step to implement. Then before adding reforms to reduce the usage of black market and stolen mobile devices, there should be a mechanism to identify the usage of such devices. Therefore, the central database and blocking mechanism, mentioned in step 2 should be implemented before adding reforms to existing regulations and policies.

The order of implementation will vary depending on the country but the steps will not change. But, it's strongly recommended to do a problem identification (Refer Section III) and analyze the existing issues before implementing below recommendations in another country. Table 6 summarizes, how the suggested policy framework steps will address the issues identified during the three user surveys conducted among consumers, operators and TRCSL.

Table 6: The issues addressed by policy framework

Policy framework component	**The relevant issue identified during consumer, operator and TRCSL user surveys which will be resolved.**
1. Increasing user awareness	Consumers - user behavior related concerns which has created a demand for black market and stolen mobile devices and inefficient processes in the country.
2. Establishing a central database and a proper blocking	Operators - unavailability of a central system and lack of policies to block black market and stolen devices. TRCSL - the operator dependency to implement a proper blocking

mechanism	mechanism and the unavailability of an automated and centralized system.
3. Adding reforms to regulations and policies	Consumers - user behavior related concerns and inefficient processes in the country. Operators – availability of black market and stolen devices in operator networks. TRCSL – manual process of acquiring information regarding lost devices

The individual goals that will be achieved by the policy framework steps to minimize the usage of black market and stolen mobile devices is mentioned in Table 6.

Table 6: Goals of each policy framework component

Policy framework component	**Goals to be achieved**
1. Increasing user awareness	1. Increase the awareness of users regarding the importance of standard of a mobile device. 2. Increase the awareness of users regarding the negative impacts of using substandard mobile devices. 3. Reduce the demand for black market and stolen mobile devices.
2. Establishing a proper blocking mechanism	1. Implement a central system to obtain a bird's eye view of mobile device usage in Sri Lanka. 2. Identify the usage of black market and stolen mobile devices in real time. 3. Provide TRCSL with an automated system to block any illegal mobile device without depending on operator feedback.
3. Adding reforms	1. Implement a process to block the usage of black market and stolen

to regulations	devices in operator networks. 2. Implement an automated process to acquire information regarding lost devices and improve efficiency.

5.3.1 Selected method of increasing user awareness

TRCSL should do an island wide awareness campaign to make the consumers aware of the serious issues that black market and stolen devices can create. This can reduce the demand for black market and stolen mobile devices.

As mentioned in 5.2.1 above, there are multiple ways of conducting an awareness campaign. But, the effectiveness of the awareness campaign varies with each alternative option. Therefore, rather than choosing one method, multiple methods should be chosen to reach the expected audience.

TRCSL should do a TV advertisement to reach the people who are spending a considerable time in front of television. A paper advertisement should be conducted to reach the wider crowd. Especially, the people living in rural areas and don't watch television will most probably read newspapers. A social media campaign is a very effective tool to reach the youth. A properly designed post in Facebook and a properly designed video in YouTube can be made viral. It is recommended to use expert advice when preparing the advertisements, Facebook posts and YouTube videos to achieve the goal of reaching maximum number of people. Distributing leaflets and conducting one to one awareness sessions are not practical options for TRCSL considering the requirement of human resources as well as the lower reachability. Also, the number of people that we can made aware of this issue is less in these two methods.

This awareness campaign which includes a TV advertisement, newspaper advertisement and a social media campaign will reduce the demand and discourage black market and stolen mobile device usage.

5.3.2 Selected method of establishing a centralized database and blocking mechanism

The problem of not having a centralized system and proper blocking mechanism is a major reason for the availability of black market and stolen mobile devices. Considering the current context of Sri Lanka where all operators are having their own EIRs, the best approach is to establish a Central EIR (CEIR) managed by TRCSL. Similar implementations have been done in France and Turkey [10].

Even though a centralized database and Counterfeit Identifier Platform blocking solution [13-16] discussed in 5.2.2.2 is the ideal solution, it is not a practical approach for Sri Lanka. Sri Lanka couldn't proceed with an onsite CEIR solution based on cost concerns and implementation complexities. Therefore, a totally new solution which will cost more than a CEIR system that store device information and block based on IMEI will not be a viable option.

Table 7 : Comparison of CEIR options

Option	Quotation value	Advantages	Disadvantages
Implementing a real time updating CEIR with onsite hardware	LKR 20 Million for software and LKR 5 million for hardware.	Real time detection of mobile devices, real time blocking capability, completely independent system as hardware is located at TRCSL	Very high cost, complex integration requirement with operator EIRs, requirement to continuously update and monitor hardware
Implementing a non-real time updating CEIR with onsite hardware	Quotation from Mylinex LKR 9 million for software and LKR 3 million for hardware	Simple integration requirement with operator EIRs, Low cost compared to real time updating CEIR, completely	High cost compared to the option of not having onsite hardware, requirement to continuously update

	Quotation from eFutureTech LKR 5 million for software and LKR 3 million for software	independent system as hardware is located at TRCSL	and monitor hardware, No real time detection of mobile devices, real time blocking capability
Implementing a non-real time updating CEIR without onsite hardware	Quotation from Mylinex LKR 9 million for software and LKR 1 million for hardware Quotation from eFutureTech LKR 5 million for software and LKR 1 million for hardware	Lowest cost option, Simple integration requirement with operator EIRs, Hardware is no need to be maintained and updated by TRCSL	Operator dependency of hardware resources, Special operator agreement is required to convince the independence of the CEIR, No real time detection of mobile devices, real time blocking capability

Considering the current context of Sri Lanka, the least complex and least cost option is the best option to implement a central database and a blocking mechanism. Therefore, a non-real time updating CEIR without onsite hardware should be implemented.

A special agreement should be formed among operators to obtain hardware resources from operator owned data centers. Due to the less complex nature of the system local software companies can implement the system for a lower price.

Initially, all operator IMEI databases should be pushed to a CEIR. Then once in a day new device detection and device change related logs should be sent to CEIR to update its database. The master database node will always get updated first. Then the same data will be replicated in slave node and DR node.

TRCSL should obtain GSMA IMEI database and maintain that as a whitelist database to identify valid IMEIs [17]. The IMEIs in the central database should be cross checked for invalid IMEIs. Invalid and fake IMEIs should be maintained in a black list database. The cloned IMEIs should be updated in the same black list. TRCSL should add the IMEIs of stolen handsets to the same black list. This blacklist database should be pushed to individual operators. Then, the operators can use this database to cross check the IMEIs of the mobile devices and identify the blacklisted devices via the EIR systems that the operators have already established.

Initially a warning message should be sent to black market device users. Later, as the final step such devices should be blocked from using the network based on the device blocking policy mentioned in 5.3.3.

5.3.3 Selected method of adding reforms to existing policy framework

When implementing reforms, similar implementations done in other countries should be considered. Section II in this thesis describes the current practices of different countries which Sri Lanka can follow and alternative options are mentioned in 5.2.3.2.

5.3.3.1 Digital platform to find lost mobile devices

. The existing manual process of making a complaint at police and TRCSL is very time consuming and ineffective. It’s a worldwide trend to move into digitized mechanisms to avoid any delays and expedite the processes. Therefore, stolen devices related complaint handling process needs to be digitized. An online GUI should be established to make lost devices related complaints. But, a person verification system should be established to verify the identity of the person who is making a complaint. The cost of implementing such a system is very high. Therefore, once a complaint is lodged via the proposed GUI, mobile operators should be requested to validate the ownership of the SIM card and the IMEI of the device. Further, the user should be requested to upload the mobile device ownership related details via the same GUI. The proposed digitized process of finding a lost mobile device is summarized below.

1. An online Graphical User Interface (GUI) should be established to inform lost mobile phone details to police.
2. Once validated by police, TRCSL should be notified via the same platform without any involvement from users.
3. The stolen device details should be added to a black list database maintained at TRCSL.
4. The CEIR should sync the black list database with operator EIRs to detect the lost device.
5. Police should be informed with the new user details of the stolen device to obtain further actions and recover the mobile device.

5.3.3.2 Illegal mobile device blocking policy

The final objective of minimizing the usage of black market and stolen mobile devices can only be achieved through a strong regulation. Even though the CEIR has the bird's eye view of all mobile devices used in the country and detects the usage of black market and stolen devices, the usage can only be reduced permanently by blocking such devices from using the mobile operator network.

Once a black market or a stolen mobile device is detected the users should be warned as the initial step. The easiest method is to use SMS message. The CEIR should detect the illegal device usage and trigger the SMS.

Then a concession period should be provided to the users before blocking the devices. A three-month concession period will be a suitable option as too lengthy concession period will allow the usage of illegal mobile devices in the country for lengthy durations.

If the illegal mobile device users continue to use the devices even after the concession period, those devices should be permanently blocked. CEIR should add the device IMEI to black list and pass it to mobile operator EIRs.

The implementation plan of the policy framework to minimize the usage of black market and stolen mobile devices is summarized in 5.3.4 bellow. The proposed implementation plan is summarized diagrammatically in Figure 18.

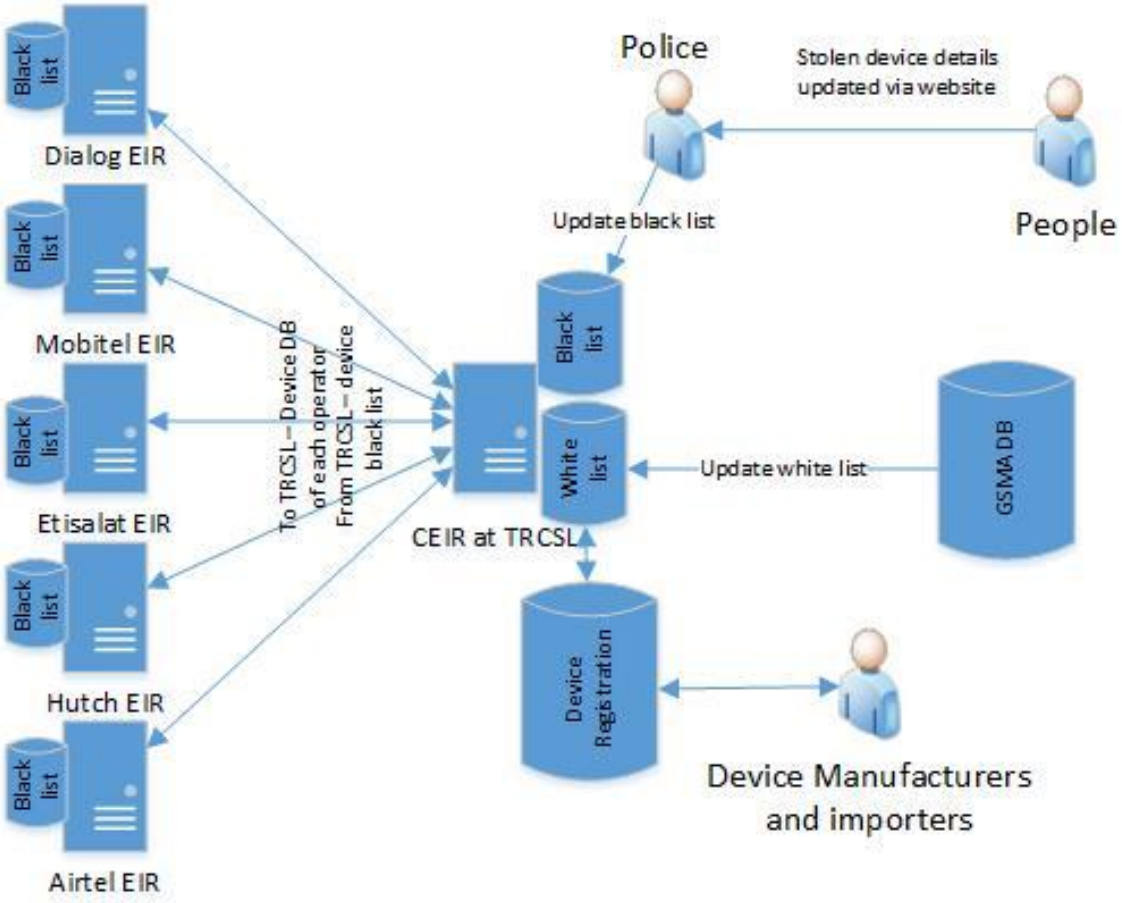

Figure 21: Proposed overall IMEI blocking solution

5.3.4 Policy framework implementation plan

1. All five mobile operators in Sri Lanka should be connected to the central database (CEIR) placed at TRCSL.

2. EIR databases should be synced to CEIR and then the new device detection and device update related logs should be passed to CEIR daily.

3. TRCSL needs to manage three mobile device databases; namely, Sri Lanka's device database with IMEIs, whitelisted IMEIs (legitimate devices) and black listed IMEIs (illegal devices).

4. White list needs to be updated with the GSMA IMEI database (GSMA IMEI database is an up to date database maintained by GSMA to include the authorized device IMEIs).

5. TRCSL also can include white listed IMEIs as per device registration requests received from device manufacturers.

6. Users should be allowed to make complaints via an online GUI

    i. User should make the complaint via an online GUI

    ii. Device ownership should be validated by the respective mobile operator by analyzing the user, SIM and the IMEI.

    iii. Police and TRCSL should be linked online and complaint details should be forwarded to TRCSL without any manual intervention from user.

7. Black market devices and stolen devices should be added to the black list maintained in CEIR and black list should be pushed to operator EIRs.

8. All black market and stolen device should be warned by sending a SMS and finally the device usage should be blocked permanently after a concession period.

CHAPTER 6: **CONCLUSION AND FUTURE WORK**

6.1 Conclusion

The first objective; conducting a literature survey to identify negative impacts was achieved by conducting a comprehensive literature surveys to identify the negative impacts due to usage of black market and stolen mobile devices. The second objective; conducting a literature survey to identify available solutions was achieved by identifying the solutions proposed by various organizations and by surveying on the solutions implemented by other countries. The third objective; conducting user surveys to identify the problems available in Sri Lanka was achieved by conducting three user surveys. A consumer user survey, an operator user survey and a survey with TRCSL were conducted to analyze the current status of the country. The final objective was to provide a policy framework and recommendations. This was achieved by proposing a three-step policy framework.

In this thesis, we have identified the issues faced by users, operators, government and industry due to the black market (counterfeit and substandard) and stolen mobile devices usage. Also, we have suggested a suitable policy framework and recommendation to minimize the usage of black market and stolen mobile devices.

Firstly, we have conducted two literature surveys to identify the negative impacts of black market and stolen mobile devices and the solutions suggested by various organizations and countries.

Then, three user surveys were conducted among the users, operators and TRCSL to identify the prevailing issues in Sri Lanka due to the usage of substandard, counterfeit and stolen mobile devices.

As per the user survey conclusions, it was identified that user behavior patterns, limitations of existing EIR systems and the outdated policies should be changed to address the issue of black market and stolen mobile devices usage.

A policy framework and recommendations that include the steps of increasing user awareness, establishing an IMEI based blocking mechanism and adding reforms to regulations is suggested to minimize the usage of black market and stolen mobile communication devices.

6.2 Future work

6.2.1 Fake IMEI identification

The major drawback in the proposed solution is the difficulty of blocking invalid IMEIs. If the illegal device manufacturer has used an IMEI from a legal device and copied the same in the device then the system doesn't have a straight forward mechanism to identify and block the illegal device.

'Counterfeit Identifier Platform' that has already been standardized by 3GPP should be implemented. This platform cross checks the IMEIs of the mobile devices with their actual capabilities and identify the black market mobile devices even if the IMEIs are fake.

6.2.2 Automated user identification

Device ownership should be validated by the respective mobile operator by analyzing the user and the IMEI. The user IMEI and the respective mobile operator can be identified by analyzing the central database at TRCSL. Then the operator database should be quarried to obtain the user information of the respective IMEI.

The steps required for the process are mentioned below.

1. Users should be asked to show the identification details via the camera
2. User's face and identification details should be cross checked and validated.
3. Device ownership should be validated by the respective mobile operator by analyzing the user data and the IMEI of the device.
4. Then the complaint should be lodged at police automatically and details should be forwarded to TRCSL.
5. TRCSL will monitor the device via CEIR and device will be blocked for usage.

Such an automated user identification process will be helpful to improve the current security situation of the country also. The same validation process can be implemented during SIM card purchase and make sure that illegal SIM card purchases are avoided.

Also, due to the automated process of identifying black market or stolen device usage in real time, it will be very difficult to use those devices for terrorist or any illegal activity. Hence, these future improvements will improve the security status of the country also.

REFERENCES

[1] “Number of Mobile Subscribers Worldwide Hits 5 Billion,” Mobile Economy 2018, 13-Jun-2017.[Online]. Available: https://www.gsma.com/newsroom/press-release/number-mobile-subscribers-worldwide-hits-5-billion/. [Accessed: 04-Oct-2018].

[2] “Combating Counterfeit and Substandard ICT Devices”, 2014. [Online]. Available: https://www.itu.int/en/ITU-T/C-I/Documents/WSHP_counterfeit/Presentations%20and%20Abstracts/S1P1-Dmytro-Protsenko.ppt. [Accessed: 04-Oct-2018].

[3] “Counterfeit/Substandard Mobile Phones – A User Guide to Governments”, 2014. [Online]. Available: https://www.itu.int/en/ITU-T/C-I/Documents/WSHP_counterfeit/Contributions/Contribution-001-MMF.pdf. [Accessed: 04-Oct-2018].

[4] “INDUSTRY COOPERATION TO TACKLE COUNTERFEITING IN MOBILE COMMUNICATIONS”,ITU, 2016. [Online]. Available: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20160628/Documents/PPT/S2P3_Thomas_Barmueller.pdf. [Accessed: 15-Oct-2018].

[5] "One in five mobile phones shipped abroad is fake - OECD", Oecd.org, 2017. [Online]. Available: http://www.oecd.org/trade/one-in-five-mobile-phones-shipped-abroad-is-fake.htm. [Accessed: 25-Nov-2018].

[6] “Statistics - telecommunications regulatory commission of Sri Lanka,” 2018.[Online].Available:http://www.trc.gov.lk/images/pdf/statis_q1_2018.pdf. [Accessed: 25-Nov-2018].

[7] A. J. Figueiredo Loureiro, D. Gallegos and G. Caldwell, "Substandard cell phones: impact on network quality and a new method to identify an unlicensed IMEI in the network," in *IEEE Communications Magazine*, vol. 52, no. 3, pp. 90-96, March 2014.

[8] J. O’brien and K. Lehtonen, "Counterfeit mobile devices - the duck test," *2015 10th International Conference on Malicious and Unwanted Software (MALWARE)*, Fajardo, 2015, pp. 144-151.

[9] D. Hui and H. Lei, "EIR Based Mobile Communication Network Security Technology," 2011 Third International Conference on Multimedia Information Networking and Security, Shanghai, 2011, pp. 477-479.

[10] Telecom Regulatory Authority of India, “Consultation Paper on Issues relating to blocking of IMEI for lost /stolen mobile handsets,” [Online]. Available:https://www.trai.gov.in/sites/default/files/consultationpaper.pdf [Accessed: 04-Dec-2018]

[11] "3rd Generation Partnership Project (3GPP) TS 22.016; Technical Specification Group Services and System Aspects", *International Mobile station Equipment Identities (IMEI) by 3rd Generation Partnership Project*.

[12] "Feature Manual - Equipment Identity Register. Tekelec", 2012, [online]Available: https:lldocs.oracle.com/cdlE525900l/doc.4401910–6272-001reva.pdf. [Accessed: 05-Jan-2019].

[13] I. Gepko, "General requirements and security architecture for mobile phone anti-cloning measures," *IEEE EUROCON 2015 - International Conference on Computer as a Tool (EUROCON)*, Salamanca, 2015, pp. 1-6.

[14] S. P. Rao, S. Holtmanns, I. Oliver and T. Aura, "Unblocking Stolen Mobile Devices Using SS7-MAP Vulnerabilities: Exploiting the Relationship between IMEI and IMSI for EIR Access," 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, 2015, pp. 1171-1176.

[15] Prof.Yatin Jog, Pushpendra Thenuan, Dhruv Khanna and Ashlesha Chavan, "Analysing Central Equipment Identity Register (CEIR) Model for Mobile Handset Tracking in India," 2016 International Journal of Scientific Research, vol. 5, no. 4, pp. 188–193.

[16] "Consultation Paper on Issues relating to blocking of IMEI for lost/stolen Mobile handsets", Telecom Regulatory Authority of India, 2010. [Online]. Available: https://main.trai.gov.in/consultation-paper-issues-relating-blocking-imei-loststolen-mobile-handsets-0. [Accessed: 06-Jan-2019].

[17] “GSMA IMEI DATABASE”, 2019. [Online]. Available: https://imeidb.gsma.com/imei/index#. [Accessed: 15-Jan-2019].

ANNEX – A: USER SURVEY

This is a survey conducted for a M.Sc. research project of University of Moratuwa to identify mobile phone usage related details in Sri Lanka. Thank you for your time and cooperation.

Name (Optional)……

1. What is your gender?
   ☐Male ☐Female

2. What is your age?
   ……..

3. What is your living district?
   …….

4. Where do you live?
   ☐Urban ☐Sub-urban ☐Rural

5. What is your monthly income level? (LKR)
   ☐ Below Rs 30,000 ☐ Below Rs 50,000 ☐ Below Rs 100,000
   ☐ Above Rs 100,000

6. What is your highest education qualification?
   ☐GCE O/L ☐GCE A/L ☐Diploma ☐ Bachelor's degree
   ☐ Post graduate

Mobile phone usage

a) Do you use mobile devices?

☐ Yes ☐ No

b) What type of mobile devices do you use?

☐Mobile phones ☐Tabs ☐Dongles

☐Other ……..

c) What kind of mobile phones do you use?

☐Feature phones ☐Android smart phones ☐IOS smart phones

☐Other ……..

d) What is the brand of your mobile phone?

☐Samsung ☐Apple ☐Huawei

☐Other ……..

e) What is the model of your mobile phone? (e.g.: Samsung galaxy S8, IPhone SE etc.)

……..

f) From where did you buy your mobile phone?

☐Authorized dealer ☐Bought from a foreign country

☐Bought from a friend ☐Other ……..

g) What were the selection criteria you considered when buying the mobile phone?

☐Cost ☐Brand ☐OS ☐Network support ☐SAR value

☐Validity of IMEI ☐Other ……..

h) If your mobile phone is lost, what should you do?

☐I should disconnect my SIM

☐I should inform the nearest police station

☐I should inform Telecommunication Regulation Commission of Sri Lanka (TRCSL)

☐Other ……..

i) Have you noted down the IMEI number of your mobile phone anywhere?

☐ Yes ☐ No

Losing a Mobile phone

a) Have you ever lost a mobile phone?

☐Yes ☐No

Please answer below questions, only if you have lost a mobile phone.

b) To what authorities did you inform about the lost mobile phone?

☐Mobile operator ☐TRCSL ☐Police ☐None

c) Did you inform the network service provider to disconnect the SIM?

☐Yes ☐No

d) How long did it take for the network service provider to disconnect the SIM after informing?

☐Less than a day ☐One day ☐More than a day ☐Did not disconnect

e) Did you make a complaint regarding the lost mobile phone at a police station?

☐Yes ☐No

f) Did you make a complaint regarding the lost mobile phone at Telecommunication Regulatory Commission of Sri Lanka (TRCSL)?

☐Yes ☐No

g) How long did it take for the authorities to find the lost mobile phone?

☐Less than a week ☐Less than a month ☐More than a month

☐Never found

h) How satisfied are you with the existing process to find a lost mobile phone?

☐Good ☐Neutral ☐Bad

i) What are your comments regarding the existing process of finding a lost mobile phone?

……
….

ANNEX – B: OPERATOR USER SURVEY

This is a survey conducted for a M.Sc. research project of University of Moratuwa to identify mobile phone usage related details in Sri Lanka. Thank you for your time and cooperation.

Name (Optional)……

1. What is the name of your company?

2. Do you have an EIR system established in your network?

3. What is the network architecture and functionality of your EIR system?

4. Do you currently monitor black market and stolen mobile devices?

5. Do you have the capability to block black market and stolen devices?

6. Do you block black market and stolen devices?

7. Have you observed any issues due to the usage of black market and stolen devices in your network?

8. Have you experienced any QoS related concerns due to the usage of black market mobile devices?